



사용 설명서

AWS Systems Manager Automation 런북 참조



AWS Systems Manager Automation 런북 참조: 사용 설명서

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

Amazon의 상표 및 트레이드 드레스는 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 런북 참조	1
실행서 콘텐츠 보기	3
API Gateway	4
AWSConfigRemediation-DeleteAPIGatewayStage	4
AWSConfigRemediation-EnableAPIGatewayTracing	5
AWSConfigRemediation-UpdateAPIGatewayMethodCaching	7
AWSSupport-TroubleshootAPIGatewayHttpErrors	8
AWS Batch	13
AWSSupport-TroubleshootAWSBatchJob	13
CloudFormation	19
AWS-DeleteCloudFormationStack	19
AWS-EnableCloudFormationSNSNotification	20
AWS-RunCfnLint	22
AWSSupport-TroubleshootCFNCustomResource	24
AWS-UpdateCloudFormationStack	26
CloudFront	27
AWSConfigRemediation-EnableCloudFrontDefaultRootObject	27
AWSConfigRemediation-EnableCloudFrontAccessLogs	29
AWSConfigRemediation-EnableCloudFrontOriginAccessIdentity	31
AWSConfigRemediation-EnableCloudFrontOriginFailover	32
AWSConfigRemediation-EnableCloudFrontViewerPolicyHTTPS	34
CloudTrail	35
AWSConfigRemediation-CreateCloudTrailMultiRegionTrail	36
AWS-EnableCloudTrail	37
AWS-EnableCloudTrailCloudWatchLogs	39
AWSConfigRemediation-EnableCloudTrailEncryptionWithKMS	40
AWS-EnableCloudTrailKmsEncryption	42
AWSConfigRemediation-EnableCloudTrailLogFileValidation	43
AWS-EnableCloudTrailLogFileValidation	44
AWS-QueryCloudTrailLogs	45
CloudWatch	48
AWS-ConfigureCloudWatchOnEC2Instance	48
AWS-EnableCWAlarm	49
AWSSupport-TroubleshootCloudWatchAgent	52

AWSSupport-TroubleshootCloudWatchAlarm	58
Amazon DocumentDB	65
AWS-EnableDocDbClusterBackupRetentionPeriod	65
CodeBuild	68
AWSConfigRemediation-ConfigureCodeBuildProjectWithKMScmk	68
AWSConfigRemediation-DeleteAccessKeysFromCodeBuildProject	70
AWS CodeDeploy	71
AWSSupport-TroubleshootCodeDeploy	71
AWS Config	73
AWSSupport-SetupConfig	73
Amazon Connect	76
AWSSupport-AssociatePhoneNumbersToConnectContactFlows	76
AWSSupport-CollectAmazonConnectContactFlowLog	84
AWS Directory Service	90
AWS-CreateDSManagementInstance	90
AWSSupport-TroubleshootADConnectorConnectivity	95
AWSSupport-TroubleshootDirectoryTrust	99
AWS AppSync	102
AWS-EnableAppSyncGraphQLApiLogging	102
Amazon Athena	104
AWS-EnableAthenaWorkGroupEncryptionAtRest	105
DynamoDB	107
AWS-ChangeDDBRWCapacityMode	107
AWS-CreateDynamoDBBackup	109
AWS-DeleteDynamoDbBackup	110
AWSConfigRemediation-DeleteDynamoDbTable	111
AWS-DeleteDynamoDbTableBackups	112
AWSConfigRemediation-EnableEncryptionOnDynamoDbTable	114
AWSConfigRemediation-EnablePITRForDynamoDbTable	115
AWS-EnableDynamoDbAutoscaling	117
AWS-RestoreDynamoDBTable	120
AWS Database Migration Service	122
AWSSupport-TroubleshootDMSTableErrors	122
AWSSupport-TroubleshootDMSEndpointConnection	128
Amazon EBS	137
AWSSupport-AnalyzeEBSResourceUsage	138

AWS-ArchiveEBSSnapshots	144
AWS-AttachEBSVolume	146
AWSSupport-CalculateEBSPerformanceMetrics	147
AWS-CopySnapshot	154
AWS-CreateSnapshot	155
AWS-DeleteSnapshot	156
AWSConfigRemediation-DeleteUnusedEBSVolume	157
AWS-DeregisterAMIs	158
AWS-DetachEBSVolume	160
AWSConfigRemediation-EnableEbsEncryptionByDefault	161
AWS-ExtendEbsVolume	162
AWSSupport-ModifyEBSSnapshotPermission	165
AWSConfigRemediation-ModifyEBSVolumeType	167
Amazon EC2	168
AWS-ASGEnterStandby	171
AWS-ASGExitStandby	172
AWS-CreateImage	173
AWS-DeleteImage	174
AWS-PatchAsgInstance	176
AWS-PatchInstanceWithRollback	178
AWS-QuarantineEC2Instance	181
AWS-ResizeInstance	183
AWS-RestartEC2Instance	184
AWS-SetupJupyter	184
AWS-StartEC2Instance	188
AWS-StopEC2Instance	189
AWS-TerminateEC2Instance	190
AWS-UpdateLinuxAmi	190
AWS-UpdateWindowsAmi	194
AWSConfigRemediation-EnableAutoScalingGroupELBHealthCheck	198
AWSConfigRemediation-EnforceEC2InstanceIMDSv2	200
AWSEC2-CloneInstanceAndUpgradeSQLServer	201
AWSEC2-CloneInstanceAndUpgradeWindows	205
AWSEC2-PatchLoadBalancerInstance	209
AWSEC2-SQLServerDBRestore	210
AWSSupport-ActivateWindowsWithAmazonLicense	215

AWSSupport-AnalyzeAWSEndpointReachabilityFromEC2	218
AWSPremiumSupport-ChangeInstanceTypeIntelToAMD	223
AWSSupport-CheckXenToNitroMigrationRequirements	228
AWSSupport-CloneXenEC2InstanceAndMigrateToNitro	231
AWSSupport-CollectSAPHANALogs	238
AWSSupport-ConfigureEC2Metadata	245
AWSSupport-ContainEC2Instance	248
AWSSupport-CopyEC2Instance	258
AWSPremiumSupport-DiagnoseDiskUsageOnLinux	264
AWSSupport-EnableWindowsEC2SerialConsole	267
AWSPremiumSupport-ExtendVolumesOnWindows	275
AWSSupport-ExecuteEC2Rescue	279
AWSSupport-ListEC2Resources	281
AWSSupport-ManageRDPSettings	284
AWSSupport-ManageWindowsService	286
AWSSupport-MigrateEC2ClassicToVPC	288
AWSSupport-MigrateXenToNitroLinux	294
AWSSupport-ResetAccess	306
AWSSupport-ResetLinuxUserPassword	308
AWSSupport-RunEC2RescueForWindowsTool	315
AWSPremiumSupport-ResizeNitroInstance	319
AWSSupport-ShareEncryptedAMIOrEBSSnapshot	326
AWSSupport-RestoreEC2InstanceFromSnapshot	330
AWSSupport-SendLogBundleToS3Bucket	334
AWSSupport-StartEC2RescueWorkflow	336
AWSSupport-TroubleshootActiveDirectoryReplication	346
AWSPremiumSupport-TroubleshootEC2DiskUsage	351
AWSSupport-TroubleshootEC2InstanceConnect	356
AWSSupport-TroubleshootLinuxMGNDRSAgentLogs	362
AWSSupport-TroubleshootRDP	365
AWSSupport-TroubleshootSSH	371
AWSSupport-TroubleshootSUSERegistration	374
AWSSupport-TroubleshootWindowsPerformance	376
AWSSupport-TroubleshootWindowsUpdate	384
AWSSupport-UpgradeWindowsAWSDrivers	390
Amazon ECS	394

AWSSupport-CollectECSInstanceLogs	394
AWS-InstallAmazonECSAgent	397
AWS-ECSRunTask	399
AWSSupport-TroubleshootECSContainerInstance	402
AWSSupport-TroubleshootECSTaskFailedToStart	404
AWS-UpdateAmazonECSAgent	409
Amazon EFS	411
AWSSupport-CheckAndMountEFS	411
Amazon EKS	414
AWS-CreateEKSClusterWithFargateProfile	415
AWS-CreateEKSClusterWithNodegroup	418
AWS-DeleteEKSCluster	422
AWS-MigrateToNewEKSSelfManagedNodeGroup	425
AWSPremiumSupport-TroubleshootEKSCluster	430
AWSSupport-TroubleshootEKSWorkerNode	434
AWS-UpdateEKSCluster	436
AWS-UpdateEKSSelfManagedNodeGroup	438
AWS-UpdateEKSSelfManagedLinuxNodeGroups	442
AWSSupport-CollectEKSLinuxNodeStatistics	445
AWSSupport-CollectEKSInstanceLogs	451
AWSSupport-SetupK8sApiProxyForEKS	454
AWSSupport-TroubleshootEbsCsiDriversForEks	465
AWSSupport-TroubleshootEKSSALBControllerIssues	474
AWSSupport-TroubleshootEKSDNSFailure	485
Elastic Beanstalk	491
AWSSupport-CollectElasticBeanstalkLogs	491
AWSConfigRemediation-EnableElasticBeanstalkEnvironmentLogStreaming ..	494
AWSConfigRemediation-EnableBeanstalkEnvironmentNotifications	495
AWSSupport-TroubleshootElasticBeanstalk	497
Elastic Load Balancing	499
AWSConfigRemediation-DropInvalidHeadersForALB	500
AWS-EnableCLBAccessLogs	501
AWS-EnableCLBConnectionDraining	503
AWSConfigRemediation-EnableCLBCrossZoneLoadBalancing	505
AWSConfigRemediation-EnableELBDeletionProtection	506
AWSConfigRemediation-EnableLoggingForALBAndCLB	507

AWSSupport-TroubleshootCLBConnectivity	509
AWSConfigRemediation-EnableNLBCrossZoneLoadBalancing	512
AWS-UpdateALBDesyncMitigationMode	513
AWS-UpdateCLBDesyncMitigationMode	515
AWSSupport-TroubleshootELBHealthChecks	517
Amazon EMR	521
AWSSupport-AnalyzeEMRLogs	522
AWSSupport-DiagnoseEMRLogsWithAthena	528
Amazon OpenSearch Service	536
AWSConfigRemediation-DeleteOpenSearchDomain	537
AWSConfigRemediation-EnforceHTTPSOnOpenSearchDomain	538
AWSConfigRemediation-UpdateOpenSearchDomainSecurityGroups	539
AWSSupport-TroubleshootOpenSearchRedYellowCluster	541
AWSSupport-TroubleshootOpenSearchHighCPU	547
EventBridge	553
AWS-AddOpsItemDedupStringToEventBridgeRule	554
AWS-DisableEventBridgeRule	555
AWS Glue	556
AWSSupport-TroubleshootGlueConnection	557
Amazon FSx	567
AWSSupport-ValidateFSxWindowsADConfig	568
GuardDuty	581
AWSConfigRemediation-CreateGuardDutyDetector	582
IAM	583
AWSSupport-TroubleshootIAMAccessDeniedEvents	583
AWS-AttachIAMToInstance	590
AWS-DeleteIAMInlinePolicy	592
AWSConfigRemediation-DeleteIAMRole	593
AWSConfigRemediation-DeleteIAMUser	595
AWSConfigRemediation-DeleteUnusedIAMGroup	597
AWSConfigRemediation-DeleteUnusedIAMPolicy	599
AWSConfigRemediation-DetachIAMPolicy	600
AWSConfigRemediation-EnableAccountAccessAnalyzer	601
AWSSupport-GrantPermissionsToIAMUser	603
AWSConfigRemediation-RemoveUserPolicies	608
AWSConfigRemediation-ReplaceIAMInlinePolicy	609

AWSConfigRemediation-RevokeUnusedIAMUserCredentials	611
AWSConfigRemediation-SetIAMPasswordPolicy	613
AWSSupport-ContainIAMPrincipal	616
AWSSupport-TroubleshootSAMLIssues	629
인시던트 감지 및 대응	634
AWSPremiumSupport-OnboardWorkloadToIDR	634
Amazon Kinesis Data Streams	642
AWS-EnableKinesisStreamEncryption	642
AWS KMS	644
AWSConfigRemediation-CancelKeyDeletion	644
AWSConfigRemediation-EnableKeyRotation	645
Lambda	647
AWSConfigRemediation-ConfigureLambdaFunctionXRayTracing	647
AWSConfigRemediation-DeleteLambdaFunction	648
AWSConfigRemediation-EncryptLambdaEnvironmentVariablesWithCMK	650
AWSConfigRemediation-MoveLambdaToVPC	651
AWSSupport-RemediateLambdaS3Event	653
AWSSupport-TroubleshootLambdaInternetAccess	655
AWSSupport-TroubleshootLambdaS3Event	659
Amazon Managed Workflows for Apache Airflow	661
AWSSupport-TroubleshootMWAAEnvironmentCreation	661
Neptune	667
AWS-EnableNeptuneDbAuditLogsToCloudWatch	667
AWS-EnableNeptuneDbBackupRetentionPeriod	668
AWS-EnableNeptuneClusterDeletionProtection	670
Amazon RDS	672
AWS-CreateEncryptedRdsSnapshot	673
AWS-CreateRdsSnapshot	675
AWSConfigRemediation-DeleteRDSCluster	677
AWSConfigRemediation-DeleteRDSClusterSnapshot	678
AWSConfigRemediation-DeleteRDSInstance	679
AWSConfigRemediation-DeleteRDSInstanceSnapshot	681
AWSConfigRemediation-DisablePublicAccessToRDSInstance	683
AWSConfigRemediation-EnableCopyTagsToSnapshotOnRDSCluster	684
AWSConfigRemediation-EnableCopyTagsToSnapshotOnRDSDBInstance	686
AWSConfigRemediation-EnableEnhancedMonitoringOnRDSInstance	688

AWSConfigRemediation-EnableMinorVersionUpgradeOnRDSDBInstance	689
AWSConfigRemediation-EnableMultiAZOnRDSInstance	691
AWSConfigRemediation-EnablePerformanceInsightsOnRDSInstance	692
AWSConfigRemediation-EnableRDSClusterDeletionProtection	695
AWSConfigRemediation-EnableRDSInstanceBackup	696
AWSConfigRemediation-EnableRDSInstanceDeletionProtection	698
AWSConfigRemediation-ModifyRDSInstancePortNumber	699
AWSSupport-ModifyRDSSnapshotPermission	701
AWSPremiumSupport-PostgreSQLWorkloadReview	703
AWS-RebootRdsInstance	719
AWSSupport-ShareRDSSnapshot	720
AWS-StartRdsInstance	723
AWS-StartStopAuroraCluster	724
AWS-StopRdsInstance	726
AWSSupport-TroubleshootConnectivityToRDS	727
AWSSupport-TroubleshootRDSIAMAuthentication	729
AWSSupport-ValidateRdsNetworkConfiguration	737
Amazon Redshift	743
AWSConfigRemediation-DeleteRedshiftCluster	743
AWSConfigRemediation-DisablePublicAccessToRedshiftCluster	745
AWSConfigRemediation-EnableRedshiftClusterAuditLogging	746
AWSConfigRemediation-EnableRedshiftClusterAutomatedSnapshot	748
AWSConfigRemediation-EnableRedshiftClusterEncryption	749
AWSConfigRemediation-EnableRedshiftClusterEnhancedVPCRouting	751
AWSConfigRemediation-EnforceSSLOnlyConnectionsToRedshiftCluster	752
AWSConfigRemediation-ModifyRedshiftClusterMaintenanceSettings	753
AWSConfigRemediation-ModifyRedshiftClusterNodeType	755
Amazon S3	757
AWS-ArchiveS3BucketToIntelligentTiering	758
AWS-ConfigureS3BucketLogging	760
AWS-ConfigureS3BucketVersioning	762
AWSConfigRemediation-ConfigureS3BucketPublicAccessBlock	763
AWSConfigRemediation-ConfigureS3PublicAccessBlock	765
AWS-CreateS3PolicyToExpireMultipartUploads	768
AWS-DisableS3BucketPublicReadWrite	769
AWS-EnableS3BucketEncryption	770

AWS-EnableS3BucketKeys	771
AWSConfigRemediation-RemovePrincipalStarFromS3BucketPolicy	773
AWSConfigRemediation-RestrictBucketSSLRequestsOnly	774
AWSSupport-TroubleshootS3PublicRead	776
AWSSupport-ConfigureS3ReplicationSameAndCrossAccount	781
AWSSupport-EmptyS3Bucket	799
AWSSupport-TroubleshootS3EventNotifications	806
AWSSupport-ContainS3Resource	813
Amazon SES	821
AWSSupport-AnalyzeSESMessagesSendingStatus	822
AWSSupport-DeploySESSendingLogsToCloudWatchLogs	825
SageMaker AI	832
AWS-DisableSageMakerNotebookRootAccess	832
AWSSupport-RequestSageMakerLimitIncrease	834
Secrets Manager	837
AWSConfigRemediation-DeleteSecret	837
AWSConfigRemediation-RotateSecret	839
Security Hub CSPM	841
AWSConfigRemediation-EnableSecurityHub	841
AWS Shield	842
AWSPremiumSupport-DDoSResiliencyAssessment	842
Amazon SNS	851
AWS-EnableSNSTopicDeliveryStatusLogging	851
AWSConfigRemediation-EncryptSNSTopic	854
AWS-PublishSNSNotification	855
Amazon SQS	856
AWS-EnableSQSEncryption	856
단계 함수	859
AWS-EnableStepFunctionsStateMachineLogging	859
Systems Manager	861
AWS-BulkDeleteAssociation	862
AWS-BulkEditOpsItems	863
AWS-BulkResolveOpsItems	866
AWS-ConfigureMaintenanceWindows	868
AWS-CreateManagedLinuxInstance	870
AWS-CreateManagedWindowsInstance	872

AWSConfigRemediation-EnableCWLoggingForSessionManager	875
AWS-ExportOpsDataToS3	876
AWS-ExportPatchReportToS3	878
AWS-SetupInventory	879
AWS-SetupManagedInstance	884
AWS-SetupManagedRoleOnEC2Instance	885
AWSSupport-TroubleshootManagedInstance	886
AWSSupport-TroubleshootPatchManagerLinux	889
AWSSupport-TroubleshootSessionManager	892
타사	897
AWS-CreateJiraIssue	898
AWS-CreateServiceNowIncident	900
AWS-RunPacker	902
Amazon VPC	904
AWS-CloseSecurityGroup	905
AWSSupport-ConfigureDNSQueryLogging	907
AWSSupport-ConfigureTrafficMirroring	910
AWSSupport-ConnectivityTroubleshooter	912
AWSSupport-TroubleshootVPN	915
AWSConfigRemediation-DeleteEgressOnlyInternetGateway	921
AWSConfigRemediation-DeleteUnusedENI	923
AWSConfigRemediation-DeleteUnusedSecurityGroup	924
AWSConfigRemediation-DeleteUnusedVPCNetworkACL	925
AWSConfigRemediation-DeleteVPCFlowLog	926
AWSConfigRemediation-DetachAndDeleteInternetGateway	928
AWSConfigRemediation-DetachAndDeleteVirtualPrivateGateway	929
AWS-DisableIncomingSSHOnPort22	931
AWS-DisablePublicAccessForSecurityGroup	933
AWSConfigRemediation-DisableSubnetAutoAssignPublicIP	934
AWSSupport-EnableVPCFlowLogs	935
AWSConfigRemediation-EnableVPCFlowLogsToCloudWatch	942
AWSConfigRemediation-EnableVPCFlowLogsToS3Bucket	944
AWS-ReleaseElasticIP	946
AWS-RemoveNetworkACLUnrestrictedSSHRDP	946
AWSConfigRemediation-RemoveUnrestrictedSourceIngressRules	948
AWSConfigRemediation-RemoveVPCDefaultSecurityGroupRules	949

AWSSupport-SetupIPMonitoringFromVPC	950
AWSSupport-TerminateIPMonitoringFromVPC	958
AWS WAF	962
AWS-AddWAFRegionalRuleToRuleGroup	962
AWS-AddWAFRegionalRuleToWebAcl	964
AWSConfigRemediation-EnableWAFCClassicLogging	967
AWSConfigRemediation-EnableWAFCClassicRegionalLogging	968
AWSConfigRemediation-EnableWAFV2Logging	970
Amazon WorkSpaces	971
AWS-CreateWorkSpace	972
AWSSupport-RecoverWorkSpace	975
X-Ray	979
AWSConfigRemediation-UpdateXRayKMSKey	979
.....	cmlxxxi

Systems Manager Automation 런북 참조

빠르게 시작할 수 있도록 미리 정의된 실행서를 AWS Systems Manager 제공합니다. 이러한 실행서는 Amazon Web Services AWS Support, 및에서 유지 관리합니다 AWS Config. 런북 참조는 Systems Manager에서 제공하는 사전 정의된 각 런북 지원, 및를 설명합니다 AWS Config.

Important

AWS Identity and Access Management (IAM) 서비스 역할을 사용하여 다른 서비스를 호출하는 자동화 워크플로를 실행하는 경우 해당 서비스 역할이 다른 서비스를 호출할 권한이 있도록 구성되어야 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 실행서에도 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 [다른 AWS 서비스를 호출하기 위한 자동화 인라인 정책 추가](#)를 참조하세요.

이 참조에는 AWS AWS Support, 및가 소유한 각 Systems Manager 실행서를 설명하는 주제가 포함되어 있습니다 AWS Config. 런북은 관련 별로 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 실행](#)을 참조하세요. 여러 대상에서의 자동화 실행에 대한 자세한 내용은 [대상 및 속도 제어를 사용하는 자동화 실행](#)을 참조하세요.

주제

- [실행서 콘텐츠 보기](#)
- [API Gateway](#)

- [AWS Batch](#)
- [CloudFormation](#)
- [CloudFront](#)
- [CloudTrail](#)
- [CloudWatch](#)
- [Amazon DocumentDB](#)
- [CodeBuild](#)
- [AWS CodeDeploy](#)
- [AWS Config](#)
- [Amazon Connect](#)
- [AWS Directory Service](#)
- [AWS AppSync](#)
- [Amazon Athena](#)
- [DynamoDB](#)
- [AWS Database Migration Service](#)
- [Amazon EBS](#)
- [Amazon EC2](#)
- [Amazon ECS](#)
- [Amazon EFS](#)
- [Amazon EKS](#)
- [Elastic Beanstalk](#)
- [Elastic Load Balancing](#)
- [Amazon EMR](#)
- [Amazon OpenSearch Service](#)
- [EventBridge](#)
- [AWS Glue](#)
- [Amazon FSx](#)
- [GuardDuty](#)
- [IAM](#)
- [인시던트 감지 및 대응](#)

- [Amazon Kinesis Data Streams](#)
- [AWS KMS](#)
- [Lambda](#)
- [Amazon Managed Workflows for Apache Airflow](#)
- [Neptune](#)
- [Amazon RDS](#)
- [Amazon Redshift](#)
- [Amazon S3](#)
- [Amazon SES](#)
- [SageMaker AI](#)
- [Secrets Manager](#)
- [Security Hub CSPM](#)
- [AWS Shield](#)
- [Amazon SNS](#)
- [Amazon SQS](#)
- [단계 함수](#)
- [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. <https://console.aws.amazon.com/systems-manager/> AWS Systems Manager 콘솔을 엽니다.
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 Gateway

AWS Systems Manager Automation은 Amazon API Gateway에 대한 사전 정의된 실행서를 제공합니다. 실행서에 대한 자세한 내용은 [실행서 작업](#)을 참조하세요. 실행서 콘텐츠를 보는 방법에 대한 자세한 내용은 [실행서 콘텐츠 보기](#)(을)를 참조하세요.

주제

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

AWSConfigRemediation-DeleteAPIGatewayStage

설명

AWSConfigRemediation-DeleteAPIGatewayStage 실행서는 Amazon API Gateway(API Gateway) 단계를 삭제합니다.이 자동화를 실행하는 AWS 리전 에서 활성화해야 AWS Config 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 예서를 AWS 리전 활성화해야 AWS Config 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

유형: 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. ANY를 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.

AWSsupport-TroubleshootAPIGatewayHttpErrors

설명

AWSsupport-TroubleshootAPIGatewayHttpErrors 실행서는 액세스 및/또는 실행 로그를 구문 분석하고 오류를 분석하여 re:Post 문서 및 AWS 설명서를 통해 수정 단계를 제공하여 배포된 Amazon API Gateway REST API를 호출할 때 5XX/4XX 오류를 해결하는 데 도움이 됩니다.

 Important

이 런북에는 다음과 같은 제한 사항이 있습니다.

- 로깅을 활성화해야 합니다. [API Gateway 콘솔을 사용하여 Amazon CloudWatch API 로깅 설정을 참조하세요.](#)
- 오류(들)가 발생하기 전에 로그가 활성화되어 있어야 합니다. 로그 캡처 및 분석은 소급하여 수행할 수 없습니다.
- 포함된 오류: 500, 502, 503, 504, 401, 403, 429.

- REST API만 지원됩니다. WebSocket 및 HTTP(v2)는 이 실행서에서 다루지 않습니다.

Important

이 실행서를 사용하면 REST API에서 캡처한 Amazon CloudWatch Logs 및 분석에 사용된 CloudWatch Logs Insights에 대해 AWS 계정에 추가 요금이 발생할 수 있습니다. 발생할 수 있는 요금에 대한 자세한 내용은 [Amazon CloudWatch 요금을](#) 참조하세요. `aws:deletestack` 단계가 실패하면 CloudFormation 콘솔로 이동하여 스택을 수동으로 삭제합니다. 이 실행서에서 만든 스택 이름은 `AWSSupport-TroubleshootAPIGatewayHttpErrors`로 시작합니다. CloudFormation 스택 삭제에 대한 자세한 내용은 AWS CloudFormation 사용 설명서의 [스택 삭제](#)를 참조하세요.

어떻게 작동하나요?

실행서는 다음 검증 및 분석 단계를 수행합니다.

- 지정된 REST API가 존재하고 필요한 권한이 있는지 확인합니다.
- 지정된 단계가 API에 존재하는지 확인합니다.
- 지정된 리소스 경로가 API에 존재하는지 확인합니다.
- 리소스에 대해 지정된 HTTP 메서드가 존재하는지 확인합니다.
- 지정된 파라미터 및 시간 범위에 대한 CloudWatch Logs를 분석하여 오류를 식별하고 문제 해결 권장 사항을 제공합니다.

[이 자동화 실행\(콘솔\)](#)

문서 유형

자동화

소유자

Amazon

플랫폼

/

필수 IAM 권한

실행서를 성공적으로 사용하려면 AutomationAssumeRole 파라미터에 다음 작업이 필요합니다.

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

IAM 정책 예제:

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

지침

다음 단계에 따라 자동화를 구성합니다.

1. Systems Manager [AWSsupport-TroubleshootAPIGatewayHttpErrors](#)의 문서로 이동합니다.

2. Execute automation(자동화 실행)을 선택합니다.

3. 입력 파라미터에 다음을 입력합니다.

- AutomationAssumeRole(선택 사항):
 - 설명: (선택 사항) SSM Automation이 사용자를 대신하여 작업을 수행하도록 허용하는 (IAM) 역할의 AWS Identity and Access Management Amazon 리소스 이름(ARN)입니다. 역할이 지정되지 않은 경우 SSM Automation은 이 실행서를 시작하는 사용자의 권한을 사용합니다.
 - 유형: `AWS::IAM::Role::Arn`
- RestApiId(필수):
 - 설명: (필수) 문제 해결이 필요한 API의 API ID입니다. 10자의 영숫자 문자열이어야 합니다.
 - 유형: `String`
 - 허용된 패턴: `^[a-zA-Z0-9]{10}$`
- StageName(필수):
 - 설명: (필수) 배포된 단계의 이름입니다. 문자, 숫자, 밑줄 또는 하이픈을 포함하는 1~128자여야 합니다.
 - 유형: `String`
 - 허용된 패턴: `^[a-zA-Z0-9_\\-]{1,128}$`
- ResourcePath(선택 사항):
 - 설명: (선택 사항) 메서드가 구성된 리소스 경로입니다. 예: `/`, `/store/items`, `/resource`.
 - 유형: `String`
 - 기본값: `/`
- HttpMethod(선택 사항):
 - 설명: (선택 사항) 구성된 리소스 경로의 메서드입니다.
 - 유형: `String`
 - 허용된 값: `[ANY, DELETE, HEAD, OPTIONS, GET, POST, PUT, PATCH]`
 - 기본값: `GET`
- StartTime(선택 사항):
 - 설명: (선택 사항) CloudWatch Logs를 쿼리하기 위한 시작 날짜 및 시간입니다. 형식: UTC 시간 대 `yyyy-MM-ddTHH:mm:ss`입니다. 지정하지 않으면 기본값은 현재 시간 3일 전입니다.

- 허용된 패턴: `^$|^([0-9]{4}-([01-9]|1[0-2])-([01-9]|1[0-9]|2[0-9]|3[0-1]))T([0-3]|([01][0-9])):[0-5][0-9]:[0-5][0-9]$`
 - 기본값: ""
 - EndTime(선택 사항):
 - 설명: (선택 사항) CloudWatch Logs 쿼리의 종료 날짜 및 시간입니다. 형식: UTC 시간대yyyy-MM-ddTHH:mm:ss입니다. 지정하지 않으면 기본값은 현재 시간입니다.
 - 유형: String
 - 허용된 패턴: `^$|^([0-9]{4}-([01-9]|1[0-2])-([01-9]|1[0-9]|2[0-9]|3[0-1]))T([0-3]|([01][0-9])):[0-5][0-9]:[0-5][0-9]$`
 - 기본값: ""
 - AccessLogs(선택 사항):
 - 설명: (선택 사항) 액세스 로그를 분석해야 하는지 여부입니다.
 - 유형: Boolean
 - 허용된 값: [true, false]
 - 기본값: false
 - RequestId(선택 사항):
 - 설명: (선택 사항) 오류가 관찰된 요청에 대한 요청 ID입니다. 유효한 UUID 형식이어야 합니다.
 - 유형: String
 - 허용된 패턴: `^$|^([0-9a-f]{8}-[0-9a-f]{4}-[0-9a-f]{4}-[0-9a-f]{4}-[0-9a-f]{12})$`
 - 기본값: ""
4. 실행을 선택합니다.
5. 자동화가 시작됩니다.
6. 문서는 다음 단계를 수행합니다.
- CheckApiExists:

제공된 REST API가 존재하고 액세스에 필요한 권한이 있는지 확인합니다.
 - CheckStageExists:

제공된 단계 이름이 지정된 API에 있는지 확인하고 액세스 로그 그룹 정보를 검색합니다.
 - CheckResourceExists:

- CheckMethodExists:

지정된 리소스에 대해 제공된 HTTP 메서드가 존재하는지 확인합니다.

- AnalyseLogs:

제공된 파라미터를 사용하여 로그를 검색하고 발견된 오류를 기반으로 권장 사항을 반환합니다. 이 단계에서는 실행 및 액세스 로그(활성화된 경우)를 모두 분석하여 4XX 및 5XX 오류를 식별하고 특정 수정 지침을 제공합니다.

7. 완료 후 출력 섹션에서 오류 분석 및 문제 해결 권장 사항을 포함한 실행의 자세한 결과를 검토합니다.

참조

Systems Manager Automation

- [이 자동화 실행\(콘솔\)](#)
- [자동화 실행](#)
- [Automation 설정](#)
- [자동화 워크플로 지원](#)

AWS Batch

AWS Systems Manager 자동화에는 대한 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 실행서는 AWS Batch 작업이에서 STARTING 상태로 진행되지 않는 문제를 해결하는 RUNNABLE 데 도움이 됩니다.

어떻게 작동하나요?

이 실행서는 다음 검사를 수행합니다.

- 컴퓨팅 환경이 INVALID 또는 DISABLED 상태인 경우.
- 컴퓨팅 환경의 Max vCPU 파라미터가 작업 대기열의 작업 볼륨을 수용할 만큼 충분히 큰 경우.
- 작업에 컴퓨팅 환경의 인스턴스 유형이 제공할 수 있는 것보다 더 많은 vCPUs 또는 메모리 리소스가 필요한 경우.
- 작업이 GPU 기반 인스턴스에서 실행되어야 하지만 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(Amazon ECS) 클러스터에 조인할 수 있는 경우 [AWSSupport-TroubleshootECSContainerInstance](#) 실행서를 실행합니다.
- 권한 문제가 작업을 실행하는 데 필요한 특정 작업을 차단하는 경우.

Important

- 이 실행서는 RUNNABLE 상태로 멈춘 작업과 동일한 AWS 리전에서 시작해야 합니다.
- 이 실행서는 Amazon ECS AWS Fargate 또는 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스에 예약된 AWS Batch 작업에 대해 시작할 수 있습니다. Amazon Elastic Kubernetes Service(Amazon EKS)의 AWS Batch 작업에 대해 자동화가 시작되면 시작이 중지됩니다.
- 인스턴스를 사용하여 작업을 실행할 수 있지만 Amazon ECS 클러스터를 등록하지 못하는 경우 이 실행서는 AWSSupport-TroubleshootECSContainerInstance 자동화 실행서를 시작하여 이유를 확인합니다. 자세한 내용은 [AWSSupport-TroubleshootECSContainerInstance](#) 실행서를 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.

- JobId

유형: 문자열

설명: (필수) RUNNABLE 상태가 멈춘 AWS Batch 작업의 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. 콘솔에서 [AWSSupport-TroubleshootAWSBatchJob](#)으로 AWS Systems Manager 이동합니다.
2. 자동화 실행을 선택합니다.
3. 입력 파라미터에 다음을 입력합니다.
 - `AutomationAssumeRole`(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.

- JobId(필수):

RUNNABLE 상태에서 멈춘 AWS Batch 작업의 ID입니다.

Input parameters

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

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

- PreflightPermissionChecks:

시작 사용자/역할에 대해 사전 IAM 권한 검사를 수행합니다. 누락된 권한이 있는 경우 이 단계에서는 전역 출력 섹션에 누락된 API 작업을 제공합니다.

- ProceedOnlyIfUserHasPermission:

실행서에 필요한 모든 작업에 대한 권한이 있는지 여부를 기준으로 분기합니다.

- AWSBatchJobEvaluation:

작업이 존재하고 RUNNABLE 상태인지 확인하는 AWS Batch 작업을 기준으로 점검을 수행합니다.

- ProceedOnlyIfBatchJobExistsAndIsInRunnableState:

작업이 존재하고 RUNNABLE 상태인지 여부에 따라 분기합니다.

- BatchComputeEnvironmentEvaluation:

AWS Batch 컴퓨팅 환경에 대해 점검을 수행합니다.

- ProceedOnlyIfComputeEnvironmentChecksAreOK:

컴퓨팅 환경 검사가 성공했는지 여부에 따라 분기합니다.

- UnderlyingInfraEvaluation:

기본 Auto Scaling 그룹 또는 스팟 플릿 요청에 대해 점검을 수행합니다.

- `ProceedOnlyIfInstancesNotJoiningEcsCluster`:

Amazon ECS 클러스터에 조인하지 않는 인스턴스가 있는지 여부에 따라 분기합니다.

- `EcsAutomationRunner`:

클러스터에 조인하지 않는 인스턴스에 대해 Amazon ECS 자동화를 실행합니다.

- `ExecutionResults`:

이전 단계를 기반으로 출력을 생성합니다.

7. 완료 후 평가 보고서 HTML 파일의 URI가 제공됩니다.

실행서의 성공적인 실행에 대한 보고서의 S3 콘솔 링크 및 Amazon S3 URI

▼ Outputs

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

[INFO]: Reviewing Compute Environment "ComputeEnvironment-egMKnoNEEWmt8eY":
[ERROR]: Job "411-██████████-6606" requires 4 vCPU core(s), 512 MiB of memory and 0 GPU core(s).
There is no Instance Type in Compute Environment : "ComputeEnvironment-egMKnoNEEWmt8eY" that satisfies these resource requirements.
To fix this, add an Instance Type to the Compute Environment that provides enough vCPU, memory, and GPU resources to run the Job.
For more details on updating a Compute Environment see https://docs.aws.amazon.com/batch/latest/userguide/creating-compute-environments.html
[WARNING]: The automation detected that you are using BEST_FIT allocation strategy for your Compute Environment "ComputeEnvironment-egMKnoNEEWmt8eY".
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-██████████-6606" exists and is in RUNNABLE status, proceeding further for next steps in execution.

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

[INFO]: Reviewing Compute Environment "ComputeEnvironment-egMKnoNEEWmt8eY":
[ERROR]: Job "411-██████████-6606" requires 4 vCPU core(s), 512 MiB of memory and 0 GPU core(s).
There is no Instance Type in Compute Environment : "ComputeEnvironment-egMKnoNEEWmt8eY" that satisfies these resource requirements.
To fix this, add an Instance Type to the Compute Environment that provides enough vCPU, memory, and GPU resources to run the Job.
For more details on updating a Compute Environment see https://docs.aws.amazon.com/batch/latest/userguide/creating-compute-environments.html
[WARNING]: The automation detected that you are using BEST_FIT allocation strategy for your Compute Environment "ComputeEnvironment-egMKnoNEEWmt8eY".
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](#)

CloudFormation

AWS Systems Manager 자동화에는 대한 사전 정의된 실행서를 제공합니다 AWS CloudFormation. 실행서에 대한 자세한 내용은 [실행서 작업](#)을 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

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

- StackNameOrId

유형: 문자열

설명: (필수) 삭제할 CloudFormation 스택의 이름 또는 고유 ID

AWS-EnableCloudFormationSNSNotification

설명

AWS-EnableCloudFormationSNSNotification 실행서는 지정한 AWS CloudFormation () 스택에 대해 Amazon Simple Notification Service(Amazon SNS CloudFormation) 알림을 활성화합니다.

[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.

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

- StackArn

유형: 문자열

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

- NotificationArn

유형: 문자열

설명: (필수) CloudFormation 스택과 연결하려는 Amazon SNS 주제의 ARN입니다.

필수 IAM 권한

실행서를 성공적으로 사용하려면 AutomationAssumeRole 파라미터에 다음 작업이 필요합니다.

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

문서 단계

- CheckCfnSnsLimits(aws:executeScript) - 지정된 CloudFormation 스택과 아직 연결되지 않은 Amazon SNS 주제의 최대 수를 확인합니다.
- EnableCfnSnsNotification(aws:executeAwsApi) - CloudFormation 스택에 대한 Amazon SNS 알림을 활성화합니다.
- VerificationCfnSnsNotification(aws:executeScript) - CloudFormation 스택에 대해 Amazon SNS 알림이 활성화되었는지 확인합니다.

출력

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

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

AWS-RunCfnLint

설명

이 실행서는 [AWS CloudFormation Linter](#)(cfn-python-lint)를 사용하여 CloudFormation 리소스 사양에 대해 YAML 및 JSON 템플릿을 검증합니다. 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) 지정된에 대해 템플릿을 테스트하기 위해 --regions 파라미터에 대해 전달할 값입니다 AWS 리전.

예: us-east-1,us-west-1

문서 단계

RunCfnLintAgainstTemplate - 지정된 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 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` - CloudFormation 스택이 동일한 AWS 계정 및에 존재하는지 확인합니다 AWS 리전.
- `checkCustomResource` - CloudFormation 스택을 분석하고, 실패한 사용자 지정 리소스를 확인하고, 실패한 사용자 지정 리소스 문제를 해결하는 방법에 대한 정보를 출력합니다.

AWS-UpdateCloudFormationStack

설명

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

[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.

- `LambdaAssumeRole`

유형: 문자열

설명: (필수) Lambda에서 수입하는 역할의 ARN입니다.

- StackNameOrId

유형: 문자열

설명: (필수) 업데이트할 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 Automation은 Amazon CloudFront에 사전 정의된 실행서를 제공합니다. 실행서에 대한 자세한 내용은 [실행서 작업](#)을 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 실행서는 사용자가 지정하는 Amazon CloudFront(CloudFront) 배포에 대한 액세스 로깅을 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.

- 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 리전 의 버킷은 지원되지 않습니다.

- CloudFrontId

유형: 문자열

설명: (필수) 액세스 로그온을 활성화하려는 CloudFront 배포의 ID입니다.

- IncludeCookies

유형: 부울

유효한 값: true | false

설명: (필수) 쿠키를 액세스 로그에 포함하려면이 파라미터를 true 로 설정합니다.

- 접두사

유형: 문자열

설명: (선택 사항) CloudFront가 배포에 대한 액세스 로그 filenames에 접두사로 추가하게 하려는 선택적 문자열(예: myprefix/)입니다.

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. 교차 계정 S3 버킷에는 사용할 수 없습니다.

문서 단계

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

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 자동화하는에 대한 사전 정의된 실행서를 제공합니다 AWS CloudTrail. 실행서에 대한 자세한 내용은 [실행서 작업](#)을 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 AWS 리전 에서 선택한 Amazon Simple Storage Service AWS CloudTrail (Amazon S3) 버킷으로 로그 파일을 전송 하는 (CloudTrail) 추적을 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 추적을 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 정책](#)을 참조하세요.

- TrailName

유형: 문자열

설명: (필수) 새로운 트레일의 이름.

AWS-EnableCloudTrailCloudWatchLogs

설명

이 실행서는 하나 이상의 AWS CloudTrail 추적 구성을 업데이트하여 Amazon CloudWatch Logs 로그 그룹에 이벤트를 전송합니다.

[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.

- CloudWatchLogsLogGroupArn

유형: 문자열

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

- CloudWatchLogsRoleArn

유형: 문자열

설명: (필수) IAM 역할 CloudWatch Logs Logs의 ARN은 지정된 로그 그룹에 쓸 것으로 가정합니다.

- TrailNames

유형: StringList

설명: (필수) 이벤트를 CloudWatch Logs로 보내려는 CloudTrail 추적의 이름에 대한 심표로 구분된 목록입니다. CloudWatch

필수 IAM 권한

실행서를 성공적으로 사용하려면 AutomationAssumeRole 파라미터에 다음 작업이 필요합니다.

- cloudtrail:UpdateTrail
- iam:PassRole

문서 단계

- aws:executeScript - 지정된 CloudTrail 추적을 업데이트하여 지정된 CloudWatch Logs 로그 그룹에 이벤트를 전달합니다.

AWSConfigRemediation-EnableCloudTrailEncryptionWithKMS

설명

AWSConfigRemediation-EnableCloudTrailEncryptionWithKMS 실행서는 지정한 AWS CloudTrail () 고객 관리형 키를 사용하여 AWS Key Management Service (CloudTrail AWS KMS) 추적을 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 추적에 true 대해 EnableLogFileValidation 파라미터를 로 설정한 경우 자세한 내용은 AWS CloudTrail 사용 설명서의 [CloudTrail 예방 보안 모범 사례](#) 주제의 "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 실행서는 AWS Key Management Service (AWS KMS) 암호화를 사용하도록 하나 이상의 AWS CloudTrail 추적 구성을 업데이트합니다.

[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.

- `KMSKeyId`

유형: 문자열

설명: (필수) `TrailName` 파라미터에 지정한 추적을 암호화하는 데 사용할 고객 관리형 키의 키 ID입니다. 값은 "alias/" 접두사가 붙은 별칭 이름, 별칭에 대해 완전히 지정된 ARN 또는 키에 대해 완전히 지정된 ARN일 수 있습니다.

- TrailNames

유형: StringList

설명: (필수) 암호화되도록 업데이트하려는 추적의 쉼표로 구분된 목록입니다.

필수 IAM 권한

실행서를 성공적으로 사용하려면 AutomationAssumeRole 파라미터에 다음 작업이 필요합니다.

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

문서 단계

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

AWSConfigRemediation-EnableCloudTrailLogFileValidation

설명

AWSConfigRemediation-EnableCloudTrailLogFileValidation 실행서는 AWS CloudTrail 추적에 대한 로그 파일 검증을 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.

- 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

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.

- 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 AWS CloudTrail (CloudTrail) 로그를 포함하는 선택한 Amazon Simple Storage Service(Amazon S3) 버킷에서 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 수

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.

- Query

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

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.

다. 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.

- **status**

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-EnableCWAAlarm

설명

AWS-EnableCWAAlarm 실행서는 아직 없는의 AWS 리소스에 대한 Amazon CloudWatch(CloudWatch) 경고 AWS 계정 를 생성합니다. CloudWatch 경보는 다음 AWS 리소스에 대해 생성됩니다.

- Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스
- Amazon Elastic Block Store(Amazon EBS) 볼륨
- Amazon Simple Storage Service(Amazon S3) 버킷
- Amazon Relational Database Service(Amazon RDS) 클러스터

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.

- ComparisonOperator

유형: 문자열

유효한 값: GreaterThanOrEqualToThreshold | GreaterThanThreshold | GreaterThanUpperThreshold | LessThanLowerOrGreaterThanUpperThreshold | LessThanLowerThreshold | LessThanOrEqualToThreshold | LessThanThreshold

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

- MetricName

유형: 문자열

설명: (필수) 경보와 연결된 지표의 이름입니다.

- 기간

유형: 정수

유효한 값: 10 | 30 | 60 | 60의 배수

설명: (필수) 통계가 적용되는 초 단위 기간입니다.

- ResourceARNs

유형: StringList

설명: (필수) CloudWatch 경보를 생성할 리소스의 쉼표로 구분된 ARNs.

- 통계

유형: 문자열

유효한 값: Average | Maximum | Minimum | SampleCount | Sum

설명: (필수) 경보와 연결된 지표의 통계입니다.

- Threshold

유형: 정수

설명: (필수) 지정된 통계와 비교할 값입니다.

필수 IAM 권한

실행서를 성공적으로 사용하려면 AutomationAssumeRole 파라미터에 다음 작업이 필요합니다.

- cloudwatch:PutMetricAlarm

문서 단계

- aws:executeScript - 파라미터에서 지정한 리소스에 대한 실행서 ResourceARNs 파라미터에 지정된 값에 따라 CloudWatch 경보를 생성합니다.

출력

EnableCWAAlarm.FailedResources: CloudWatch 경보가 생성되지 않은 리소스 ARNs의 맵 목록과 실패 이유입니다.

EnableCWAAlarm.SuccessfulResources: CloudWatch 경보가 성공적으로 생성된 리소스 ARNs 목록입니다.

AWSSupport-TroubleshootCloudWatchAgent

설명

AWSSupport-TroubleshootCloudWatchAgent 실행서는 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스의 Amazon CloudWatch 에이전트 문제 해결을 자동화합니다. Amazon EC2 실행서는 일련의 기본 및 (선택 사항) 확장 검사를 통해 이 문제 해결을 수행합니다.

기본 검사에는 다음이 포함됩니다.

- AWS Identity and Access Management (IAM) 인스턴스 프로파일 확인
- 필요한 Amazon CloudWatch Agent IAM 권한이 Amazon EC2 인스턴스에 연결되어 있는지 확인

확장된 검사는 제공된 Amazon EC2 인스턴스 ID가 Systems Manager 관리형 인스턴스인 경우에만 수행됩니다. 이러한 확장 검사에는 다음이 포함됩니다.

- 인스턴스에서 Amazon CloudWatch Agent의 상태 확인
- Amazon CloudWatch Agent의 로그를 분석하여 일반적인 문제 및 관련 문제 해결 단계 확인
- Amazon EC2 인스턴스에서 관련 로그 및 구성 파일을 압축하고 선택적으로 선택한 Amazon Simple Storage Service(Amazon S3) 버킷에 업로드합니다.
- 인스턴스와 필수 엔드포인트 간의 연결 확인 수행

Important

RunVpcReachabilityAnalyzer 파라미터가 로 설정되면 true이 런북은 하위 런북을 호출해야 하는지 여부를 결정합니다. AWSSupport-AnalyzeAWSEndpointReachabilityFromEC2. 하위 실행서는 관련 비용이 있는 VPC Reachability Analyzer를 사용합니다. 요금에 대한 자세한 내용은 [Amazon VPC 요금](#) 설명서를 참조하세요.

Important

이 실행서는 IAM 인스턴스 프로파일 역할에 필요한 권한만 확인합니다. 대신 .aws/credentials 파일에 정의된 자격 증명을 사용하는 경우 verifyIamPermissions 단계의 결과가 부정확할 수 있습니다.

어떻게 작동 하나요?

실행서는 다음 단계를 수행합니다.

- `getInstanceProfile`: 제공된 Amazon EC2 인스턴스에 IAM 인스턴스 프로파일이 연결되어 있는지 확인합니다.
- `verifyIamPermissions`: 인스턴스와 연결된 인스턴스 프로파일을 확인하여 필요한 IAM 권한이 적용되었는지 확인합니다.
- `getInstanceInformation`: 인스턴스에 활성 Systems Manager 에이전트가 있는지 확인하고 인스턴스의 OS 유형을 가져옵니다.
- `getAgentStatus`: 인스턴스에서 Amazon CloudWatch Agent의 상태를 확인합니다(확장 검사).
- `analyzeLogs/analyzeLogsWindows`: OS 유형에 따라 Amazon CloudWatch Agent 로그의 결과를 분석하고 출력합니다.
- `collectLogs/collectLogsWindows`: OS 유형에 따라 관련 Amazon CloudWatch Agent 문제 해결 파일을 번들링하고 출력합니다.
- `checkEndpointReachability/checkEndpointReachabilityWindows`: 인스턴스가 OS 유형에 따라 필요한 엔드포인트에 도달할 수 있는지 확인합니다.
- `analyzeAwsEndpointReachabilityFromEC2`: 하위 자동화 런북을 호출하여 선택한 인스턴스가 필요한 엔드포인트에 도달하는지 확인합니다(활성화된 경우).

[이 자동화 실행\(콘솔\)](#)

문서 유형

자동화

소유자

Amazon

플랫폼

/

필수 IAM 권한

실행서를 성공적으로 사용하려면 `AutomationAssumeRole` 파라미터에 다음 작업이 필요합니다.

- ec2:DescribeInstances
- iam:GetInstanceProfile
- iam:GetRole
- iam:ListAttachedRolePolicies
- iam:ListRolePolicies
- iam:GetRolePolicy
- iam:GetPolicy
- iam:GetPolicyVersion
- iam:SimulatePrincipalPolicy
- ssm:DescribeInstanceInformation
- ssm:SendCommand
- ssm:GetCommandInvocation
- ssm:DescribeInstanceAssociationsStatus
- ssm:StartAutomationExecution

예제 정책:

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

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

지침

다음 단계에 따라 자동화를 구성합니다.

1. Systems Manager [AWSSupport-TroubleshootCloudWatchAgent](#)의 문서로 이동합니다.
2. Execute automation(자동화 실행)을 선택합니다.
3. 입력 파라미터에 다음을 입력합니다.
 - AutomationAssumeRole(선택 사항):
 - 설명: (선택 사항) Systems Manager Automation이 사용자를 대신하여 작업을 수행하도록 허용하는 IAM 역할의 ARN입니다. 역할을 지정하지 않은 경우, Systems Manager Automation에서 이 실행서를 시작하는 사용자의 권한을 사용합니다.
 - 유형: `AWS::IAM::Role::Arn`
 - InstanceId(필수):
 - 설명: (필수) Amazon CloudWatch 에이전트 문제를 해결하려는 Amazon EC2 인스턴스의 ID입니다. Amazon CloudWatch
 - 유형: `AWS::EC2::Instance::Id`
 - 패턴 허용: `^i-[0-9a-f]{8,17}$`
 - S3UploadBucket(선택 사항):
 - 설명: (선택 사항) 수집된 Amazon CloudWatch Agent 로그를 업로드할 Amazon S3 버킷의 이름입니다. Amazon CloudWatch Amazon EC2 인스턴스 프로파일에는 이 버킷에 파일을 업로드할 수 있는 올바른 권한이 있어야 합니다. 또한 대상 Amazon EC2 인스턴스가 Systems Manager 관리형 인스턴스여야 합니다.
 - 유형: `AWS::S3::Bucket::Name`
 - 패턴 허용: `^$|^[a-z0-9][a-z0-9.-]{1,61}[a-z0-9]$`
 - 기본값: `""`
 - S3BucketOwnerAccountId(선택 사항):
 - 설명: (선택 사항) Amazon CloudWatch Agent 로그를 업로드하려는 Amazon S3 버킷을 소유한 AWS 계정 번호입니다. Amazon CloudWatch 이 파라미터를 수정하지 않으면 실행서는 자동화가 실행되는 사용자 또는 역할의 AWS 계정 ID를 사용합니다.

- 유형: String
 - 패턴 허용: `^\{\{\{ global:ACCOUNT_ID \}\}\}$|^[0-9]{12}$`
 - 기본값: `{{ global:ACCOUNT_ID }}`
 - CheckEC2Endpoint(선택 사항):
 - 설명: (선택 사항) 에이전트 구성에서 옵션을 사용하여 에이전트가 수집한 지표 `append_dimensions`에 Amazon EC2 지표 차원을 추가할 `true`지 지정합니다. `append_dimensions`를 사용하는 경우 Amazon CloudWatch Agent는 Amazon EC2 API 엔드포인트에 연결해야 하므로 확장 검사를 통해 추가 연결 테스트를 수행합니다.
 - 유형: String
 - 허용된 값: `[true, false]`
 - 기본값: `false`
 - RunVpcReachabilityAnalyzer(선택 사항):
 - 설명: (선택 사항) 네트워크 문제가 확장 검사에 의해 결정되거나 지정된 인스턴스 ID가 관리형 인스턴스가 아닌 경우 `AWSSupport-AnalyzeAWSEndpointReachabilityFromEC2` 하위 자동화를 실행 `true`하도록 지정합니다.
 - 유형: Boolean
 - 기본값: `false`
 - RetainVpcReachabilityAnalysis(선택 사항):
 - 설명: (선택 사항)이 인 경우에만 관련이 `RunVpcReachabilityAnalyzer` 있습니다 `true`. VPC Reachability Analyzer에서 생성한 네트워크 인사이트 경로 및 관련 분석을 유지 `true`하려면 지정합니다. 기본적으로 이러한 리소스는 성공적인 분석 후 삭제됩니다.
 - 유형: Boolean
 - 기본값: `false`
4. 실행을 선택합니다.
 5. 자동화가 시작됩니다.
 6. 문서는 다음 단계를 수행합니다.

- getInstanceProfile:

제공된 Amazon EC2 인스턴스에 IAM 인스턴스 프로파일이 연결되어 있는지 확인합니다.

- branchOnInstanceProfileStatus:

인스턴스 프로파일이 인스턴스에 연결된 경우 자동화를 분기하여 필요한 인스턴스 프로파일 권한을 확인합니다.

- `verifyIamPermissions`:

인스턴스와 연결된 인스턴스 프로파일을 확인하여 필요한 IAM 권한이 적용되는지 확인합니다.

- `getInstanceInformation`:

인스턴스에 활성 Systems Manager 에이전트가 있는지 확인하고 인스턴스의 OS 유형을 가져옵니다.

- `branchOnManagedInstance`:

자동화를 분기하여 인스턴스가 관리되는지 확장 검사를 수행합니다.

- `getAgentStatus`:

인스턴스에서 Amazon CloudWatch Agent의 상태를 확인합니다.

- `branchOnInstanceOsType`:

자동화를 분기하여 OS를 기반으로 특정 로그 수집/분석 명령을 실행합니다.

- `analyzeLogs/analyzeLogsWindows`:

OS 유형에 따라 Amazon CloudWatch Agent 로그의 결과를 분석하고 출력합니다.

- `collectLogs/collectLogsWindows`:

OS 유형에 따라 관련 Amazon CloudWatch Agent 문제 해결 파일을 번들링하고 출력합니다.

- `checkEndpointReachability/checkEndpointReachabilityWindows`:

인스턴스가 OS 유형에 따라 필요한 엔드포인트에 도달할 수 있는지 확인합니다.

- `branchOnRunVpcReachabilityAnalyzer`:

활성화되고 네트워크 문제가 감지되면 자동화를 분기하여 VPC 연결성 분석을 실행합니다.

- `generateEndpoints`:

확장 검사 실패 및 값을 확인할 엔드포인트를 생성합니다 `CheckEC2Endpoint`.

- `analyzeAwsEndpointReachabilityFromEC2`:

자동화 실행서를 호출 `AWSSupport-AnalyzeAWSEndpointReachabilityFromEC2`하여 선택한 인스턴스가 필요한 엔드포인트에 도달하는지 확인합니다.

- `outputFindings`:

자동화 실행 단계의 결과를 출력합니다.

7. 완료 후 출력 섹션에서 실행의 자세한 결과를 검토합니다.

참조

Systems Manager Automation

- [이 자동화 실행\(콘솔\)](#)
- [자동화 실행](#)
- [Automation 설정](#)
- [자동화 워크플로 지원](#)

AWSsupport-TroubleshootCloudWatchAlarm

설명

AWSsupport-TroubleshootCloudWatchAlarm 실행서는 잘못 구성되거나 문제가 있는 Amazon CloudWatch(CloudWatch) 경보 관련 문제를 식별하고 해결하는 데 도움이 됩니다. 이는 AWS APIs 및 알려진 경보 평가 로직을 활용하여 모니터링되는 지표에서 지연되거나 누락된 데이터 포인트를 감지하므로 경보 작업이 누락되거나 지연될 수 있습니다. 이 실행서는 Amazon CloudWatch(CloudWatch) 경보 관련 문제를 조사하고 해결하기 위한 구조화된 접근 방식을 제공합니다.

어떻게 작동하나요?

실행서는 다음 단계를 AWSsupport-TroubleshootCloudWatchAlarm 수행합니다.

- Amazon CloudWatch(CloudWatch) 경보 세부 정보와 AlarmTriggerTimestamp 파라미터 값을 확인하여 2,592,000초(30일) 내에 있는지 확인합니다.
- 경보가 지표 또는 지표 수학을 기반으로 하는지 또는 이상 탐지기 경보인지 확인합니다.
- 경보가 데이터 상태가 부족한지 확인합니다.
- 경보에 사용된 지표(들)가 ListMetrics 값과 일치하는지 확인합니다.
- 지정된 타임스탬프에서 지표에 데이터 포인트(들)가 누락되었는지 확인합니다.
- 지정된 타임스탬프에 대한 최신 기록을 가져옵니다.
- 지연되거나 누락된 지표(들)로 인해 경보가 트리거되지 않았는지 확인합니다.
- 경보의 활성화된 작업(들)이 전송되었는지/전송되었는지 확인합니다.
- 모든 진단 결과를 결합하는 문제 해결 보고서를 생성합니다.

이 자동화 실행(콘솔)

문서 유형

자동화

소유자

Amazon

플랫폼

Linux, macOS, Windows

파라미터

필수 IAM 권한

실행서를 성공적으로 사용하려면 AutomationAssumeRole 파라미터에 다음 작업이 필요합니다.

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

JSON

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

```

        "cloudwatch:ListMetrics"
      ],
      "Resource": "*"
    }
  ]
}

```

지침

다음 단계에 따라 자동화를 구성합니다.

1. Systems Manager [AWSSupport-TroubleshootCloudWatchAlarm](#)의 문서로 이동합니다.
2. Execute automation(자동화 실행)을 선택합니다.
3. 입력 파라미터에 다음을 입력합니다.
 - AutomationAssumeRole(선택 사항):
 - 유형: String
 - 설명: (선택 사항) 사용자를 대신하여 Systems Manager Automation을 통해 작업을 수행할 수 있도록 허용하는 AWS AWS Identity and Access Management (IAM) 역할의 Amazon 리소스 이름(ARN)입니다. 역할이 지정되지 않은 경우 Systems Manager Automation은 이 실행서를 시작하는 사용자의 권한을 사용합니다.
 - CloudWatchMetricAlarmName(필수):
 - 유형: String
 - 설명: (필수) 문제를 해결할 Amazon CloudWatch(CloudWatch) 지표 경보의 이름입니다.
 - 허용된 패턴: `^[a-zA-Z0-9.:;,\-\_&()] {1,255}$`
 - AlarmTriggerTimestamp(필수):
 - 유형: String
 - 설명: (필수) 경보 문제가 발생한 시점의 UTC 타임스탬프입니다. 이 정보는 문제를 해결하고 문제가 발생한 컨텍스트를 이해하는 데 매우 중요합니다. 타임스탬프 값은 오늘부터 지난 30일 이내의 시간이어야 하며 형식이어야 합니다 YYYY-MM-DDTHH:mm:ssZ. 예시: 2024-10-29T09:04:00Z
 - 허용된 패턴: `^((\d{4})-(\d{2})-(\d{2})T(\d{2}):(\d{2}):(\d{2}))Z$`
4. 실행을 선택합니다.
5. 자동화가 시작됩니다.
6. 문서는 다음 단계를 수행합니다.

- **VerifyRunbookInputs**

Amazon CloudWatch(CloudWatch) 경보 세부 정보와 AlarmTriggerTimestamp 파라미터 값을 확인하여 2,592,000초(30일) 내에 있는지 확인합니다.

- **UpdateSSMDocumentInputChecksVariable**

변수를 SSMDocumentInputChecks VerifyRunbookInputs 단계의 SSMDocumentInputChecks 값으로 업데이트합니다.

- **BranchOnAlarmIsVerified**

런북의 입력 확인 AlarmTriggerTimestamp 및에 분기합니다CloudWatchAlarmName.

- **CheckMetricAlarmType**

경보가 지표 또는 지표 수학을 기반으로 하는지 또는 이상 탐지기 경보인지 확인합니다.

- **CheckAlarmInInsufficientDataState**

경보가 데이터 상태가 부족한지 확인합니다.

- **UpdateInsufficientDataChecksVariable**

변수를 InsufficientDataChecks CheckAlarmInInsufficientDataState 단계의 InsufficientDataChecks 값으로 업데이트합니다.

- **BranchOnAlarmHasInsufficientData**

CheckAlarmInInsufficientDataState 단계의 AlarmHasInsufficientData 값을 분기합니다. 기본 단계는 입니다CheckMetricMismatch.

- **CheckMetricMismatch**

경보에 사용된 지표(들)가 ListMetrics 값과 일치하는지 확인합니다.

- **UpdateMetricMismatchChecksVariable**

변수를 MetricMismatchChecks CheckMetricMismatch 단계의 MetricMismatchChecks 값으로 업데이트합니다.

- **BranchOnMetricsMatched**

CheckMetricMismatch 단계의 MetricsMatched 값을 분기합니다. 기본 단계는 입니다CheckMissingDatapoint.

- **CheckMissingDatapoint**

지정된 타임스탬프에서 지표에 데이터 포인트(들)가 누락되었는지 확인합니다.

- **UpdateMetricMissingDatapointsChecksVariable**

변수를 MetricMissingDatapointsChecks CheckMissingDatapoint 단계의 MetricMissingDatapointsChecks 값으로 업데이트합니다.

- **BranchOnMetricMissingDatapoint**

CheckMissingDatapoint 단계의 MetricMissingDatapoint 값을 분기합니다. 기본 단계는 입니다GetAlarmHistoryDetails.

- **GetAlarmHistoryDetails**

지정된 타임스탬프에 대한 최신 기록을 가져옵니다.

- **UpdateAlarmHistoryChecksVariable**

변수를 AlarmHistoryChecks GetAlarmHistoryDetails 단계의 AlarmHistoryChecks 값으로 업데이트합니다.

- **BranchOnAlarmHistoryFound**

GetAlarmHistoryDetails 단계의 AlarmHistoryFound 값을 분기합니다. 기본 단계는 입니다CheckDelayedMetric.

- **CheckDelayedMetric**

지연되거나 누락된 지표(들)로 인해 경보가 트리거되지 않았는지 확인합니다.

- **UpdateDelayedMetricChecksVariable**

변수를 DelayedMetricChecks CheckDelayedMetric 단계의 DelayedMetricChecks 값으로 업데이트합니다.

- **BranchOnMetricDelayedAndDatapointsMeetThreshold**

CheckDelayedMetric 단계의 MetricDelayed 및 DatapointsMeetThreshold 값을 분기합니다. 기본 단계는 입니다GenerateReport.

- **CheckActionDelivered**

경보의 활성화된 작업(들)이 전송되었는지/전송되었는지 확인합니다.

- **UpdateActionDeliveredChecksVariable**

ActionDeliveredChecks CheckActionDelivered 단계의 출력ActionDeliveredChecks으로 변수를 업데이트합니다.

- **GenerateReport**

이전 단계의 출력을 컴파일하고 보고서를 출력합니다.

7. 실행이 완료되면 출력 섹션에서 실행의 자세한 결과를 검토합니다.

- GenerateReport.Report

제공된 Amazon CloudWatch(CloudWatch) 지표 경보에 대한 보고서입니다.

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

=====
1. Validating SSM Document input parameters:
=====

# [PASSED]: Found a metric alarm with name Demo-Alarm

=====

2. Checking alarm's data state:
```



```
=====
# [PASSED]: The alarm is not in INSUFFICIENT_DATA state, alarm's
state is: ALARM
=====
```

```
=====
3. Checking if the alarm experienced metric mismatches:
=====
```

```
=====
# [PASSED]: Metric matches with the configured metric for Alarm.
=====
```

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

```
=====
# [PASSED]: Metric has datapoints
=====
```

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

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

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

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

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

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

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

참조

Systems Manager Automation

- [이 자동화 실행\(콘솔\)](#)
- [자동화 실행](#)
- [Automation 설정](#)
- [Support Automation Workflows 랜딩 페이지](#)

Amazon DocumentDB

AWS Systems Manager Automation은 Amazon DocumentDB(MongoDB 호환)를 위한 사전 정의된 실행서를 제공합니다. 실행서에 대한 자세한 내용은 [실행서 작업](#)을 참조하세요. 실행서 콘텐츠를 보는 방법에 대한 자세한 내용은 [실행서 콘텐츠 보기](#)(을)를 참조하세요.

주제

- [AWS-EnableDocDbClusterBackupRetentionPeriod](#)

AWS-EnableDocDbClusterBackupRetentionPeriod

설명

AWS-EnableDocDbClusterBackupRetentionPeriod 실행서는 지정한 Amazon DocumentDB 클러스터에 대한 백업 보존 기간을 활성화합니다. 이 기능은 자동 백업이 유지되는 총 일수를 설정합니다. 클러스터를 수정하려면 클러스터가 엔진 유형이 인 사용 가능한 상태여야 합니다docdb.

[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.

- DBClusterResourceId

유형: 문자열

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

- BackupRetentionPeriod

유형: 정수

설명: (필수) 자동 백업이 유지되는 일수입니다. 7~35일의 값이어야 합니다.

- PreferredBackupWindow

유형: 문자열

설명: (선택 사항) 07:14-07:44와 같이 hh24:mm-hh24:mm 형식의 UTC(Universal Time Coordinated)의 일일 시간 범위입니다. 값은 30분 이상이어야 하며 기본 유지 관리 기간과 충돌할 수 없습니다.

- `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 유형이 다른 Amazon RDS 엔진 유형에 docdb 대한 의도하지 않은 변경을 방지하는지 확인합니다.
- `VerifyDocDbStatus(aws:waitAwsResourceProperty)` - Amazon DocumentDB 클러스터 상태가 인지 확인합니다available.
- `ModifyDocDbRetentionPeriod(aws:executeAwsApi)` - 지정된 Amazon DocumentDB 클러스터에 제공된 값을 사용하여 보존 기간을 설정합니다.
- `VerifyDocDbBackupsEnabled(aws:executeScript)` - Amazon DocumentDB 클러스터의 보존 기간과 지정된 경우 기본 백업 기간이 성공적으로 설정되었는지 확인합니다.

출력

`ModifyDocDbRetentionPeriod.ModifyDbClusterResponse` - `ModifyDBCluster` API 작업의 응답입니다.

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

CodeBuild

AWS Systems Manager 자동화하는에 대한 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 실행서는 지정한 AWS CodeBuild () 고객 관리형 키를 사용하여 AWS Key Management Service (CodeBuild AWS KMS) 프로젝트의 빌드 아티팩트를 암호화합니다.이 자동화를 실행하는 AWS 리전 에서 활성화해야 AWS Config 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.

- KMSKeyId

유형: 문자열

설명: (필수) ProjectId 파라미터에 사용자가 지정하는 CodeBuild 프로젝트를 암호화하는 데 사용하려는 AWS KMS 고객 관리형 키의 Amazon 리소스 이름(ARN)입니다.

- ProjectId

유형: 문자열

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

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 지정하는 CodeBuild 프로젝트에서 암호화를 활성화합니다.
- aws:assertAwsResourceProperty - CodeBuild 프로젝트에서 암호화가 활성화되었는지 확인합니다.

출력

UpdateLambdaConfig.UpdateFunctionConfigurationResponse - UpdateFunctionConfiguration API 호출의 응답입니다.

AWSConfigRemediation-DeleteAccessKeysFromCodeBuildProject

설명

AWSConfigRemediation-DeleteAccessKeysFromCodeBuildProject 실행서는 지정한 AWS CodeBuild (CodeBuild) 프로젝트에서 AWS_ACCESS_KEY_ID 및 AWS_SECRET_ACCESS_KEY 환경 변수를 삭제합니다. 이 자동화를 실행하는 AWS 리전 에서 활성화해야 AWS Config 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 자동화에는 대한 사전 정의된 실행서를 제공합니다 AWS CodeDeploy. 실행서에 대한 자세한 내용은 [실행서 작업](#)을 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 인스턴스에 AWS Identity and Access Management (IAM) 인스턴스 프로파일이 연결되어 있지 않습니다.
- 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 자동화에는 대한 사전 정의된 실행서를 제공합니다 AWS Config. 실행서에 대한 자세한 내용은 [실행서 작업](#)을 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,에서 제공하는 구성 레코더 AWS Config,가 구성 스냅샷 및 구성 기록 파일을 AWS Config 전송하는 Amazon Simple Storage Service(Amazon S3) 버킷이 있는 전송 채널을 생성합니다. AggregatorAccountId 및 AggregatorAccountRegion 파라미터에 값을 지정하면 실행서는 여러 AWS 계정 및 여러에서 AWS Config 구성 및 규정 준수 데이터를 수집하기 위한 데이터 집계 권한

도 생성합니다 AWS 리전. 여러 계정 및 리전의 데이터를 집계하는 것에 대해 자세히 알아보려면 AWS Config 개발자 안내서의 [다중 계정 다중 리전 데이터 집계](#)를 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) 여러 계정 및의 AWS Config 구성 및 규정 준수 데이터를 집계하기 위해 집계자를 추가할 AWS 계정 의 ID입니다 AWS 리전. 이 계정은 집계자가 소스 계정을 승인하는 데도 사용됩니다.

- AggregatorAccountRegion

유형: 문자열

설명: (선택 사항) 집계자를 추가하여 여러 계정 및 리전의 AWS Config 구성 및 규정 준수 데이터를 집계할 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.

- Partition

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 Config 에 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 Automation은 Amazon Connect용 사전 정의된 실행서를 제공합니다. 실행서에 대한 자세한 내용은 [실행서 작업](#)을 참조하세요. 실행서 콘텐츠를 보는 방법에 대한 자세한 내용은 [실행서 콘텐츠 보기](#)(을)를 참조하세요.

주제

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

AWSSupport-AssociatePhoneNumbersToConnectContactFlows

설명

는 전화번호를 Amazon Connect 인스턴스의 고객 응대 흐름에 연결하는 데 AWSSupport-AssociatePhoneNumbersToConnectContactFlows 도움이 됩니다. 전화번호와 고객 응대 흐름의 매핑을 입력 심표로 구분된 값(CSV) 파일에 제공하여 실행서는 14.5분 이내에 가능한 한 많은 전화번호를 고객 응대 흐름에 연결합니다. 실행서는 시간 제한 내에 연결할 수 없는 모든 전화번호 및 고객 응대 흐름 페어의 CSV 파일을 생성하므로 다음 실행에서 입력할 수 있습니다.

어떻게 작동하나요?

실행서는 Amazon Simple Storage Service(S3) 버킷에 저장된 매핑 데이터의 CSV 파일을 사용하여 전화번호를 Amazon Connect 인스턴스의 고객 응대 흐름에 연결하는 데 AWSSupport-AssociatePhoneNumbersToConnectContactFlows 도움이 됩니다. Amazon S3 입력 CSV 파일은 [E.164](#) 형식의 PhoneNumber 값으로 다음 형식과 일치해야 합니다.

입력 CSV 파일의 예

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

또한 자동화 실행서는 DestinationFileBucket 및에 지정된 대상 위치에 다음 파일을 생성합니다 DestinationFilePath.

- **automation:EXECUTION_ID/ResourceIdList.csv:**
AssociatePhoneNumberContactFlow API에 필요한 PhoneNumberId 및 ContactFlowId 페어가 포함된 임시 파일입니다.
- **automation:EXECUTION_ID/ErrorResourceList.csv:** 형식과 같이 오류로 인해 처리할 수 없는 전화번호 및 고객 응대 흐름 페어 ResourceNotFoundException가 포함된 파일입니다 PhoneNumber,ContactFlowName,ErrorMessage.
- **automation:EXECUTION_ID/NonProcessedResourceList.csv:** 처리되지 않은 전화번호와 고객 응대 흐름 페어가 포함된 파일입니다. 실행서는 14.5분(AWS Lambda 함수 제한 시간 15분 - 버퍼 30초) 이내에 가능한 한 많은 전화번호와 고객 응대 흐름을 처리하려고 시도합니다. 시간 제약으로 인해 처리할 수 없는 전화번호/연락 흐름이 있는 경우 런북은 다음 런북 실행을 위한 입력으로 사용할 수 있도록 CSV 파일에 전화번호/연락 흐름을 포함합니다.

문서 유형

자동화

소유자

Amazon

플랫폼

Linux, macOS, Windows

파라미터

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:::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"
  }
]
}

```

LambdaRoleArn 파라미터를 제공하는 경우 런북을 성공적으로 사용하려면 역할에 다음 작업이 필요합니다.

JSON

```
{
```



```
"Version":"2012-10-17",
"Statement": [
  {
    "Action": [
      "logs:CreateLogGroup"
    ],
    "Resource": "arn:aws:logs:us-east-1:111122223333:*",
    "Effect": "Allow"
  },
  {
    "Action": [
      "logs:CreateLogStream",
      "logs:PutLogEvents"
    ],
    "Resource": "arn:aws:logs:us-east-1:111122223333:*",
    "Effect": "Allow"
  },
  {
    "Action": [
      "connect:AssociatePhoneNumberContactFlow"
    ],
    "Resource": "*",
    "Effect": "Allow"
  },
  {
    "Action": [
      "s3:PutObject",
      "s3:GetObject"
    ],
    "Resource": "arn:aws:s3:::amzn-s3-demo-bucket/DESTINATION_FILE_PATH*",
    "Effect": "Allow"
  }
]
```

지침

다음 단계에 따라 자동화를 구성합니다.

1. Systems Manager [AWSSupport-AssociatePhoneNumbersToConnectContactFlows](#)의 문서로 이동합니다.

2. Execute automation(자동화 실행)을 선택합니다.

3. 입력 파라미터에 다음을 입력합니다.

- AutomationAssumeRole(선택 사항)

Systems Manager Automation이 사용자를 대신하여 작업을 수행하도록 허용하는 (IAM) 역할의 Amazon 리소스 이름 AWS AWS Identity and Access Management (ARN)입니다. 역할이 지정되지 않은 경우 Systems Manager Automation은 이 실행서를 시작하는 사용자의 권한을 사용합니다.

- ConnectInstanceId(필수)

Amazon Connect 인스턴스의 ID입니다.

- SourceFileBucket(필수)

전화번호와 고객 응대 흐름 페어가 포함된 CSV 파일을 저장하는 Amazon S3 버킷입니다.

- SourceFilePath(필수)

전화번호와 고객 응대 흐름 페어가 포함된 CSV 파일의 Amazon S3 객체 키입니다. 예를 들어 path/to/input.csv입니다.

- DestinationFileBucket(필수)

자동화가 중간 파일 및 결과 보고서를 배치할 Amazon S3 버킷입니다.

- DestinationFilePath(선택 사항)

중간 파일 및 결과 보고서를 저장해야 DestinationFileBucket 하는 Amazon S3 객체 경로입니다. 예를 들어를 지정하면 path/to/files/파일이 아래에 저장됩니다s3://[DestinationFileBucket]/path/to/files/[automation:EXECUTION_ID]/.

- S3BucketOwnerAccount(선택 사항)

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

- S3BucketOwnerRoleArn(선택 사항)

Amazon S3 버킷 및 계정에서 퍼블릭 액세스 설정, 버킷 암호화 구성, 버킷 ACLs입니다. 이 파라미터를 지정하지 않으면 실행서는 이 실행서를 시작하는 AutomationAssumeRole (지정된 경우) 또는 사용자(지정되지 않은 경우)AutomationAssumeRole를 사용합니다. 실행서 설명의 필수 권한 섹션을 참조하세요.

- LambdaRoleArn(선택 사항)

AWS Lambda 함수가 필요한 AWS 서비스 및 리소스에 액세스할 수 있도록 허용하는 IAM 역할의 ARN입니다. 역할이 지정되지 않은 경우 이 자동화는 계정에서 Lambda에 대한 IAM 역할을 하나 생성합니다.

4. 실행을 선택합니다.

5. 자동화가 시작됩니다.

6. 문서는 다음 단계를 수행합니다.

- CheckConnectInstanceExistence

에 제공된 Amazon Connect 인스턴스가 ConnectInstanceId 존재하는지 확인합니다.

- CheckS3BucketPublicStatus

에 지정된 Amazon S3 버킷SourceFileBucket이 익명 또는 퍼블릭 읽기 또는 쓰기 액세스 권한을 DestinationFileBucket 허용하는지 확인합니다.

- CheckSourceFileExistenceAndSize

에 지정된 소스 CSV 파일이 SourceFilePath 있는지, 파일 크기가 25MiB 제한을 초과하는지 확인합니다.

- GenerateResourceIdMap

에 지정된 소스 CSV 파일을 다운로드SourceFilePath하고 각 리소스에 ContactFlowId 대해 PhoneNumberId 및를 식별합니다. 완료되면 , PhoneNumber, ContactFlowName및가 포함된 CSV 파일을 PhoneNumberId에 지정된 대상 Amazon S3 버킷ContactFlowId에 업로드합니다DestinationFileBucket. 특정 번호에 대해 식별할 수 PhoneNumberId 없는 경우 CSV 파일에서 필드가 비어 있습니다.

- AssociatePhoneNumbersToContactFlows

AWS CloudFormation 스택을 사용하여 계정에 AWS Lambda 함수를 생성합니다. AWS Lambda 함수는 각 번호를 SourceFileBucket 및에 지정된 소스 CSV 파일에 나열된 고객 응대 흐름에 연결하고 AWS CloudFormation 스택SourceFilePath은 함수를 호출합니다. AWS Lambda 함수는 제한 시간(15분) 전에 고객 응대 흐름에 최대한 많은 전화번호를 매핑합니다. 오류로 인해 처리할 수 없는 전화번호 및 고객 응대 흐름 목록은에 업로드됩니다[automation:EXECUTION_ID]/ErrorResourceList.csv. 단일 실행에서 처리할 수 있는 최대 전화번호 수를 초과하여 처리할 수 없는 전화번호는에 업로드됩니다[automation:EXECUTION_ID]/NonProcessedResourceList.csv. 이 단계가 실패하면

DescribeCloudFormationErrorFromStackEvents 단계로 이동하여 AWS CloudFormation 스택 이벤트에서 실패한 이유를 표시합니다.

- WaitForPhoneNumberContactFlowAssociationCompletion

전화번호를 고객 응대 흐름에 매핑하는 AWS Lambda 함수가 생성되고 AWS CloudFormation 스택이 호출을 완료할 때까지 기다립니다.

- GenerateReport

고객 응대 흐름에 매핑된 전화번호 수, 오류로 인해 처리할 수 없는 전화번호 수, 단일 실행에서 처리할 수 있는 최대 전화번호 수를 초과하여 처리할 수 없는 전화번호 수를 포함하는 보고서를 생성합니다. 보고서에는 해당하는 [automation:EXECUTION_ID]/NonProcessedResourceList.csv 경우 [automation:EXECUTION_ID]/ErrorResourceList.csv 또는의 위치(Amazon S3 URI 및 Amazon S3 콘솔 URL)도 표시됩니다.

- DeleteCloudFormationStack

매핑을 위한 Lambda 함수를 포함하여 AWS CloudFormation 스택을 삭제합니다.

- DescribeCloudFormationErrorFromStackEvent

AssociatePhoneNumbersToContactFlows 단계 AWS CloudFormation 스택의 오류를 설명합니다.

7. 완료되면 출력 섹션에서 실행의 자세한 결과를 검토합니다.

- GenerateReport.OutputPayload

전화번호 및 고객 응대 흐름 연결의 출력입니다. 이 보고서에는 다음 정보가 포함되어 있습니다.

- 입력 CSV 파일에 나열된 전화번호 및 고객 응대 흐름 페어 수
- 입력 CSV 파일에 지정된 고객 응대 흐름과 연결된 전화번호 수
- 오류로 인해 고객 응대 흐름과 연결할 수 없는 전화번호 수
- 시간 제약으로 인해 고객 응대 흐름과 연결되지 않은 전화번호 수
- 오류로 인해 연결할 수 없는 전화번호 및 고객 응대 흐름 페어가 포함된 CSV 파일의 위치 (Amazon S3 URI 및 Amazon S3 콘솔 URL)
- 시간 제약으로 인해 연결되지 않은 전화번호 및 고객 응대 흐름 페어가 포함된 CSV 파일의 위치 (Amazon S3 URI 및 Amazon S3 콘솔 URL)
- DescribeCloudFormationErrorFromStackEvents.Events

AssociatePhoneNumbersToContactFlows 단계가 실패할 경우 AWS CloudFormation 스택 이벤트를 표시하는 출력입니다.

전화번호와 고객 응대 흐름이 적은 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
"}

```

오류 또는 시간 제약으로 인해 연결되지 않은 전화번호와 고객 응대 흐름 및 전화번호가 많은 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: 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 실행서는 특정 고객 응대 ID에 대한 Amazon Connect 고객 응대 흐름 로그를 수집하는 데 사용됩니다. 실행서는 Amazon Connect 인스턴스 ID와 연락처 ID를 제공하여 고객 응대 흐름 로그에서 Amazon CloudWatch 로그 그룹의 고객 응대를 검색하고 요청 파라미터에 지정된 Amazon Simple Storage Service(Amazon S3) 버킷에 업로드합니다. 실행서는 로그를 다운로드할 수 있도록 Amazon S3 콘솔 URL 및 AWS CLI 명령을 제공하는 출력을 생성합니다.

어떻게 작동하나요?

AWSSupport-CollectAmazonConnectContactFlowLog 자동화 실행서는 구성된 CloudWatch 로그 그룹에 저장된 특정 연락처 ID에 대한 Amazon Connect 고객 응대 흐름 로그를 수집하여 지정된 Amazon S3 버킷에 업로드하는 데 도움이 됩니다. Amazon Connect 고객 응대 흐름에서 수집된 로그의 보안을 지원하기 위해 자동화는 Amazon S3 버킷 구성을 평가하여 버킷이 퍼블릭 read 또는 write 액세스 권한을 부여하고 S3BucketOwnerAccountId 파라미터에 지정된 AWS 계정이 소유하는지 확인합니다. Amazon S3 버킷이 AWS Key Management Service 키를 사용한 서버 측 암호화(SSE-KMS)를 사용하는 경우 이 자동화를 실행하는 사용자 또는 AWS Identity and Access Management (IAM) 역할에 AWS KMS 키에 대한 kms:GenerateDataKey 권한이 있는지 확인합니다. Amazon Connect 인스턴스에서 생성된 로그에 대한 자세한 내용은 [Amazon CloudWatch 로그 그룹에 저장된 흐름 로그를](#) 참조하세요.

 Important

CloudWatch Logs Insights 쿼리에는 쿼리되는 데이터의 양에 따라 요금이 발생합니다. 프리 티어 고객은 서비스 할당량을 초과하는 사용에 대해서만 요금이 부과됩니다. 자세한 내용은 [Amazon CloudWatch 요금](#)을 참조하세요.

[이 자동화 실행\(콘솔\)](#)

문서 유형

자동화

소유자

Amazon

플랫폼

Linux, macOS, Windows

파라미터

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 Manager [AWSsupport-CollectAmazonConnectContactFlowLog](#)의 문서로 이동합니다.
2. Execute automation(자동화 실행)을 선택합니다.
3. 입력 파라미터에 다음을 입력합니다.

- AutomationAssumeRole(선택 사항):

Systems Manager Automation이 사용자를 대신하여 작업을 수행하도록 허용하는 (IAM) 역할의 Amazon 리소스 이름 AWS Identity and Access Management (ARN)입니다. 역할이 지정되지 않은 경우 Systems Manager Automation은 이 실행서를 시작하는 사용자의 권한을 사용합니다.

- ConnectInstanceId(필수):

Amazon Connect 인스턴스의 ID입니다.

- ContactId(필수):

고객 응대 흐름 로그를 수집하려는 고객 응대의 ID입니다.

- S3BucketName(필수):

고객 응대 흐름 로그를 업로드하려는 계정의 Amazon S3 버킷 이름입니다. 버킷 정책이 수집된 로그에 액세스할 필요가 없는 당사자에게 불필요한 읽기/쓰기 권한을 부여하지 않는지 확인합니다.

- S3ObjectPrefix(선택 사항):

업로드된 고객 응대 흐름 로그에 대한 Amazon S3 버킷의 Amazon S3 객체 경로입니다. 예를 들어 CollectedLogs를 지정하면 로그가 로 업로드됩니다 `s3://your-s3-bucket/CollectedLogs/ContactFlowLog_[ContactId][AWSAccountId].gz`. 이 파라미터를 지정하지 않으면 Systems Manager Automation 실행 ID가 사용됩니다. 예: `s3://your-s3-bucket/[automation:EXECUTION_ID]/ContactFlowLog[ContactId]_[AWSAccountId].gz`. 참고: 값을 지정 S3ObjectPrefix하고 동일한 [ContactId]를 사용하여 이 자동화를 실행하면 고객 응대 흐름 로그를 덮어씁니다.

- S3BucketOwnerAccount(선택 사항):

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

- S3BucketOwnerRoleArn(선택 사항):

Amazon S3 버킷 및 계정을 가져올 수 있는 권한이 있는 IAM 역할의 ARN은 퍼블릭 액세스 설정, 버킷 암호화 구성, 버킷 ACLs, 버킷 정책 상태를 차단하고 객체를 버킷에 업로드합니다. 이 파라미터를 지정하지 않으면 실행서는 이 실행서를 시작하는 AutomationAssumeRole (지정된 경우) 또는 사용자(지정되지 않은 경우) AutomationAssumeRole를 사용합니다. 실행서 설명의 필수 권한 섹션을 참조하세요.

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

4. 실행을 선택합니다.

5. 자동화가 시작됩니다.

6. 문서는 다음 단계를 수행합니다.

- CheckConnectInstanceExistence

에 제공된 Amazon Connect 인스턴스 ConnectInstanceId가 인지 확인합니다 ACTIVE.

- CheckS3BucketPublicStatus

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

- GenerateLogSearchTimeRange

DescribeContact API에서 LastUpdateTimestamp 반환한 StartTime 및를 기반으로 EndTime StartQuery 단계의 InitiationTimestamp 및를 생성합니다. StartTime는 1시간 전 InitiationTimestamp이고 EndTime는 1시간 후입니다 LastUpdateTimestamp.

- StartQuery

ContactId에 제공된 Amazon Connect 인스턴스와 연결된 CloudWatch Logs 로그 그룹에 제공된에 대한 쿼리 로그를 시작합니다ConnectInstanceId. 런타임 60분 후 쿼리 제한 시간이 초과되었습니다. 쿼리 시간이 초과되면 검색되는 시간 범위를 줄입니다. CloudWatch 콘솔에서 현재 진행 중인 쿼리와 최근 쿼리 기록을 볼 수 있습니다. 자세한 내용은 [실행 중인 쿼리 또는 쿼리 기록 보기를](#) 참조하세요.

- WaitForQueryCompletion

제공된가 완료될 때까지 CloudWatch Logs 쿼리 로그ContactId를 기다립니다. 쿼리는 런타임 60분 후에 시간 초과됩니다. 쿼리 시간이 초과되면 검색되는 시간 범위를 줄입니다. Amazon Connect 콘솔에서 현재 진행 중인 쿼리와 최근 쿼리 기록을 볼 수 있습니다. 자세한 내용은 [실행 중인 쿼리 또는 쿼리 기록 보기를](#) 참조하세요.

- UploadContactFlowLog

쿼리 결과를 가져오고 고객 응대 흐름 로그를에 지정된 Amazon S3 버킷에 업로드합니다S3BucketName.

- GenerateReport

고객 응대 흐름 로그가 업로드된 Amazon S3 콘솔 URL과 로그 파일을 다운로드하는 데 사용할 수 있는 CLI AWS 명령 예제를 반환합니다.

7. 완료되면 출력 섹션에서 실행의 자세한 결과를 검토합니다.

- GenerateReport.OutputPayload

실행서가 지정된 고객 응대에 대한 고객 응대 흐름 로그를 성공적으로 검색했음을 알려주는 출력입니다. 이 보고서에는 로그 파일을 다운로드할 수 있도록 Amazon S3 콘솔 URL과 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 자동화에는 대한 사전 정의된 실행서를 제공합니다 AWS Directory Service. 실행서에 대한 자세한 내용은 [실행서 작업](#)을 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: 인스턴스를 시작하는 데 사용할 (선택 사항) Amazon Machine Image (AMI) ID입니다. 기본적으로 인스턴스는 최신 Microsoft Windows Server 2019 기본 AMI로 시작됩니다.

- DirectoryId

유형: 문자열

설명: (필수) 디렉터리의 Directory Service 디렉터리 ID입니다.

- IamInstanceProfileName

유형: 문자열

설명: (선택 사항) IAM 인스턴스 프로파일 이름입니다. 기본적으로 이름이 AmazonSSMDirectoryServiceInstanceProfileRole인 인스턴스 프로파일이 없는 경우 이름이 AmazonSSMDirectoryServiceInstanceProfileRole인 인스턴스 프로파일이 생성됩니다.

기본값: AmazonSSMDirectoryServiceInstanceProfileRole

- 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: (선택 사항) 시작할 인스턴스의 유형입니다. 기본값은 t3.medium입니다.

- KeyPairName

유형: 문자열

설명: (선택 사항) 인스턴스를 시작할 때 사용할 키 페어입니다. Windows는 ED25519 키 페어를 지원하지 않습니다. 기본적으로 인스턴스는 키 페어(NoKeyPair) 없이 시작됩니다.

기본값: NoKeyPair

- RemoteAccessCidr

유형: 문자열

설명: (선택 사항) CIDR에서 지정한 IPs에 개방된 RDP용 포트(포트 범위 3389)가 있는 보안 그룹을 생성합니다(기본값은 0.0.0.0/0). 보안 그룹이 이미 존재하는 경우, 해당 보안 그룹이 수정되지 않으며 규칙이 변경되지 않습니다.

기본값: 0.0.0.0/0

- SecurityGroupName

유형: 문자열

설명: (선택 사항) 보안 그룹 이름입니다. 기본적으로 이름이 AmazonSSMDirectoryServiceSecurityGroup인 보안 그룹이 없는 경우 이름이 AmazonSSMDirectoryServiceSecurityGroup인 보안 그룹이 생성됩니다.

기본값: AmazonSSMDirectoryServiceSecurityGroup

- Tags

유형: MapList

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

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

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 시작된 인스턴스를 디렉터리에 조인하는 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 및 Amazon CloudWatch 인터페이스 VPC 엔드포인트가 AD 커넥터와 동일한 Virtual Private Cloud(VPC)에 존재하는지 확인합니다.

사전 요구 사항 검사가 성공적으로 완료되면, 실행서는 AD Connector와 동일한 서브넷에서 두 개의 Amazon Elastic Compute Cloud(Amazon EC2) Linux t2.micro 인스턴스를 시작합니다. 그런 다음, netcat 및 nslookup 유틸리티를 사용하여 네트워크 연결 테스트를 수행합니다.

[이 자동화 실행\(콘솔\)](#)

Important

이 실행서를 사용하면 자동화 중에 생성된 Amazon EC2 인스턴스, Amazon Elastic Block Store 볼륨 및 Amazon Machine Image (AMI)에 AWS 계정 대해에 추가 요금이 발생할 수 있습니다.

니다. 자세한 내용은 [Amazon Elastic Compute Cloud 요금](#) 및 [Amazon Elastic Block Store 요금](#)을 참조하세요.

aws:deletestack 단계가 실패하면 AWS CloudFormation 콘솔로 이동하여 스택을 수동으로 삭제합니다. 이 실행서에서 만든 스택 이름은 AWSSupport-TroubleshootADConnectorConnectivity로 시작합니다. CloudFormation 스택 삭제에 대한 자세한 내용은 AWS CloudFormation 사용 설명서의 [스택 삭제](#)를 참조하세요.

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

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

- Ec2InstanceProfile

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 IAM 권한

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 AWS Security Token Service 및 Amazon CloudWatch 인터페이스 엔드포인트가 AD 커넥터와 동일한 VPC에 존재하는지 확인합니다.
- `aws:executeScript` - 이전 단계에서 수행한 검사의 출력을 컴파일합니다.
- `aws:branch` - 이전 단계의 출력에 따라 자동화를 분기합니다. 보안 그룹 및 네트워크 ACL에 필요한 아웃바운드 및 인바운드 규칙이 누락된 경우 여기서 자동화가 중지됩니다.
- `aws:createStack` - Amazon EC2 인스턴스를 시작하여 연결 테스트를 수행할 CloudFormation 스택을 생성합니다.
- `aws:executeAwsApi` - 새로 시작한 Amazon EC2 인스턴스의 ID를 수집합니다.
- `aws:waitForAwsResourceProperty` - 새로 시작한 첫 번째 Amazon EC2 인스턴스를 AWS Systems Manager가 관리하는 것으로 보고될 때까지 기다립니다.
- `aws:waitForAwsResourceProperty` - 새로 시작한 두 번째 Amazon EC2 인스턴스를 AWS Systems Manager가 관리하는 것으로 보고될 때까지 기다립니다.
- `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` - CloudFormation 스택을 삭제합니다.
- `aws:executeScript` - 자동화가 CloudFormation 스택을 삭제하지 못하는 경우 스택을 수동으로 삭제하는 방법에 대한 지침을 출력합니다.

AWSSupport-TroubleshootDirectoryTrust

설명

AWSSupport-TroubleshootDirectoryTrust 실행서는 AWS Managed Microsoft AD 와 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 ID AWS Managed Microsoft AD 입니다.

- RemoteDomainCidrs

유형: 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)의 기본 포트 요구 사항입니다 AWS Managed Microsoft AD. 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)의 기본 포트 요구 사항입니다 AWS Managed Microsoft AD. 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:executeAwsApi -에 대한 정보를 가져옵니다 AWS Managed Microsoft AD.
- aws:branch - TrustId 입력 파라미터에 값이 제공된 경우 자동화를 분기합니다.
- aws:executeAwsApi - 신뢰 관계에 대한 정보를 가져옵니다.
- aws:executeAwsApi - RemoteDomainName에 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 CIDRs을 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. AWS Managed Microsoft AD 에에 대한 조건부 전달자가 있고 RemoteDomainCidrs가 비 RFC 1918 IP 주소인 AWS Managed Microsoft AD 경우 필수 IP 경로RemoteDomainCidrs가에 추가되었는지 확인합니다.
- aws:executeScript - 보안 그룹 규칙을 평가합니다.
- aws:executeScript - 네트워크 ACL을 평가합니다.

출력

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

evalAclEntries.output -와 연결된 네트워크 ACLs이 신뢰 생성에 필요한 트래픽을 AWS Managed Microsoft AD 허용하는지 여부를 평가한 결과입니다.

evaluateRemoteDomainCidr.output - RemoteDomainCidrs가 유효한 값인지 평가한 결과입니다. 에 AWS Managed Microsoft AD 에 대한 조건부 전달자가 있고 RemoteDomainCidrs가 비 RFC 1918 IP 주소인 AWS Managed Microsoft AD 경우 필수 IP 경로RemoteDomainCidrs가에 추가되었는지 확인합니다.

AWS AppSync

AWS Systems Manager 자동화하는에 대한 사전 정의된 실행서를 제공합니다 AWS AppSync. 실행서에 대한 자세한 내용은 [실행서 작업](#)을 참조하세요. 실행서 콘텐츠를 보는 방법에 대한 자세한 내용은 [실행서 콘텐츠 보기](#)(을)를 참조하세요.

주제

- [AWS-EnableAppSyncGraphQLApiLogging](#)

AWS-EnableAppSyncGraphQLApiLogging

설명

AWS-EnableAppSyncGraphQLApiLogging 실행서는 지정한 AWS AppSync GraphQL API에 대한 필드 수준 로깅 및 요청 수준 로깅을 활성화합니다. 로깅이 이미 활성화된 경우에도 실행서는 지정된 GraphQL API에 변경 사항을 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.

- ApId

유형: 문자열

설명: (필수) 로깅을 활성화하려는 API의 ID입니다.

- FieldLogLevel

유형: 문자열

유효한 값: ERROR | ALL

설명: (필수) 필드 로깅 수준입니다.

- CloudWatchLogsRoleArn

유형: 문자열

설명: (필수)가 Amazon CloudWatch Logs에 게시하도록 AWS AppSync 수입하는 서비스 역할의 ARN입니다.

- ExcludeVerboseContent

유형: 부울

기본값: False

설명: (선택 사항) 로깅 수준에 관계없이 헤더, 컨텍스트 및 평가된 매핑 템플릿과 같은 정보를 제외True하려면 로 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 분기합니다.
- aws:executeAwsApi - 실행서의 입력 파라미터에 지정된 값을 기반으로 AWS AppSync GraphQL API의 로깅 구성을 업데이트합니다.

출력

- EnableApiLoggingWithApiKeyOrAwsIamAuthorization.UpdateGraphQLApiResponse: UpdateGraphQLApi 호출의 응답입니다.
- EnableApiLoggingWithLambdaAuthorization.UpdateGraphQLApiResponse: UpdateGraphQLApi 호출의 응답입니다.
- EnableApiLoggingWithCognitoAuth.UpdateGraphQLApiResponse: UpdateGraphQLApi 호출의 응답입니다.
- EnableApiLoggingWithOpenIdAuthorization.UpdateGraphQLApiResponse: UpdateGraphQLApi 호출의 응답입니다.

Amazon Athena

AWS Systems Manager Automation은 Amazon Athena용 사전 정의된 실행서를 제공합니다. 실행서에 대한 자세한 내용은 [실행서 작업](#)을 참조하세요. 실행서 콘텐츠를 보는 방법에 대한 자세한 내용은 [실행서 콘텐츠 보기](#)(을)를 참조하세요.

주제

- [AWS-EnableAthenaWorkGroupEncryptionAtRest](#)

AWS-EnableAthenaWorkGroupEncryptionAtRest

설명

AWS-EnableAthenaWorkGroupEncryptionAtRest 실행서는 지정한 Amazon Athena 작업 그룹에 대해 저장 시 암호화를 활성화합니다.

[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.

- WorkGroup

유형: 문자열

설명: (필수) 저장 시 암호화를 활성화하려는 작업 그룹입니다.

- EncryptionOption

유형: 문자열

유효한 값: SSE_S3 | SSE_KMS | CSE_KMS

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

- KmsKeyId

유형: 문자열

설명: (선택 사항) AWS KMS 암호화 옵션을 사용하는 경우 사용하려는 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 작업 그룹에 최소 수준의 암호화를 적용합니다. 활성화하면 작업 그룹 사용자는 쿼리를 제출할 때 관리자가 설정한 최소 수준 이상으로만 암호화를 설정할 수 있습니다. 이 설정은 Spark 지원 작업 그룹에는 적용되지 않습니다.

- EnforceWorkGroupConfiguration

유형: 부울

기본값: True

설명: (선택 사항) 로 설정하면 작업 그룹의 True설정이 클라이언트 측 설정을 재정의합니다. 로 설정하면 False클라이언트 측 설정이 사용됩니다.

필수 IAM 권한

실행서를 성공적으로 사용하려면 AutomationAssumeRole 파라미터에 다음 작업이 필요합니다.

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

문서 단계

- aws:branch - EncryptionOption 파라미터에 지정된 암호화 옵션을 기반으로 분기합니다.
- aws:executeAwsApi -이 단계에서는 Athena 작업 그룹을 지정된 암호화 설정으로 업데이트합니다.
- aws:executeAwsApi - 지정된 암호화 설정으로 Athena 작업 그룹을 업데이트합니다.
- aws:assertAwsResourceProperty - 작업 그룹에 대한 암호화가 활성화되었는지 확인합니다.

DynamoDB

AWS Systems Manager 자동화는 Amazon DynamoDB용 사전 정의된 실행서를 제공합니다. 실행서에 대한 자세한 내용은 [실행서 작업](#)을 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 실행서는 하나 이상의 Amazon DynamoDB(DynamoDB) 테이블의 읽기/쓰기 용량 모드를 온디맨드 모드 또는 프로비저닝 모드로 변경합니다.

[이 자동화 실행\(콘솔\)](#)

문서 유형

자동화

소유자

Amazon

플랫폼

데이터베이스 수

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.

- CapacityMode

유형: 문자열

유효한 값: PROVISIONED | PAY_PER_REQUEST

설명: (필수) 원하는 읽기/쓰기 용량 모드입니다. 온디맨드(pay-per-request)에서 프로비저닝된 용량으로 전환할 때는 초기 프로비저닝된 용량 값을 설정해야 합니다. 초기 프로비저닝된 용량 값은 지난 30분 동안 테이블 및 글로벌 보조 인덱스의 소비된 읽기 및 쓰기 용량을 기반으로 추정됩니다.

- ReadCapacityUnits

유형: 정수

기본값: 0

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

- TableNames

유형: 문자열

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

- WriteCapacityUnits

유형: 정수

기본값: 0

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

필수 IAM 권한

실행서를 성공적으로 사용하려면 AutomationAssumeRole 파라미터에 다음 작업이 필요합니다.

- dynamodb:DescribeTable
- dynamodb:UpdateTable

문서 단계

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

출력

ChangeDDBRWCapacityMode.SuccessesTables - 용량 모드가 성공적으로 변경된 DynamoDB 테이블 이름 목록

ChangeDDBRWCapacityMode.FailedTables - 용량 모드 변경이 실패한 DynamoDB 테이블 이름의 맵 리스트와 실패 이유.

AWS-CreateDynamoDBBackup

설명

Amazon DynamoDB 테이블의 백업본을 생성합니다.

[이 자동화 실행\(콘솔\)](#)

문서 유형

자동화

소유자

Amazon

플랫폼

데이터베이스 수

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 수

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.

- 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 수

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 수

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 실행서는 KMSKeyId 파라미터에 지정한 AWS Key Management Service () 고객 관리형 키를 사용하여 Amazon DynamoDB(DynamoDB AWS KMS) 테이블을 암호화합니다.

[이 자동화 실행\(콘솔\)](#)

문서 유형

자동화

소유자

Amazon

플랫폼

데이터베이스 수

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) TableName 파라미터에 지정하는 DynamoDB 테이블을 암호화하는 데 사용할 고객 관리형 키에 대한 ARN입니다.

- TableName

유형: 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 SSESpecification에 대한 Enabled 속성이 true로 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 수

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 실행서는 지정한 프로비저닝된 용량 Amazon DynamoDB 테이블에 대해 Application Auto Scaling을 활성화합니다. Application Auto Scaling은 트래픽 패턴에 따라 프로비저닝된 처리량 용량을 동적으로 조정합니다. 자세한 내용은 Amazon [DynamoDB 개발자 안내서의 DynamoDB Auto Scaling을 사용하여 처리량 용량 자동 관리](#)를 참조하세요. DynamoDB

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.

- TableName

유형: 문자열

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

- MinReadCapacity

유형: 정수

설명: (필수) DynamoDB 테이블의 프로비저닝된 처리량 읽기 용량 단위의 최소 수입니다.

- MaxReadCapacity

유형: 정수

설명: (필수) DynamoDB 테이블의 프로비저닝된 처리량 읽기 용량 단위의 최대 수입니다.

- TargetReadCapacityUtilization

유형: 정수

설명: (필수) 원하는 목표 읽기 용량 사용률입니다. 대상 사용률은 특정 시점에서 사용된 프로비저닝된 처리량의 백분율입니다. Auto Scaling 대상 사용률 값을 20~90%로 설정할 수 있습니다.

- ReadScaleOutCooldown

유형: 정수

설명: (필수) 이전 읽기 용량 스케일 아웃 활동이 적용될 때까지 초 단위로 대기하는 시간입니다.

- ReadScaleInCooldown

유형: 정수

설명: (필수) 읽기 용량 축소 활동이 완료된 후 다른 축소 활동이 시작되기까지의 초 단위 시간입니다.

- MinWriteCapacity

유형: 정수

설명: (필수) DynamoDB 테이블의 프로비저닝된 처리량 쓰기 단위의 최소 수입니다.

- MaxWriteCapacity

유형: 정수

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

- TargetWriteCapacityUtilization

유형: 정수

설명: (필수) 원하는 대상 쓰기 용량 사용률입니다. 대상 사용률은 특정 시점에서 사용된 프로비저닝된 처리량의 백분율입니다. Auto Scaling 대상 사용률 값을 20~90%로 설정할 수 있습니다.

- WriteScaleOutCooldown

유형: 정수

설명: (필수) 이전 쓰기 용량 스케일 아웃 활동이 적용될 때까지 초 단위로 대기하는 시간입니다.

- WriteScaleInCooldown

유형: 정수

설명: (필수) 쓰기 용량 축소 활동이 완료된 후 다른 축소 활동이 시작되기까지의 초 단위 시간입니다.

필수 IAM 권한

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) - API 제한을 방지하기 위해 대기합니다.
- PutScalingPolicyWrite(aws:executeAwsApi) - DynamoDB 테이블의 대상 쓰기 용량 사용률을 구성합니다.
- PutScalingPolicyWriteDelay(aws:sleep) - API 제한을 방지하기 위해 대기합니다.
- RegisterAppAutoscalingTargetRead(aws:executeAwsApi) - DynamoDB 테이블의 최소 및 최대 읽기 용량 단위를 구성합니다.
- RegisterAppAutoscalingTargetReadDelay(aws:sleep) - API 제한을 방지하기 위해 대기합니다.
- PutScalingPolicyRead(aws:executeAwsApi) - DynamoDB 테이블의 대상 읽기 용량 사용률을 구성합니다.
- VerifyDynamoDbAutoscalingEnabled(aws:executeScript) - 지정한 값에 따라 DynamoDB 테이블에 대해 Application Auto Scaling이 활성화되어 있는지 확인합니다.

출력

- RegisterAppAutoscalingTargetWrite.Response
- PutScalingPolicyWrite.Response
- RegisterAppAutoscalingTargetRead.Response
- PutScalingPolicyRead.Response
- 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 수

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 시점에서의 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.

AWS Database Migration Service

AWS Systems Manager 자동화에는 대한 사전 정의된 실행서를 제공합니다 AWS Database Migration Service. 실행서에 대한 자세한 내용은 [실행서 작업](#)을 참조하세요. 실행서 콘텐츠를 보는 방법에 대한 자세한 내용은 [실행서 콘텐츠 보기](#)(을)를 참조하세요.

주제

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

AWSSupport-TroubleshootDMSTableErrors

설명

AWS Systems Manager AWSSupport-TroubleshootDMSTableErrors 자동화 실행서는 데이터베이스 마이그레이션 작업 또는 서버리스 복제에서 Table errors 찾을 수 있는 문제 해결 프로세스를 자동화하는 데 도움이 됩니다 AWS Database Migration Service. 이러한 오류는 AWS DMS 서비스에서 생성

된 데이터베이스 마이그레이션 작업 또는 서버리스 복제를 통해 테이블이 소스 엔드포인트(소스 데이터베이스)에서 대상 엔드포인트(대상 데이터베이스)로 마이그레이션되지 않을 때 발생합니다. 이 실행서는 CloudWatch 로그의 서명 오류 메시지를 분석합니다. 특히 기존 데이터베이스 마이그레이션 작업의 작업 로그와 서버리스 복제의 서버리스 로그에 중점을 둡니다. 또한 AWS DMS 마이그레이션 Table error 중에에서 발생하는 일반적인 오류 메시지에 대한 대상 제안 및 수정 단계를 제공합니다.

어떻게 작동하나요?

실행서는 다음 단계를 수행합니다.

- 데이터베이스 마이그레이션 작업 또는 서버리스 복제일 수 있는 제공된 AWS DMS ARN에 대한 정보를 가져옵니다.
- DescribeReplicationTasks API(데이터베이스 마이그레이션 작업의 경우) 및 DescribeReplications API(서버리스 복제의 경우) 응답의 FreshStartDate 값을 확인하여 제공된 AWS DMS 리소스가 한 번 이상 시작되었는지 확인합니다. 리소스가 시작되지 않은 경우 자동화에 오류가 발생합니다.
- 리소스가 시작된 경우 자동화는 TableStatistics 정보를 사용하여 TableError 상태의 테이블을 확인합니다. 오류가 발견되지 않으면 자동화는 지정된 데이터베이스 마이그레이션 작업 또는 서버리스 복제에서 테이블 오류가 발견되지 않았음을 확인하는 메시지를 표시한 후 워크플로를 종료합니다.
- TableError 상태의 테이블이 발견되면 자동화는 지정된 AWS DMS 리소스에 대해 CloudWatch 로깅이 활성화되어 있는지 확인합니다. 로깅이 활성화되지 않은 경우 로깅이 활성화되지 않았음을 나타내는 메시지가 표시된 후 자동화가 워크플로를 종료합니다.

참고: 자동화는 이러한 로그를 사용하여 TableError 상태의 테이블 문제를 분석하고 식별하기 때문에 CloudWatch 로깅이 활성화될 것으로 예상됩니다.

- 로깅이 활성화된 경우 자동화는 CloudWatch 로그를 분석하고 TableError 상태인 각 테이블에 대한 보고서를 생성합니다. 보고서에는 일반적인 오류 메시지에 대한 제안이 포함되어 있으며 소스 엔드포인트에서 AWS DMS 대상 엔드포인트로의 성공적인 테이블 마이그레이션을 방해하는 문제를 식별하고 해결하는 데 도움이 되는 관련 오류 로그를 AWS DMS 제공합니다.

[이 자동화 실행\(콘솔\)](#)

문서 유형

자동화

소유자

Amazon

플랫폼

/

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.

- DMSArn

유형: 문자열

설명: (필수) 데이터베이스 마이그레이션 작업 또는 서버리스 복제의 ARN

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

- StartTimeRange

유형: 문자열

설명: (선택 사항)이 파라미터는 지정된 데이터베이스 마이그레이션 작업 또는 서버리스 복제에 대한 CloudWatch 로그 분석의 시간 범위 시작을 정의합니다. 제공된 경우이 특정 시간부터 생성된 로그만 수집 및 분석됩니다. startDate와 사이의 시간 범위가 endDate 너무 길면 워크플로가 시간 초과될 수 있습니다. 값은 ISO 6081 날짜/시간 형식으로 제공해야 합니다.

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

- EndTimeRange

유형: 문자열

설명: (선택 사항)이 파라미터는 지정된 데이터베이스 마이그레이션 작업 또는 서버리스 복제에 대한 CloudWatch 로그 분석의 시간 범위 종료를 설정합니다. 제공된 경우이 특정 시간까지 생성된 로그

만 수집 및 분석됩니다. startDate와 사이의 시간 범위가 endDate 너무 길면 워크플로가 시간 초과될 수 있습니다. 값은 ISO 6081 날짜/시간 형식으로 제공해야 합니다.

허용된 패턴: `^\d{4}-(\d{2})-(\d{2})T(\d{2}):(\d{2}):(\d{2})\.\d{3}Z$`

필수 IAM 권한

실행서를 성공적으로 사용하려면 AutomationAssumeRole 파라미터에 다음 작업이 필요합니다.

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

자동화 수임 역할에 대한 IAM 정책 예시

JSON

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

```

        "Resource": "*"
    }
}

```

지침

다음 단계에 따라 자동화를 구성합니다.

1. Systems Manager [AWSSupport-TroubleshootDMSTableErrors](#)의 문서로 이동합니다.

2. Execute automation(자동화 실행)을 선택합니다.

3. 입력 파라미터에 다음을 입력합니다.

- AutomationAssumeRole(선택 사항):

Systems Manager Automation이 사용자를 대신하여 작업을 수행하도록 허용하는 (IAM) 역할의 Amazon 리소스 이름 AWS AWS Identity and Access Management (ARN)입니다. 역할이 지정되지 않은 경우 Systems Manager Automation은 이 실행서를 시작하는 사용자의 권한을 사용합니다.

- DMSArn

테이블 오류가 있는 데이터베이스 마이그레이션 작업 또는 서버리스 복제의 ARN입니다.

- StartTimeRange

(선택 사항) 지정된 데이터베이스 마이그레이션 작업 또는 서버리스 복제의 CloudWatch 로그를 분석하기 위한 시간 범위의 시작을 정의하는 ISO 6081 날짜 시간 형식입니다.

- EndTimeRange

(선택 사항) 지정된 데이터베이스 마이그레이션 작업 또는 서버리스 복제의 CloudWatch 로그를 분석하기 위한 시간 범위의 끝을 정의하는 ISO 6081 날짜 시간 형식입니다.

4. 페이지 하단에서 실행 버튼을 선택합니다.

5. 자동화가 시작됩니다.

6. 문서는 다음 단계를 수행합니다.

- validateDMSInputTypeAndGatherDetails

지정된 AWS DMS ARN 입력을 검증하고 다음 단계에서 필요한 데이터베이스 마이그레이션 작업 또는 서버리스 복제의 기본 세부 정보를 수집합니다.

- branchOnTableErrors

위 단계에서 발견된 테이블 오류 수를 기준으로 워크플로를 분기합니다. 개수가 0보다 크면 - branchOnCWLoggingStatus 단계로 진행합니다. 그렇지 않으면 - outputNoTableErrors 단계로 진행합니다.

- outputNoTableErrors

지정된 데이터베이스 마이그레이션 작업 또는 서버리스 복제에서 테이블 오류를 찾을 수 없다는 메시지를 출력합니다.

- branchOnCWLoggingStatus

위 단계에서 찾은 CloudWatch 로깅 상태를 기반으로 워크플로를 분기합니다. 활성화된 경우 - gatherTableDetails 단계로 진행합니다. 그렇지 않으면 - outputNoCWLoggingEnabled 단계로 진행합니다.

- outputNoCWLoggingEnabled

지정된 데이터베이스 마이그레이션 작업 또는 서버리스 복제에서 CloudWatch 로깅이 활성화되지 않았다는 메시지를 출력합니다.

- gatherTableDetails

실패한 테이블의 FullLoadEndTime 타임스탬프를 수집하고 시간 범위 값을 계산하여 CloudWatch 로그를 분석합니다.

- analyzeCloudWatchLogs

서명 오류 메시지를 기반으로 CloudWatch 로그 그룹에서 찾은 로그를 분석하고 사용자에게 보고서를 반환합니다.

7. 실행이 완료되면 출력 섹션에서 실행의 자세한 결과를 검토합니다.

- 테이블 없음 오류 출력

제공된 데이터베이스 마이그레이션 작업 또는 서버리스 복제에서 테이블 오류를 찾을 수 없는 경우 자동화는 동일한 출력을 표시합니다.

- CloudWatch 로그인이 활성화되지 않음의 출력

제공된 데이터베이스 마이그레이션 작업 또는 서버리스 복제에서 CloudWatch 로깅이 활성화되지 않은 경우 자동화는 동일한 출력을 표시하고 로깅을 활성화하는 단계를 제공합니다.

- 로그 분석 보고서

제공된 데이터베이스 마이그레이션 작업 또는 서버리스 복제에서 Table error 상태의 테이블을 식별하고, 오류 유형을 구분하고, 발생한 오류 메시지를 나열하고, 식별된 각 테이블에 대해 대상 수정 단계 및 제안을 제공하는 보고서를 출력합니다.

참조

Systems Manager Automation

- [이 자동화 실행\(콘솔\)](#)
- [자동화 실행](#)
- [Automation 설정](#)
- [Support Automation Workflows 랜딩 페이지](#)

AWSSupport-TroubleshootDMSEndpointConnection

설명

AWSSupport-TroubleshootDMSEndpointConnection 실행서는 AWS Database Migration Service 복제 인스턴스와 AWS DMS 엔드포인트 간의 연결 문제를 진단하고 해결하는 데 도움이 됩니다. 자동화는 [Reachability Analyzer](#) 검사를 사용하여 네트워크 연결을 테스트하고 네트워크 구성을 분석하여 성공적인 AWS DMS 마이그레이션을 방해할 수 있는 잠재적 연결 문제를 식별합니다.

Important

이 실행서를 실행하기 전에 AWS DMS 콘솔 또는 API를 사용하여 AWS DMS 복제 인스턴스와 엔드포인트 간의 연결을 테스트해야 합니다. 연결을 테스트하지 않은 경우 먼저 테스트하십시오. 그렇지 않으면 이 실행서를 다시 실행해야 할 수 있습니다. 정확한 연결 테스트를 위해 AWS DMS 복제 인스턴스와 엔드포인트 모두 사용 가능한 상태여야 합니다.

Important

이 실행서는 Lambda 요금이 발생하는 AWS Lambda 함수를 생성하고 호출합니다. 또한 각 Reachability Analyzer 분석 실행에는 요금이 발생합니다. 요금 세부 정보는 네트워크 분석 탭의 [Amazon VPC 요금](#) 페이지 및 [AWS Lambda 요금](#)을 참조하세요.

어떻게 작동하나요?

실행서는 다음 단계를 통해 AWS DMS 연결에 대한 체계적인 분석을 수행합니다.

1단계: 리소스 검증 및 사전 조건

- **엔드포인트 검증:** AWS DMS 엔드포인트가 있는지 확인하고, 구성(서버 이름, 포트, 엔진 유형)을 검색하고, 데이터베이스 엔진이 문제 해결에 지원되는지 확인합니다.
- **연결 테스트 상태:** 이전 테스트 시도의 실패 메시지를 포함하여 API를 AWS DMS DescribeConnections 사용하여 복제 인스턴스와 엔드포인트 간의 현재 연결 테스트 상태를 검색합니다.
- **복제 인스턴스 분석:** Amazon VPC ID, 서브넷 ID, 보안 그룹 IDs를 포함한 네트워크 구성 세부 정보를 수집하고 복제 인스턴스에 연결된 탄력적 네트워크 인터페이스(ENI)를 식별합니다.

2단계: DNS 확인 및 네트워크 경로 검색

- **Amazon VPC 기반 DNS 확인:** 복제 인스턴스와 동일한 Amazon VPC 내에 임시 Lambda 함수를 생성하여 Amazon VPC 컨텍스트 내에서 엔드포인트 호스트 이름을 IP 주소로 확인함으로써 정확한 프라이빗 DNS 확인을 보장합니다.
- **대상 식별:** 엔드포인트가 동일한 Amazon VPC 내에 있는지(ENI 사용) 아니면 외부에 있는지(해결된 IP 주소 사용)를 기반으로 Reachability Analyzer에 적합한 대상을 결정합니다.
- **IPv6 호환성 검사:** Reachability Analyzer는 IPv6 주소를 지원하지 않으므로 확인된 주소가 IPv4인지 확인합니다. IPv6

3단계: 포괄적인 네트워크 경로 분석

- **Reachability Analyzer 실행:** 복제 인스턴스 ENI에서 대상(엔드포인트 ENI 또는 IP 주소)으로의 Network Insights 경로를 생성하고 포괄적인 분석을 실행하여 지정된 포트에서 TCP 연결을 테스트합니다.
- **다중 계층 네트워크 분석:** 라우팅 테이블, 보안 그룹, 네트워크 ACLs, 인터넷 게이트웨이, NAT 게이트웨이, Amazon VPC 피어링 연결 및 전송 게이트웨이를 포함한 전체 네트워크 경로를 검사하여 연결 장벽을 식별합니다.
- **세부 설명 생성:** 연결 실패의 경우 정확한 규칙 번호, CIDR 블록, 포트 범위 및 프로토콜 제한을 포함하여 트래픽을 차단하는 각 네트워크 구성 요소에 대한 구체적인 설명을 제공합니다.

4단계: 보고서 생성 및 리소스 정리

- 포괄적인 보고: 연결 테스트 요약, 네트워크 경로 분석 결과 및 문제 해결 지침이 포함된 특정 장애 설명이 포함된 세부 보고서를 생성합니다.
- 리소스 관리: PersistReachabilityAnalyzerResults 파라미터가 추가 조사를 위해 분석 결과를 유지하도록 설정되지 않은 한 생성된 리소스(Lambda 함수, IAM 역할, Network Insights 경로)를 자동으로 정리합니다.
- 오류 처리: 지원되지 않는 데이터베이스 엔진, 리소스 누락, DNS 해결 실패, 권한 문제 등 다양한 장애 시나리오에 대한 특정 오류 보고서를 제공합니다.

실행서는 Amazon Aurora, Amazon DocumentDB, Amazon DynamoDB, Amazon Neptune, Amazon Redshift, Amazon S3, Azure SQL Database, DB2, MySQL, Oracle, PostgreSQL, SQL Server 등을 비롯한 여러 데이터베이스 엔진의 연결 문제 해결을 지원합니다.

[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`
- `cloudformation:DescribeStacks`
- `cloudformation:DescribeStackEvents`
- `dms:DescribeEndpoints`
- `dms:DescribeReplicationInstances`
- `dms:DescribeConnections`
- `iam:GetRole`
- `iam:PassRole`

- iam:SimulatePrincipalPolicy
- lambda:CreateFunction
- lambda>DeleteFunction
- lambda:GetFunction
- lambda:InvokeFunction
- lambda:ListTags
- lambda:TagResource
- lambda:UntagResource
- lambda:UpdateFunctionCode

선택적 IAM 권한

다음 권한은 LambdaRoleArn 파라미터를 제공하지 않고 자동화가 Lambda 실행 역할을 생성하도록 하려는 AutomationAssumeRole 경우에만 내에서 필요합니다.

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

Important

위에서 언급한 작업 외에도 [Reachability Analyzer](#) 테스트가 성공적으로 수행되도록에는 [AmazonVPCReachabilityAnalyzerFullAccessPolicy](#)가 [연결된 관리형 정책](#)으로 AutomationAssumeRole 있어야 합니다.

예제 정책:

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

```

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

```

```

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

```

지침

다음 단계에 따라 자동화를 구성합니다.

1. Systems Manager [AWSSupport-TroubleshootDMSEndpointConnection](#)의 문서로 이동합니다.
2. Execute automation(자동화 실행)을 선택합니다.
3. 입력 파라미터에 다음을 입력합니다.
 - AutomationAssumeRole(선택 사항):
 - 설명: (선택 사항) SSM Automation이 사용자를 대신하여 작업을 수행하도록 허용하는 (IAM) 역할의 AWS Identity and Access Management Amazon 리소스 이름(ARN)입니다. 역할이 지정되지 않은 경우 SSM Automation은 이 실행서를 시작하는 사용자의 권한을 사용합니다.
 - 유형: AWS::IAM::Role::Arn
 - DmsEndpointArn(필수)

- 설명: (필수) AWS Database Migration Service 엔드포인트의 Amazon 리소스 이름(ARN)입니다.
- 유형: String
- 허용된 패턴: `^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):dms:[a-z0-9-]+:\d{12}:endpoint:[A-Z0-9]{1,48}$`
- DmsReplicationInstanceArn(필수)
 - 설명: (필수) AWS Database Migration Service 복제 인스턴스의 Amazon 리소스 이름(ARN)입니다.
 - 유형: String
 - 허용된 패턴: `^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):dms:[a-z0-9-]+:\d{12}:rep:[A-Z0-9]+$`
- PersistReachabilityAnalyzerResults(선택 사항)
 - 설명: (선택 사항) Network Insights 분석 실행 결과를 유지해야 하는지 여부를 알리는 플래그입니다.
 - 유형: Boolean
 - 허용된 값: `[true, false]`
 - 기본값: `false`
- LambdaRoleArn(선택 사항)
 - 설명: (선택 사항) AWS Lambda 함수가 필요한 AWS 서비스 및 리소스에 액세스할 수 있도록 허용하는 (IAM) 역할의 Amazon 리소스 이름 AWS AWS Identity and Access Management (ARN)입니다. 역할이 지정되지 않은 경우 Systems Manager Automation은 계정에서 Lambda에 대한 하나의 IAM 역할을 생성합니다.
 - 유형: `AWS::IAM::Role::Arn`
 - 기본값: `""`
- 확인(필수)
 - 설명: (필수) `yes`를 입력하여이 실행서가 계정에 Lambda 함수를 생성하고 LambdaRoleArn가 제공되지 않으면 IAM 역할을 생성함을 확인합니다.
 - 유형: String
 - 허용된 패턴: `^[Yy][Ee][Ss]$`

4. 실행을 선택합니다.

5. 자동화가 시작됩니다.

6. 문서는 다음 단계를 수행합니다.

- DescribeEndpointAndCheckEngine:

AWS DMS 엔드포인트 구성을 검색하고 데이터베이스 엔진 유형이 문제 해결에 지원되는지 확인합니다. 엔드포인트 구성에서 서버 이름, 포트 및 엔진 유형을 추출합니다.

- BranchOnEndpointAndCheckEngineErrors:

엔드포인트 검증의 오류를 기반으로 자동화를 분기합니다. 오류가 발견되면 자동화는 오류 보고서를 생성합니다. 그렇지 않으면 연결 테스트를 계속합니다.

- GetTestConnectionStatus:

DescribeConnections API를 사용하여 AWS DMS 엔드포인트의 연결 상태 및 오류 메시지를 검색합니다. 이 단계에서는 연결 테스트가 수행되었는지 확인하고 실패 메시지를 캡처합니다.

- BranchOnTestConnectionStatusErrors:

연결 테스트 상태 오류를 기반으로 자동화를 분기합니다. 오류가 감지되면 자동화는 오류 보고서를 생성하고, 그렇지 않으면 복제 인스턴스 분석을 진행합니다.

- DescribeReplicationInstance:

Amazon VPC ID, 서브넷 ID, 보안 그룹 IDs 포함한 AWS DMS 복제 인스턴스의 네트워크 구성 세부 정보를 검색하고 연결된 탄력적 네트워크 인터페이스(ENI)를 식별IDs.

- ValidateResourcePermissions:

실행 역할에 자동화 프로세스 중에 생성될 리소스를 정리하는 데 필요한 권한이 있는지 확인합니다.

- CreateDNSResolverLambda:

복제 인스턴스와 동일한 Amazon VPC 내에 배포된 Lambda 함수가 포함된 AWS CloudFormation 스택을 생성합니다. 이 함수는 Amazon VPC 컨텍스트 내에서 프라이빗 IP 주소로 DNS 이름을 확인하는 데 사용됩니다.

- DescribeCloudFormationErrorFromStackEvents:

CloudFormation 스택 생성에 실패하면 이 단계에서는 스택 이벤트의 오류를 설명하여 문제 해결을 위한 자세한 실패 정보를 제공합니다.

- GetDNSResolverLambdaName:

후속 단계에서 사용할 CloudFormation 스택 출력에서 DNS 해석기 Lambda 함수의 이름을 검색합니다.

- **ResolveDmsEndpoint:**

Lambda 함수를 호출하여 AWS DMS 엔드포인트 호스트 이름을 Amazon VPC 내에서 IP 주소로 확인합니다. 이렇게 하면 정확한 프라이빗 DNS 확인이 보장되고 IPv4 호환성이 검증됩니다.

- **BranchOnResolveDmsEndpointErrors:**

DNS 확인 오류를 기반으로 자동화를 분기합니다. 엔드포인트를 확인할 수 없거나 IPv6 주소로 확인되면 자동화가 오류 보고서를 생성합니다.

- **GetReachabilityAnalyzerTarget:**

Amazon VPC 구성 및 엔드포인트 위치를 기반으로 Reachability Analyzer에 적합한 대상을 식별합니다. ENI(동일한 Amazon VPC 엔드포인트의 경우) 또는 IP 주소(외부 엔드포인트의 경우)를 대상으로 사용할지 여부를 결정합니다.

- **GenerateErrors:**

이전 단계에서 오류가 발생할 때 포괄적인 오류 보고서를 생성합니다. 여기에는 엔드포인트 검증 오류, 연결 테스트 실패 또는 특정 문제 해결 지침이 포함된 DNS 해결 문제에 대한 세부 정보가 포함됩니다.

- **GenerateReport:**

연결 상태, Reachability Analyzer를 사용한 네트워크 경로 분석 결과, 연결 장벽에 대한 자세한 설명, 해결을 위한 권장 조치가 포함된 포괄적인 문제 해결 보고서를 생성합니다.

- **CheckStackExists:**

CloudFormation 스택이 성공적으로 생성되었으며 정리 중에 삭제해야 하는지 확인합니다. 이 단계는 자동화 성공 또는 실패에 관계없이 적절한 리소스 관리를 보장합니다.

- **DeleteDNSResolverLambda:**

DNS 해석기 Lambda 함수 및 관련 리소스(가 로 설정되지 않은 경우 true)PersistReachabilityAnalyzerResults가 포함된 CloudFormation 스택을 삭제하여 자동화 완료 후 남은 리소스가 남아 있지 않도록 합니다.

7. 완료되면 출력 섹션에서 실행의 자세한 결과를 검토합니다.

- **GetTestConnectionStatus.status**

AWS DMS 복제 인스턴스와 엔드포인트 간의 현재 연결 테스트 상태(예: 성공, 실패, 테스트).

- **DescribeCloudFormationErrorFromStackEvents.Events**

CloudFormation 스택 생성에 실패하면이 출력에는 인프라 배포 문제를 진단하는 데 도움이 되는 스택 생성 프로세스의 자세한 오류 이벤트가 포함됩니다.

- [GenerateReport.report](#)

연결 분석 결과, Reachability Analyzer 결과, 네트워크 경로 분석, 식별된 특정 연결 장벽, 관련 AWS 설명서 링크가 포함된 자세한 문제 해결 권장 사항이 포함된 포괄적인 문제 해결 보고서입니다.

- [GenerateErrors.report](#)

자동화 프로세스 중에 오류가 발생하는 경우이 출력은 특정 실패 이유, 영향을 받는 리소스, 자동화를 다시 시도하기 전에 문제를 해결하기 위한 지침을 포함한 자세한 오류 보고서를 제공합니다.

참조

Systems Manager Automation

- [이 자동화 실행\(콘솔\)](#)
- [자동화 실행](#)
- [Automation 설정](#)
- [Support Automation Workflows 랜딩 페이지](#)

Amazon EBS

AWS Systems Manager Automation은 Amazon Elastic Block Store에 사전 정의된 실행서를 제공합니다. 실행서에 대한 자세한 내용은 [실행서 작업](#)을 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 실행서는 Amazon Elastic Block Store(Amazon EBS)의 리소스 사용량을 분석하는 데 사용됩니다. 볼륨 사용량을 분석하고 지정된 AWS 리전에서 중단된 볼륨, 이미지 및 스냅샷을 식별합니다.

어떻게 작동하나요?

실행서는 다음 네 가지 작업을 수행합니다.

1. Amazon Simple Storage Service(Amazon S3) 버킷이 있는지 확인하거나 새 Amazon S3 버킷을 생성합니다.
2. 모든 Amazon EBS 볼륨을 사용 가능한 상태로 수집합니다.
3. 소스 볼륨이 삭제된 모든 Amazon EBS 스냅샷을 수집합니다.
4. 종료되지 않은 Amazon Elastic Compute Cloud(AMIs)를 수집합니다.Amazon EC2

실행서는 CSV 보고서를 생성하여 사용자가 제공한 Amazon S3 버킷에 저장합니다. 제공된 버킷은 끝에 설명된 AWS 보안 모범 사례에 따라 보호되어야 합니다. 사용자가 제공한 Amazon S3 버킷이 계정에 없는 경우 실행서는 이름 형식이 이고 <User-provided-name>-awssupport-YYYY-MM-DD 사용자 지정 AWS Key Management Service (AWS KMS) 키로 암호화되며 객체 버전 관리가 활성화되고 퍼블릭 액세스가 차단되고 SSL/TLS 사용 요청이 필요한 새 Amazon S3 버킷을 생성합니다.

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

- 버킷에 대한 퍼블릭 액세스를 차단합니다(IsPublic로 설정False).
- Amazon S3 액세스 로깅을 켭니다.

- [버킷에 대한 SSL 요청만 허용합니다.](#)
- 객체 버전 관리를 켭니다.
- AWS Key Management Service (AWS KMS) 키를 사용하여 버킷을 암호화합니다.

Important

이 실행서를 사용하면 Amazon S3 버킷 및 객체 생성에 대해 계정에 추가 요금이 발생할 수 있습니다. 발생할 수 있는 요금에 대한 자세한 내용은 [Amazon S3 요금](#)을 참조하세요.

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: 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 않는지 확인합니다. 지정된 버킷이 계정에 없는 경우 자동화는 이름 형식 로 자동화가 시작되고 사용자 지정 AWS KMS 키로 <User-provided-name>-awssupport-YYYY-MM-DD암호화된 리전에 새 버킷을 생성합니다.

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 생성할 새 Amazon S3 버킷을 암호화하기 위한 사용자 지정 AWS KMS 키 Amazon 리소스 이름(ARN)입니다. Amazon S3 사용자 지정 AWS KMS 키 ARN을 지정하지 않고 버킷 생성을 시도하면 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 정책 예제:

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [{
    "Sid": "ReadOnlyPermissions",
    "Effect": "Allow",
    "Action": [
      "ec2:DescribeImages",
      "ec2:DescribeInstances",
      "ec2:DescribeSnapshots",
      "ec2:DescribeVolumes",
      "ssm:DescribeAutomationExecutions"
    ],
    "Resource": "*"
  }, {
    "Sid": "KMSGeneratePermissions",
    "Effect": "Allow",
    "Action": ["kms:GenerateDataKey", "kms:Decrypt"],
    "Resource": "arn:aws:kms:us-east-1:111122223333:key/1234abcd-12ab-34cd-56ef-1234567890ab"
  }, {
    "Sid": "S3ReadOnlyPermissions",
    "Effect": "Allow",
    "Action": [
      "s3:GetBucketAcl",
      "s3:GetBucketPolicyStatus",
      "s3:GetBucketPublicAccessBlock",
      "s3:ListBucket"
    ],
    "Resource": [
      "arn:aws:s3:::amzn-s3-demo-bucket1",
      "arn:aws:s3:::amzn-s3-demo-bucket2/"
    ]
  }
]}
```

```

    }, {
      "Sid": "S3CreatePermissions",
      "Effect": "Allow",
      "Action": [
        "s3:CreateBucket",
        "s3:PutObject",
        "s3:PutBucketLogging",
        "s3:PutBucketPolicy",
        "s3:PutBucketPublicAccessBlock",
        "s3:PutBucketTagging",
        "s3:PutBucketVersioning",
        "s3:PutEncryptionConfiguration"
      ],
      "Resource": "*"
    }
  ]
}

```

지침

다음 단계에 따라 자동화를 구성합니다.

1. AWS Systems Manager 콘솔에서 [AWSSupport-AnalyzeEBSResourceUsage](#)로 이동합니다.
2. 입력 파라미터의 경우, 다음 내용을 입력합니다.

- AutomationAssumeRole(선택 사항):

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

- S3BucketName(필수):

보고서를 업로드할 계정의 Amazon S3 버킷입니다.

- CustomerManagedKmsKeyArn(선택 사항):

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

Input parameters

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

S3 Bucket

Example: s3-bucket-name

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

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

3. 실행을 선택합니다.

4. 자동화가 시작됩니다.

5. 자동화 실행서는 다음 단계를 수행합니다.

- checkConcurrency:

리전에서이 실행서를 한 번만 시작하도록 합니다. 실행서가 진행 중인 다른 실행을 찾으면 오류가 반환되고 종료됩니다.

- verifyOrCreateS3bucket:

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

- gatherAmiDetails:

Amazon EC2 인스턴스에서 사용하지 않는 AMIs를 검색**<region>-images.csv**하여 이름 형식의 보고서를 생성하고 Amazon S3 버킷에 업로드합니다.

- gatherVolumeDetails:

Amazon EBS 볼륨이 사용 가능한 상태인지 확인하고 이름 형식의 보고서를 생성하여 Amazon S3 버킷에 **<region>-volume.csv**업로드합니다.

- gatherSnapshotDetails:

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

6. 완료 후에는 Outputs 섹션에서 실행의 세부 결과를 검토합니다.

▼ Outputs	
gatherVolumeDetails.gatherVolumeDetailsOutput No volume found in available state in region eu-central-1	verifyOrCreateS3bucket.createdNewBucket true
gatherAmiDetails.gatherAmiDetailsOutput File eu-central-1-image.csv have been uploaded to bucket aws-support-ssm-[REDACTED]1-awssupport-2023-11-27. Please review the file carefully and verify if you need to keep those AMI.	
gatherSnapshotDetails.gatherSnapshotDetailsOutput File eu-central-1-snapshot.csv have been uploaded to bucket aws-support-ssm-[REDACTED]1-awssupport-2023-11-27. Please review the file carefully and verify if you need to keep those snapshots.	

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(Amazon EBS) 볼륨에 대한 스냅샷을 보관하는 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

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.

- 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. RetentionDays에 대한 값을 지정하는 경우, 이 파라미터에 대한 값을 지정하지 마십시오.

- RetentionDays

유형: 문자열

설명: (선택 사항) 보관하려는 스냅샷의 이전 일 수입니다. RetentionCount에 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 EC2) 인스턴스에 Amazon Elastic Block Store(Amazon EBS) 볼륨을 연결합니다.

[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.

- 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-CalculateEBSPerformanceMetrics 실행서는 성능 지표를 계산하고 CloudWatch 대시보드에 게시하여 Amazon EBS 성능 문제를 진단하는 데 도움이 됩니다. 대시보드에는 대상 Amazon EBS 볼륨 또는 대상 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스에 연결된 모

든 볼륨의 예상 평균 IOPS 및 처리량이 표시됩니다. Amazon EC2 인스턴스의 경우 인스턴스의 평균 IOPS 및 처리량도 표시됩니다. 실행서는 계산된 관련 CloudWatch 지표를 표시하는 새로 생성된 CloudWatch 대시보드로 연결되는 링크를 출력합니다. CloudWatch 대시보드는 이름이 인 계정에 생성됩니다. `AWSSupport-<ResourceId>-EBS-Performance-<automation:EXECUTION_ID>`.

어떻게 작동하나요?

실행서는 다음 단계를 수행합니다.

- 지정된 타임스탬프가 유효한지 확인합니다.
- 리소스 ID(Amazon EBS 볼륨 또는 Amazon EC2 인스턴스)가 유효한지 확인합니다.
- Amazon EC2를 ResourceID로 제공하면 해당 Amazon EC2 인스턴스의 실제 총 IOPS/처리량과 Amazon EC2 인스턴스에 연결된 모든 Amazon EBS 볼륨의 추정 평균 IOPS/처리량 그래프가 포함된 CloudWatch 대시보드가 생성됩니다. Amazon EC2.
- Amazon EBS 볼륨을 ResourceID로 제공하면 해당 볼륨에 대한 예상 평균 IOPS/처리량 그래프가 포함된 CloudWatch 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 마이크로 버스팅이 가능합니다.

Note

버스트 가능 볼륨(gp2, sc2 및 st1)의 경우 버스트 밸런스가 있을 때까지 최대 IOPS/처리량을 고려해야 합니다. 버스트 밸런스가 완전히 활용된 후, 즉 0이 되면 기존 IOPS/처리량 지표를 고려합니다.

Important

CloudWatch 대시보드를 생성하면 계정에 추가 요금이 발생할 수 있습니다. 자세한 내용은 [Amazon CloudWatch 요금 안내서](#)를 참조하세요.

이 자동화 실행(콘솔)

문서 유형

자동화

소유자

Amazon

플랫폼

Linux, macOS, Windows

파라미터

필수 IAM 권한

실행서를 성공적으로 사용하려면 AutomationAssumeRole 파라미터에 다음 작업이 필요합니다.

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

샘플 정책

JSON

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

```

    }
  ]
}

```

지침

다음 단계에 따라 자동화를 구성합니다.

1. Systems Manager [AWSSupport-CalculateEBSPerformanceMetrics](#)의 문서로 이동합니다.
2. Execute automation(자동화 실행)을 선택합니다.
3. 입력 파라미터에 다음을 입력합니다.

- AutomationAssumeRole(선택 사항):

Systems Manager Automation이 사용자를 대신하여 작업을 수행하도록 허용하는 (IAM) 역할의 Amazon 리소스 이름 AWS AWS Identity and Access Management (ARN)입니다. 역할이 지정되지 않은 경우 Systems Manager Automation은 이 실행서를 시작하는 사용자의 권한을 사용합니다.

- ResourceID(필수):

Amazon EC2 인스턴스 또는 Amazon EBS 볼륨의 ID입니다.

- 시작 시간(필수):

CloudWatch에서 데이터를 보는 시작 시간입니다. 시간은 형식yyyy-mm-ddThh:mm:ss과 UTC 형식이어야 합니다.

- 종료 시간(필수):

CloudWatch에서 데이터를 보는 종료 시간입니다. 시간은 형식yyyy-mm-ddThh:mm:ss과 UTC 형식이어야 합니다.

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

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

- CheckResourceIDAndTimeStamps:

종료 시간이 시작 시간보다 1분 이상 크고 제공된 리소스가 존재하는지 확인합니다.

- CreateCloudWatchDashboard:

Amazon EBS 성능을 계산하고 리소스 ID를 기반으로 그래프를 표시합니다. 파라미터 리소스 ID에 Amazon EBS 볼륨 ID를 제공하는 경우 이 실행서는 Amazon EBS 볼륨의 예상 평균 IOPS 및 예상 평균 처리량이 포함된 CloudWatch 대시보드를 생성합니다. 파라미터 리소스 ID에 Amazon EC2 인스턴스 ID를 제공하는 경우 이 실행서는 Amazon EC2 인스턴스의 평균 총 IOPS 및 평균 총 처리량과 Amazon EC2 인스턴스에 연결된 모든 Amazon EBS 볼륨의 예상 평균 IOPS 및 예상 평균 처리량이 포함된 CloudWatch 대시보드를 생성합니다 Amazon EC2.

7. 완료되면 출력 섹션에서 실행의 자세한 결과를 검토합니다.

```
▼ Outputs

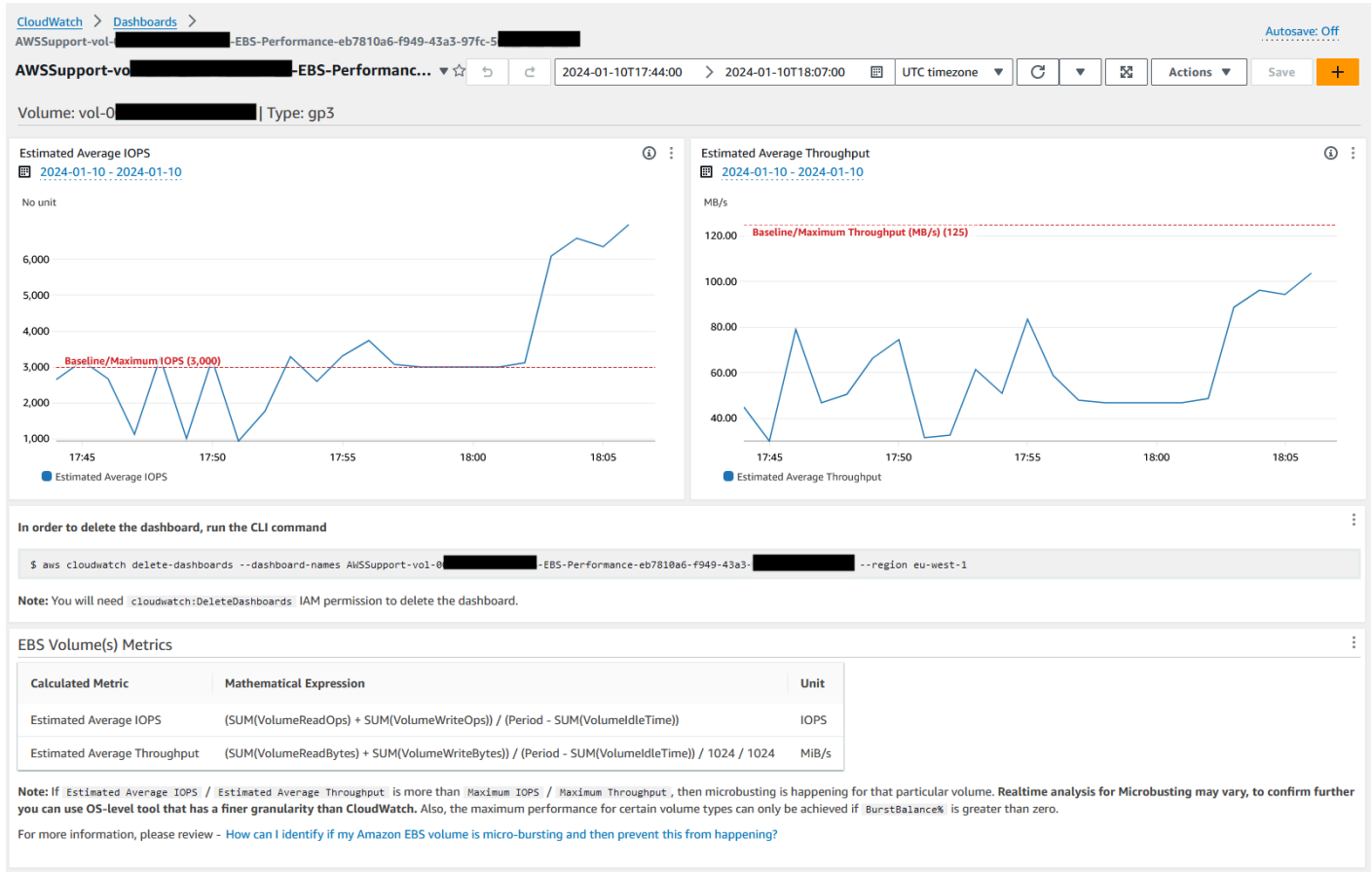
CreateCloudWatchDashboard.CloudWatchDashboardLink
https://console.aws.amazon.com/cloudwatch/home?region=us-east-1#dashboards:name=AWSsupport-i-██████████:EBS-Performance-443096c1-df23-44ba-96dd-2d005b5ae971

CreateCloudWatchDashboard.CloudWatchDashboardMessage
Open the CloudWatch Dashboard URL in your browser to see the performance metrics for the target resource 'i-██████████'.
You can delete the CloudWatch Dashboard from the CloudWatch console.
```

리소스 ID를 Amazon EC2 인스턴스로 사용하는 CloudWatch 대시보드 예제



리소스 ID를 Amazon EBS 볼륨 ID로 사용하는 CloudWatch 대시보드 예제



참조

Systems Manager Automation

- [이 자동화 실행\(콘솔\)](#)
- [자동화 실행](#)
- [Automation 설정](#)
- [Support Automation Workflows 랜딩 페이지](#)

AWS 서비스 설명서

- [Amazon EBS 볼륨이 마이크로 버스팅 중인지 식별한 다음 이를 방지하려면 어떻게 해야 하나요?](#)
- [CloudWatch를 사용하여 EC2 인스턴스에 대한 집계 Amazon EBS 성능 지표를 보려면 어떻게 해야 합니까?](#)

AWS-CopySnapshot

설명

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

- 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

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.

- 설명

유형: 문자열

설명: (선택 사항) 스냅샷에 대한 설명입니다.

- Volumeld

유형: 문자열

설명: (필수) 볼륨의 ID입니다.

AWS-DeleteSnapshot

설명

Amazon EBS 볼륨 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.

- 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

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.

- CreateSnapshot

유형: Boolean

설명: (선택 사항) true(으)로 설정하면, 자동화가 Amazon EBS 볼륨이 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 파라미터에서 지정하는 Amazon EBS 볼륨이 사용 중이 아닌지 확인하고 CreateSnapshot 파라미터에 대해 선택하는 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 지정하는 Amazon EBS 볼륨을 삭제합니다.
- aws:executeScript - Amazon EBS 볼륨이 삭제되었는지 확인합니다.

AWS-DeregisterAMIs

설명

AWS-DeregisterAMIs 실행서는 AMIs에 적용한 태그를 지정하여 Amazon Machine Images(AMIs) 등록을 취소할 수 있도록 도와줍니다.

[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.

- 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) 보존하려는 AMIs의 개수입니다. Age에 대한 값을 지정하는 경우, 이 파라미터에 대한 값을 지정하지 마십시오.

- 나이

유형: 문자열

설명: (선택 사항) 보존하려는 AMIs의 이전 일 수입니다. RetainNumber에 대한 값을 지정하는 경우, 이 파라미터에 대한 값을 지정하지 마십시오.

- TagKey

유형: 문자열

설명: (필수) 등록을 취소하려는 AMIs에 할당된 태그의 키입니다.

- TagValue

유형: 문자열

설명: (필수) 등록을 취소하려는 AMIs에 할당된 태그의 값입니다.

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 - TagKey 및 TagValue 파라미터를 사용하여 지정하는 태그를 사용하여 AMIs 등록을 취소합니다.

AWS-DetachEBSVolume

설명

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

[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.

- LambdaAssumeRole

유형: 문자열

설명: (선택 사항) Lambda에서 수입하는 역할의 ARN입니다.

- Volumeld

유형: 문자열

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

AWSConfigRemediation-EnableEbsEncryptionByDefault

설명

AWSConfigRemediation-EnableEbsEncryptionByDefault 실행서는 자동화를 실행하는 AWS 계정 AWS 리전 및의 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

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.

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 볼륨 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

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.

- DriveLetter

유형: 문자열

설명: (선택 사항) 확장하려는 파일 시스템이 있는 드라이브의 문자입니다. 이 파라미터는 Windows 인스턴스에 대해 필요합니다.

- InstanceId

유형: 문자열

설명: (선택 사항) 확장하려는 Amazon EBS 볼륨을 연결할 Amazon EC2 인스턴스의 ID입니다.

- KeepSnapshot

유형: Boolean

기본값: true

설명: (선택 사항) Amazon EBS 볼륨 크기를 늘리기 전에 생성한 스냅샷을 보관할지 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 수정하려는 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(Amazon EBS) 스냅샷에 대한 권한을 수정하는 데 도움이 됩니다. 이 실행서를 사용하여 Public 또는 Private 스냅샷을 만들거나 다른 AWS 계정과 공유할 수 있습니다. 기본 KMS 키로 암호화된 스냅샷은 이 실행서를 사용하는 다른 계정과 공유할 수 없습니다.

[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.

- AccountIds

유형: StringList

기본값: 없음

설명: (선택 사항) 스냅샷을 공유하려는 계정의 ID입니다. 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.

- Private

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) 수정하려는 권한이 있는 Amazon EBS 스냅샷의 ID입니다.

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 파라미터에서 제공된 스냅샷의 ID를 확인합니다. ID를 확인한 후, 스크립트는 암호화된 스냅샷을 확인하고 해당 내용이 발견된 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 Public에서 Private(으)로 변경합니다.

출력

ValidateSnapshots.EncryptedSnapshots

SharewithOtherAccounts.Result

MakePrivate.Result

MakePrivate.Commands

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 설명서 [의 볼륨 수정 진행 상황 모니터링](#)을 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.

- EbsVolumeld

유형: 문자열

설명: (필수) 수정하려는 Amazon EBS 볼륨의 ID입니다.

- EbsVolumeType

유형: 문자열

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

설명: Amazon EBS 볼륨을 변경하려는 볼륨 유형입니다. Amazon EBS 볼륨 유형에 대한 자세한 내용은 [Amazon EC2 사용 설명서의 Amazon EBS 볼륨 유형](#)을 참조하세요. Amazon 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-use인지 확인합니다.
- aws:executeAwsApi - EbsVolumeId 파라미터에서 지정하는 Amazon EBS 볼륨을 수정합니다.
- aws:waitForAwsResourceProperty - 볼륨 유형이 EbsVolumeType 파라미터에서 지정한 값으로 변경되었는지 확인합니다.

Amazon EC2

AWS Systems Manager 자동화는 Amazon Elastic Compute Cloud에 대한 사전 정의된 실행서를 제공합니다. Amazon Elastic Block Store용 런북은 런북 참조의 [Amazon EBS](#) 섹션에 있습니다. 실행서에 대한 자세한 내용은 [실행서 작업](#)을 참조하세요. 실행서 콘텐츠를 보는 방법에 대한 자세한 내용은 [실행서 콘텐츠 보기](#)(을)를 참조하세요.

주제

- [AWS-ASGEnterStandby](#)
- [AWS-ASGExitStandby](#)
- [AWS-CreatelImage](#)
- [AWS-DeletelImage](#)
- [AWS-PatchAsgInstance](#)
- [AWS-PatchInstanceWithRollback](#)
- [AWS-QuarantineEC2Instance](#)
- [AWS-ResizeInstance](#)
- [AWS-RestartEC2Instance](#)
- [AWS-SetupJupyter](#)
- [AWS-StartEC2Instance](#)
- [AWS-StopEC2Instance](#)
- [AWS-TerminateEC2Instance](#)
- [AWS-UpdateLinuxAmi](#)
- [AWS-UpdateWindowsAmi](#)
- [AWSConfigRemediation-EnableAutoScalingGroupELBHealthCheck](#)
- [AWSConfigRemediation-EnforceEC2InstanceIMDSv2](#)
- [AWSEC2-CloneInstanceAndUpgradeSQLServer](#)
- [AWSEC2-CloneInstanceAndUpgradeWindows](#)
- [AWSEC2-PatchLoadBalancerInstance](#)
- [AWSEC2-SQLServerDBRestore](#)
- [AWSsupport-ActivateWindowsWithAmazonLicense](#)
- [AWSsupport-AnalyzeAWSEndpointReachabilityFromEC2](#)
- [AWSPremiumSupport-ChangeInstanceTypeIntelToAMD](#)
- [AWSsupport-CheckXenToNitroMigrationRequirements](#)
- [AWSsupport-CloneXenEC2InstanceAndMigrateToNitro](#)
- [AWSsupport-CollectSAPHANALogs](#)
- [AWSsupport-ConfigureEC2Metadata](#)

- [AWSSupport-ContainEC2Instance](#)
- [AWSSupport-CopyEC2Instance](#)
- [AWSPremiumSupport-DiagnoseDiskUsageOnLinux](#)
- [AWSSupport-EnableWindowsEC2SerialConsole](#)
- [AWSPremiumSupport-ExtendVolumesOnWindows](#)
- [AWSSupport-ExecuteEC2Rescue](#)
- [AWSSupport-ListEC2Resources](#)
- [AWSSupport-ManageRDPSettings](#)
- [AWSSupport-ManageWindowsService](#)
- [AWSSupport-MigrateEC2ClassicToVPC](#)
- [AWSSupport-MigrateXenToNitroLinux](#)
- [AWSSupport-ResetAccess](#)
- [AWSSupport-ResetLinuxUserPassword](#)
- [AWSSupport-RunEC2RescueForWindowsTool](#)
- [AWSPremiumSupport-ResizeNitroInstance](#)
- [AWSSupport-ShareEncryptedAMIOrEBSSnapshot](#)
- [AWSSupport-RestoreEC2InstanceFromSnapshot](#)
- [AWSSupport-SendLogBundleToS3Bucket](#)
- [AWSSupport-StartEC2RescueWorkflow](#)
- [AWSSupport-TroubleshootActiveDirectoryReplication](#)
- [AWSPremiumSupport-TroubleshootEC2DiskUsage](#)
- [AWSSupport-TroubleshootEC2InstanceConnect](#)
- [AWSSupport-TroubleshootLinuxMGNDRSAgentLogs](#)
- [AWSSupport-TroubleshootRDP](#)
- [AWSSupport-TroubleshootSSH](#)
- [AWSSupport-TroubleshootSUSERegistration](#)
- [AWSSupport-TroubleshootWindowsPerformance](#)
- [AWSSupport-TroubleshootWindowsUpdate](#)

- [AWSSupport-UpgradeWindowsAWSDrivers](#)

AWS-ASGEnterStandby

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: Boolean

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

필수 IAM 권한

실행서를 성공적으로 사용하려면 AutomationAssumeRole 파라미터에 다음 작업이 필요합니다.

JSON

```
{
  "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.

JSON

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



```

        "Effect": "Allow",
        "Action": "ec2:DeregisterImage",
        "Resource": "*"
    }
}

```

AWS-PatchAsgInstance

설명

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

[이 자동화 실행\(콘솔\)](#)

Important

이 실행서는 실행 중에 대상 인스턴스에 AutoPatchInstanceInASG 태그를 적용합니다. 이 태그는 실행서가 동일한 인스턴스에서 동시에 두 번 실행되지 않도록 합니다. 패치 규정 준수 지표는 아닙니다. 패치 적용 단계가 실패하더라도 실행서 실행 상태에서서를 보고Completed하더라도 태그 값은 여전히 로 설정될 수 있습니다Failed.

인스턴스에서 패치 규정 준수를 확인하려면 [DescribeInstancePatchStates](#) 또는 [ListComplianceItems](#) 대신 사용합니다.

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

단계 번호	단계 이름	자동화 작업
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 completed가 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.

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.

- Instanceld

유형: 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 Store는의 도구입니다 AWS Systems Manager. 파라미터를 생성하는 것에 대한 자세한 내용은 AWS Systems Manager 사용 설명서의 [파라미터 생성](#)을 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.

- Amild

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: SSManagedInstanceProfileRole

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

- StackName

유형: 문자열

기본값: CreateManagedInstanceStack{{automation:EXECUTION_ID}}

설명: (선택 사항) 자동화에서 사용할 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.

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

- InstanceId

유형: 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

유형: 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.

- InstanceIds

유형: 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

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.

허용된 패턴: `^$|^arn:aws[a-z0-9-]*:iam::(\d{12}|\{\{global:ACCOUNT_ID\}\}):role/[w/.@+=-]{1,1017}$`

- 유효한 IAM 역할 ARN 또는 빈 문자열이어야 합니다. arn의 AWS 계정 ID 대신 시스템 변수를 사용할 `{{global:ACCOUNT_ID}}` 수 있습니다.

- ExcludePackages

유형: 문자열

기본값: 없음

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

허용된 패턴: `^(none|[a-zA-Z0-9\s,._+:=<>()\[\]/*-]+)$`

- "없음"이거나 문자, 숫자, 공백 및 다음 문자로 구성된 쉼표로 구분된 항목 목록이어야 합니다. , . _ + : = < > () [] / * -

- **lamInstanceProfileName**

유형: 문자열

기본값: ManagedInstanceProfile

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

허용된 패턴: `^[\w+=, .@-]{1,128}$`

- 1~128자여야 하며 문자, 숫자 및 다음 문자만 포함해야 합니다. + = , . @ - _

- **IncludePackages**

유형: 문자열

기본값: all

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

허용된 패턴: `^(all|[a-zA-Z0-9\s, ._:=<>()\[\]/*-]+)$`

- "모두" 또는 문자, 숫자, 공백 및 다음 문자로 구성된 쉼표로 구분된 항목 목록이어야 합니다. , . _ + : = < > () [] / * -

- **InstanceType**

유형: 문자열

기본값: t2.micro

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

허용된 패턴: `^[a-z0-9]+(-[a-z0-9]+)*\.[a-z0-9]+$`

- 두 부분 모두 소문자와 숫자를 포함하고 접두사에 하이픈을 포함할 수 있는 prefix.suffix 형식이어야 합니다.

- **MetadataOptions**

기본값: {"HttpEndpoint": "enabled", "HttpTokens": "optional"}

설명: (선택 사항) 인스턴스에 대한 메타데이터 옵션입니다. 자세한 내용은 [InstanceMetadataOptionsRequest](#)를 참조하세요.

허용된 패턴: `^\{[^\<>\$;|&\\]*\}$`

• 중괄호 { }로 묶어야 하며 다음 문자를 포함할 수 없습니다. < > \$; | & \

- PostUpdateScript

유형: 문자열

기본값: 없음

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

허용된 패턴: `^(none|https?:\/\/[\w\-. _~:\/?#\[\]\@!$&'()*+ , ; =% ]+)$`

• "없음" 또는 유효한 HTTP/HTTPS URL이어야 합니다.

- PreUpdateScript

유형: 문자열

기본값: 없음

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

허용된 패턴: `^(none|https?:\/\/[\w\-. _~:\/?#\[\]\@!$&'()*+ , ; =% ]+)$`

• "없음" 또는 유효한 HTTP/HTTPS URL이어야 합니다.

- SecurityGroupIds

유형: 문자열

설명: (필수)에 적용할 보안 그룹의 IDs를 쉼표로 구분한 목록입니다AMI.

허용된 패턴: `^sg-[a-z0-9]{8,17}$`

• "sg-"로 시작하고 8~17자의 소문자 또는 숫자로 시작해야 합니다.

- SourceAmild

유형: 문자열

설명: (필수) 소스 Amazon 머신 이미지 ID입니다.

허용된 패턴: ^ami-[a-z0-9]{8,17}\$

- "ami-"로 시작하고 8~17자의 소문자 또는 숫자로 시작해야 합니다.
- SubnetId

유형: 문자열

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

허용된 패턴: ^\$|^subnet-[a-z0-9]{8,17}\$

- 비어 있거나 "subnet-"으로 시작한 다음 8~17자의 소문자 또는 숫자로 시작해야 합니다.
- TargetAmiName

유형: 문자열

기본값: UpdateLinuxAmi_from_{{SourceAmiId}}_on_{{global:DATE_TIME}}

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

허용된 패턴: ^[a-zA-Z0-9() \[\] \{ } . / ' @ _ : -]{3,128}\$

- 3~128자여야 하며 문자, 숫자, 공백 및 다음 문자만 포함해야 합니다. () [] { } . / ' @ _ : -

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~Windows Server 2022를 지원합니다.

⚠ Important

AWS 반가상화 드라이버는 이러한 버전과 호환되지 않으므로 이 실행서는 Windows Server 2025 이상 버전을 지원하지 않습니다. 자세한 내용은 [Windows 인스턴스용 반가상화 드라이버](#)를 참조하세요.

⚠ Important

인스턴스가 VPC 엔드포인트를 AWS Systems Manager 사용하여 연결되면 us-east-1 리전에서 사용하지 않는 한 이 실행서는 실패합니다. 이 실행서를 사용하려면 인스턴스에 TLS 1.2가 활성화되어 있어야 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.

- Categories

유형: 문자열

설명: (선택 사항)하나 이상의 업데이트 범주를 지정합니다. 쉼표로 분리된 값을 사용하여 범주를 필터링할 수 있습니다. 옵션: Application, Connectors, CriticalUpdates, DefinitionUpdates, DeveloperKits, Drivers, FeaturePacks, Guidance, Microsoft, SecurityUpdates, ServicePacks, Tools, UpdateRollups, Updates. 유효한 형식에는 CriticalUpdates 등 단일 항목이 포함됩니다. 또는 쉼표로 구분된 목록(CriticalUpdates,SecurityUpdates)을 지정할 수 있습니다. 참고: 쉼표 앞/뒤에 공백이 없어야 합니다.

- ExcludeKbs

유형: 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

유형: 문자열

기본값: ManagedInstanceProfile

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

- IncludeKbs

유형: 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

유형: 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": "enabled", "HttpTokens": "optional"}

설명: (선택 사항) 인스턴스에 대한 메타데이터 옵션입니다. 자세한 내용은 [InstanceMetadataOptionsRequest](#)를 참조하세요.

- PostUpdateScript

유형: 문자열

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

- PreUpdateScript

유형: 문자열

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

- PublishedDateAfter

유형: 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

유형: 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

유형: 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

유형: 문자열

설명: (필수)에 적용할 보안 그룹의 IDs를 쉼표로 구분한 목록입니다AMI.

- SeverityLevels

유형: 문자열

설명: (선택 사항) 업데이트와 연결되는 하나 이상의 MSRC 심각도를 지정합니다. 심표로 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 심표로 구분된 목록을 지정할 수 있습니다.

- SourceAmild

유형: 문자열

설명: (필수) 소스 AMI ID입니다.

- SubnetId

유형: 문자열

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

- TargetAmiName

유형: 문자열

기본값: UpdateWindowsAmi_from_{{SourceAmild}}_on_{{global:DATE_TIME}}

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

파라미터

- `InstanceId`

유형: 문자열

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

- `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.

- `HttpPutResponseHopLimit`

유형: 정수

설명: (선택 사항) IMDS 서비스에서 요청자로의 호출 응답 제한입니다. 컨테이너를 호스팅하는 EC2 인스턴스의 경우를 2 이상으로 설정합니다. 변경하지 않으려면 0으로 설정합니다(기본값).

허용되는 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 required으로 설정합니다.
- `aws:assertAwsResourceProperty` - Amazon EC2 인스턴스에서 IMDS2가 필요한지 확인합니다.

AWSEC2-CloneInstanceAndUpgradeSQLServer

설명

SQL Server 2008 이상을 실행 중인 Windows Server용 EC2 인스턴스에서 AMI를 생성한 다음, 이 AMI를 SQL Server 최신 버전으로 업그레이드합니다. SQL Server의 영어 버전만 지원됩니다.

다음 업그레이드 경로가 지원됩니다.

- SQL Server 2008에서 SQL Server 2017, 2016 또는 2014로
- SQL Server 2008 R2에서 SQL Server 2017, 2016 또는 2014로
- SQL Server 2012에서 SQL Server 2019, 2017, 2016 또는 2014로

- SQL Server 2014에서 SQL Server 2019, 2017 또는 2016으로
- SQL Server 2016에서 SQL Server 2019 또는 2017로

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

이 업그레이드는 완료하는 데 2시간이 걸릴 수 있는 다단계 프로세스입니다. 자동화는 인스턴스에서 AMI를 생성한 다음, 지정된 SubnetID의 새로운 AMI에서 임시 인스턴스를 시작합니다. 원래 인스턴스와 연결된 보안 그룹이 임시 인스턴스에 적용됩니다. 이제 자동화는 임시 인스턴스에서 TargetSQLVersion에 대한 현재 위치 업그레이드를 수행합니다. 업그레이드 후, 이 자동화는 임시 인스턴스에서 새 AMI를 생성한 다음 임시 인스턴스를 종료합니다.

VPC에서 새 AMI를 시작하여 애플리케이션 기능을 테스트할 수 있습니다. 테스트를 완료하고 나서나 다른 업그레이드를 수행하기 전에는 업그레이드된 인스턴스로 완전히 전환하기에 앞서 애플리케이션 중단 시간을 예약하십시오.

Note

새 AMI에서 시작된 EC2 인스턴스의 컴퓨터 이름을 수정하려면, [SQL Server의 독립 실행형 인스턴스를 호스팅하는 컴퓨터 이름 바꾸기](#)를 참조하세요.

이 자동화 실행(콘솔)

문서 유형

자동화

소유자

Amazon

플랫폼

Windows

파라미터

사전 조건

- TLS 버전 1.2.
- SQL Server의 영어 버전만 지원됩니다.
- EC2 인스턴스는 버전이 Windows Server 2008 R2 이상 및 SQL Server 2008 이상인 Windows Server를 사용해야 합니다.
- 인스턴스에 SSM Agent가 설치되었는지 확인합니다. 자세한 내용은 [Windows Server용 EC2 인스턴스에 SSM Agent 설치 및 구성](#)을 참조하세요.
- AWS Identity and Access Management (IAM) 인스턴스 프로파일 역할을 사용하도록 인스턴스를 구성합니다. 자세한 내용은 [Systems Manager용 IAM 인스턴스 프로파일 생성](#)을 참조하세요.
- 인스턴스 부트 디스크에 20GB의 사용 가능한 디스크 공간이 있는지 확인합니다.
- 기존 보유 라이선스 사용(BYOL) SQL Server 버전을 사용하는 인스턴스의 경우 다음 추가 사전 조건이 적용됩니다.
 - 대상 SQL Server 설치 미디어가 포함된 EBS 스냅샷 ID를 제공합니다. 방법:
 1. EC2 인스턴스에서 Windows Server 2008 R2 이상을 실행 중인지 확인합니다.
 2. 인스턴스가 실행 중인 동일 가용 영역에서 6GB EBS 볼륨을 생성합니다. 볼륨을 인스턴스에 연결합니다. 예를 들면 드라이브 D에 탑재합니다.
 3. ISO를 마우스 오른쪽 버튼으로 클릭하고 인스턴스(예를 들면 드라이브 E)에 탑재합니다.
 4. 드라이브 E:\에서 드라이브 D:\로 ISO의 내용을 복사합니다.
 5. 2단계에서 생성한 6GB 볼륨의 EBS 스냅샷을 생성합니다.

제한 사항

- 이 업그레이드는 Windows 인증을 사용하여 SQL Server에서만 수행할 수 있습니다.
- 인스턴스에서 대기 중인 보안 패치 업데이트가 없는지 확인합니다. 제어판을 열고 나서 업데이트 확인을 선택합니다.
- HA 및 미러링 모드의 SQL 서버 배포는 지원되지 않습니다.

파라미터

- `IamInstanceProfile`

유형: 문자열

설명: (필수) IAM 인스턴스 프로파일입니다.

- `InstanceId`

유형: 문자열

설명: (필수) Windows Server 2008 R2 이상 및 SQL Server 2008 이상을 실행 중인 인스턴스입니다.

- KeepPreUpgradeImageBackUp

유형: 문자열

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

- SubnetId

유형: 문자열

설명: (필수) 업그레이드 프로세스에 대한 서브넷을 제공합니다. 서브넷에 AWS 서비스, Amazon S3 및 Microsoft(패치를 다운로드하기 위해)에 대한 아웃바운드 연결이 있는지 확인합니다.

- SQLServerSnapshotId

유형: 문자열

설명: (조건) 대상 SQL Server 설치 미디어의 스냅샷 ID입니다. 이 파라미터는 BYOL SQL Server 버전을 사용하는 인스턴스에 필요합니다. 이 파라미터는 SQL Server 라이선스 포함 인스턴스 (Microsoft SQL Server와 함께 AWS 제공된 Windows Server용 Amazon Machine Image를 사용하여 시작된 인스턴스)의 경우 선택 사항입니다.

- RebootInstanceBeforeTakingImage

유형: 문자열

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

- TargetSQLVersion

유형: 문자열

설명: (선택 사항) 대상 SQL Server 버전을 선택합니다.

가능한 대상:

- SQL Server 2019
- SQL Server 2017

- SQL Server 2016
- SQL Server 2014

기본 대상: SQL Server 2016

출력

AMIId: SQL Server 최신 버전으로 업그레이드된 인스턴스에서 생성된 AMI의 ID입니다.

AWSEC2-CloneInstanceAndUpgradeWindows

설명

2008 R2, Windows Server 2012 R2, 2016, 2019 또는 2022 인스턴스에서 Amazon Machine Image (AMI)를 생성한 다음을 Windows Server 2016, 2019, 2022 또는 2025AMI로 업그레이드합니다. 지원되는 업그레이드 경로는 다음과 같습니다.

- Windows Server 2008 R2~Windows Server2016.
- 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 2016~Windows Server2025.
- Windows Server 2019에서 Windows Server 2022로
- Windows Server 2019~Windows Server2025.
- Windows Server 2022~Windows Server2025.

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 SubnetId의 새로 생성된 AMI에서 임시 인스턴스를 시작합니다. 원래 인스턴스와 연결된 보안 그룹이 임시 인스턴스에 적용됩니다. 이제 자동화는 임시 인스턴스에서 TargetWindowsVersion에 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 위

치 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, 2019 또는 2022 Standard 및 Datacenter 에디션

사전 조건

- TLS 버전 1.2.
- 인스턴스에 SSM Agent가 설치되었는지 확인합니다. 자세한 내용은 [Windows Server용 EC2 인스턴스에 SSM Agent 설치 및 구성](#)을 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 SubnetId를 지정하는 것이 좋습니다.
- 인스턴스 서브넷에는 Amazon S3 AWS 서비스와 같은에 대한 액세스와 Microsoft에서 패치를 다운로드할 수 있는 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, 2019 및 2022 인스턴스에서만 작동합니다.
- Systems Manager에 필요한 권한을 제공하는 AWS Identity and Access Management (IAM) 인스턴스 프로파일Windows Server로 인스턴스를 구성합니다. 자세한 내용은 [Systems Manager용 IAM 인스턴스 프로파일 생성](#)을 참조하세요.
- 인스턴스의 부트 디스크에 20GB의 사용 가능한 디스크 공간이 있는지 확인합니다.

- 인스턴스가 AWS제공 Windows 라이선스를 사용하지 않는 경우 2012 R2 설치 미디어가 포함된 Amazon EBS 스냅샷 ID Windows Server를 지정합니다. 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.
- Windows Server 2025년 업그레이드의 경우 소스 인스턴스는 [Nitro 기반](#)이어야 합니다.

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)

파라미터

- AlternativeKeyPairName

유형: 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.

- BYOLWindowsMediaSnapshotId

유형: 문자열

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

- `IamInstanceProfile`

유형: 문자열

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

- `InstanceId`

유형: 문자열

설명: (필수) 2008 R2, 2012 R2, 2016, 2019 또는 2022를 실행하는 EC2 인스턴스입니다. Windows Server R2

- `KeepPreUpgradeImageBackUp`

유형: 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`

유형: 문자열

설명: (필수) 업그레이드 프로세스를 위한 서브넷으로, 소스 EC2 인스턴스가 상주합니다. 서브넷에 AWS 서비스, Amazon S3 및 Microsoft에 대한 아웃바운드 연결이 있는지 확인합니다(패치를 다운로드하려면).

- `TargetWindowsVersion`

유형: 문자열

설명: (필수) 대상 Windows 버전을 선택합니다.

기본값: 2025

- `RebootInstanceBeforeTakingImage`

유형: 문자열

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

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 사용](#)을 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.

- S3BucketLog

유형: 문자열

설명: (선택 사항) 명령 출력 응답을 저장하는 데 사용할 Amazon S3 버킷의 이름입니다. 소유한 버킷 또는 공유된 버킷을 지정할 수 있습니다. 이 파라미터를 제공하는 경우 runCommandAssumeRole도 제공해야 합니다.

- runCommandAssumeRole

유형: 문자열

설명: (선택 사항) 인스턴스에서 명령을 실행하는 데 사용할 IAM 역할의 ARN입니다. 역할은 ssm.amazonaws.com 서비스 보안 주체와 신뢰 관계가 있어야 하며, AmazonSSMManagedInstanceCore 정책이 연결되어 있어야 하고, S3BucketLog에 지정된 Amazon S3 버킷에 대한 쓰기 권한이 있어야 합니다.

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.

온프레미스 SQL Server 데이터베이스의 백업과 복원을 SQL Server 2017 Linux를 실행하는 EC2 인스턴스로 자동화하려면 AWS서명된 PowerShell 스크립트를 사용할 수 있습니다. [MigrateSQLServerToEC2Linux](#).

⚠ 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

사전 조건

이 자동화를 실행하려면, 다음 필수 조건을 충족해야 합니다.

- 이 자동화를 실행하는 IAM 사용자 또는 역할에는 [필수 IAM 권한](#)에 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 생성](#)을 참조하세요.
 - SSM Agent가 EC2 인스턴스에 설치되어야 합니다. 자세한 내용은 [Linux용 EC2 인스턴스에 SSM Agent 설치 및 구성](#)을 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 기능](#)을 참조하세요.

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.

기본 값: 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.

기본 값: 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. 서브넷에는 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.

기본 값: 100

필수 IAM 권한

실행서를 성공적으로 사용하려면 AutomationAssumeRole 파라미터에 다음 작업이 필요합니다.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "ec2:CreateTags",
        "ec2:DescribeImages",
        "ec2:DescribeInstanceStatus",
        "ec2:DescribeInstances",
        "ec2:RebootInstances",
        "ec2:RunInstances",
        "ssm:DescribeInstanceInformation",
        "ssm:GetAutomationExecution",
        "ssm:ListCommandInvocations",
        "ssm:ListCommands",
        "ssm:SendCommand",
        "ssm:StartAutomationExecution"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": "iam:PassRole",
      "Resource": "arn:aws:iam::111122223333:role/ROLENAME"
    }
  ]
}
```

}

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 로 설정true하면 자동화가에서 관리하지 AWS Systems Manager않지만 인스턴스를 중지하고 시작해야 하는 인스턴스를 성공적으로 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 라이선스](#)를 참조하십시오.

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 true로 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 true로 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 SelectedInstanceSubnet을 사용하고, 새 VPC를 생성하려면 CreateNewVPC를 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-StartEC2RescueWorkflow에서 필요한 권한을 참조하세요.

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:runCommand를 실행하여 Windows 정품 인증을 수정하는 PowerShell 스크립트를 실행합니다.
 - b. (오프라인 정품 인증 수정) 입력 인스턴스가 관리형 인스턴스가 아닌 경우:
 - i. aws:assertAwsResourceProperty - AllowOffline 플래그가 true으로 설정되었는지 확인합니다. 만일 그렇다면 오프라인 수정이 시작되며, 그렇지 않은 경우 자동화가 종료됩니다.
 - ii. aws:executeAutomation - Windows 정품 인증 오프라인 수정 스크립트를 사용하여 AWSSupport-StartEC2RescueWorkflow를 호출합니다. 이 스크립트는 OS 버전에 따라 EC2Config 또는 EC2Launch 중 하나를 사용합니다.
 - iii. aws:executeAwsApi - AWSSupport-StartEC2RescueWorkflow에서 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 연

결을 분석합니다. IPv6는 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.
- 지정된 VPC에 AWS PrivateLink 엔드포인트가 AWS 서비스 있는지 확인합니다. 엔드포인트가 발견되면, 자동화가 privateDns 속성이 켜져 있는지 확인합니다.
- AWS PrivateLink 엔드포인트가 기본 엔드포인트 정책을 사용하고 있는지 확인합니다.

고려 사항

- 소스와 대상 간의 분석 실행당 요금이 부과됩니다. 자세한 내용은 [Amazon VPC 요금](#)을 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 할당량](#)을 참조하세요.
- 프록시, 로컬 DNS 해석기 또는 호스트 파일 사용과 같은 운영 체제 수준 구성은 Reachability Analyzer가 PASS를 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

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.

- 소스

유형: 문자열

설명: (필수) 접근성을 분석하려는 Amazon EC2 인스턴스 또는 네트워크 인터페이스의 ID입니다.

- ServiceEndpoint

유형: 문자열

설명: (필수) 접근성을 분석하려는 서비스 엔드포인트의 호스트 이름입니다.

- RetainVpcReachabilityAnalysis

유형: 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 인스턴스 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 Business + Support, Enterprise Support 또는 통합 운영 구독이 필요합니다. 자세한 내용은 [AWS Support 플랜 비교](#)를 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 시작](#)을 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) yes을 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.large`는 `m5a.large`로 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) 로 설정하면 `yes` 실행서는 CloudFormation 스택의 일부인 인스턴스에서 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) yes로 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 지정](#)을 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 상태가 running, 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 `stopping`인 경우, Amazon EC2 인스턴스가 완전히 중지될 때까지 자동화가 `aws:waitForAwsResourceProperty`를 실행합니다.
 - b. `running` 또는 `pending`인 경우, Amazon EC2 인스턴스가 상태 검사를 통과할 때까지 자동화가 `aws:waitForAwsResourceProperty`를 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 않은지 확인합니다. 일부 제품은 일부 인스턴스 유형에서는 사용할 수 없습니다.
7. `aws:branch`: 자동화가 Amazon EC2 인스턴스가 CloudFormation 스택의 일부인지 확인할지 여부에 따라 자동화를 분기합니다.
 - a. `aws:cloudformation:stack-name` 태그가 인스턴스에 적용되면 자동화가 실행 `aws:assertAwsResourceProperty`되어 인스턴스가 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.

- 17aws:changeInstanceState: Amazon EC2 인스턴스를 중지합니다.
- 18aws:changeInstanceState: 중지 상태에서 멈춘 경우, 인스턴스를 강제로 중지합니다.
- 19aws:executeAwsApi: 인스턴스 유형을 대상 AMD 인스턴스 유형으로 변경합니다.
- 20aws:sleep: 최종 일관성을 위해 인스턴스 유형을 변경한 후 3초 동안 기다립니다.
- 21aws:branch: 이전 인스턴스 상태를 기반으로 자동화를 분기합니다. 해당 내용이 running이었을 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.
- 22aws: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` - 지정된 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-CloneXenEC2InstanceAndMigrateToNitro

설명

AWSSupport-CloneXenEC2InstanceAndMigrateToNitro 실행서는 현재 Amazon EC2 Xen 플랫폼에서 실행 중인 복제된 Amazon Elastic Compute Cloud(Amazon EC2) Linux 인스턴스를 Amazon EC2 Nitro 플랫폼에서 실행하도록 복제, 준비 및 마이그레이션합니다. [Amazon EC2](#) 이 자동화는 세 가지 브랜치로 나뉩니다.

- 예비 검사: 대상 Amazon EC2 인스턴스가 Nitro 플랫폼에서 이미 실행 중인지 확인하고, 수명 주기 상태를 결정하고, 운영 체제를 검증하고, Systems Manager 연결을 확인하는 등 마이그레이션을 진행하기 위한 모든 사전 조건을 평가합니다.
- 테스트: 대상 Amazon EC2 인스턴스AMI에서 테스트를 생성하고 테스트 Amazon EC2 인스턴스를 시작하여 계속하기 전에 마이그레이션 프로세스를 검증합니다.

- CloneAndMigrate: 대상 Amazon EC2 인스턴스의 복제본을 생성하고, 필요한 드라이버를 설치하고, Nitro 플랫폼용 시스템을 구성하고, 인스턴스 유형을 원하는 Nitro 유형으로 변경합니다.

⚠ Important

대상 Amazon EC2 인스턴스를 중지하기 위한 승인을 제공하기 전에 인스턴스에서 실행 중인 모든 애플리케이션이 정상적으로 닫혀 있는지 확인합니다. Amazon EC2 인스턴스에 탄력적 IP 주소가 연결되어 있지 않으면 인스턴스가 중지되고 시작되면 자동 퍼블릭 IPv4 주소가 변경됩니다.

⚠ Important

고지 사항: 이 실행서를 실행하면 Amazon EC2 인스턴스, Amazon EBS 볼륨 및에 대해 계정에 추가 요금이 발생할 수 있습니다. 자세한 내용은 [Amazon EC2 요금](#) 및 [Amazon EBS 요금](#)을 참조하세요.

⚠ Important

사전 조건

대상 Amazon EC2 인스턴스는 필요한 경우 패키지 관리자를 unzip 사용하여 kernel-devel, gcc, patch, rpm-build, wget, linux-headers, 등의 드라이버 및 종속성을 설치하기 위해 dracut make리포지토리에 대한 아웃바운드 액세스가 필요합니다.

지원되는 운영 체제

- Red Hat Enterprise Linux(RHEL) 8 및 9
- Amazon Linux 2 및 AL2023
- Ubuntu Server 18.04 LTS, 20.04 및 22.04
- Debian 11 및 12(AWS 파티션만 해당)
- SUSE12SP5 및 SUSE15SP(5,6)

어떻게 작동하나요?

실행서는 다음과 같은 상위 수준 단계를 수행합니다.

- 사전 조건을 검증하고 인스턴스가 마이그레이션에 적합한지 확인합니다.
- 마이그레이션이 성공AMI할 수 있도록를 생성하고 테스트합니다.
- 향상된 네트워킹(ENA) 속성을 활성화하고 최신 ENA 드라이버를 설치합니다.
- initramfs에서 NVMe 모듈을 확인하고 구성합니다.
- /etc/fstab을 분석하고 수정하여 디바이스 이름을 UUIDs.
- 예측 가능한 인터페이스 이름 지정을 비활성화하고 영구 네트워크 규칙을 제거합니다.
- 복제된 인스턴스 유형을 원하는 Nitro 유형으로 변경합니다.
- Nitro 인스턴스를 시작하기 위한 Golden Image로 사용할 수 AMI 있는 최종를 생성합니다.

[이 자동화 실행\(콘솔\)](#)

문서 유형

자동화

소유자

Amazon

플랫폼

Linux

파라미터

필수 IAM 권한

실행서를 성공적으로 사용하려면 AutomationAssumeRole 파라미터에 다음 작업이 필요합니다.

- autoscaling:DescribeAutoScalingInstances
- ec2:CreateImage
- ec2:CreateTags
- ec2:DescribeImages
- ec2:DescribeInstanceAttribute
- ec2:DescribeInstances
- ec2:DescribeInstanceStatus

- ec2:DescribeInstanceTypeOfferings
- ec2:DescribeInstanceTypes
- ec2:DeregisterImage
- ec2:ModifyInstanceAttribute
- ec2:RunInstances
- ec2:StartInstances
- ec2:StopInstances
- ec2:TerminateInstances
- iam:PassRole
- sns:Publish
- ssm:DescribeAutomationExecutions
- ssm:DescribeInstanceInformation
- ssm:SendCommand

IAM 정책 예제:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "autoscaling:DescribeAutoScalingInstances",
        "ec2:CreateImage",
        "ec2:CreateTags",
        "ec2:DescribeImages",
        "ec2:DescribeInstanceAttribute:",
        "ec2:DescribeInstances",
        "ec2:DescribeInstanceStatus",
        "ec2:DescribeInstanceTypes",
        "ec2:DeregisterImage",
        "ec2:ModifyInstanceAttribute",
        "ec2:RunInstances",
        "ec2:StartInstances",
        "ec2:StopInstances",
        "ec2:TerminateInstances",
```

```

        "iam:PassRole",
        "ssm:DescribeAutomationExecutions",
        "ssm:DescribeInstanceInformation",
        "ssm:SendCommand"
    ],
    "Resource": "*"
}
]
}

```

지침

다음 단계에 따라 자동화를 구성합니다.

1. Systems Manager [AWSSupport-CloneXenEC2InstanceAndMigrateToNitro](#)의 문서로 이동합니다.
2. **Execute automation**을 선택합니다.
3. 입력 파라미터에 다음을 입력합니다.
 - AutomationAssumeRole(선택 사항):
 - 설명: (선택 사항) Systems Manager Automation이 사용자를 대신하여 작업을 수행할 수 있도록 허용하는 AWS Identity and Access Management (IAM) 역할의 ARN입니다. 역할을 지정하지 않은 경우, Systems Manager Automation에서는 이 실행서를 시작하는 사용자의 권한을 사용합니다.
 - 유형: `AWS::IAM::Role::Arn`
 - TargetInstanceId(필수):
 - 설명: (필수) Nitro 플랫폼으로 마이그레이션하려는 대상 Amazon EC2 인스턴스의 인스턴스 ID입니다.
 - 유형: `AWS::EC2::Instance::Id`
 - NitroInstanceType(선택 사항):
 - 설명: (선택 사항) 대상 Nitro 인스턴스 유형을 입력합니다. Nitro M5, M6, C5, C6, R5, R6 및 T3 인스턴스만 지원됩니다(예: t3.small). 기본값: m5.xlarge.
 - 유형: `String`
 - 허용된 패턴: `^(m5a?z?d?n?|c5a?d?n?|r5a?d?n?b?|(c|m|r)6(a|i)?d?)\\.(2|4|8|12|16|24|32)?xlarge$|^t3a?\\.(x|x2|x3)?large|nano|micro|small|medium)$`

- 기본값: m5.xlarge
- SNSTopicArn(필수):
 - 설명: (필수) 승인 알림을 위해 Amazon SNS 주제의 ARN을 제공합니다. 이 Amazon SNS 주제는 자동화 실행 중에 승인 알림을 보내는 데 사용됩니다.
 - 유형: String
 - 허용된 패턴: `^arn:(aws|aws-cn|aws-us-gov|aws-iso(-[a-z]))?:sns:(us(-gov|-isob)?|ap|ca|af|me|cn|eu|sa)-(central|(north|south)?(east|west)?)-\\d:\\d{12}:[a-zA-Z0-9_.-]{1,256}$`
- ApproverIAM(필수):
 - 설명: (필수) 작업을 승인하거나 거부할 수 있는 AWS 인증된 보안 주체 목록을 제공합니다. 최대 승인자 수는 10명입니다.
 - 유형: StringList
 - 허용된 패턴: `^[a-zA-Z0-9_+,.@\\-\\/] {1,128}$|^arn:(aws|aws-cn|aws-us-gov|aws-iso(-[a-z]))?:(sts|iam)::[0-9]{12}:[a-zA-Z0-9_+,.@\\-\\/] {1,256}$`
- MinimumRequiredApprovals(선택 사항):
 - 설명: (선택 사항) 자동화를 재개하는 데 필요한 최소 승인 수입니다. 기본값: 1.
 - 유형: 정수
 - 기본값: 1
- DeleteResourcesOnFailure(선택 사항):
 - 설명: (선택 사항) 복제된 Amazon EC2 인스턴스를 종료할지 여부와 자동화가 실패할 AMI 경우.
 - 유형: Boolean
 - 허용된 값: [true, false]
 - 기본값: true
- 승인(필수):
 - 설명: (필수)이 자동화 실행서에서 수행하는 작업의 전체 세부 정보를 읽고 단계를 승인하면 '예, 이해하고 승인합니다'라고 작성하세요.
 - 유형: String
 - 허용된 패턴: `^Yes, I understand and acknowledge$`
- AllowInstanceStoreInstances(선택 사항):

- 설명: (선택 사항) 사용자가 yes을 지정하는 경우, 실행서는 인스턴스 스토어 볼륨이 연결된 인스턴스에서 실행됩니다. 경고: 인스턴스가 중지되면 인스턴스 스토어 볼륨의 데이터가 손실됩니다. 이 파라미터는 우발적인 데이터 손실을 방지하는 데 도움이 됩니다.
- 유형: Boolean
- 허용된 값: [yes, no]
- 기본값: no

4. 실행을 선택합니다.

5. 자동화가 시작됩니다.

6. 문서는 다음 단계를 수행합니다.

- **checkConcurrency:**

현재 Amazon EC2 인스턴스를 대상으로 하는 이 실행서의 실행이 하나만 있는지 확인합니다.

- **getTargetInstanceProperties:**

대상 Amazon EC2 인스턴스의 세부 정보를 가져옵니다.

- **checkIfNitroInstanceTypeIsSupportedInAZ:**

대상 Nitro 인스턴스 유형이 대상 Amazon EC2 인스턴스와 동일한 가용 영역에서 지원되는지 여부를 결정합니다.

- **createTestImage:**

제공된 인스턴스AMI에서 테스트를 생성합니다.

- **launchTestInstanceInSameSubnet:**

대상 Amazon EC2 인스턴스와 동일한 구성을 AMI 사용하여 테스트에서 테스트 Amazon EC2 인스턴스를 시작합니다.

- **approvalToStopTargetInstance:**

지정된 보안 주체가 대상 인스턴스를 중지할 때까지 기다립니다.

- **createBackupImage:**

백업을 위해 제공된 인스턴스AMI에서 생성합니다.

- **launchInstanceInSameSubnet:**

소스 Amazon EC2 인스턴스와 동일한 구성을 AMI 사용하여 백업에서 새 Amazon EC2 인스턴스를 시작합니다.

- **checkAndInstallENADrivers:**

Amazon EC2 인스턴스에서 향상된 네트워킹 어댑터(ENA) 드라이버의 가용성을 결정하고 누락된 경우를 설치합니다.

- **checkAndAddNVMEDrivers:**

복제된 Amazon EC2 인스턴스에서 NVMe 드라이버의 가용성을 결정하고 누락된 경우를 설치합니다.

- **checkAndModifyFSTABEntries:**

디바이스 이름이에서 사용되는지 여부를 결정/etc/fstab하고 찾은 경우 UUIDs로 바꿉니다.

- **setNitroInstanceTypeForClonedInstance:**

복제된 Amazon EC2 인스턴스에 대해 제공된 대상 Amazon EC2 인스턴스 유형을 설정합니다.

- **approvalForCreatingImageAfterDriversInstallation:**

복제된 Amazon EC2 인스턴스가 Nitro 플랫폼에서 성공적으로 부팅되면 사용자 승인을 기다립니다.

- **createImageAfterDriversInstallation:**

새 Amazon EC2 인스턴스가 Nitro 플랫폼에서 성공적으로 부팅된 경우에만 새 Amazon EC2 인스턴스에서 이미지를 생성합니다.

7. 완료되면 출력 섹션에서 실행의 자세한 결과를 검토합니다.

참조

AWS Systems Manager 자동화

- [이 자동화 실행\(콘솔\)](#)
- [자동화 실행](#)
- [Automation 설정](#)
- [자동화 워크플로 지원](#)

AWSSupport-CollectSAPHANALogs

설명

AWSsupport-CollectSAPHANALogs 실행서는 AWS 배포 시 SAP의 일부인 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스의 SAP HANA에서 시스템 로그를 수집합니다. Amazon EC2 인스턴스는 AWS Systems Manager (Systems Manager)에서 관리해야 합니다. 실행서는 필수 패키지를 확인하고 누락된 경우 이를 설치하며, 감지된 운영 체제에 적합한 로그 수집 도구를 실행하고, 선택적으로 수집된 로그를 Amazon Simple Storage Service(Amazon S3) 버킷에 업로드합니다.

 Important

이 실행서는 /var/log 파티션에 최소 200MB의 사용 가능한 디스크 공간이 필요합니다. 이 실행서를 실행하면 대상 Amazon EC2 인스턴스에 추가 패키지가 설치될 수 있습니다. Acknowledgement 파라미터를 로 설정하여 이를 승인해야 합니다Yes. Amazon S3에 로그를 저장하면 표준 Amazon S3 스토리지 및 요청 요금이 발생합니다.

지원되는 운영 체제

- Red Hat Enterprise Linux 8.4 이상
- SUSE Linux Enterprise Server 12 SP5
- SUSE Linux Enterprise Server 15 SP3 이상

누락된 경우 설치된 패키지

SUSE Linux Enterprise Server:

- supportutils
- yast2-support
- supportutils-plugin-suse-public-cloud
- supportutils-plugin-ha-sap
- crmsh
- unzip
- curl
- aws-cli (선택 사항, InstallAWSCLI가 로 설정된 경우 설치됨Yes)

Red Hat Enterprise Linux:

- sos

- `crm_report`
- `unzip`
- `curl`
- `aws-cli` (선택 사항, InstallAWSCLI가 로 설정된 경우 설치됨Yes)

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: `AWS::EC2::Instance::Id`

설명: (필수) 로그를 수집해야 하는 SAP 워크로드를 실행하는 Amazon EC2 인스턴스의 ID입니다.

- `확인`

유형: 문자열

유효한 값: Yes

설명: (필수)이 실행서는 로그 수집을 위해 대상 Amazon EC2 인스턴스에 추가 패키지를 설치할 수 있음을 확인합니다.

- S3LogDestination

유형: AWS::S3::Bucket::Name

설명: (선택 사항) 로그가 업로드되는 Amazon S3 버킷의 이름입니다. 버킷은 퍼블릭이 아니어야 하며 동일한 AWS 계정에 속해야 합니다. 제공되지 않으면 로그가 인스턴스 로컬 스토리지에 저장됩니다.

- S3Prefix

유형: 문자열

기본값: AWSSupport-CollectSAPHANALogs

허용되는 패턴: ^\$|^([a-zA-Z0-9][-. /a-zA-Z0-9]{0,255})\$

설명: (선택 사항) 로그가 저장되는 Amazon S3 버킷 접두사입니다. 제공되지 않은 경우 기본값은 `AWSSupport-CollectSAPHANALogs`.

- InstallAWSCLI

유형: 문자열

유효한 값: Yes | No

기본값: 아니요

설명: (선택 사항) 인스턴스에 AWS CLI를 설치할지 여부입니다. Yes인 경우 실행서는 아직 없는 경우 AWS CLI를 설치합니다.

필수 IAM 권한

실행서를 성공적으로 사용하려면 `AutomationAssumeRole` 파라미터에 다음 작업이 필요합니다.

- `ssm:DescribeInstanceInformation`
- `ssm:SendCommand`
- `ssm:GetCommandInvocation`
- `s3:GetBucketPublicAccessBlock`

- s3:GetBucketAcl
- s3:GetBucketLocation
- s3:GetBucketOwnershipControls
- s3:GetEncryptionConfiguration
- s3:PutObject

문서 단계

1. AssertInstanceIsSSMManaged - 대상 Amazon EC2 인스턴스가 Systems Manager에서 관리되고 PingStatus의가 있는지 확인합니다Online. 인스턴스를 관리하지 않으면 실행서가 취소됩니다.
2. GetInstanceInformation - 적절한 로그 수집 방법을 결정하는 데 사용되는 플랫폼 이름을 포함하여 지정된 Amazon EC2 인스턴스에 대한 정보를 검색합니다.
3. CollectLogs - 인스턴스에서 셸 스크립트를 실행하여 로그를 수집합니다. SUSE Linux Enterprise Server 인스턴스의 경우 스크립트는 supportconfig. Red Hat Enterprise Linux 인스턴스의 경우를 사용합니다sos report. HA 클러스터의 경우 스크립트는 crm report 명령을 사용하여 지난 7일 동안의 추가 HA 로그도 수집합니다. 누락된 경우 필수 패키지가 설치됩니다.
4. BranchOnS3BucketProvided - Amazon S3 버킷이 제공되었는지 여부에 따라 실행을 분기합니다S3LogDestination. 버킷이 제공되지 않은 경우 실행서는 건너뛰니다GenerateReport. 그렇지 않으면 로 진행됩니다CheckS3BucketPublicStatus.
5. CheckS3BucketPublicStatus -에 지정된 Amazon S3 버킷S3LogDestination이 서버 측 암호화(SSE)로 구성되어 있는지, 익명 또는 퍼블릭 읽기 또는 쓰기 액세스 권한을 허용하는지 확인합니다. 또한 실제 버킷 소유자가 예상 버킷 소유자와 동일한지 확인합니다. 이 단계가 실패하면 런북은 업로드GenerateReport하지 않고 계속됩니다.
6. UploadLogstoS3 - 수집된 로그를 지정된 Amazon S3 버킷에 업로드합니다. InstallAWSCLI이로 설정되어 Yes 있고 AWS CLI가 설치되지 않은 경우 스크립트는 업로드하기 전에 AWS CLI를 설치합니다.
7. GenerateReport - 로그 수집 프로세스에 대한 보고서를 생성합니다. Amazon S3 버킷이 제공된 경우 로그가 업로드된 Amazon S3 버킷 이름과 접두사가 포함됩니다. 그렇지 않으면 로그가 인스턴스에 로컬로 저장되었음을 나타냅니다. 또한 이전 단계가 실패한 이유도 보고합니다.

출력

GenerateReport.Summary - 로그 수집 결과의 요약입니다.

`GenerateReport.LogLocation` - 로그가 저장된 위치, 인스턴스의 로컬 경로 또는 Amazon S3 URI.

`GenerateReport.Status` - 로그 수집 실행의 전체 상태입니다.

지침

다음 단계에 따라 자동화를 구성합니다.

1. Systems Manager [AWSSupport-CollectSAPHANALogs](#)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 IAM 역할의 ARN입니다. 역할이 지정되지 않은 경우 Systems Manager Automation은 이 실행서를 시작하는 사용자의 권한을 사용합니다.

- InstanceID(필수):

SAP 워크로드를 실행하는 Amazon EC2 인스턴스의 ID입니다.

- 승인(필수):

를 입력하여 실행서가 대상 Amazon EC2 인스턴스에 추가 패키지를 설치할 수 있음을 Yes 확인합니다.

- S3LogDestination(선택 사항):

로그를 업로드할 Amazon S3 버킷의 이름입니다. 제공되지 않으면 로그가 인스턴스에 로컬로 저장됩니다.

- S3Prefix(선택 사항):

저장된 로그의 Amazon S3 버킷 접두사입니다. 기본값은 `AWSSupport-CollectSAPHANALogs`입니다.

- InstallAWSCLI(선택 사항):

인스턴스에 없는 경우 AWS CLI를 자동으로 설치Yes하려면 선택합니다. 기본값은 No입니다.

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

- **AssertInstanceIsSSMManaged**

대상 Amazon EC2 인스턴스가 Systems Manager에서 관리되고 PingStatus의가 있는지 확인합니다Online.

- **GetInstanceInformation**

플랫폼 이름을 포함하여 지정된 Amazon EC2 인스턴스에 대한 정보를 검색합니다.

- **CollectLogs**

셸 스크립트를 실행하여 용 SLES 또는 supportconfig용를 사용하여 로그sos report를 수집합니다RHEL. HA 클러스터의 경우는를 사용하여 지난 7일간의 HA 로그도 수집합니다crm report.

- **BranchOnS3BucketProvided**

Amazon S3 버킷이 제공되지 않은 GenerateReport 경우 로 건너뛰고, 그렇지 않으면 로 진행합니다CheckS3BucketPublicStatus.

- **CheckS3BucketPublicStatus**

Amazon S3 버킷에 SSE가 활성화되어 있고, 퍼블릭 액세스를 허용하지 않으며, 동일한 AWS 계정이 소유하고 있는지 확인합니다.

- **UploadLogsToS3**

수집된 로그를 지정된 Amazon S3 버킷에 업로드합니다. InstallAWSCLI가 Yes 있고 아직 없는 경우 AWS CLI를 설치합니다.

- **GenerateReport**

로그 위치 및 모든 단계 실패를 포함하여 로그 수집 결과의 요약을 생성합니다.

7. 완료 후 출력 섹션에서 실행의 자세한 결과를 검토합니다.

참조

Systems Manager Automation

- [이 자동화 실행\(콘솔\)](#)
- [자동화 실행](#)
- [Automation 설정](#)
- [Support Automation Workflows 랜딩 페이지](#)

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 설명서 [의 인스턴스 메타데이터 서비스 구성](#)을 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.

- EnforceIMDSv2

유형: 문자열

유효한 값: required | optional

기본값: optional

설명: (선택 사항) IMDSv2를 강제 시행합니다. required을 선택하는 경우, Amazon EC2 인스턴스는 IMDSv2만 사용하게 됩니다. optional을 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 설명서 [의 인스턴스 메타데이터 서비스 구성](#)을 참조하세요.

- HttpPutResponseHopLimit

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

유형: 문자열

설명: (필수) 구성하려는 메타데이터 설정이 있는 Amazon EC2 인스턴스의 ID입니다.

- MetadataAccess

유형: 문자열

유효한 값: enabled | disabled

기본값: enabled

설명: (선택 사항) Amazon EC2 인스턴스에서 인스턴스 메타데이터 액세스를 허용하거나 거부합니다. disabled을 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. branchOnMetadataAccess - MetadataAccess 파라미터 값을 기반으로 자동화를 분기합니다.
2. disableMetadataAccess- ModifyInstanceMetadataOptions API 작업을 호출하여 메타데이터 엔드포인트 액세스를 비활성화합니다.
3. branchOnHttpPutResponseHopLimit - HttpPutResponseHopLimit 파라미터 값을 기반으로 자동화를 분기합니다.
4. maintainHopLimitAndConfigureImdsVersion - HttpPutResponseHopLimit이 0이면, 현재 홉 제한치를 유지하고 기타 메타데이터 옵션을 변경합니다.
5. waitBeforeAssertingIMDSv2State - IMDSv2 상태를 단정하기 전에 30초 동안 기다립니다.
6. setHopLimitAndConfigureImdsVersion - HttpPutResponseHopLimit이 0보다 크면, 지정된 입력 파라미터를 사용하여 메타데이터 옵션을 구성합니다.
7. waitBeforeAssertingHopLimit -메타데이터 옵션을 단정하기 전에 30초 동안 기다립니다.
8. assertHopLimit - HttpPutResponseHopLimit 속성이 지정한 값으로 설정되어 있음을 단정합니다.
9. branchVerificationOnIMDSv2Option - EnforceIMDSv2 파라미터 값을 기반으로 검증을 분기합니다.
- 10assertIMDSv2IsOptional - HttpTokens 값이 optional로 설정되어 있음을 단정합니다.
- 11assertIMDSv2IsEnforced - HttpTokens 값이 required로 설정되어 있음을 단정합니다.

12.waitBeforeAssertingMetadataState - 메타데이터 상태가 비활성화되어 있음을 단정하기 전에 30초 동안 기다립니다.

13.assertMetadatalIsDisabled - 메타데이터가 disabled임을 단정합니다.

14.describeMetadataOptions - 지정한 변경 내용이 적용된 후 메타데이터 옵션을 가져옵니다.

출력

describeMetadataOptions.State

describeMetadataOptions.MetadataAccess

describeMetadataOptions.IMDSv2

describeMetadataOptions.HttpPutResponseHopLimit

AWSSupport-ContainEC2Instance

설명

AWSSupport-ContainEC2Instance 실행서는 [잠재적으로 손상되거나 의심스러운 상황에 직면했을 때 Amazon EC2 인스턴스를 격리하려면 어떻게 해야 합니까?](#) 문서에 설명된 절차에 대한 자동화된 솔루션을 제공합니다. 자동화는 지정한 값에 따라 분기됩니다.

어떻게 작동하나요?

이 Automation 실행서는 일련의 조정된 단계를 통해 Amazon EC2 인스턴스의 네트워크 액세스를 AWSSupport-ContainEC2Instance 수행합니다. Contain 모드에서 실행되면 먼저 입력 파라미터를 검증하고 인스턴스가 종료되지 않았는지 확인합니다. 그런 다음 이후 복원을 위해 현재 보안 그룹 구성을 Amazon S3 버킷에 백업합니다. 실행서는 임시 "모든 액세스" 보안 그룹과 최종 "컨테이너먼트" 보안 그룹의 두 보안 그룹을 생성합니다. 인스턴스의 네트워크 인터페이스를 원래 보안 그룹에서 모든 액세스 보안 그룹으로, 마지막으로 격리 보안 그룹으로 점진적으로 전환합니다. 지정된 경우 인스턴스의 암호화되지 않은 백업과 암호화된 AMI 백업을 모두 생성합니다. Auto Scaling 그룹의 인스턴스의 경우 필요한 Auto Scaling 그룹 수정을 처리하고 인스턴스를 대기 상태로 전환합니다. Release 모드에서 실행되면 Amazon S3의 백업된 설정을 사용하여 인스턴스를 원래 네트워크 구성으로 복원합니다. 실행서는 실제 변경 없이 작업을 미리 볼 수 있는 DryRun 파라미터를 지원하며, 억제 및 릴리스 워크플로 전반에 걸친 포괄적인 오류 처리 및 보고 메커니즘을 포함합니다.

⚠ Important

- 이 실행서는 보안 그룹 수정, 생성AMI, Auto Scaling 그룹과의 상호 작용 등 승격된 권한이 필요한 다양한 작업을 수행합니다. 이러한 작업은 잠재적으로 권한 상승으로 이어지거나 계정의 다른 워크로드에 영향을 미칠 수 있습니다. AutomationAssumeRole 파라미터에 지정된 역할에 부여된 권한을 검토하고 의도된 사용 사례에 적합한지 확인해야 합니다. IAM 권한에 대한 자세한 내용은 다음 AWS 설명서를 참조하세요 [AWS Identity and Access Management \(IAM\) Permissions](#) [AWS Systems Manager Automation Permissions](#).
- 이 실행서는 워크로드를 사용할 수 없거나 중단시킬 수 있는 변경 작업을 수행합니다. 특히 대상 Amazon EC2 인스턴스와 연결된 보안 그룹을 수정하여 네트워크 연결에 영향을 미칠 수 있습니다. 또한 인스턴스가 Auto Scaling 그룹의 일부인 경우 실행서는 그룹의 구성을 수정하여 조정 동작에 영향을 미칠 수 있습니다.
- 격리 프로세스 중에 이 실행서는 보안 그룹 및와 같은 추가 리소스를 생성합니다AMI. 이러한 리소스는 식별을 위해 태그가 지정되어 있지만, 이러한 리소스의 생성에 대해 알고 격리 프로세스가 완료된 후 적절한 정리 또는 관리를 보장해야 합니다.
- Action 파라미터가 로 설정된 경우 Release 이 실행서는 Amazon EC2 인스턴스의 구성을 원래 상태로 복원하려고 시도합니다. 그러나 복원 프로세스가 실패하여 인스턴스가 일관되지 않은 상태로 유지될 위험이 있습니다. 실행서는 이러한 실패 시 수동 복원에 대한 지침을 제공하지만 복원 프로세스 중에 잠재적 문제를 처리할 준비가 되어 있어야 합니다.

프로덕션 환경에서 실행하기 전에 실행서를 철저히 검토하고, 실행서의 잠재적 영향을 이해하고, 비프로덕션 환경에서 테스트하는 것이 좋습니다.

이 자동화 실행(콘솔)

문서 유형

자동화

소유자

Amazon

플랫폼

/

필수 IAM 권한

실행서를 성공적으로 사용하려면 AutomationAssumeRole 파라미터에 다음 작업이 필요합니다.

- autoscaling:CreateOrUpdateTags
- Autoscaling:DeleteTags
- autoscaling:DescribeAutoScalingGroups
- autoscaling:DescribeAutoScalingInstances
- autoscaling:DescribeTags
- autoscaling:EnterStandby
- autoscaling:ExitStandby
- autoscaling:UpdateAutoScalingGroup
- ec2:AuthorizeSecurityGroupEgress
- ec2:AuthorizeSecurityGroupIngress
- ec2:CopyImage
- ec2:CreateImage
- ec2:CreateSecurityGroup
- ec2:CreateSnapshot
- ec2:CreateTags
- ec2>DeleteSecurityGroup
- ec2>DeleteTags
- ec2:DescribeImages
- ec2:DescribeInstances
- ec2:DescribeSecurityGroups
- ec2:DescribeSnapshots
- ec2:DescribeTags
- ec2:ModifyNetworkInterfaceAttribute
- ec2:RevokeSecurityGroupEgress
- kms:CreateGrant
- kms:DescribeKey
- kms:GenerateDataKeyWithoutPlaintext
- kms:ReEncryptFrom

- kms:ReEncryptTo
- s3:CreateBucket
- s3:DeleteObjectTagging
- s3:GetAccountPublicAccessBlock
- s3:GetBucketAcl
- s3:GetBucketLocation
- s3:GetBucketOwnershipControls
- s3:GetBucketPolicy
- s3:GetBucketPolicyStatus
- s3:GetBucketPublicAccessBlock
- s3:GetObject
- s3:ListBucket
- s3:PutAccountPublicAccessBlock
- s3:PutBucketPolicy
- s3:PutBucketVersioning
- s3:PutObject
- s3:PutObjectTagging

정책 예제:

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "ReadOperations",
      "Effect": "Allow",
      "Action": [
        "autoscaling:DescribeAutoScalingGroups",
        "autoscaling:DescribeAutoScalingInstances",
        "autoscaling:DescribeTags",
        "ec2:DescribeImages",
        "ec2:DescribeInstances",
```

```

    "ec2:DescribeSecurityGroups",
    "ec2:DescribeSnapshots",
    "ec2:DescribeTags",
    "kms:DescribeKey",
    "s3:GetAccountPublicAccessBlock",
    "s3:GetBucketAcl",
    "s3:GetBucketLocation",
    "s3:GetBucketOwnershipControls",
    "s3:GetBucketPolicy",
    "s3:GetBucketPolicyStatus",
    "s3:GetBucketPublicAccessBlock",
    "s3:GetObject",
    "s3:ListBucket"
  ],
  "Resource": "*"
},
{
  "Sid": "WriteOperations",
  "Effect": "Allow",
  "Action": [
    "autoscaling:CreateOrUpdateTags",
    "autoscaling:DeleteTags",
    "autoscaling:EnterStandby",
    "autoscaling:ExitStandby",
    "autoscaling:UpdateAutoScalingGroup",
    "ec2:AuthorizeSecurityGroupEgress",
    "ec2:AuthorizeSecurityGroupIngress",
    "ec2:CopyImage",
    "ec2:CreateImage",
    "ec2:CreateSecurityGroup",
    "ec2:CreateSnapshot",
    "ec2:CreateTags",
    "ec2>DeleteSecurityGroup",
    "ec2>DeleteTags",
    "ec2:ModifyNetworkInterfaceAttribute",
    "ec2:RevokeSecurityGroupEgress",
    "kms:CreateGrant",
    "kms:GenerateDataKeyWithoutPlaintext",
    "kms:ReEncryptFrom",
    "kms:ReEncryptTo",
    "s3:CreateBucket",
    "s3>DeleteObjectTagging",
    "s3:PutAccountPublicAccessBlock",
    "s3:PutBucketPolicy",

```

```

    "s3:PutBucketVersioning",
    "s3:PutObject",
    "s3:PutObjectTagging"
  ],
  "Resource": "*"
}
]
}
```

지침

다음 단계에 따라 자동화를 구성합니다.

1. Systems Manager [AWSSupport-ContainEC2Instance](#)의 문서로 이동합니다.
2. Execute automation(자동화 실행)을 선택합니다.
3. 입력 파라미터에 다음을 입력합니다.
 - AutomationAssumeRole(선택 사항):
 - 설명: (선택 사항) 사용자를 대신하여 Systems Manager Automation을 통해 작업을 수행할 수 있도록 허용하는 AWS AWS Identity and Access Management (IAM) 역할의 Amazon 리소스 이름(ARN)입니다. 역할이 지정되지 않은 경우 Systems Manager Automation은 이 실행서를 시작하는 사용자의 권한을 사용합니다.
 - 유형: AWS::IAM::Role::Arn
 - 작업(필수):
 - 설명: (필수) Amazon EC2 인스턴스를 Contain 격리하거나 이전 백업에서 Amazon EC2 인스턴스 구성 원래 구성을 복원하려고 Restore하려면 선택합니다.
 - 유형: 문자열
 - 허용된 패턴: Contain|Restore
 - DryRun(선택 사항):
 - 설명: (선택 사항) 로 설정하면 true 자동화가 명령을 실행하지 않고, 대신 각 단계를 자세히 설명하면서 시도한 작업을 보고합니다. 기본값: true.
 - 유형: Boolean
 - 허용된 값: true|false
 - CreateAMIBackup(선택 사항):

- 설명: (선택 사항) 로 설정하면 억제 작업을 수행하기 전에 Amazon EC2 인스턴스trueAMI의가 생성됩니다.
- 유형: Boolean
- 허용된 값: true|false
- KmsKey(선택 사항):
 - 설명: (선택 사항) 암호화된 대상 Amazon EC2 인스턴스를 생성하는 데 사용할 AWS KMS 키 AMI의 ID입니다. 기본값은 로 설정됩니다alias/aws/ebs.
 - 유형: 문자열
 - 허용된 패턴: `^(((arn:(aws|aws-cn|aws-us-gov):kms:([a-z]{2}|[a-z]{2}-gov)-[a-z]+-[0-9]{1}:[0-9]{12}:key/)?([a-f0-9]{8}-[a-f0-9]{4}-[a-f0-9]{4}-[a-f0-9]{4}-[a-f0-9]{12}|mrk-[a-f0-9]{32}))|(arn:(aws|aws-cn|aws-us-gov):kms:([a-z]{2}|[a-z]{2}-gov)-[a-z]+-[0-9]{1}:[0-9]{12}:)?alias/.{1,}))$`
- BackupS3BucketName(조건부):
 - 설명: (조건부) Amazon S3 버킷은 Action가 in 경우 구성을 업로드Contain하고가 in 경우 구성을 복원Action합니다Release. 참고: 제공된 버킷이 계정에 없는 경우 자동화는 사용자를 대신하여 Amazon S3 버킷을 생성합니다.
 - 유형: AWS::S3::Bucket::Name
- TagIdentifier(선택 사항):
 - 설명: (선택 사항) 격리 워크플로 중에이 실행서에 의해 생성되거나 수정된 AWS 리소스에 추가Key=BatchId, Value=78925될 형식의 태그입니다. 이 태그를 사용하여 격리 프로세스 중에 연결된 리소스를 식별하고 관리할 수 있습니다. 복원 워크플로 중에이 파라미터로 지정된 태그가 리소스에서 제거됩니다. 참고: 태그 키와 값은 대/소문자를 구분합니다.
 - 유형: 문자열
 - 허용된 패턴: `^$|^([Kk][Ee][Yy]=[\\+\\-\\=\\.\\_\\:\\\\/@a-zA-Z0-9]{1,128},[Vv][Aa][Ll][Uu][Ee]=[\\+\\-\\=\\.\\_\\:\\\\/@a-zA-Z0-9]{0,128})$`
- BackupS3BucketAccess(조건부):
 - 설명: (조건부) 억제 작업을 실행한 후 백업 Amazon S3 버킷에 대한 액세스가 허용되는 IAM 사용자 또는 역할의 ARN입니다. 이 파라미터는이 Action 일 때 필요합니다Contain. 또는이 없는 AutomationAssumeRole경우 자동화가 실행 중인 컨텍스트의 사용자가 목록에 자동으로 추가됩니다.
 - 유형: 문자열

- 허용된 패턴: `^$|^arn:(aws|aws-cn|aws-us-gov|aws-iso(-[a-z]))?:iam::[0-9]{12}:(role|user)\\[/\\w+\\[/=, .@-]+$`
- IngressTrafficRules(선택 사항):
 - 설명: (선택 사항) Amazon EC2 인스턴스에 적용할 형식으로 Cidr, IpProtocol, FromPort 및 ToPort를 사용하여 심표로 구분[{"Cidr": "1.2.3.4/32", "IpProtocol": "tcp", "FromPort": "22", "ToPort": "22"}]된 보안 그룹 수신 규칙 맵입니다. 규칙이 제공되지 않으면 수신 규칙이 없는 보안 그룹이 Amazon EC2 인스턴스에 연결되어 들어오는 트래픽에서 효과적으로 격리됩니다.
 - 유형: MapList
 - 허용된 패턴: `^\\{\\}\\$|^\\{\\\"Cidr\\\":\\\"[\\x00-\\x7F+]{1,128}\\\",\\\"IpProtocol\\\":\\\"[\\x00-\\x7F+]{1,128}\\\",\\\"FromPort\\\":\\\"[\\x00-\\x7F+]{1,128}\\\",\\\"ToPort\\\":\\\"[\\x00-\\x7F+]{0,255}\\\"}\\}`
- EgressTrafficRules(선택 사항):
 - 설명: (선택 사항) Amazon EC2 인스턴스에 적용할 형식으로 Cidr, IpProtocol, FromPort 및 ToPort를 사용하여 심표로 구분[{"Cidr": "1.2.3.4/32", "IpProtocol": "tcp", "FromPort": "22", "ToPort": "22"}]된 보안 그룹 송신 규칙 맵입니다. 규칙이 제공되지 않으면 송신 규칙이 없는 보안 그룹이 Amazon EC2 인스턴스에 연결되어 모든 발신 트래픽을 효과적으로 방지합니다.
 - 유형: MapList
 - 허용된 패턴: `^\\{\\}\\$|^\\{\\\"Cidr\\\":\\\"[\\x00-\\x7F+]{1,128}\\\",\\\"IpProtocol\\\":\\\"[\\x00-\\x7F+]{1,128}\\\",\\\"FromPort\\\":\\\"[\\x00-\\x7F+]{1,128}\\\",\\\"ToPort\\\":\\\"[\\x00-\\x7F+]{0,255}\\\"}\\}`
- BackupS3KeyName(선택 사항):
 - 설명: (선택 사항) Action이 로 설정된 경우 Restore자동화가 대상 Amazon EC2 인스턴스 구성을 복원하는 데 사용할 Amazon S3 키를 지정합니다. Amazon EC2 Amazon S3 키는 일반적으로 형식을 따릅니다{year}/{month}/{day}/{hour}/{minute}/{automation_execution_id}.json. 키는 이전 억제 자동화 실행의 출력에서 가져올 수 있습니다.
 - 유형: 문자열
 - 허용된 패턴: `^[a-zA-Z0-9\\.\-\\_\\!\\*\\'\\(\\)]{0,1024}$`

4. 실행을 선택합니다.

5. 자동화가 시작됩니다.

6. 문서는 다음 단계를 수행합니다.

- **ValidateRequiredInputs**

모든 필수 입력이 제공되었는지 확인합니다.

- **AssertInstancelIsNotTerminated**

대상 Amazon EC2 인스턴스가 종료(삭제)되지 않았는지 확인합니다.

- **GetAutoScalingInstanceInfo**

대상 Amazon EC2 인스턴스가 Auto Scaling 그룹의 일부인 경우 Amazon EC2 인스턴스 수명 주기 및 그룹 이름을 가져옵니다.

- **CheckBackupS3BucketName**

대상 Amazon S3 버킷이 객체에 read 대한 또는 write 퍼블릭 액세스 권한을 부여할 가능성이 있는지 확인합니다. 버킷이 없는 경우 새 Amazon S3 BackupS3BucketName 버킷이 생성됩니다.

- **BranchOnActionAndMode**

입력 파라미터 Action 및 Mode 기반으로 자동화를 분기합니다DryRun.

- **BranchOnAutoScalingGroupMembership**

대상 Amazon EC2 인스턴스가 Auto Scaling 그룹의 일부인지 여부와 수명 주기 상태를 기반으로 자동화를 분기합니다.

- **DescribeAutoScalingGroups**

연결된 Amazon EC2 Auto Scaling 그룹 구성을 가져오고 저장합니다.

- **ModifyAutoScalingGroup**

억제 작업에 연결된 Amazon EC2 Auto Scaling 그룹 구성을 수정하여 Amazon EC2 인스턴스를 Standby 상태로 설정하고 Auto Scaling 그룹 MinSize 용량을 조정합니다.

- **BackupInstanceSecurityGroups**

대상 Amazon EC2 인스턴스 보안 그룹의 구성을 가져오고 저장합니다.

- **CreateAllAccessSecurityGroup**

대상 Amazon EC2 인스턴스의 보안 그룹을 대체하는 모든 수신 트래픽을 허용하는 임시 보안 그룹을 생성합니다.

- **CreateContainmentSecurityGroup**

지정된 수신 및 송신 규칙을 사용하여 제한적인 격리 보안 그룹을 생성하고 임시 모든 액세스 그룹을 해당 그룹으로 대체합니다.

- BranchOnCreateAMIBackup

CreateAMIBackup 입력 파라미터를 기반으로 자동화를 분기합니다.

- AssertSourceInstanceRootVolumelsEbs

대상 Amazon EC2 인스턴스 루트 볼륨이 Amazon EBS인지 확인합니다.

- CreateImage

대상 Amazon EC2 인스턴스AMI의를 생성합니다.

- RestoreInstanceConfiguration

백업에서 대상 Amazon EC2 인스턴스 구성을 복원합니다.

- ReportContain

억제 작업에 대한 모의 실행 세부 정보를 출력합니다.

- ReportRestore

복원 작업에 대한 모의 실행 세부 정보를 출력합니다.

- ReportRestoreFailure

복원 워크플로 실패 시나리오 중에 대상 Amazon EC2 인스턴스 원래 구성을 복원하는 지침을 제공합니다.

- ReportContainmentFailure

억제 워크플로 실패 시나리오 중에 대상 Amazon EC2 인스턴스 원래 구성을 복원하는 지침을 제공합니다.

- FinalOutput

억제 작업의 세부 정보를 출력합니다.

7. 실행이 완료되면 출력 섹션에서 실행의 자세한 결과를 검토합니다.

- FinalOutput.Output

DryRun이 False로 설정된 경우 이 실행서에서 수행하는 억제 작업의 세부 정보를 출력합니다.

- RestoreInstanceConfiguration.Output

DryRun이 False로 설정된 경우 이 실행서에서 수행하는 복원 작업을 출력합니다.

- ReportContainment.Output

DryRun이 True로 설정된 경우 이 실행서에서 수행하는 억제 작업의 세부 정보를 출력합니다.

- ReportRestore.Output

DryRun이 True로 설정된 경우 이 실행서에서 수행하는 복원 작업의 세부 정보를 출력합니다.

- ReportContainmentFailure.Output

억제 워크플로 실패 시나리오 중에 대상 Amazon EC2 인스턴스 원래 구성을 복원하는 지침을 제공합니다.

- ReportRestoreFailure.Output

복원 워크플로 실패 시나리오 중에 대상 Amazon EC2 인스턴스 원래 구성을 복원하는 지침을 제공합니다.

참조

Systems Manager Automation

- [이 자동화 실행\(콘솔\)](#)
- [단순한 자동화 실행](#)
- [자동화 설정](#)
- [자동화 워크플로 지원](#)

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 지정하면 자동화는 대상 인스턴스AMI의를 생성하고 이를 AWS 리전 지정한 AMI에 복사한 다음 지정한 서브넷AMI의에서 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. waitForAvailableDestinationAmi단계 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-Classical이 활성화된 경우, 시작이 되지 않습니다.

- SubnetId

유형: 문자열

설명: (선택 사항) 인스턴스를 복사하려는 서브넷의 ID입니다. 대상 리전에서 EC2-Classical이 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 true를 지정하는 경우, 자동화는 소스 인스턴스의 AMI를 삭제하지 않습니다. 이 파라미터에 false를 지정하는 경우, 자동화가 AMI의 등록을 취소하고 관련 스냅샷을 삭제합니다.

- **KeepImageDestinationRegion**

유형: 부울

유효한 값: true | false

기본값: true

설명: (선택 사항) 이 파라미터에 true를 지정하는 경우, 자동화가 지정한 리전에 복사된 AMI를 삭제하지 않습니다. 이 파라미터에 false를 지정하는 경우, 자동화가 AMI의 등록을 취소하고 관련 스냅샷을 삭제합니다.

- **NoRebootInstanceBeforeTakingImage**

유형: 부울

유효한 값: true | false

기본값: false

설명: (선택 사항) 이 파라미터에 true를 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 AMI를 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` - AMI를 대상 리전으로 복사합니다.
- `waitForAvailableDestinationAmi` - 복사한 AMI 상태가 `available`가 될 때까지 기다립니다.
- `destinationRegionLaunchInstance` - 복사한 AMI를 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

AWSPremiumSupport-DiagnoseDiskUsageOnLinux

설명

AWSPremiumSupport-DiagnoseDiskUsageOnLinux 실행서는 대상 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스의 Amazon Elastic Block Store(Amazon EBS) 볼륨을 분석하여 확장이 필요한지 확인합니다. 실행서 입력 파라미터에 정의된 임계값과 비교하여 각 볼륨의 사용량, 파일 시스템 유형 및 확장 기록을 확인합니다. 스크립트는 최근 수정 사항, 지원되는 파일 시스템 및 AWS 볼륨 제한과 같은 요소를 고려합니다. 그런 다음 확장 대상인 볼륨이 있는 경우 각 볼륨에 대한 관련 세부 정보와 함께 출력합니다.

어떻게 작동하나요?

이 실행서는 다음 작업을 수행합니다.

- 대상 인스턴스가 Systems Manager에서 관리되고 Windows를 실행하지 않는지 확인합니다.
- 플랫폼 및 루트 디바이스 유형을 포함한 인스턴스 세부 정보를 검색합니다.
- Amazon EC2 인스턴스에서 사용하는 볼륨을 가져옵니다.
- Linux에서 사전 확인을 실행하여 디스크 사용량을 분석하고 확장 후보를 결정합니다.
- 관련 세부 정보와 함께 확장 대상 볼륨을 출력합니다.

Important

AWSPremiumSupport-* 실행서에 액세스하려면 Business + Support, Enterprise Support 또는 통합 운영 구독이 필요합니다. 자세한 내용은 [AWS Support 플랜 비교](#)를 참조하세요.

이 자동화 실행(콘솔)

필수 IAM 권한

실행서를 성공적으로 사용하려면 AutomationAssumeRole 파라미터에 다음 작업이 필요합니다.

- ssm:DescribeInstanceInformation
- ec2:DescribeInstances
- ec2:DescribeVolumes

- ssm:SendCommand
- ssm:ListCommandInvocations

예제 정책:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "ssm:DescribeInstanceInformation",
        "ec2:DescribeInstances",
        "ec2:DescribeVolumes",
        "ssm:SendCommand",
        "ssm:ListCommandInvocations"
      ],
      "Resource": "*"
    }
  ]
}
```

지침

다음 단계에 따라 자동화를 구성합니다.

1. Systems Manager [AWSPremiumSupport-DiagnoseDiskUsageOnLinux](#)의 문서로 이동합니다.
2. Execute automation(자동화 실행)을 선택합니다.
3. 입력 파라미터에 다음을 입력합니다.
 - AutomationAssumeRole(선택 사항):
 - 설명: (선택 사항) Systems Manager Automation이 사용자를 대신하여 작업을 수행할 수 있도록 허용하는 IAM 역할의 Amazon 리소스 이름(ARN)입니다. 역할을 지정하지 않은 경우, Systems Manager Automation에서는 이 실행서를 시작하는 사용자의 권한을 사용합니다.
 - 유형: AWS::IAM::Role::Arn
 - InstanceId(필수):
 - 설명: (필수) Amazon EC2 인스턴스의 ID입니다.

- 유형: String
 - 패턴 허용: `^i-[0-9a-f]{8,17}$`
 - VolumeExpansionUsageTrigger(필수):
 - 설명: (필수) 확장을 트리거하는 데 필요한 파티션 공간의 최소 사용량(백분율).
 - 유형: String
 - 패턴 허용: `^[0-9]{1,2}$`
 - VolumeExpansionCapSize(필수):
 - 설명: (필수) Amazon EBS 볼륨이 (GiB)로 증가할 최대 크기입니다.
 - 유형: String
 - 패턴 허용: `^[0-9]{1,4}$`
 - VolumeExpansionGibIncrease(필수):
 - 설명: (필수) 볼륨의 GiB 증가. VolumeExpansionGibIncrease와 사이의 최대 순 증가VolumeExpansionPercentageIncrease량이 사용됩니다.
 - 유형: String
 - 패턴 허용: `^[0-9]{1,4}$`
 - VolumeExpansionPercentageIncrease(필수):
 - 설명: (필수) 볼륨의 백분율을 늘립니다. VolumeExpansionGibIncrease와 사이의 최대 순 증가VolumeExpansionPercentageIncrease량이 사용됩니다.
 - 유형: String
 - 패턴 허용: `^[0-9]{1,2}$`
4. 실행을 선택합니다.
 5. 자동화가 시작됩니다.
 6. 문서는 다음 단계를 수행합니다.
 - AssertInstanceIsManagedInstance:

대상 인스턴스가 Systems Manager에서 관리되는지 확인합니다.
 - DescribeInstance:

대상 Amazon EC2 인스턴스를 설명하고 Platform, 및를 포함한 인스턴스 세부 정보를 검색합니다RootDeviceType.
 - BranchOnPlatform:

플랫폼 유형을 분기하고 Windows와 다른 경우 실행을 진행합니다.

- DescribeVolumes:

Amazon EC2 인스턴스에서 사용하는 볼륨을 가져옵니다.

- RunPreChecksOnLinux:

이전 단계에서 수집한 볼륨에 대해 검사를 실행합니다.

7. 완료되면 출력 섹션에서 실행의 자세한 결과를 검토합니다.

참조

Systems Manager Automation

- [이 자동화 실행\(콘솔\)](#)
- [자동화 실행](#)
- [Automation 설정](#)
- [자동화 워크플로 지원](#)

AWSsupport-EnableWindowsEC2SerialConsole

설명

실행서는 Amazon EC2 Windows 인스턴스에서 Amazon EC2 직렬 콘솔, 특수 관리 콘솔(SAC) 및 부팅 메뉴를 활성화하는 데 AWSsupport-EnableWindowsEC2SerialConsole 도움이 됩니다. Amazon Elastic Compute Cloud(Amazon EC2) 직렬 콘솔 기능을 사용하면 Amazon EC2 인스턴스의 직렬 포트에 액세스하여 부팅, 네트워크 구성 및 기타 문제를 해결할 수 있습니다. 실행서는 실행 중 상태이고에서 관리하는 인스턴스 AWS Systems Manager와 중지 상태이거나에서 관리하지 않는 인스턴스에서 기능을 활성화하는 데 필요한 단계를 자동화합니다 AWS Systems Manager.

어떻게 작동하나요?

AWSsupport-EnableWindowsEC2SerialConsole 자동화 실행서는 Microsoft Windows Server를 실행하는 Amazon EC2 인스턴스에서 SAC 및 부팅 메뉴를 활성화하는 데 도움이 됩니다. 실행 중 상태이고에서 관리하는 인스턴스의 경우 AWS Systems Manager실행서는 AWS Systems Manager Run Command PowerShell 스크립트를 실행하여 SAC 및 부팅 메뉴를 활성화합니다. 중지 상태이거나에서 관리하지 않는 인스턴스의 경우 AWS Systems Manager실행서는 [AWSsupport-StartEC2RescueWorkflow](#)를 사용하여 임시 Amazon EC2 인스턴스를 생성하여 필요한 변경을 오프라인으로 수행합니다.

자세한 내용은 [Windows 인스턴스용 Amazon EC2 직렬 콘솔을 참조하세요.](#)

⚠ Important

- 인스턴스에서 SAC를 활성화하면 암호 검색에 의존하는 Amazon EC2 서비스가 Amazon EC2 콘솔에서 작동하지 않습니다. 자세한 내용은 [SAC를 사용하여 Windows 인스턴스 문제 해결](#)을 참조하세요.
- 직렬 콘솔에 대한 액세스를 구성하려면 계정 수준에서 직렬 콘솔 액세스 권한을 부여한 다음 사용자에게 액세스 권한을 부여하도록 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 참조하세요](#).
- 계정에서 직렬 콘솔이 활성화되어 있는지 확인하려면 [직렬 콘솔에 대한 계정 액세스 상태 보기](#)를 참조하세요.
- 직렬 콘솔 액세스는 [Nitro 시스템에 구축된 가상화된 인스턴스에서만 지원됩니다](#).

자세한 내용은 Amazon EC2 직렬 콘솔 [사전 조건을 참조하세요](#).

문서 유형

자동화

소유자

Amazon

플랫폼

Windows

파라미터

필수 IAM 권한

실행서를 성공적으로 사용하려면 AutomationAssumeRole 파라미터에 다음 작업이 필요합니다.

JSON

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

```

{
  "Effect": "Allow",
  "Action": [
    "autoscaling:DescribeAutoScalingInstances",
    "ec2:GetSerialConsoleAccessStatus",
    "ec2:Describe*",
    "ec2:createTags",
    "ec2:createImage",
    "ssm:DescribeAutomationExecutions",
    "ssm:DescribeInstanceInformation",
    "ssm:GetAutomationExecution",
    "ssm:ListCommandInvocations",
    "ssm:ListCommands"
  ],
  "Resource": "*"
},
{
  "Effect": "Allow",
  "Action": [
    "ec2:AttachVolume",
    "ec2:DetachVolume",
    "ec2:ModifyInstanceAttribute",
    "ec2:RebootInstances",
    "ec2:StartInstances",
    "ec2:StopInstances",
    "iam:GetInstanceProfile",
    "ssm:GetParameters",
    "ssm:SendCommand",
    "ssm:StartAutomationExecution"
  ],
  "Resource": [
    "arn:aws:ec2:us-east-1:111122223333:instance/i-02573cafcfEXAMPLE",
    "arn:aws:ec2:us-east-1:111122223333:volume/vol-049df61146EXAMPLE",
    "arn:aws:iam:111122223333:instance-profile/instance-profile-name",
    "arn:aws:ssm:us-east-1:111122223333:parameter/aws/service/*",
    "arn:aws:ssm:us-east-1:*:document/AWSSupport-StartEC2RescueWorkflow",
    "arn:aws:ssm:us-east-1:*:document/AWS-ConfigureAWSPackage",
    "arn:aws:ssm:us-east-1:*:document/AWS-RunPowerShellScript",
    "arn:aws:ssm:us-east-1:111122223333:automation-execution/*"
  ]
}

```

```

    },
    {
      "Effect": "Allow",
      "Action": [
        "cloudformation:CreateStack"
      ],
      "Resource": "*",
      "Condition": {
        "StringLike": {
          "aws:RequestTag/Name": "AWSSupport-EC2Rescue: *"
        },
        "ForAllValues:StringEquals": {
          "aws:TagKeys": [
            "AWSSupport-EC2Rescue-AutomationExecution",
            "Name"
          ]
        }
      }
    }
  ],
  {
    "Effect": "Allow",
    "Action": [
      "cloudformation>DeleteStack",
      "cloudformation:DescribeStackEvents",
      "cloudformation:DescribeStackResource",
      "cloudformation:DescribeStacks",
      "ec2:AttachVolume",
      "ec2:DetachVolume",
      "ec2:RebootInstances",
      "ec2:StopInstances",
      "ec2:TerminateInstances",
      "ssm:SendCommand"
    ],
    "Resource": "*",
    "Condition": {
      "StringLike": {
        "aws:ResourceTag/Name": "AWSSupport-EC2Rescue: *"
      }
    }
  }
],
{
  "Effect": "Allow",
  "Action": [
    "ec2:CreateLaunchTemplate",

```

```

        "ec2:DeleteLaunchTemplate",
        "ec2:RunInstances"
    ],
    "Resource": "*",
    "Condition": {
        "ForAnyValue:StringEquals": {
            "aws:CalledVia": [
                "cloudformation.amazonaws.com"
            ]
        }
    }
},
{
    "Effect": "Allow",
    "Action": "iam:PassRole",
    "Resource": "*",
    "Condition": {
        "StringEquals": {
            "iam:PassedToService": [
                "ssm.amazonaws.com",
                "ec2.amazonaws.com"
            ]
        }
    }
}
]
}

```

지침

다음 단계에 따라 자동화를 구성합니다.

1. AWS Systems Manager 콘솔 **AWSSupport-EnableWindowsEC2SerialConsole**에서 로 이동합니다.
2. **Execute automation(자동화 실행)**을 선택합니다.
3. 입력 파라미터에 다음을 입력합니다.
 - **InstanceId:** (필수)
Amazon EC2 직렬 콘솔, (SAC) 및 부팅 메뉴를 활성화하려는 Amazon EC2 인스턴스의 ID입니다.
 - **AutomationAssumeRole:** (선택 사항)

Systems Manager Automation이 사용자를 대신하여 작업을 수행할 수 있도록 허용하는 IAM 역할의 Amazon 리소스 이름(ARN)입니다. 역할이 지정되지 않은 경우 Systems Manager Automation은 실행서를 시작하는 사용자의 권한을 사용합니다.

- `HelperInstanceType`: (조건부)

런북이 오프라인 인스턴스에 대해 Amazon EC2 직렬 콘솔을 구성하기 위해 프로비저닝하는 Amazon EC2 인스턴스의 유형입니다.

- `HelperInstanceProfileName`: (조건부)

헬퍼 인스턴스에 대한 기존 IAM 인스턴스 프로파일의 이름입니다. 중지 상태이거나에서 관리하지 않는 인스턴스에서 SAC 및 부팅 메뉴를 활성화하는 경우 AWS Systems Manager필요합니다. IAM 인스턴스 프로파일을 지정하지 않으면 자동화가 사용자를 대신하여 하나를 생성합니다.

- `SubnetId`: (조건부)

헬퍼 인스턴스의 서브넷 ID입니다. 기본적으로 제공된 인스턴스가 있는 서브넷과 동일한 서브넷을 사용합니다.

Important

사용자 지정 서브넷을 제공하는 경우 해당 서브넷은 `InstanceId`와 동일한 가용 영역에 있어야 하며 Systems Manager 엔드포인트에 대한 액세스를 허용해야 합니다. 이는 대상 인스턴스가 중지 상태이거나에서 관리하지 않는 경우에만 필요합니다 AWS Systems Manager.

- `CreateInstanceBackupBeforeScriptExecution`: (선택 사항)

SAC 및 부팅 메뉴를 활성화하기 전에 `True`를 지정하여 Amazon EC2 인스턴스의 Amazon Machine Image(AMI) 백업을 생성합니다. AMI가 자동화 완료 이후에도 지속됩니다. AMI에 대한 액세스를 보호하거나 삭제하는 것은 사용자의 책임입니다.

- `BackupAmazonMachineImagePrefix`: (조건부)

`CreateInstanceBackupBeforeScriptExecution` 파라미터가 `로` 설정된 경우 생성되는 Amazon Machine Image(AMI)의 접두사입니다`True`.

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

- **CheckIfEc2SerialConsoleAccessEnabled:**

계정 수준에서 Amazon EC2 직렬 콘솔 액세스가 활성화되어 있는지 확인합니다. 참고: 직렬 콘솔에 대한 액세스는 기본적으로 사용할 수 없습니다. 자세한 내용은 [Amazon EC2 직렬 콘솔에 대한 액세스 구성을 참조하세요.](#)

- **CheckIfEc2InstanceIsWindows:**

대상 인스턴스 플랫폼이 Windows인 경우 어설션합니다.

- **GetInstanceType:**

대상 인스턴스의 인스턴스 유형을 검색합니다.

- **CheckIfInstanceTypeIsNitro:**

인스턴스 유형 하이퍼바이저가 Nitro 기반인지 확인합니다. 직렬 콘솔 액세스는 Nitro 시스템에 구축된 가상화된 인스턴스에서만 지원됩니다.

- **CheckIfInstanceIsInAutoScalingGroup:**

DescribeAutoScalingInstances API를 호출하여 Amazon EC2 인스턴스가 Amazon EC2 Auto Scaling 그룹의 일부인지 확인합니다. 인스턴스가 Amazon EC2 Auto Scaling 그룹의 일부인 경우 Porting Assistant for .NET 인스턴스가 대기 수명 주기 상태에 있는지 확인합니다.

- **WaitForEc2InstanceStateStablized:**

인스턴스가 실행 중이거나 중지될 때까지 기다립니다.

- **GetEc2InstanceState:**

인스턴스의 현재 상태를 가져옵니다.

- **BranchOnEc2InstanceState:**

이전 단계에서 검색된 인스턴스 상태를 기반으로 분기합니다. 인스턴스 상태가 실행 중이면 CheckIfEc2InstanceIsManagedBySSM 단계로 이동하고 그렇지 않으면 CheckIfHelperInstanceProfileIsProvided 단계로 이동합니다.

- **CheckIfEc2InstanceIsManagedBySSM:**

인스턴스가에서 관리되는지 확인합니다 AWS Systems Manager. 관리형인 경우 실행서는 PowerShell Run Command를 사용하여 SAC 및 부팅 메뉴를 활성화합니다.

- **BranchOnPreEC2RescueBackup:**

- `CreateAmazonMachineImageBackup`:

인스턴스의 AMI 백업을 생성합니다.

- `EnableSACAndBootMenu`:

PowerShell Run Command 스크립트를 실행하여 SAC 및 부팅 메뉴를 활성화합니다.

- `RebootInstance`:

Amazon EC2 인스턴스를 재부팅하여 구성을 적용합니다. 인스턴스가 온라인 상태이고에서 관리하는 경우 마지막 단계입니다 AWS Systems Manager.

- `CheckIfHelperInstanceProfilesProvided`:

임시 Amazon EC2 인스턴스를 사용하여 SAC 및 부팅 메뉴를 오프라인으로 활성화하기 전에 `HelperInstanceProfileName` 지정된 이 존재하는지 확인합니다.

- `RunAutomationToInjectOfflineScriptForEnablingSACAndBootMenu`:

인스턴스가 중지 상태이거나에서 관리하지 않는 경우를 실행 `AWSSupport-StartEC2RescueWorkflow`하여 SAC 및 부팅 메뉴를 활성화합니다 AWS Systems Manager.

- `GetExecutionDetails`:

백업 및 오프라인 스크립트 출력의 이미지 ID를 검색합니다.

7. 완료되면 출력 섹션에서 실행의 자세한 결과를 검토합니다.

- `EnableSACAndBootMenu.Output`:

`EnableSACAndBootMenu` 단계의 명령 실행 출력입니다.

- `GetExecutionDetails.OfflineScriptOutput`:

`RunAutomationToInjectOfflineScriptForEnablingSACAndBootMenu` 단계에서 실행된 오프라인 스크립트의 출력입니다.

- `GetExecutionDetails.BackupBeforeScriptExecution`:

`CreateInstanceBackupBeforeScriptExecution` 입력 파라미터가 `True`인 경우 가져온 AMI 백업의 이미지 ID입니다.

참조

- [이 자동화 실행\(콘솔\)](#)
- [자동화 실행](#)
- [Automation 설정](#)
- [Support Automation Workflows 랜딩 페이지](#)

AWSPremiumSupport-ExtendVolumesOnWindows

설명

AWSPremiumSupport-ExtendVolumesOnWindows 실행서는 대상 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스에서 Amazon Elastic Block Store(Amazon EBS) 볼륨, 해당 파티션 및 파일 시스템을 확장합니다.

중요 고려 사항

- 작업 영향 및 볼륨 상태: Amazon EBS 볼륨 수정은 modifying, optimizing 및의 세 단계로 이루어집니다. completed. 이 자동화는 볼륨이 optimizing 상태에 도달하면 파일 시스템 확장을 진행합니다. optimizing 상태 중에는 파티션 크기 조정 중에 일시적인 성능 영향과 잠재적인 파일 시스템 수준 중단이 발생할 수 있습니다. [Amazon EBS 볼륨 수정 진행 상황을 모니터링할](#) 수 있습니다.
- 비용 및 제한 사항: Amazon EBS 볼륨 크기를 늘리면 월별 스토리지 비용이 증가합니다. 자세한 내용은 [Amazon EBS 요금을](#) 참조하세요. 이 실행서에서 생성된 백업 AMI 및 관련 스냅샷은 크기와 보관 기간에 따라 추가 요금이 발생합니다. 일부 볼륨 유형의 경우 확장 후 GB 당 동일한 IOPS 비율을 유지해야 하는 경우 프로비저닝된 IOPS를 수정해야 할 수 있습니다.
- 백업 및 복구: 런북은 볼륨을 변경하기 전에 백업 AMI를 생성합니다. AMI 및 연결된 스냅샷은 계정에서 자동으로 제거되지 않습니다. 더 이상 필요하지 않은 경우 이러한 백업을 수동으로 제거해야 합니다. 장애가 발생할 경우 스냅샷을 [사용하여 Amazon EBS 볼륨 교체에 설명된 대로 연결된 AMI의 스냅샷에서 볼륨을](#) 복구할 수 있습니다.

어떻게 작동하나요?

이 실행서는 다음 작업을 수행합니다.

- 대상 인스턴스가 Systems Manager에서 관리되고 Windows Server를 실행 중인지 확인합니다.
- 현재 Amazon EC2 인스턴스를 대상으로 하는 이 실행서의 실행이 하나만 있는지 확인합니다.
- 대상 인스턴스에서 백업 Amazon Machine Image(AMI)를 생성합니다.

- 확장을 위해 지정된 Amazon EBS 볼륨을 확장합니다.
- PowerShell 명령을 사용하여 대상 인스턴스의 파일 시스템 확장

Important

AWSPremiumSupport-* 실행서에 액세스하려면 Business + Support, Enterprise Support 또는 통합 운영 구독이 필요합니다. 자세한 내용은 [AWS Support 플랜 비교](#)를 참조하세요.

이 자동화 실행(콘솔)

필수 IAM 권한

실행서를 성공적으로 사용하려면 AutomationAssumeRole 파라미터에 다음 작업이 필요합니다.

- ec2:DescribeInstances
- ec2:CreateImage
- ec2:DescribeImages
- ec2:DescribeVolumes
- ec2:ModifyVolume
- ssm:SendCommand
- ssm:ListCommandInvocations
- ssm:DescribeInstanceInformation

IAM 정책 예제:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "ec2:DescribeInstances",
        "ec2:CreateImage",
        "ec2:DescribeImages",
        "ec2:DescribeVolumes",
        "ec2:ModifyVolume",

```

```

        "ssm:SendCommand",
        "ssm:DescribeInstanceInformation",
        "ssm:ListCommandInvocations"
    ],
    "Resource": "*"
}
]
}

```

지침

다음 단계에 따라 자동화를 구성합니다.

1. Systems Manager [AWSPremiumSupport-ExtendVolumesOnWindows](#)의 문서로 이동합니다.

2. Execute automation(자동화 실행)을 선택합니다.

3. 입력 파라미터에 다음을 입력합니다.

- AutomationAssumeRole(선택 사항):
 - 설명: (선택 사항) Systems Manager Automation이 사용자를 대신하여 작업을 수행할 수 있도록 허용하는 IAM 역할의 Amazon 리소스 이름(ARN)입니다. 역할을 지정하지 않은 경우, Systems Manager Automation에서는 이 실행서를 시작하는 사용자의 권한을 사용합니다.
 - 유형: AWS::IAM::Role::Arn
- InstanceId(필수):
 - 설명: (필수) Amazon EC2 인스턴스의 ID입니다.
 - 유형: String
 - 패턴 허용: ^i-[0-9a-f]{8,17}\$
- VolumeExpansionCapSize(필수):
 - 설명: (필수) Amazon EBS 볼륨이 증가할 최대 크기(GiB)입니다.
 - 유형: String
 - 패턴 허용: ^[0-9]{1,4}\$
- DiagnosticResults(필수):
 - 설명: (필수) DiagnoseDiskUsage 문서의 사전 확인 스크립트 결과로, 한 줄 CSV 형식입니다. 문자열은 로 시작하고 각 볼륨에 대해 쉼표로 구분된 볼륨 정보가 EXTEND; 이어지며 볼륨은 세미콜론으로 구분됩니다. 각 볼륨의 정보에는 볼륨 ID, 드라이브 문자, 확장 플래그(확장하려면 1, 건너뛰려면 0), GB의 새 크기, AWS 리전 및 이유/작업이 포함됩니다.
 - 유형: String

- 패턴 허용: `^EXTEND;[0-9a-zA-Z\\.%;\\-\\/\\s]{7,5400}$`

4. 실행을 선택합니다.

5. 자동화가 시작됩니다.

6. 문서는 다음 단계를 수행합니다.

- `AssertInstanceIsManagedInstance`:

대상 인스턴스가 Systems Manager에서 관리되는지 확인합니다.

- `DescribeInstance`:

대상 Amazon EC2 인스턴스의 플랫폼 정보를 검색합니다.

- `BranchOnPlatform`:

대상 Amazon EC2 인스턴스 플랫폼이 Windows Server인지 확인합니다.

- `CheckConcurrency`:

현재 Amazon EC2 인스턴스를 대상으로 하는 이 실행서의 실행이 하나만 있는지 확인합니다.

- `CreateImage`:

대상 인스턴스에서 백업 Amazon Machine Image(AMI)를 생성합니다.

- `WaitUntillImageReady`:

Amazon Machine Image(AMI)가 생성을 완료하고 available 상태에 도달할 때까지 기다립니다.

- `ExtendEBSVolume`:

확장을 위해 지정된 대상 인스턴스의 Amazon EBS 볼륨을 확장합니다.

- `DescribeVolumes`:

확장을 위해 지정된 대상 인스턴스의 Amazon EBS 볼륨을 설명합니다.

- `ExtendFilesystem`:

PowerShell 명령을 사용하여 대상 인스턴스의 파일 시스템을 확장합니다.

7. 완료 후 출력 섹션에서 실행의 자세한 결과를 검토합니다.

참조

Systems Manager Automation

- [이 자동화 실행\(콘솔\)](#)
- [자동화 실행](#)
- [Automation 설정](#)
- [자동화 워크플로 지원](#)
- [Amazon EBS 볼륨 수정 요청](#)

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 Manager 자동화는 새 VPC를 생성합니다. 또는 SelectedInstanceSubnet을 사용하여 인스턴스와 동일한 서브넷을 사용하거나 사용자 지정 서브넷 ID를 지정합니다.

 Important

서브넷은 UnreachableInstanceId와 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

이 `AWSSupport-ListEC2Resources` 실행서는 Amazon EC2 인스턴스에 대한 정보와 Amazon Elastic Block Store(Amazon EBS) 볼륨, 탄력적 IP 주소, AWS 리전 지정한의 Amazon EC2 Auto

Scaling 그룹과 같은 관련 리소스를 반환합니다. 기본적으로, 정보는 모든 리전에서 수집되며 자동화 출력본에 표시됩니다. 선택적으로, 쉘표로 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.

- BucketName

유형: 문자열

설명: (선택 사항) 수집된 정보가 업로드되는 S3 버킷의 이름입니다.

- DisplayResourceDeletionDocumentation

유형: 문자열

기본값: true

설명: (선택 사항) true로 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 AutomationAssumeRole에 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-Stop를 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

유형: 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

유형: 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 available이면 VPC에서 지정하는 DestinationSubnetId의 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 available이면 VPC에서 지정하는 DestinationSubnetId의 이 AMI에서 새 Amazon EC2 인스턴스가 시작됩니다. EC2-Classic에서 실행 중인 Amazon EC2 인스턴스에 탄력적 IP 주소가 연결된 경우, 자동화를 통해 지정하는 DestinationSubnetId이 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 리전 의 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 유형](#)으로 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 요금](#)을 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.
- 인스턴스가에서 관리되는지 확인합니다 AWS Systems Manager.

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

FullMigration을 OperationType로 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 생성](#)을 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 AMI를 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&Migrate와 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.
- `getXenInstanceTypeInfoDetails` - 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 AMI를 생성합니다.
- `createImageAfterDriversInstallation` - Golden AMI로 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 예약 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 스택에서 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 승인을 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.
- `checkENAAtributeForTargetInstance` - 대상 Amazon EC2 인스턴스에 대해 향상된 네트워킹(ENA) 속성이 켜져 있는지 확인합니다.
- `enableENAAtributeForTargetInstance` - 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.

다. 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.

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 참조하세요.

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-StartEC2RescueWorkflow를 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-StartEC2RescueWorkflow를 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 실행서는 직렬 콘솔을 사용하여 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스에 액세스해야 하는 사용자에게 특히 유용합니다. 실행서는 자동으로 생성된 AWS Identity and Access Management (IAM) 역할 또는 지정한 사용자 지정 IAM 인스턴스 프로파일을 AWS 계정 사용하여 임시 Amazon EC2 인스턴스를 생성합니다. 사용자 지정 (IAM) 인스턴스 프로파일에는 암호가 포함된 AWS Secrets Manager 보안 암호 값을 검색할 수 있는 권한이 있어야 합니다.

실행서는 대상 Amazon EC2 인스턴스를 중지하고, 루트 Amazon Elastic Block Store(Amazon EBS) 볼륨을 분리하고, 이를 임시 Amazon EC2 인스턴스에 연결합니다. 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 생성](#)을 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 임의의 퍼블릭 IPv4 주소가 해제됩니다. 인스턴스를 중지할 때 발생하는 상황에 대한 자세한 내용은 Amazon EC2 사용 설명서의 [인스턴스 중지 및 시작을 참조하세요](#).
- 대상 Amazon EC2 인스턴스에 연결된 Amazon EBS 볼륨이 고객 관리형 AWS Key Management Service (AWS KMS) 키로 암호화된 경우 AWS KMS 키가 deleted 또는가 아닌지 확인합니다. disabled 그렇지 않으면 인스턴스가 시작되지 않습니다.
- 사용자 지정 IAM 인스턴스 프로파일을 사용하려면 검증AutomationAssumeRole을 위한 IAM GetInstanceProfile 권한이 있어야 하며, 사용자 지정 인스턴스 프로파일 자체에는 Systems Manager 및 Secrets Manager 액세스 권한이 포함되어야 합니다. 실행서는 인스턴스 프로파일 존재를 미리 검증하지만 인스턴스 프로파일에 필요한 액세스 권한이 없는 경우 헬퍼 인스턴스 작업 중에 실패합니다.

[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) 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 암호가 포함된 Secrets Manager 보안 암호의 ARN입니다.

- SecurityGroupId

유형: 문자열

설명: (선택 사항) 임시 Amazon EC2 인스턴스에 연결할 보안 그룹의 ID입니다. 이 파라미터에 대한 값을 제공하지 않으면 기본 Amazon Virtual Private Cloud(Amazon VPC) 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: **Yes**을 입력하여 이 자동화 중에 대상 Amazon EC2 인스턴스가 중지된다는 것을 확인합니다. Amazon EC2 인스턴스가 중지되면, 메모리 또는 인스턴스 스토어 볼륨에 저장된 모든 데이터가 손실되고 자동 퍼블릭 IPv4 주소가 해제됩니다. 자세한 내용은 [Amazon EC2 사용 설명서](#)의 인스턴스 중지 및 시작을 참조하세요.

- InstanceProfileName

유형: 문자열

설명: (선택 사항) 헬퍼 Amazon EC2 인스턴스에 연결할 IAM 인스턴스 프로파일의 이름입니다. 제공되지 않으면 필요한 권한이 있는 임시 인스턴스 프로파일이 자동으로 생성됩니다. 사용자 지정 인스턴스 프로파일에는 지정된 Secrets Manager 보안 암호 및 Systems Manager에 액세스할 수 있는 권한이 있어야 합니다.

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:DescribeInstanceState`
- `ec2:DescribeSnapshotAttribute`
- `ec2:DescribeSnapshots`
- `ec2:DescribeSnapshotTierStatus`
- `ec2:DescribeVolumes`
- `ec2:DescribeVolumeStatus`
- `ec2:DetachVolume`
- `ec2:RunInstances`
- `ec2:StartInstances`
- `ec2:StopInstances`
- `ec2:TerminateInstances`
- `cloudformation:CreateStack`
- `cloudformation>DeleteStack`
- `cloudformation:DescribeStackResource`
- `cloudformation:DescribeStacks`
- `cloudformation:ListStacks`
- `logs:CreateLogDelivery`

- logs:CreateLogGroup
- logs>DeleteLogDelivery
- logs>DeleteLogGroup
- logs:DescribeLogGroups
- logs:DescribeLogStreams
- logs:PutLogEvents
- iam:GetInstanceProfile

문서 단계

1. aws:branch - 대상 Amazon EC2 인스턴스 중지에 대한 동의 여부를 기반으로 분기합니다.
2. aws:assertAwsResourceProperty - Amazon EC2 인스턴스 상태가 running 또는 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 파라미터에서 지정하는 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 또는 인지 확인합니다x86_64.
9. aws:assertAwsResourceProperty - Amazon EC2 인스턴스 종료 동작이 stop 아닌 인지 확인합니다terminate.
- 10aws:branch - Amazon EC2 인스턴스가 스팟 인스턴스가 아닌지 확인합니다. 그렇지 않으면, 자동화가 종료됩니다.
- 11aws:executeScript - Amazon EC2 인스턴스가 Auto Scaling 그룹에 속하지 않도록 합니다. 인스턴스가 Auto Scaling 그룹의 일부인 경우, 자동화는 Amazon EC2 인스턴스가 Standby 수명 주기 상태에 있음을 확인합니다.
- 12aws:branch - 사용자 지정 IAM 인스턴스 프로파일 이름이 제공되었는지 여부에 따라 자동화를 분기합니다.

- 13aws:assertAwsResourceProperty - 사용자 지정 IAM 인스턴스 프로파일이 존재하는지 확인하고 이름이 입력 파라미터와 일치하는지 확인합니다.
- 14aws:createStack - 지정한 OS 사용자의 암호를 재설정하는 데 사용되는 임시 Amazon EC2 인스턴스를 생성합니다.
- 15aws:waitForAwsResourceProperty - 새로 시작된 임시 Amazon EC2 인스턴스가 실행될 때까지 기다립니다.
- 16aws:executeAwsApi - 임시 Amazon EC2 인스턴스의 ID를 가져옵니다.
- 17aws:waitForAwsResourceProperty - 임시 Amazon EC2 인스턴스가 Systems Manager에서 관리하는 대로 보고될 때까지 기다립니다.
- 18aws:changeInstanceState - 대상 Amazon EC2 인스턴스를 중지합니다.
- 19aws:changeInstanceState - 중지 상태에서 멈출 경우 대상 Amazon EC2 인스턴스를 강제로 중지합니다.
- 20aws:branch - 대상 Amazon EC2 인스턴스의 루트 볼륨 스냅샷이 요청되었는지 여부에 따라 자동화를 분기합니다.
- 21aws:executeAwsApi - 대상 Amazon EC2 인스턴스 루트 Amazon EBS 볼륨의 스냅샷을 생성합니다.
- 22aws:waitForAwsResourceProperty - 스냅샷이 completed 상태가 될 때까지 기다립니다.
- 23aws:executeAwsApi - 대상 Amazon EC2 인스턴스에서 Amazon EBS 루트 볼륨을 분리합니다.
- 24aws:waitForAwsResourceProperty - 대상 Amazon EC2 인스턴스에서 Amazon EBS 루트 볼륨이 분리될 때까지 기다립니다.
- 25aws:executeAwsApi - 루트 Amazon EBS 볼륨을 임시 Amazon EC2 인스턴스에 연결합니다.
- 26aws:waitForAwsResourceProperty - Amazon EBS 루트 볼륨이 임시 Amazon EC2 인스턴스에 연결될 때까지 기다립니다.
- 27aws:runCommand - 임시 Amazon EC2 인스턴스에서 Run Command를 사용하여 셸 스크립트를 실행하여 대상 사용자 암호를 재설정합니다.
- 28aws:executeAwsApi - 임시 Amazon EC2 인스턴스에서 Amazon EBS 루트 볼륨을 분리합니다.
- 29aws:waitForAwsResourceProperty - Amazon EBS 루트 볼륨이 임시 Amazon EC2 인스턴스에서 분리될 때까지 기다립니다.
- 30aws:executeAwsApi - 오류 후 임시 Amazon EC2 인스턴스에서 Amazon EBS 루트 볼륨을 분리합니다.
- 31aws:waitForAwsResourceProperty - 오류 후 Amazon EBS 루트 볼륨이 임시 Amazon EC2 인스턴스에서 분리될 때까지 기다립니다.

- 32aws:branch - 오류 발생 시 복구 경로를 결정하기 위해 루트 볼륨의 스냅샷이 요청되었는지 여부에 따라 자동화를 분기합니다.
- 33aws:executeAwsApi - 루트 Amazon EBS 볼륨을 대상 Amazon EC2 인스턴스에 다시 연결합니다.
- 34aws:waitForAwsResourceProperty - Amazon EBS 루트 볼륨이 Amazon EC2 인스턴스에 연결될 때까지 기다립니다.
- 35aws:executeAwsApi - 대상 Amazon EC2 인스턴스 루트 볼륨 스냅샷에서 새 Amazon EBS 볼륨을 생성합니다.
- 36aws:waitForAwsResourceProperty - 새 Amazon EBS 볼륨이 available 상태가 될 때까지 기다립니다.
- 37aws:executeAwsApi - 새 Amazon EBS 볼륨을 대상 인스턴스에 루트 볼륨으로 연결합니다.
- 38aws:waitForAwsResourceProperty - Amazon EBS 볼륨이 attached 상태가 될 때까지 기다립니다.
- 39aws:executeAwsApi - 실행서가 CloudFormation 스택을 생성하거나 업데이트하지 못하는 경우 CloudFormation 스택 이벤트를 설명합니다.
- 40aws:branch - 이전 Amazon EC2 인스턴스 상태에 따라 자동화를 분기합니다. 상태가 running이면, 인스턴스가 시작됩니다. 인스턴스가 stopped 상태였다면, 자동화는 계속됩니다.
- 41aws:changeInstanceState - 필요한 경우 Amazon EC2 인스턴스를 시작합니다.
- 42aws:waitForAwsResourceProperty - CloudFormation 스택이 터미널 상태가 될 때까지 기다렸다가 삭제합니다.
- 43aws:executeAwsApi - 임시 Amazon EC2 인스턴스를 포함한 CloudFormation 스택을 삭제합니다.

AWSSupport-RunEC2RescueForWindowsTool

설명

AWSSupport-RunEC2RescueForWindowsTool 실행서는 대상 Amazon Elastic Compute Cloud(Amazon EC2) Windows 관리형 인스턴스에서 Amazon EC2 Rescue for Windows Server 문제 해결 도구를 실행하여 일반적인 문제를 해결하는 데 도움이 됩니다. 이 실행서는 세 가지 주요 작업을 지원합니다.

- **ResetAccess:** 로컬 관리자 암호를 재설정합니다. 암호는 무작위로 생성되어 AWS Systems Manager 파라미터 스토어에 로 안전하게 저장됩니다/EC2Rescue/Password/<instance_id>.

파라미터를 제공하지 않으면 암호가 기본 AWS Key Management Service (AWS KMS) 키로 암호화됩니다. `alias/aws/ssm`. 선택적으로 AWS KMS 키 ID를 지정하여 자체 키로 암호를 암호화할 수 있습니다.

- **CollectLogs**: 운영 체제에서 로그 및 구성 파일을 수집하여 `/collect:all` 옵션으로 Amazon EC2 Rescue를 실행하여 계정의 Amazon Simple Storage Service(Amazon S3) 버킷에 업로드합니다.
- **FixAll**: `/rescue:all` 옵션으로 Amazon EC2 Rescue를 실행하여 현재 인스턴스에 연결된 오프라인 Windows 루트 볼륨의 문제를 감지하고 해결하려고 시도합니다.

Important

이 실행서를 사용하려면 대상 인스턴스가 AWS Tools for Windows PowerShell이 설치된 Windows 관리형 인스턴스여야 합니다. 실행서는 Systems Manager Distributor 패키지를 사용하여 Amazon EC2 Rescue for Windows Server 도구를 설치합니다. `AWSSupport-EC2Rescue`.

어떻게 작동하나요?

실행서는 다음 단계를 수행합니다.

- Systems Manager Distributor 패키지를 사용하여 Amazon EC2 Rescue for Windows Server 문제 해결 도구를 설치합니다.
- 제공된 파라미터를 사용하여 지정된 작업(`ResetAccessCollectLogs`, 또는 `FixAll`)을 실행합니다.
- 의 경우 `ResetAccess`: 보안 암호를 생성하여 파라미터 스토어에 저장합니다.
- 의 경우 `CollectLogs`: 시스템 로그를 수집하여 지정된 Amazon S3 버킷에 업로드합니다.
- 의 경우 `FixAll`: 지정된 오프라인 볼륨의 문제를 해결하려고 시도합니다.

[이 자동화 실행\(콘솔\)](#)

문서 유형

자동화

소유자

Amazon

플랫폼

Windows

파라미터

필수 IAM 권한

실행서를 성공적으로 사용하려면 AutomationAssumeRole 파라미터에 다음 작업이 필요합니다.

- ssm:SendCommand
- ssm:ListCommandInvocations
- ssm:DescribeInstanceInformation
- ssm:GetCommandInvocation
- ssm:PutParameter (ResetAccess 작업의 경우)
- kms:Encrypt (사용자 지정 AWS KMS 키를 사용한 ResetAccess 작업의 경우)
- s3:PutObject (CollectLogs 작업의 경우)
- s3:GetBucketAcl (CollectLogs 작업의 경우)
- s3:GetBucketPolicy (CollectLogs 작업의 경우)
- s3:GetBucketPolicyStatus (CollectLogs 작업의 경우)

예제 정책:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "ssm:SendCommand",
        "ssm:ListCommandInvocations",
        "ssm:DescribeInstanceInformation",
        "ssm:GetCommandInvocation",
        "ssm:PutParameter",
        "kms:Encrypt",
        "s3:PutObject",
        "s3:GetBucketAcl",
        "s3:GetBucketPolicy",

```

```

        "s3:GetBucketPolicyStatus"
      ],
      "Resource": "*"
    }
  ]
}

```

지침

다음 단계에 따라 자동화를 구성합니다.

1. Systems Manager [AWSSupport-RunEC2RescueForWindowsTool](#)의 문서로 이동합니다.
2. Execute automation(자동화 실행)을 선택합니다.
3. 입력 파라미터에 다음을 입력합니다.
 - 명령(필수):
 - 설명: (필수) 수행할 작업입니다.
 - 유형: String
 - 허용 값: [ResetAccess, CollectLogs, FixAll]
 - 기본값: ResetAccess
 - 파라미터(필수):
 - 설명: (필수) 명령의 파라미터:
 - 의 경우ResetAccess: AWS KMS 키 ID 또는 별칭(기본값: alias/aws/ssm)
 - 의 경우CollectLogs: 로그를 업로드할 Amazon S3 버킷 이름입니다.
 - 의 경우FixAll: 오프라인 문제 해결의 디바이스 이름(예: xvdf)
 - 유형: String
 - 패턴 허용: `^[0-9a-z][a-z0-9-.]{3,63}$|^((dev\/[a-z0-9]{2,10}|xv[a-z0-9]{1,10})$|^((alias\\aws\\ssm|[a-zA-Z0-9-/_]{1,32}))$`
4. 실행을 선택합니다.
5. 자동화가 시작됩니다.
6. 문서는 다음 단계를 수행합니다.
 - installEC2Rescue:

Systems Manager Distributor 패키지를 사용하여 Amazon EC2 Rescue for Windows Server 문제 해결 도구를 설치합니다 [AWSSupport-EC2Rescue](#).

- `runEC2RescueForWindows`:

명령 파라미터에 지정된 작업으로 PowerShell 스크립트를 실행하여 요청된 작업을 수행합니다.

7. 완료 후 출력 섹션에서 실행의 자세한 결과를 검토합니다.

참조

Systems Manager Automation

- [이 자동화 실행\(콘솔\)](#)
- [자동화 실행](#)
- [Automation 설정](#)
- [자동화 워크플로 지원](#)
- [Systems Manager Run Command와 함께 Windows Server용 Amazon EC2 Rescue 사용](#)

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. 인스턴스가 AWS CloudFormation 스택의 일부인 경우에도 실행서는 인스턴스 유형을 변경하지 않습니다. 이러한 동작 중 하나를 변경하려면 AllowInstanceStoreInstances 및 AllowCloudFormationInstances 파라미터의 yes을 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 실행](#)을 참조하세요.

두 파라미터 중 하나에 값을 지정하지 않으면, 자동화가 실패합니다.

Important

AWSPremiumSupport-* 실행서에 액세스하려면 Business + Support, Enterprise Support 또는 통합 운영 구독이 필요합니다. 자세한 내용은 [AWS Support 플랜 비교](#)를 참조하세요.

고려 사항

- 이 실행서를 사용하기 전에 인스턴스를 백업해 두는 것이 좋습니다.
- 인스턴스 유형 변경의 호환성에 대한 자세한 내용은 [인스턴스 유형 변경 호환성](#)을 참조하세요.
- 자동화가 실패하고 원래 인스턴스 유형으로 롤백되는 경우, [인스턴스 유형 변경 문제 해결](#)을 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 시작](#)을 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) yes를 지정하면 CloudFormation 스택의 일부인 인스턴스에서 실행서가 실행됩니다.

- DryRun

유형: 문자열

유효한 값: no | yes

기본값: 아니요

설명: (선택 사항) yes을 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 대소문자를 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`를 실행합니다.
 - b. `running` 또는 `pending`인 경우, Amazon EC2 인스턴스가 상태 검사를 통과할 때까지 자동화가 `aws:waitForAwsResourceProperty`를 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`: 자동화가 Amazon EC2 인스턴스가 CloudFormation 스택의 일부인지 확인할지 여부에 따라 자동화를 분기합니다.
 - a. `aws:executeScript` `DescribeStackResources` API 작업을 호출하여 Amazon EC2 인스턴스가 CloudFormation 스택에 속하지 않도록 합니다.
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.

17aws: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.

18aws:branch: DryRun 파라미터 값이 yes으로 설정되었는지 여부에 따라 자동화를 분기합니다. yes인 경우, 자동화가 종료됩니다.

19aws:branch: 원본 인스턴스 유형과 대상 인스턴스 유형이 동일한 내용인지 확인합니다. 동일하면, 자동화가 종료됩니다.

20aws:executeAwsApi: 현재 인스턴스 상태를 가져옵니다.

21aws:changeInstanceState: Amazon EC2 인스턴스를 중지합니다.

22aws:changeInstanceState: 인스턴스가 stopping 상태에서 멈춘 경우, 인스턴스를 강제로 중지합니다.

23aws:executeAwsApi: 인스턴스 유형을 대상 인스턴스 유형으로 변경합니다.

24aws:sleep: 최종 일관성을 위해 인스턴스 유형을 변경한 후 3초 동안 기다립니다.

25aws:branch: 이전 인스턴스 상태를 기반으로 자동화를 분기합니다. 해당 내용이 running이었을 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 멈춘 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.

26aws:sleep: 실행서를 종료하기 전에 기다립니다.

AWSsupport-ShareEncryptedAMIorEBSSnapshot

설명

이 실행서는 암호화된 또는 Amazon Elastic Block Store 스냅샷 Amazon Machine Image을 다른 Amazon Web Services 계정과 공유하는 프로세스를 자동화합니다. 이 실행서는 AWS Key Management Service 키 정책 수정 및 리소스 권한 업데이트를 포함하여 암호화된 리소스의 교차 계정 공유에 대한 복잡한 요구 사항을 처리합니다.

이 자동화는 AWS 보안 블로그 문서 [계정 간에 암호화된 AMI를 공유하여 암호화된 Amazon Elastic Compute Cloud 인스턴스를 시작하는 방법에](#) 설명된 단계를 수행합니다.

중요 고려 사항

- 이 실행서는 리소스를 수정합니다. 실행서는 AWS KMS 고객 관리형 키(CMK) 정책에 교차 계정 권한을 추가하고 대상 계정에 AMI 시작 권한 또는 Amazon EBS 스냅샷 생성 볼륨 권한을 부여합니다.
- 추가 비용 적용: 리소스(다른 리전 또는 AWS 관리형 키 암호화)를 복사할 때 새 AMI 또는 Amazon EBS 스냅샷 및 리전 간 데이터 전송에 대해 추가 비용이 발생합니다.
- 대상 계정 ID 확인: 이 실행서는 계정 존재를 검증할 수 없으므로 대상 계정 ID를 다시 확인합니다.
- 수동 확인을 통한 자동 롤백: 이 실행서는 실패 시 변경 사항을 자동으로 롤백하려고 시도합니다. 그러나 롤백 자체가 실패할 경우 계정에 추가 AMI/스냅샷 복사본이 남아 있지 않고, 리소스 LaunchPermission/CreateVolumePermission 속성에 의도하지 않은 계정이 포함되어 있지 않으며, AWS KMS 키 정책이 원래 상태인지 확인하십시오.

어떻게 작동하나요?

실행서는 다음과 같은 상위 수준 단계를 수행합니다.

- 입력 리소스 존재, 상태 및 암호화 구성을 검증합니다.
- 대상 계정과 현재 리소스 공유 권한을 확인합니다.
- AWS KMS 키 정책을 분석하고 필요한 모든 변경 사항에 대한 포괄적인 미리 보기를 생성합니다.
- 변경을 수행하기 전에 지정된 보안 주체의 승인을 요청합니다.
- 리소스 복사(필요한 경우), 권한 업데이트 및 AWS KMS 키 정책 수정을 포함하여 승인된 변경 사항을 실행합니다.

- 필요한 경우 롤백 정보가 포함된 포괄적인 실행 보고서를 제공합니다.

이 자동화 실행(콘솔)

필수 IAM 권한

실행서를 성공적으로 사용하려면 AutomationAssumeRole 파라미터에 다음 작업이 필요합니다.

AutomationAssumeRole 파라미터에는 다음 작업이 필요합니다.

- ec2:DescribeImages
- ec2:DescribeSnapshots
- ec2:DescribeImageAttribute
- ec2:DescribeSnapshotAttribute
- ec2:ModifyImageAttribute
- ec2:ModifySnapshotAttribute
- ec2:CopyImage
- ec2:CopySnapshot
- ec2:DeregisterImage
- ec2>DeleteSnapshot
- kms:DescribeKey
- kms:GetKeyPolicy
- kms:PutKeyPolicy
- kms>CreateGrant
- kms:GenerateDataKey*
- kms:ReEncrypt*
- kms:Decrypt
- accessanalyzer:CheckAccessNotGranted

지침

다음 단계에 따라 자동화를 구성합니다.

1. Systems Manager [AWSSupport-ShareEncryptedAMI0rEBSSnapshot](#)의 문서로 이동합니다.
2. Execute automation(자동화 실행)을 선택합니다.

3. 입력 파라미터에 다음을 입력합니다.

- **AutomationAssumeRole(선택 사항):**

Systems Manager Automation이 사용자를 대신하여 작업을 수행하도록 허용하는 AWS AWS Identity and Access Management 역할의 Amazon 리소스 이름입니다. 역할을 지정하지 않은 경우, Systems Manager Automation에서는 이 실행서를 시작하는 사용자의 권한을 사용합니다.

- **승인자(필수):**

작업을 승인하거나 거부할 수 있는 AWS 인증된 보안 주체의 목록입니다. 최대 승인자 수 10 명입니다. 사용자 이름, 사용자 ARN, IAM 역할 ARN 또는 IAM 수임 역할 ARN 형식 중 하나를 사용하여 보안 주체를 지정할 수 있습니다.

- **ResourceId(필수):**

AMI 또는 공유할 Amazon EBS 스냅샷 ID(예: ami-123456789012 또는 snap-123456789012).

- **DestinationAccountId(필수):**

리소스를 공유할 12자리 AWS 계정 ID입니다.

- **CustomerManagedKeyId(선택 사항):**

AWS KMS 리소스를 다시 암호화하기 위한 CMK ID입니다. 리소스가 AWS 관리형 키로 암호화되거나 리전 간 복사를 위해 DestinationRegion이 지정된 경우 필요합니다. 리전 간 복사의 경우 이 키가 대상 리전에 있어야 합니다.

- **DestinationRegion(선택 사항):**

리소스를 복사할 AWS 리전입니다. 기본값은 현재 리전입니다. 다른 리전을 지정하면 CustomerManagedKeyId 파라미터에 지정된 AWS KMS CMK를 사용하여 리소스가 대상 리전으로 복사됩니다.

4. 실행을 선택합니다.

5. 자동화가 시작됩니다.

6. 문서는 다음 단계를 수행합니다.

- **ValidateResources:**

입력 리소스 존재, 상태, 암호화 구성을 검증하고 공유에 필요한 변경 사항을 결정합니다.

- **BranchOnResourcePermission:**

리소스 공유 권한을 확인해야 하는지 여부에 따라 워크플로를 분기합니다.

- **CheckResourcePermission:**

대상 계정에 리소스에 대한 필수 공유 권한이 있는지 확인합니다.

- **AnalyzeChanges:**

AWS KMS 키 정책을 분석하고 필요한 모든 변경 사항에 대한 포괄적인 미리 보기를 생성합니다.

- **BranchOnChanges:**

변경 사항에 승인이 필요한지 여부에 따라 워크플로를 분기합니다.

- **GetApproval:**

지정된 AWS IAM 보안 주체의 승인이 필요한 변경을 진행할 때까지 기다립니다.

- **ExecuteChanges:**

실패 시 롤백과 함께 승인된 변경 사항을 실행합니다.

- **Results:**

암호화된 AMI 또는 스냅샷 공유 프로세스 중에 수행된 모든 작업을 요약하는 포괄적인 실행 보고서를 생성합니다.

7. 완료 후에는 Outputs 섹션에서 실행의 세부 결과를 검토합니다.

대상 계정에 필요한 AWS AWS Identity and Access Management 정책

대상 계정의 IAM 역할 또는 사용자는 암호화된 공유에서 암호화된 Amazon EC2 인스턴스를 시작AMI 하거나 암호화된 공유 Amazon EBS 스냅샷에서 볼륨을 생성하도록 다음 IAM 권한을 구성해야 합니다.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "kms:DescribeKey",
        "kms:ReEncrypt*",
        "kms:CreateGrant",
        "kms:Decrypt"
      ],
      "Resource": [
        "arn:aws:kms:<region>:<account-id>:key/<key-id>"
      ]
    }
  ]
}
```

```

    }
  ]
}

```

참조

Systems Manager Automation

- [이 자동화 실행\(콘솔\)](#)
- [자동화 실행](#)
- [Automation 설정](#)
- [자동화 워크플로 지원](#)
- [AWS KMS 키 공유](#)

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 찾으려 하는 마지막 날짜입니다.

- InplaceSwap

유형: 부울

유효한 값: true | false

설명: (선택 사항) 이 파라미터의 값을 true로 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 true로 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 찾으려 하는 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.

21aws:executeAwsApi - 인스턴스를 시작합니다.

22aws:waitForAwsResourceProperty - 인스턴스 상태가 available가 될 때까지 기다립니다.

23aws:waitForAwsResourceProperty - 인스턴스에 대한 시스템 및 인스턴스 상태 확인이 통과할 때까지 기다립니다.

24aws:executeScript - 스크립트를 실행하여 볼륨을 성공적으로 생성하는 데 사용할 수 있는 스냅샷을 찾습니다.

25aws:executeScript - 스크립트를 실행하여 자동화가 식별한 스냅샷에서 새로 생성된 볼륨을 사용하거나 SnapshotId 파라미터에 지정한 스냅샷에서 생성한 볼륨을 사용하여 인스턴스를 복구합니다.

26aws: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 수집하는데 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 `EC2Rescue`를 설치합니다.
2. `aws:runCommand` - `EC2Rescue`를 사용하여 Windows 문제 해결 로그를 수집하는 PowerShell 스크립트를 실행합니다.
3. `aws:runCommand` - `EC2Rescue`를 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 볼륨이 헬퍼 인스턴스(EC2Rescue 인스턴스)에 연결되고 탑재됩니다. 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 Machine Images(AMIs)에서 생성된 Amazon EC2 인스턴스는 이 자동화에서 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:EC2RESCUE_ACCOUNT_ID	{{ global:ACCOUNT_ID }}	123456789012
\$env:EC2RESCUE_DATE	{{ global:DATE }}	2018-09-07
\$env:EC2RESCUE_DATE_TIME	{{ global:DATE_TIME }}	2018-09-07_18.09.59
\$env:EC2RESCUE_EC2RW_DIR	Windows용 EC2Rescue 설치 경로	C:\Program Files\Amazon\EC2Rescue
\$env:EC2RESCUE_EC2RW_DIR	Windows용 EC2Rescue 설치 경로	C:\Program Files\Amazon\EC2Rescue
\$env:EC2RESCUE_EXECUTION_ID	{{ automation: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 EBS 드라이브	xvdf

변수	설명	예시 값
\$env:EC2RESCUE_OFFLINE_KERNEL_VER	오프라인 Windows 커널 버전	6.1.7601.24214
\$env:EC2RESCUE_OFFLINE_OS_ARCHITECTURE	오프라인 Windows 아키텍처	AMD64
\$env:EC2RESCUE_OFFLINE_OS_CAPTION	오프라인 Windows 캡션	Windows Server 2008 R2 Datacenter
\$env:EC2RESCUE_OFFLINE_OS_TYPE	오프라인 Windows OS 유형	Server
\$env:EC2RESCUE_OFFLINE_PROGRAM_FILES_DIR	오프라인 Windows 프로그램 파일 디렉터리 경로	D:\Program Files
\$env:EC2RESCUE_OFFLINE_PROGRAM_FILES_X86_DIR	오프라인 Windows 프로그램 파일 x86 디렉터리 경로	D:\Program Files (x86)
\$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	{{ global:REGION }}	us-west-1
\$env:EC2RESCUE_S3_BUCKET	{{ S3BucketName }}	amzn-s3-demo-bucket
\$env:EC2RESCUE_S3_PREFIX	{{ S3Prefix }}	myprefix/
\$env:EC2RESCUE_SOURCE_INSTANCE	{{ InstanceId }}	i-abcdefgh123456789

변수	설명	예시 값
\$script:EC2RESCUE_OFFLINE_WINDOWS_INSTALL	오프라인 Windows 설치 메타 데이터	고객 Powershell 객체

Linux:

변수	설명	예시 값
EC2RESCUE_ACCOUNT_ID	{{ global:ACCOUNT_ID }}	123456789012
EC2RESCUE_DATE	{{ global:DATE }}	2018-09-07
EC2RESCUE_DATE_TIME	{{ global:DATE_TIME }}	2018-09-07_18.09.59
EC2RESCUE_EC2RL_DIR	Linux용 EC2Rescue 설치 경로	/usr/local/ec2rl-1.1.3
EC2RESCUE_EXECUTION_ID	{{ automation:EXECUTION_ID }}	7ef8008e-219b-4aca-8bb5-65e2e898e20b
EC2RESCUE_OFFLINE_DEVICE	오프라인 디바이스 이름	/dev/xvdf1
EC2RESCUE_OFFLINE_EBS_DEVICE	오프라인 루트 볼륨 EBS 드라이브	/dev/sdf
EC2RESCUE_OFFLINE_SYSTEM_ROOT	오프라인 루트 볼륨 탑재 지점	/mnt/mount
EC2RESCUE_PYTHON	Python 버전	python2.7
EC2RESCUE_REGION	{{ global:REGION }}	us-west-1
EC2RESCUE_S3_BUCKET	{{ S3BucketName }}	amzn-s3-demo-bucket
EC2RESCUE_S3_PREFIX	{{ S3Prefix }}	myprefix/

변수	설명	예시 값
EC2RESCUE_SOURCE_INSTANCE	{{ InstanceId }}	i-abcdefgh123456789

문서 유형

자동화

소유자

Amazon

플랫폼

Linux, macOS, Windows

파라미터

- AMIPrefix

유형: 문자열

기본값: AWSsupport-EC2Rescue

설명: (선택 사항) 백업 AMI 이름의 접두사입니다.

- 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.

- CreatePostEC2RescueBackup

유형: 문자열

유효한 값: true | false

기본값: false

설명: (선택 사항) 시작하기 전에 스크립트를 실행한 후 InstanceId의 AMI를 생성하려면 true로 설정합니다. AMI가 자동화 완료 이후에도 지속됩니다. AMI에 대한 액세스를 보호하거나 AMI를 삭제하는 일은 고객의 책임입니다.

- CreatePreEC2RescueBackup

유형: 문자열

유효한 값: true | false

기본값: false

설명: (선택 사항) 스크립트를 실행하기 전에 InstanceId의 AMI를 생성하려면 true로 설정합니다. AMI가 자동화 완료 이후에도 지속됩니다. AMI에 대한 액세스를 보호하거나 AMI를 삭제하는 일은 고객의 책임입니다.

- EC2RescueInstanceType

유형: 문자열

유효한 값: t2.small | t2.medium | t2.large | t3.small | t3.medium | t3.large | i3.large

기본값: t3.medium

설명: (선택 사항) EC2Rescue 인스턴스의 EC2 인스턴스 유형입니다.

- InstanceId

유형: 문자열

설명: (필수) EC2 인스턴스의 ID입니다. 중요: AWS Systems Manager Automation은 이 인스턴스를 중지합니다. 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 Linux이면 Bash를 사용하고, Windows이면 PowerShell을 사용합니다.

- S3BucketName

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 ID입니다. 기본적으로 제공된 인스턴스가 상주하는 동일 서브넷이 사용됩니다. 중요: 사용자 지정 서브넷을 제공하는 경우 서브넷이 InstanceId와 동일한 가용 영역이어야 하며 SSM 엔드포인트와의 통신을 허용해야 합니다.

- UniqueId

유형: 문자열

기본값: {{ automation:EXECUTION_ID }}

설명: (선택 사항) 자동화의 고유한 식별자입니다.

필수 IAM 권한

실행서를 성공적으로 사용하려면 AutomationAssumeRole 파라미터에 다음 작업이 필요합니다.

자동화를 실행하는 사용자에게 AmazonSSMAutomationRole IAM 관리형 정책이 연결되도록 하는 것이 좋습니다. 해당 정책 외에도, 사용자에게 다음이 필요합니다.

JSON

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

```

        "Action": [
            "lambda:InvokeFunction",
            "lambda:DeleteFunction",
            "lambda:GetFunction"
        ],
        "Resource": "arn:aws:lambda:*:111122223333:function:AWSSupport-
EC2Rescue-*",
        "Effect": "Allow"
    },
    {
        "Action": [
            "s3:GetObject",
            "s3:GetObjectVersion"
        ],
        "Resource": [
            "arn:aws:s3:::awssupport-ssm.*/*.template",
            "arn:aws:s3:::awssupport-ssm.*/*.zip"
        ],
        "Effect": "Allow"
    },
    {
        "Action": [
            "iam:CreateRole",
            "iam:CreateInstanceProfile",
            "iam:GetRole",
            "iam:GetInstanceProfile",
            "iam:PutRolePolicy",
            "iam:DetachRolePolicy",
            "iam:AttachRolePolicy",
            "iam:PassRole",
            "iam:AddRoleToInstanceProfile",
            "iam:RemoveRoleFromInstanceProfile",
            "iam>DeleteRole",
            "iam>DeleteRolePolicy",
            "iam>DeleteInstanceProfile"
        ],
        "Resource": [
            "arn:aws:iam::111122223333:role/AWSSupport-EC2Rescue-*",
            "arn:aws:iam::111122223333:instance-profile/AWSSupport-EC2Rescue-
*"
        ],
        "Effect": "Allow"
    },
    {

```



```

    "Action": [
        "lambda:CreateFunction",
        "ec2:CreateVpc",
        "ec2:ModifyVpcAttribute",
        "ec2:DeleteVpc",
        "ec2:CreateInternetGateway",
        "ec2:AttachInternetGateway",
        "ec2:DetachInternetGateway",
        "ec2:DeleteInternetGateway",
        "ec2:CreateSubnet",
        "ec2:DeleteSubnet",
        "ec2:CreateRoute",
        "ec2:DeleteRoute",
        "ec2:CreateRouteTable",
        "ec2:AssociateRouteTable",
        "ec2:DisassociateRouteTable",
        "ec2:DeleteRouteTable",
        "ec2:CreateVpcEndpoint",
        "ec2:DeleteVpcEndpoints",
        "ec2:ModifyVpcEndpoint",
        "ec2:Describe*"
    ],
    "Resource": "*",
    "Effect": "Allow"
}
]
}

```

문서 단계

1. aws:executeAwsApi - 제공된 인스턴스를 설명합니다.
2. aws:executeAwsApi - 제공된 인스턴스의 루트 볼륨을 설명합니다.
3. aws:assertAwsResourceProperty - 루트 볼륨 디바이스 유형이 EBS인지 확인합니다.
4. aws:assertAwsResourceProperty - 루트 볼륨이 암호화되지 않았는지 확인합니다.
5. aws:assertAwsResourceProperty- 제공된 서브넷 ID를 확인합니다.
 - a. (현재 인스턴스 서브넷 사용) - *SubnetId = SelectedInstanceSubnet*인 경우를 실행aws:createStack하여 EC2Rescue CloudFormation 스택을 배포합니다.
 - b. (새 VPC 생성) - *SubnetId = CreateNewVPC*인 경우를 실행aws:createStack하여 EC2Rescue CloudFormation 스택을 배포합니다.

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 헬퍼 인스턴스를 생성하도록 EC2Rescue 스택 업데이트

8. `aws:waitForAwsResourceProperty` - EC2Rescue CloudFormation 스택 업데이트가 완료될 때까지 기다립니다.

9. `aws:executeAwsApi` - EC2Rescue 헬퍼 인스턴스 ID를 가져오는 EC2Rescue CloudFormation 스택 출력을 설명합니다.

10. `aws:waitForAwsResourceProperty` - EC2Rescue 헬퍼 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` - `CreatePreEC2RescueBackup` 입력 값을 확인합니다.

a. (EC2Rescue 이전 백업 생성) - `*CreatePreEC2RescueBackup = true*`인 경우

b. `aws:executeAwsApi` - 제공된 인스턴스의 AMI 백업을 생성합니다.

c. `aws:createTags` - AMI 백업에 태그를 지정합니다.

15. `aws:runCommand` - EC2Rescue 헬퍼 인스턴스에 EC2Rescue를 설치합니다.

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 연결합니다.

`aws:sleep` - 10초 동안 대기 상태로 유지합니다.

`aws:runCommand` - Powershell에서 제공된 오프라인 스크립트를 실행합니다.

b. (인스턴스가 Linux인 경우):

`aws:executeAwsApi` - 루트 볼륨을 EC2Rescue 헬퍼 인스턴스에 `*/dev/sdf*`로 연결합니다.

`aws:sleep` - 10초 동안 대기 상태로 유지합니다.

`aws:runCommand` - Bash에서 제공된 오프라인 스크립트를 실행합니다.

18 `aws:changeInstanceState` - EC2Rescue 헬퍼 인스턴스를 중지합니다.

19 `aws:changeInstanceState` - EC2Rescue 헬퍼 인스턴스를 강제 중지합니다.

20 `aws:executeAwsApi` - 루트 볼륨을 EC2Rescue 헬퍼 인스턴스에서 분리합니다.

21 `aws:executeAwsApi` - 루트 볼륨을 제공된 인스턴스에 다시 연결합니다.

22 `aws:assertAwsResourceProperty` - `CreatePostEC2RescueBackup` 입력 값을 확인합니다.

a. (EC2Rescue 이후 백업 생성) - `*CreatePostEC2RescueBackup = true`인 경우

b. `aws:executeAwsApi` - 제공된 인스턴스의 AMI 백업을 생성합니다.

c. `aws:createTags` - AMI 백업에 태그를 지정합니다.

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

`runScriptForLinux.Output`

`runScriptForWindows.Output`

`preScriptBackup.ImageId`

`postScriptBackup.ImageId`

AWSSupport-TroubleshootActiveDirectoryReplication

설명

AWSSupport-TroubleshootActiveDirectoryReplication 실행서는 대상 도메인 컨트롤러 인스턴스의 공통 설정을 확인하여 Microsoft Active Directory(AD) 도메인 컨트롤러 복제 실패 문제를 해결하는 데 도움이 됩니다. 이 실행서는 제공된 도메인 컨트롤러 인스턴스에 대해 일련의 PowerShell 명령을 실행하여 현재 복제 상태를 확인하고 잠재적으로 도메인 복제 문제를 일으킬 수 있는 오류를 보고합니다. 실

행서는 중지된 경우 복제 중요 서비스(Netlogon, W32Time, 및 KDC)를 선택적으로 시작하고 대상 인스턴스 w32tm /resync /force에서 RPCSS를 실행하여 시스템 시간을 동기화할 수 있습니다.

Important

AWS 관리형 Microsoft AD는 이 실행서의 범위에 속하지 않습니다.

Important

자동화가 대상 인스턴스에서 명령을 실행하는 동안 대상 인스턴스 파일 시스템이 변경됩니다. 이러한 변경 사항에는 로그 디렉터리(\$env:ProgramData\TroubleshootActiveDirectoryReplication) 및 보고서 파일 생성이 포함됩니다.

어떻게 작동하나요?

실행서는 다음과 같은 검사 및 작업을 수행합니다.

- 대상 인스턴스가 Windows를 실행하고 Systems Manager에서 관리되는지 확인합니다.
- PowerShell 스크립트를 실행하여 Active Directory 복제 구성 및 상태를 확인합니다.
- 보안 그룹 및 네트워크 ACL 설정에서 복제 파트너 연결을 확인합니다.
- 시간 동기화 및 중요 서비스 상태를 해결합니다.
- 분석을 위해 지정된 Amazon S3 버킷에 로그 파일을 업로드합니다.

[이 자동화 실행\(콘솔\)](#)

문서 유형

자동화

소유자

Amazon

플랫폼

Windows

파라미터

필수 IAM 권한

실행서를 성공적으로 사용하려면 AutomationAssumeRole 파라미터에 다음 작업이 필요합니다.

- ec2:DescribeInstances
- secretsmanager:GetSecretValue
- ssm:DescribeInstanceInformation
- ssm:SendCommand
- ssm:GetCommandInvocation
- s3:GetBucketAcl
- s3:GetBucketPolicy
- s3:GetBucketPolicyStatus
- s3:GetBucketPublicAccessBlock
- s3:PutObject

정책 예제:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "ec2:DescribeInstances",
        "secretsmanager:GetSecretValue",
        "ssm:DescribeInstanceInformation",
        "ssm:SendCommand",
        "ssm:GetCommandInvocation",
        "s3:GetBucketAcl",
        "s3:GetBucketPolicy",
        "s3:GetBucketPolicyStatus",
        "s3:GetBucketPublicAccessBlock",
        "s3:PutObject"
      ],
      "Resource": "*"
    }
  ]
}
```

```
    }
  ]
}
```

AWS Secrets Manager 설정

복제 확인 PowerShell 스크립트는 런타임 호출을 통해 사용자 이름과 암호를 검색하여 대상 Microsoft Active Directory 도메인 컨트롤러에 연결합니다 AWS Secrets Manager. [AWS Secrets Manager 보안 암호 생성](#)의 단계에 따라 새 AWS Secrets Manager 보안 암호를 생성합니다. 형식의 키/값 페어를 사용하여 사용자 이름과 암호를 저장해야 합니다{"username":"EXAMPLE-USER", "password":"EXAMPLE-PASSWORD"}. AWS Secrets Manager 보안 암호를 생성한 후 보안 암호 ARN에 대한 secretsmanager:GetSecretValue 권한을 대상 도메인 컨트롤러 IAM 인스턴스 프로파일 역할에 부여해야 합니다.

지침

다음 단계에 따라 자동화를 구성합니다.

1. Systems Manager [AWSSupport-TroubleshootActiveDirectoryReplication](#)의 문서로 이동합니다.
2. Execute automation(자동화 실행)을 선택합니다.
3. 입력 파라미터에 다음을 입력합니다.
 - AutomationAssumeRole(선택 사항):
 - 설명: (선택 사항) Systems Manager Automation이 사용자를 대신하여 작업을 수행하도록 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.
 - 유형: AWS::IAM::Role::Arn
 - InstanceId(필수):
 - 설명: (필수) Active Directory 복제 문제를 해결하려는 Amazon EC2 도메인 컨트롤러 인스턴스의 ID입니다. 제공된 인스턴스는 도메인 컨트롤러여야 합니다.
 - 유형: AWS::EC2::Instance::Id
 - SecretsManagerArn(필수):
 - 설명: (필수) Enterprise Admin 또는 Active Directory 도메인 및 포리스트 구성에 액세스할 수 있는 동등한 권한이 있는 Active Directory 사용자 이름과 암호가 포함된 AWS Secrets Manager

보안 암호의 ARN입니다. 형식의 키/값 페어를 사용하여 사용자 이름과 암호를 저장해야 합니다 {"username": "EXAMPLE-USER", "password": "EXAMPLE-PASSWORD"}. 보안 암호 ARN에 대한 secretsmanager:GetSecretValue 권한을 대상 도메인 컨트롤러 IAM 인스턴스 프로파일 역할에 연결해야 합니다.

- 유형: String
 - 허용된 패턴: ^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):secretsmanager:[a-z0-9-]{2,20}:[0-9]{12}:secret:[a-zA-Z0-9]{1}[a-zA-Z0-9\\/_+=.@-]{1,256}\$
 - TimeSync(선택 사항):
 - 설명: (선택 사항) Check 또는를 선택합니다Sync. Check를 선택하면 실행서가 현재 시스템 시간 동기화 상태를 출력합니다. Sync이 선택된 경우 실행서는 대상 인스턴스w32tm /resync /force에서를 실행하여 강제 시간 재동기화를 시도합니다.
 - 유형: String
 - 허용되는 값: [Check, Sync]
 - 기본값: Check
 - ServiceAction(선택 사항):
 - 설명: (선택 사항) Check 또는를 선택합니다Fix. 를 선택하면 실행서가 Check, Netlogon, Windows Time service (W32Time) Remote Procedure Call (RPC) Service및 Key Distribution Center (KDC) 서비스의 현재 상태를 출력합니다. Fix이 선택되면 런북은 중지된 서비스가 있는 경우 이러한 서비스를 시작하려고 시도합니다.
 - 유형: String
 - 허용된 값: [Check, Fix]
 - 기본값: Check
 - LogDestination(필수):
 - 설명: (필수) 명령 출력을 업로드하기 위한 AWS 계정의 Amazon S3 버킷입니다.
 - 유형: String
4. 실행을 선택합니다.
 5. 자동화가 시작됩니다.
 6. 문서는 다음 단계를 수행합니다.
 - assertIfOperatingSystemIsWindows:

제공된 대상 Amazon EC2 인스턴스의 운영 체제가 Windows인지 확인합니다.

- assertIfInstanceIsSsmManaged:

Systems Manager에서 Amazon EC2 인스턴스를 관리하는지 확인합니다. 그렇지 않으면 자동화가 종료됩니다.

- **checkReplication:**

지정된 도메인 컨트롤러 인스턴스에서 PowerShell 스크립트를 실행하여 Active Directory 도메인 복제 구성 및 상태를 가져옵니다.

- **checkInstanceSgAndNACL:**

대상 도메인 컨트롤러 인스턴스와 연결된 보안 그룹 및 네트워크 ACL에서 복제 파트너에 대한 트래픽을 허용하는지 확인합니다.

- **troubleshootReplication:**

PowerShell 스크립트를 실행하여 시간 동기화 및 중요 서비스 상태를 해결합니다.

- **verifyS3BucketPublicStatus:**

에 지정된 Amazon S3 버킷이 익명 또는 퍼블릭 읽기 또는 쓰기 액세스 권한을 LogDestination 허용하는지 확인합니다.

- **runUploadScript:**

PowerShell 스크립트를 실행하여 LogDestination 파라미터에 지정된 AAmazon S3 버킷에 로그 아카이브를 업로드하고 OS에서 아카이브된 로그 파일을 삭제합니다. 로그 파일은 문제 해결에 사용하거나 복제 문제를 해결할 때 AWS Support와 공유할 수 있습니다.

7. 완료 후 출력 섹션에서 실행의 자세한 결과를 검토합니다.

참조

Systems Manager Automation

- [이 자동화 실행\(콘솔\)](#)
- [자동화 실행](#)
- [Automation 설정](#)
- [자동화 워크플로 지원](#)

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 Business + Support, Enterprise Support 또는 통합 운영 구독이 필요합니다. 자세한 내용은 [AWS Support 플랜 비교](#)를 참조하세요.

이 문서는 AWS Managed Services (AMS)와 공동으로 작성되었습니다. AMS를 사용하면 AWS 인프라를 보다 효율적이고 안전하게 관리할 수 있습니다. 또한 AMS는 운영 유연성, 향상된 보안 및 규정 준수, 용량 최적화, 비용 절감 식별을 제공합니다. 자세한 내용은 [AWS Managed Services](#) 단원을 참조하십시오.

[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: Boolean

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 EC2 Instance Connect를 사용하여 Amazon Elastic Compute Cloud(Amazon [Amazon EC2](#)) 인스턴스에 대한 연결을 방해하는 오류를 분석하고 감지하는 데 도움이 됩니다. 지원되지 않는 Amazon Machine Image(AMI), OS 수준 패키지 설치 또는 구성 누락, (IAM) 권한 누락 AWS Identity and Access Management 또는 네트워크 구성 문제로 인한 문제를 식별합니다.

어떻게 작동하나요?

실행서는 Amazon EC2 인스턴스 ID, 사용자 이름, 연결 모드, 소스 IP CIDR, SSH 포트 및 Amazon EC2 Instance Connect에 문제가 발생한 IAM 역할 또는 사용자의 Amazon 리소스 이름(ARN)을 사용합니다. 그런 다음 Amazon EC2 Instance Connect를 사용하여 Amazon EC2 인스턴스에 연결하기 위한 [사전 조건](#)을 확인합니다.

- 인스턴스가 실행 중이고 정상 상태입니다.

- 인스턴스는 Amazon EC2 Instance Connect에서 지원하는 AWS 리전에 있습니다.
- 인스턴스의 AMI는 Amazon EC2 Instance Connect에서 지원됩니다.
- 인스턴스는 인스턴스 메타데이터 서비스(IMDSv2)에 도달할 수 있습니다.
- Amazon EC2 Instance Connect 패키지가 OS 수준에서 올바르게 설치 및 구성되어 있습니다.
- 네트워크 구성(보안 그룹, 네트워크 ACL 및 라우팅 테이블 규칙)을 사용하면 Amazon EC2 Instance Connect를 통해 인스턴스에 연결할 수 있습니다.
- Amazon EC2 Instance Connect를 활용하는 데 사용되는 IAM 역할 또는 사용자는 Amazon EC2 인스턴스에 키를 푸시할 수 있는 액세스 권한이 있습니다.

Important

- 인스턴스 AMI, IMDSv2 연결성 및 Amazon EC2 Instance Connect 패키지 설치를 확인하려면 인스턴스가 SSM 관리형이어야 합니다. 그렇지 않으면 해당 단계를 건너뛰니다. 자세한 내용은 [Amazon EC2 인스턴스가 관리형 노드로 표시되지 않는 이유를 참조하세요](#).
- 네트워크 검사는 SourceIpCIDR이 입력 파라미터로 제공되는 경우 보안 그룹 및 네트워크 ACL 규칙이 트래픽을 차단하는지 여부만 감지합니다. 그렇지 않으면 SSH 관련 규칙만 표시 됩니다.
- [Amazon EC2 Instance Connect 엔드포인트](#)를 사용하는 연결은 이 실행서에서 검증되지 않습니다.
- 프라이빗 연결의 경우 자동화는 SSH 클라이언트가 소스 시스템에 설치되어 있고 인스턴스의 프라이빗 IP 주소에 도달할 수 있는지 확인하지 않습니다.

문서 유형

자동화

소유자

Amazon

플랫폼

Linux

파라미터

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. AWS Systems Manager 콘솔 [AWSsupport-TroubleshootEC2InstanceConnect](#)에서 로 이동합니다.
2. Execute automation(자동화 실행)을 선택합니다.
3. 입력 파라미터에 다음을 입력합니다.
 - InstanceId(필수):

Amazon EC2 Instance Connect를 사용하여 연결할 수 없는 대상 Amazon EC2 인스턴스의 ID입니다.

- AutomationAssumeRole(선택 사항):

Systems Manager Automation이 사용자를 대신하여 작업을 수행할 수 있도록 허용하는 IAM 역할의 ARN입니다. 역할이 지정되지 않은 경우 Systems Manager Automation은 이 실행서를 시작하는 사용자의 권한을 사용합니다.

- 사용자 이름(필수):

Amazon EC2 Instance Connect를 사용하여 Amazon 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 ARN입니다.

- SSHPort(선택 사항):

Amazon EC2 인스턴스에 구성된 SSH 포트입니다. 기본값은 22입니다. 포트 번호는 사이어야 합니다1-65535.

- SourceNetworkType(선택 사항):

Amazon EC2 인스턴스에 대한 네트워크 액세스 방법:

- 브라우저: AWS Management Console에서 연결합니다.
- 퍼블릭: 인터넷을 통해 퍼블릭 서브넷에 있는 인스턴스에 연결합니다(예: 로컬 컴퓨터).
- 프라이빗: 인스턴스의 프라이빗 IP 주소를 통해 연결합니다.
- SourceIpCIDR(선택 사항):

Amazon EC2 Instance Connect를 사용하여 로그인 디바이스(예: 로컬 컴퓨터)의 IP 주소가 포함된 소스 CIDR입니다. 예: 172.31.48.6/32. 퍼블릭 또는 프라이빗 액세스 모드에 값이 제공되지 않으면 실행서는 Amazon EC2 인스턴스 보안 그룹 및 네트워크 ACL 규칙이 SSH 트래픽을 허용하는지 여부를 평가하지 않습니다. 대신 SSH 관련 규칙이 표시됩니다.

Input parameters	
InstanceId (Required) The ID of the Amazon EC2 instance you want to troubleshoot EC2 Instance Connect. ☐ Show interactive instance picker AWS::EC2::Instance::Id	
AutomationAssumeRole (Optional) The Amazon Resource Name (ARN) of the AWS Identity and Access Management (IAM) role that allows Systems Manager Automation to perform the actions on your behalf. If no role is specified, Systems Manager Automation uses the permissions of the user that starts this runbook. String	Username (Required) The username used to connect to the EC2 instance using EC2 Instance Connect. It is used to evaluate if IAM access is granted for this particular user. String
EC2InstanceConnectRoleOrUser (Required) The Amazon Resource Name (ARN) of the AWS Identity and Access Management (IAM) role or user that is being used to leverage EC2 Instance Connect and push keys to the instance. String	SSHPort (Optional) The SSH port configured on the EC2 instance. Default value is '22'. The port number must be between '1-65535'. 22
SourceNetworkType (Optional) The network access method to the EC2 instance: "Browser" : you are connecting to the EC2 instance using your browser by clicking the connect button from the console. "Public" : you are accessing the EC2 instance located in a public subnet over the Internet (example: from your local computer). "Private" : you are connecting to your instance through its private IP address. Browser	SourceIpCIDR (Optional) The source CIDR that includes the IP address of the device you will be logging from using EC2 Instance Connect (such as your local computer). Example: 172.31.48.0/20. None

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 SSM 관리형인 경우 Systems Manager 인스턴스의 ping 상태 및 운영 체제 세부 정보를 가져옵니다.

- CheckIfAWSRegionSupported

Amazon EC2 인스턴스가 Amazon EC2 Instance Connect 지원 AWS 리전에 있는지 확인합니다.

- BranchOnIfAWSRegionSupported

AWS 리전이 Amazon EC2 Instance Connect에서 지원되는 경우 실행을 계속합니다. 그렇지 않으면 출력이 생성되고 자동화가 종료됩니다.

- CheckIfInstanceAMIsSupported

인스턴스와 연결된 AMI가 Amazon EC2 Instance Connect에서 지원되는지 확인합니다.

- BranchOnIfInstanceAMIsSupported

인스턴스 AMI가 지원되는 경우 메타데이터 연결성 및 Amazon EC2 Instance Connect 패키지 설치 및 구성과 같은 OS 수준 검사를 수행합니다. 그렇지 않으면 API를 사용하여 AWS HTTP 메타데이터가 활성화되어 있는지 확인한 다음 네트워크 확인 단계로 이동합니다.

- CheckIMDSReachabilityFromOs:

대상 Amazon EC2 Linux 인스턴스에서 Bash 스크립트를 실행하여 IMDSv2에 도달할 수 있는지 확인합니다.

- CheckEICPackageInstallation:

대상 Amazon EC2 Linux 인스턴스에서 Bash 스크립트를 실행하여 Amazon EC2 Instance Connect 패키지가 제대로 설치 및 구성되었는지 확인합니다.

- CheckSSHConfigFromOs:

대상 Amazon EC2 Linux 인스턴스에서 Bash 스크립트를 실행하여 구성된 SSH 포트가 입력 파라미터 'SSHPort.'와 일치하는지 확인합니다.

- CheckMetadataHTTPEndpointIsEnabled:

인스턴스 메타데이터 서비스 HTTP 엔드포인트가 활성화되어 있는지 확인합니다.

- CheckEICNetworkAccess:

네트워크 구성(보안 그룹, 네트워크 ACL 및 라우팅 테이블 규칙)이 Amazon EC2 Instance Connect를 통해 인스턴스에 연결할 수 있는지 확인합니다.

- CheckIAMRoleOrUserPermissions:

Amazon EC2 Instance Connect를 활용하는 데 사용된 IAM 역할 또는 사용자에게 제공된 사용자 이름을 사용하여 Amazon EC2 인스턴스에 키를 푸시할 수 있는 액세스 권한이 있는지 확인합니다.

- MakeFinalOutput:

모든 이전 단계의 출력을 통합합니다.

7. 완료되면 출력 섹션에서 실행의 자세한 결과를 검토합니다.

대상 인스턴스에 필요한 모든 사전 조건이 있는 경우 실행:

```
▼ Outputs

MakeFinalOutput.ExecutionLogs
Starting the check of EC2 Instance Connect pre-requisites for the instance 'i-██████████'.

### Checking if the AWS region is supported by EC2 Instance Connect ###
SUCCESS: The EC2 instance is located in the AWS region 'eu-west-1' which is one of EC2 Instance Connect supported regions

### Checking if the Amazon Machine Image (AMI) associated to the EC2 instance is supported ###
SUCCESS: The instance AMI 'Ubuntu 22.04' is supported by EC2 Instance Connect

### Checking if Instance Metadata service (IMDSv2) is reachable ###
SUCCESS: Instance metadata is reachable.

### Checking if EC2 Instance Connect package is installed and configured on the instance: https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ec2-instance-connect-set-up.html ###
SUCCESS: 'ec2-instance-connect' package is installed
SUCCESS: 'ec2-instance-connect' is properly configured

|
### Checking SSH configuration at the OS-level ###
WARNING: If you configured a Firewall in the EC2 instance make sure that it allows SSH traffic from the source ip CIDR
INFO: SSH is configured to listen on port 22.
SUCCESS: The configured SSH port (22) matches the provided input port (22).

### Checking Network configuration requirements to access the instance through EC2 Instance Connect using 'Browser' access mode and port '22' ###
SUCCESS: The instance has a public IPv4 address.
SUCCESS: Subnet subnet-██████████ is public.
SUCCESS: SSH access is allowed by security group id 'sg-██████████'
SUCCESS: 'Inbound' NACL allows connection through EC2 instance connect, using the rule: '100'
SUCCESS: 'Outbound' NACL allows connection through EC2 instance connect, using the rule: '100'
SUCCESS: Network requirements to connect to the instance 'i-██████████' using EC2 instance connect are satisfied

### Checking if the required permissions are granted to the IAM identity 'arn:aws:iam:██████████:role/Admin' used to connect to the instance 'i-██████████' through EC2 Instance Connect with the username 'ubuntu' ###
SUCCESS: The IAM identity 'arn:aws:iam:██████████:role/Admin' includes the 'ec2:DescribeInstances' access permission
SUCCESS: The IAM identity 'arn:aws:iam:██████████:role/Admin' includes the 'ec2:SendSSHPublicKey' access permission
```

대상 인스턴스의 AMI가 지원되지 않는 실행:

```
▼ Outputs

MakeFinalOutput.ExecutionLogs
Starting the check of EC2 Instance Connect pre-requisites for the instance 'i-██████████'.

### Checking if the AWS region is supported by EC2 Instance Connect ###
SUCCESS: The EC2 instance is located in the AWS region 'eu-west-1' which is one of EC2 Instance Connect supported regions

### Checking if the Amazon Machine Image (AMI) associated to the EC2 instance is supported ###
ERROR: The instance AMI 'SLES 15.5' is not supported by EC2 Instance Connect. Please make sure to use one of the AMIs listed here: https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ec2-instance-connect-prerequisites.html#ec2-prereqs-ami-
```

참조

Systems Manager Automation

- [이 자동화 실행\(콘솔\)](#)

- [자동화 실행](#)
- [Automation 설정](#)
- [Support Automation Workflows 랜딩 페이지](#)

AWS 서비스 설명서

- [Amazon EC2 Instance Connect를 사용하여 Amazon EC2 인스턴스에 연결하는 문제를 해결하려면 어떻게 해야 하나요?](#)

AWSSupport-TroubleshootLinuxMGNDRSAgentLogs

설명

AWSSupport-TroubleshootLinuxMGNDRSAgentLogs 자동화 실행서는 소스 서버를 AWS 클라우드로 마이그레이션하기 위해 Linux 서버에 AWS Application Migration Service (AWS MGN) 및 AWS Elastic Disaster Recovery (AWS DRS) 복제 에이전트를 설치할 때 발생하는 일반적인 오류를 감지하는 데 사용됩니다.

어떻게 작동하나요?

실행서는 AWS MGN 또는 AWS DRS 설치 로그가 파라미터로 `aws_replication_agent_installer.log` 업로드되는 Amazon Simple Storage Service(Amazon S3) 경로를 AWSSupport-TroubleshootLinuxMGNDRSAgentLogs 사용합니다. 그런 다음 다음 작업을 수행합니다.

- 검증: 제공된 로그 파일이 유효한지, 하나 이상의 에이전트 설치가 포함되어 있는지 확인합니다.
- 구문 분석: 알려진 AWS MGN 또는 AWS DRS 오류에 대해 로그 파일의 최신 에이전트 설치를 철저히 구문 분석합니다.
- 오류 감지 및 해결: 구문 분석을 기반으로 에이전트 설치 프로세스 중에 오류 또는 문제를 감지하고 나열합니다. 감지된 각 오류에 대해 실행서는 문제를 해결하거나 완화하는 데 도움이 되는 자세한 단계를 제공합니다.

[이 자동화 실행\(콘솔\)](#)

문서 유형

자동화

소유자

Amazon

플랫폼

Linux

파라미터

필수 IAM 권한

실행서를 성공적으로 사용하려면 AutomationAssumeRole 파라미터에 다음 작업이 필요합니다.

- s3:GetObject
- s3:ListBucket

지침

다음 단계에 따라 자동화를 구성합니다.

1. Systems Manager [AWSSupport-TroubleshootLinuxMGNDRSAgentLogs](#)의 문서로 이동합니다.
2. Execute automation(자동화 실행)을 선택합니다.
3. 입력 파라미터에 다음을 입력합니다.
 - AutomationAssumeRole(선택 사항):

Systems Manager Automation이 사용자를 대신하여 작업을 수행하도록 허용하는 (IAM) 역할의 Amazon 리소스 이름 AWS AWS Identity and Access Management (ARN)입니다. 역할이 지정되지 않은 경우 Systems Manager Automation은 이 실행서를 시작하는 사용자의 권한을 사용합니다.

- BucketName(필수):

복제 에이전트 로그가 저장되는 Amazon S3 버킷의 이름입니다.

- S3ObjectKey(필수):

복제 에이전트 설치 관리자 로그 파일이 저장되는 Amazon S3 객체의 키입니다. 예: Amazon S3 URI가 s3://bucket_name/path/to/file/aws_replication_agent_installer.log인 경우를 입력해야 합니다 path/to/file/aws_replication_agent_installer.log.

- ServiceName(필수):

복제 에이전트가 설치된 서비스의 이름입니다. 허용되는 값: AWS MGN 또는 AWS DRS

Input parameters	
AutomationAssumeRole (Optional) The Amazon Resource Name (ARN) of the AWS Identity and Access Management (IAM) role that allows Systems Manager Automation to perform the actions on your behalf. If no role is specified, Systems Manager Automation uses the permissions of the user that starts this runbook. ↻	BucketName (Required) The name of the Amazon S3 bucket where the replication agent log is stored. s3bucket-name ↻
S3ObjectKey (Required) The key of S3 object where the replication agent installer log file is stored. Example: if S3 URI is `s3://bucket_name/path/to/file/aws_replication_agent_installer.log` then you should provide `path/to/file/aws_replication_agent_installer.log` as input. aws_replication_agent_installer.log	ServiceName (Required) The name of the service for which the Replication agent is done: **AWS MGN** : AWS Application Migration Service. **AWS DRS** : AWS Elastic Disaster Recovery. AWS MGN

4. 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 복제 에이전트 로그 파일을 읽고 알려진 AWS MGN 또는 AWS DRS 오류를 검색합니다.

- **MakeFinalOutput**

발견된 오류 및 문제 해결 권장 사항에 대한 정보를 포함하여 이전 검사의 출력을 생성합니다.

7. 완료되면 출력 섹션에서 실행의 자세한 결과를 검토합니다.

▼ 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)을 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 ID가 지정되지 않은 경우 AWS Systems Manager 자동화는 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-TroubleshootRDP는 AWSSupport-ExecuteEC2Rescue을 호출하여 오프라인 수정을 수행합니다 - AWSSupport-ExecuteEC2Rescue에 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-ManageWindowsService를 호출합니다.

`aws:executeAutomation` - RDP 설정을 가져오는 `AWSSupport-ManageRDPSettings`를 호출합니다.

c. (온라인 수정) Action = `FixAll`인 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 = `Custom`인 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 = true`를 단정합니다

b. `aws:assertAwsResourceProperty` - Action = `FixAll`를 단정합니다.

c. `aws:assertAwsResourceProperty` - `SubnetId`의 값을 단정합니다.

(제공된 인스턴스의 서브넷 사용) `SubnetId`가 `SELECTED_INSTANCE_SUBNET`인 경우

`aws:executeAwsApi` - 현재 인스턴스의 서브넷을 검색합니다.

`aws:executeAutomation` - 제공된 인스턴스의 서브넷을 사용하여 `AWSSupport-ExecuteEC2Rescue`를 실행합니다.

d. (제공된 사용자 지정 서브넷 사용) `SubnetId`가 `SELECTED_INSTANCE_SUBNET`이 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 주제](#)를 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.

- Instanceld

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 ID가 지정되지 않은 경우 AWS Systems Manager 자동화는 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-TroubleshootSSH는 AWSSupport-ExecuteEC2Rescue을 호출하여 오프라인 수정을 수행합니다 - AWSSupport-ExecuteEC2Rescue에 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-ConfigureAWSPackage를 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-ExecuteEC2Rescue를 실행합니다.
 - v. (제공된 사용자 지정 서브넷 사용) SubnetId가 SelectedInstanceSubnet이 아니면 `aws:executeAutomation`을 통해 제공된 SubnetId 값을 사용하여 AWSSupport-ExecuteEC2Rescue를 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 관리되는지 확인합니다 AWS Systems Manager.
- `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-susecloud.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 `169.254.169.254`에 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

실행서는 Amazon Elastic Compute Cloud(Amazon EC2) Windows 인스턴스에서 진행 중인 성능 문제를 해결하는 AWSSupport-TroubleshootWindowsPerformance 데 도움이 됩니다. 실행서는 대상 인스턴스에서 로그를 캡처하고 CPU, 메모리, 디스크 및 네트워크 성능 지표를 분석합니다. 선택적으로 자동화는 프로세스 덤프를 캡처하여 성능 저하의 잠재적 원인을 파악하는 데 도움이 될 수 있습니다.

또한 이 실행서를 설치하도록 허용하는 경우 자동화는 최신 [EC2Rescue](#) 도구를 사용하여 이벤트 및 시스템 로그를 캡처합니다.

어떻게 작동하나요?

실행서는 다음 단계를 수행합니다.

- Amazon EC2 인스턴스에서 사전 조건을 확인합니다.
- Amazon EC2 Windows 인스턴스의 루트 디스크에 성능 로그를 생성합니다.
- 캡처된 로그를 폴더에 저장합니다. C:\ProgramData\Amazon\SSM\TroubleshootWindowsPerformance
- Amazon Simple Storage Service(Amazon S3) 버킷이 제공되고 자동화 수입 역할에 필요한 권한이 있는 경우 캡처된 로그가 Amazon S3 버킷에 업로드됩니다.
- 최신 EC2Rescue 도구를 Amazon EC2 Windows 인스턴스에 설치하여 설치하도록 선택한 경우 이벤트 및 시스템 로그를 캡처하지만에서 캡처한 프로세스 덤프 및 로그는 분석하지 않습니다EC2Rescue.

Important

- 이 실행서를 실행하려면 Amazon EC2 Windows 인스턴스에서 관리해야 합니다 AWS Systems Manager. 자세한 내용은 [Amazon EC2 인스턴스가 관리형 노드로 표시되지 않는 이유를 참조하세요](#).
- 이 실행서를 실행하려면 Amazon EC2 Windows 인스턴스가 Windows 8.1 / Windows Server 2012 R2(6.3) 이상의 PowerShell 4.0 이상에서 실행 중이어야 합니다. 자세한 내용은 [Windows 운영 체제 버전을 참조하세요](#).
- 성능 로그를 생성하려면 루트 디바이스에 최소 10GB의 여유 공간이 필요합니다. 루트 디스크 크기가 100GB보다 큰 경우 여유 공간은 디스크 크기의 10%보다 커야 합니다. 실행 중에 프로세스를 덤프하는 경우 여유 공간은 10GB보다 커야 하며, 프로세스가 10GB를 초과하는 메모리를 소비할 때 프로세스가 소비하는 총 메모리 크기보다 커야 합니다.
- 루트 디바이스에서 생성된 로그는 자동으로 삭제되지 않습니다.
- 실행서는 EC2Rescue 도구를 제거하지 않습니다. 자세한 내용은 [Windows ServerEC2Rescue용 사용을 참조하세요](#).

- 성능에 영향을 미치는 동안이 자동화를 실행하는 것이 가장 좋습니다. AWS Systems Manager 상태 관리자 연결을 사용하거나 AWS Systems Manager 유지 관리 기간을 예약하여 주기적으로 실행할 수도 있습니다.

[이 자동화 실행\(콘솔\)](#)

문서 유형

자동화

소유자

Amazon

플랫폼

Windows

파라미터

필수 IAM 권한

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 프로파일에 연결된 IAM 역할 또는 인스턴스에 구성된 IAM 사용자는 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 Manager [AWSSupport-TroubleshootWindowsPerformance](#)의 문서로 이동합니다.
2. Execute automation(자동화 실행)을 선택합니다.
3. 입력 파라미터에 다음을 입력합니다.

- AutomationAssumeRole(선택 사항):

Systems Manager Automation이 사용자를 대신하여 작업을 수행하도록 허용하는 (IAM) 역할의 Amazon 리소스 이름 AWS AWS Identity and Access Management (ARN)입니다. 역할이 지정되지 않은 경우 Systems Manager Automation은 이 실행서를 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 시작 시 성능에 영향을 미칠 수 있는 프로세스에 대해 하나의 프로세스 덤프를 캡처할 수 있습니다. 인스턴스 루트 볼륨에는 최소 10GB의 여유 공간이 필요합니다(루트 볼륨 크기가 100GB보다 크면 디스크 크기의 10%를 초과하고, 프로세스가 10GB를 초과하는 메모리를 소비하면 프로세스가 소비하는 총 메모리 크기에 10GB를 더한 값).

- LogCaptureDuration(선택 사항):

문제가 있는 동안이 자동화가 로그를 캡처하는 ~ 사이의 분 수입니다. 기본값은 5입니다.

- **LogUploadBucketName**(선택 사항):

로그를 업로드하려는 계정의 Amazon S3 버킷입니다. 버킷은 서버 측 암호화(SSE)로 구성되어야 하며, 버킷 정책은 캡처된 로그에 액세스할 필요가 없는 당사자에게 불필요한 읽기/쓰기 권한을 부여해서는 안 됩니다. Amazon EC2 Windows 인스턴스는 Amazon S3 버킷에 액세스할 수 있어야 합니다.

- **InstallEC2RescueTool**(선택 사항):

실행서가 최신 버전의 EC2Rescue 도구를 설치하여 Windows 이벤트 및 시스템 로그를 캡처할 수 있도록 Yes하려면 로 설정합니다. 기본값은 No입니다.

- **승인**(필수):

이 자동화 실행서에서 수행하는 작업에 대한 전체 세부 정보를 읽고 동의하는 경우를 입력합니다. Yes, I understand and acknowledge.

Input parameters

InstanceId
(Required) The ID of the Amazon EC2 Windows instance you want to troubleshoot performance issues.

☒ Show interactive instance picker

AutomationAssumeRole
(Optional) The Amazon Resource Name (ARN) of the AWS Identity and Access Management (IAM) role that allows Systems Manager Automation to perform the actions on your behalf. If no role is specified, Systems Manager Automation uses the permissions of the user that starts this runbook.

LogCaptureDuration
(Optional) The number of minutes this automation should capture logs while the issue is present. Default is `5` minutes. You can specify a value between `1` and up to `15` minutes.

InstallEC2RescueTool
(Optional) Set it to `True` if you allow the runbook to install the latest version of the `EC2Rescue` tool to capture the Windows Events and System logs. Default value `No`.

CaptureProcessDump
(Optional) The process dump type to capture. The automation can capture one process dump for the process which is potentially causing the performance impact in the beginning of the automation. The instance root volume will require to have at least 10 GB free space (greater than 10% of the disk size when the root volume size is bigger than 100 GB and 10GB plus the total memory size consumed by the process when the process consumes more than 10GB memory).

LogUploadBucketName
(Optional) The Amazon S3 bucket in your account to upload the logs to. Please make sure the bucket is configured with server-side encryption (SSE), and the bucket policy does not grant unnecessary read/write permissions to parties that do not need to access the logs. Also please make sure EC2 Windows instance has necessary access to the S3 Bucket.

Acknowledgement
(Required) Please read the complete details of the actions performed by this automation runbook and write 'Yes, I understand and acknowledge' if you acknowledge the steps.

4. 실행을 선택합니다.

5. 자동화가 시작됩니다.

6. 문서는 다음 단계를 수행합니다.

- **CheckConcurrency:**

인스턴스를 대상으로 하는 이 실행서의 실행이 하나만 있는지 확인합니다. 실행서가 동일한 인스턴스를 대상으로 하는 다른 실행을 찾으면 오류가 반환되고 종료됩니다.

- **AssertInstanceIsWindows:**

Amazon EC2 인스턴스가 Windows 운영 체제에서 실행되고 있다고 주장합니다. 그렇지 않으면, 자동화가 종료됩니다.

- **AssertInstanceIsManagedInstance:**

Amazon EC2 인스턴스가 관리된다고 주장합니다 AWS Systems Manager. 그렇지 않으면 자동화가 종료됩니다.

- **VerifyPrerequisites:**

인스턴스 OS에서 PowerShell 버전을 확인하고 Systems Manager를 통해 인스턴스를 연결하여 PowerShell 명령을 실행할 수 있도록 합니다. 이 자동화는 Windows 8.1 / Server 2012 R2(6.3) 이상 버전에서 실행되는 PowerShell 4.0 이상을 지원합니다. 버전이 이전 버전인 경우 자동화가 실패합니다. Amazon S3 버킷에 로그를 업로드하도록 선택하면 이 자동화는 AWS Tools for PowerShell 모듈을 사용할 수 있는지 확인합니다. 그렇지 않으면 자동화가 종료됩니다.

- **BranchOnProcessDump:**

성능에 영향을 미치는 프로세스의 덤프를 캡처하도록 설정했는지 여부를 기준으로 분기합니다.

- **CaptureProcessDump:**

인스턴스에 이 자동화를 실행할 공간이 충분한지 확인합니다(가장 높은 CPU/메모리를 선택한 경우).

- **CapturePerformanceLogs:**

디스크 공간을 다시 확인하고 인스턴스에서 PowerShell 스크립트를 실행하여 성능 모니터와 Windows 성능 레코더 로깅을 시작합니다. 정의된 이 충족되면 스크립트 LogCaptureDuration가 중지됩니다.

- **SummarizePerformanceLogs:**

이전 단계인에서 생성된 XML 보고서를 요약 CapturePerformanceLogs하여 자동화에 출력으로 표시된 가장 많은 WorkingSet64(메모리) 및 % 프로세서 시간(CPU)을 소비하는 책임 있는 프로세스를 찾습니다. LogicalDisk, 네트워크 인터페이스, 메모리, TCPv4, IPv4 및 UDPv4 사용에 대한 유사한 정보를 생성하여 analysis_output.log 출력 폴더에 저장합니다.

- **BranchOnInstallEC2Rescue:**

Amazon EC2 인스턴스에 최신 EC2Rescue 도구를 설치하도록 설정한 경우 분기합니다.

- **InstallEC2RescueTool:**

인스턴스 OS에 EC2Rescue 도구를 설치하여를 사용하여 EC2Rescue 로그를 캡처합니다AWS-ConfigureAWSPackage.

- **RunEC2RescueTool:**

인스턴스 OS에서 EC2Rescue 도구를 실행하여 필요한 모든 로그를 캡처합니다.는 공간을 절약하는 데 필요한 로그만 EC2Rescue 캡처합니다.

- **BranchOnIfS3BucketProvided:**

로그를 업로드LogUploadBucketName하는 데 사용할 수 있는 버킷 이름이 있는지 확인하기 위해의 사용자 입력을 기반으로 분기합니다.

- **GetS3BucketPublicStatus:**

Amazon S3 버킷이 제공되는지 여부를 결정하고 제공되는 경우 Amazon S3 버킷이 퍼블릭이 아니며 SSE로 구성되어 있는지 확인합니다.

- **UploadLogResult:**

제공된 Amazon S3 버킷에 로그를 업로드합니다. PowerShell 버전이 5.0 이상인 경우 로그를 ZIP 아카이브로 압축하고 업로드합니다. 업로드가 완료된 후 ZIP 파일을 삭제합니다. PowerShell 버전이 5.0 미만인 경우 파일을 폴더에 직접 업로드합니다.

- **CleanUpLogsOnFailure:**

실패 시 CapturePerformanceLogs 단계에서 생성된 모든 로그를 정리합니다. SSM 에이전트가 제대로 작동하지 않거나 Windows 시스템이 응답하지 않는 경우 CleanUpLogsOnFailure 단계가 실패하거나 제한 시간이 초과될 수 있습니다.

7. 완료되면 출력 섹션에서 실행의 자세한 결과를 검토합니다.

대상 인스턴스에 필요한 모든 사전 조건이 있는 실행입니다.

▼ Outputs

CaptureProcessDump.Output

No output available yet because the step is not successfully executed

CapturePerformanceLogs.Output

The instance has enough space to capture performance logs.

WPR capture process is in 'Stopped' state.

Data Collector Set TroubleshootWindowsPerformance [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 %
sppsv	Processor	0.00	106.00	9.00
WmiPrvSE##2	Processor	0.00	90.00	2.00
MsMpEng	Processor	0.00	38.00	0.75
GenValObj	Processor	0.00	30.00	0.28
svchost##42	Processor	0.00	29.00	0.17

Top 5 Processes which consumed most WorkingSet64 memory as below (in MB):

Process	Counter	Min MB	Max MB	Avg MB
MsMpEng	WorkingSet	220.00	260.00	236.00
Registry	WorkingSet	78.00	193.00	120.00
powershell	WorkingSet	90.00	92.00	92.00
LogonUI	WorkingSet	43.00	43.00	43.00
dwm	WorkingSet	38.00	38.00	38.00

대상 인스턴스가 Linux 플랫폼에 있고 실행에 실패한 실행입니다. 단계 ID를 선택하여 실패 세부 정보를 확인합니다.

▼ Outputs

CapturePerformanceLogs.Output

No output available yet because the step is not successfully executed

CleanUpLogsOnFailure.Output

No output available yet because the step is not successfully executed

SummarizePerformanceLogs.Output

No output available yet because the step is not successfully executed

VerifyPrerequisites.Output

No output available yet because the step is not successfully executed

CaptureProcessDump.Output

No output available yet because the step is not successfully executed

RunEC2RescueTool.Output

No output available yet because the step is not successfully executed

UploadLogResult.Output

No output available yet because the step is not successfully executed

Execution status

Overall status

❌ Failed

Failed

1

All executed steps

2

Cancelled

0

Succeeded

1

TimedOut

0

Executed steps (2)

Find Steps

< 1 >

Step ID	Step #	Step name	Action	Status	Start time	End time
████████████████████	1	CheckConcurrency	aws:executeScript	✅ Success	Tue, 19 Mar 2024 16:13:38 GMT	Tue, 19 Mar 2024 16:14:47 GMT
████████████████████0a3a9	2	AssertInstanceIsWindows	aws:assertAwsResourceProperty	❌ Failed	Tue, 19 Mar 2024 16:15:00 GMT	Tue, 19 Mar 2024 16:15:01 GMT

단계의 실패 세부 정보입니다AssertInstanceIsWindows.

Failure details

Failure message
Step fails when it is Execute/Cancelling action. Property value 'Linux' from the API output is not in the desired values. Desired values: ['Windows']. Please refer to Automation Service Troubleshooting Guide for more diagnosis details.

FailureType	FailureStage
Verification	Invocation
VerificationErrorMessage	
Property value 'Linux' from the API output is not in the desired values. Desired values: ['Windows'].	

참조

Systems Manager Automation

- [이 자동화 실행\(콘솔\)](#)
- [자동화 실행](#)
- [Automation 설정](#)
- [Support Automation Workflows 랜딩 페이지](#)

AWSSupport-TroubleshootWindowsUpdate

설명

AWSSupport-TroubleshootWindowsUpdate 실행서는 Amazon Elastic Compute Cloud(Amazon EC2) Windows 인스턴스에 대한 Windows 업데이트에 실패할 수 있는 문제를 식별하는 데 사용됩니다.

어떻게 작동하나요?

실행서는 다음 단계를 수행합니다.

- 대상 Amazon EC2 인스턴스가에서 관리되는지 확인합니다 AWS Systems Manager.
- AWS Systems Manager 에이전트(SSM 에이전트) 및 Windows Server 버전이 Systems Manager 패치 작업에 지원되는지 확인합니다.
- Windows 업데이트에 권장되는 사용 가능한 디스크 공간과 재부팅이 보류 중인지 확인합니다. 보류 중인 재부팅은 일반적으로 업데이트가 보류 중임을 나타내며 추가 업데이트를 수행하기 전에 재부팅이 필요합니다.
- 연결 문제를 해결하는 데 도움이 될 수 있도록 운영 체제 수준에서 프록시 설정을 구성합니다.
- Amazon Simple Storage Service(Amazon S3) 엔드포인트 연결 테스트를 수행하고 [GetDeployablePatchSnapshotForInstance](#) API 작업을 호출하여 관리형 노드가 사용하는 패치 기준에 대한 현재 스냅샷을 검색합니다.

- 연결이 실패하면은 AWSSupport-AnalyzeAWSEndpointReachabilityFromEC2 실행서를 실행하여 Amazon S3 엔드포인트에 대한 인스턴스의 연결을 분석할 수 있는 옵션을 제공합니다.
- Windows 업데이트 구성을 검증하고 Windows Server Update Services(WSUS)(해당하는 경우)를 테스트합니다.

Important

- Active Directory 도메인 컨트롤러는 지원되지 않습니다.
- Windows Server 버전 2008 R2 또는 이전 버전은 지원되지 않습니다.
- SSM 에이전트 1.2.371 또는 이전 버전은 지원되지 않습니다.
- AWSSupport-AnalyzeAWSEndpointReachabilityFromEC2 실행서는 [VPC Reachability Analyzer](#)를 사용하여 소스와 서비스 엔드포인트 간의 네트워크 연결을 분석합니다. 소스와 대상 간의 분석 실행당 요금이 부과됩니다. 자세한 내용은 [Amazon VPC 요금](#)을 참조하세요.
- Systems Manager가 지원되는 일부 리전에서는 AWSSupport-AnalyzeAWSEndpointReachabilityFromEC2 실행서를 사용할 수 없습니다.

[이 자동화 실행\(콘솔\)](#)

문서 유형

자동화

소유자

Amazon

플랫폼

Windows

파라미터

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 실행서를 실행하려면 [이 문서에](#) 나열된 권한을 `AWSSupport-AnalyzeAWSEndpointReachabilityFromEC2` 추가합니다.

지침

다음 단계에 따라 자동화를 구성합니다.

1. Systems Manager [AWSSupport-TroubleshootWindowsUpdate](#)의 문서로 이동합니다.
2. Execute automation(자동화 실행)을 선택합니다.
3. 입력 파라미터에 다음을 입력합니다.

- `AutomationAssumeRole`(선택 사항):

Systems Manager Automation이 사용자를 대신하여 작업을 수행하도록 허용하는 (IAM) 역할의 Amazon 리소스 이름 AWS AWS Identity and Access Management (ARN)입니다. 역할이 지정되지 않은 경우 Systems Manager Automation은 이 실행서를 시작하는 사용자의 권한을 사용합니다.

- `InstanceId`(필수):

Windows 업데이트가 실패한 Amazon EC2 인스턴스의 ID를 입력합니다.

- `RunVpcReachabilityAnalyzer`(선택 사항):

네트워크 문제가 확장 검사에 의해 결정되거나 지정된 인스턴스 ID가 관리형 인스턴스가 아닌 경우 `AWSSupport-AnalyzeAWSEndpointReachabilityFromEC2` 자동화를 실행 `true`하도록 지정합니다. 이 하위 자동화에 대한 자세한 내용은 [설명서를](#) 참조하세요. 기본값은 `false`입니다.

- `RetainVpcReachabilityAnalysis`(선택 사항):

RunVpcReachabilityAnalyzer가 인 경우에만 관련이 있습니다true. 에서 생성한 네트워크 인사이트 경로 및 관련 분석을 유지true하려면를 지정합니다Reachability Analyzer. 기본적으로 이러한 리소스는 성공적인 분석 후 삭제됩니다. 분석을 유지하기로 선택한 경우 하위 실행서는 분석을 삭제하지 않으며 Amazon VPC 콘솔에서 시각화할 수 있습니다. 콘솔 링크는 하위 자동화 출력에서 사용할 수 있습니다. 기본값입니다false.

Input parameters

InstanceId
(Required) The ID of the Amazon EC2 instance.

☒ Show interactive instance picker

AWS::EC2::Instance::Id

AutomationAssumeRole
(Optional) The Amazon Resource Name (ARN) of the AWS Identity and Access Management (IAM) role that allows Systems Manager Automation to perform the actions on your behalf. If no role is specified, Systems Manager Automation uses the permissions of the user that starts this runbook.

RunVpcReachabilityAnalyzer
(Optional) Specify 'true' to run the 'AWSsupport-AnalyzeAWSEndpointReachabilityFromEC2' automation if a network issue is determined by the extended checks, or if the instance ID specified is not a managed instance. For more information on this child automation, please refer to the documentation above. This parameter defaults to 'false'.

false

RetainVpcReachabilityAnalysis
(Optional) Only relevant if 'RunVpcReachabilityAnalyzer' is true. Specify 'true' to retain the network insight path and related analyses created by VPC Reachability Analyzer. By default, those resources are deleted after successful analysis. If you choose to retain the analysis, the child runbook does not delete the analysis and you can visualize it in the VPC console. The console link will be available in the child automation output. This parameter defaults to 'false'.

false

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

- **getWindowsServerAndSSMAgentVersion:**

대상 인스턴스가에서 관리되는지 AWS Systems Manager 확인하고 SSM 에이전트 버전 및 Windows 버전에 대한 세부 정보를 가져옵니다.

- **assertIfInstanceIsSsmManaged:**

Amazon EC2 인스턴스가 AWS Systems Manager (SSM)에서 관리되는지 확인합니다. 그렇지 않으면 자동화가 종료됩니다.

- **CheckProxy:**

Windows 인스턴스의 모든 프록시 유형을 확인합니다.

- **CheckPrerequisites:**

SSM 에이전트 버전과 Windows 버전을 가져와서 Active Directory 도메인 컨트롤러(DC)인지 확인합니다. 인스턴스가 DC이거나 SSM 에이전트 또는 Windows 버전이 지원되지 않는 경우 실행서는 중지됩니다.

- **CheckDiskSpace:**

Windows 업데이트를 수행하기에 충분한 경우 Windows 인스턴스에서 사용 가능한 디스크 공간을 가져오고 검증합니다.

- **CheckPendingReboot:**

Windows 인스턴스를 통해 보류 중인 재부팅이 있는지 확인합니다.

- **CheckS3Connectivity:**

인스턴스와의 Amazon S3 엔드포인트에 도달할 수 있는지 확인합니다Patchbaseline.

- **branchOnRunVpcReachabilityAnalyzer:**

RunVpcReachabilityAnalyzer이 true이면 자동화를 분기하여 디버깅 Amazon S3 연결에 대한 심층 분석을 실행합니다.

- **GenerateEndpoints:**

Amazon S3 엔드포인트에 대한 확장 연결 검사를 수행할 엔드포인트를 생성합니다.

- **analyzeAwsEndpointReachabilityFromEC2:**

자동화 실행서를 호출AWSSupport-AnalyzeAWSEndpointReachabilityFromEC2하여 선택한 인스턴스가 필요한 엔드포인트에 도달하는지 확인합니다.

- **CheckWindowsUpdateServices:**

Windows 업데이트 서비스 상태 및 시작 유형을 확인합니다.

- **CheckWindowsUpdateSettings:**

Windows 인스턴스를 통해 구성된 Windows 업데이트 정책을 확인합니다.

- **CheckWSUSSettings:**

Windows 업데이트가 WSUS 또는 Microsoft Update Catalog로 구성되어 있는지 확인하고 연결을 확인합니다.

- **CheckWUGlobalSettings:**

Windows 인스턴스를 통해 구성된 Windows 업데이트 전역 설정을 확인합니다.

- **GenerateLogs:**

Windows 업데이트 로그 및 CBS 로그를 인스턴스 데스크톱에 다운로드하고 Windows 이벤트 로그에 장애가 있는지 확인합니다.

• FinalReport:

모든 단계에 대한 전체 보고서를 생성합니다.

7. 완료되면 출력 섹션에서 실행의 자세한 결과를 검토합니다.

```
FinalReport.Results
"
=====Prerequisites Check=====
Result: [PASSED]
INFO: The target instance is not an Active Directory Domain Controller.
INFO: The platform 10.0.20348 is supported.
INFO: The SSM Agent version 3.2.1705.0 is supported.

=====Disk Space Check=====
Result: [PASSED]
INFO: Disk space on drive C: is recommended to run Windows updates.

=====Pending Reboot Check=====
Result: [PASSED]
INFO: There is no pending reboot.

=====Amazon S3 Connectivity Check=====
Result: [PASSED]
Calling GetDeployablePatchSnapshotForInstance API ...
VERBOSE: Invoking AWS Systems Manager operation 'GetDeployablePatchSnapshotForInstance' in region 'eu-west-1'
Downloading Windows Patching file...
Downloading Windows Patching file, attempt: 1/5...
INFO: Deployable Patch Snapshot downloaded successfully

=====AWSSupport-AnalyzeAWSEndpointReachabilityFromEC2=====
Result: [PASSED]
Calling GetDeployablePatchSnapshotForInstance API ...
VERBOSE: Invoking AWS Systems Manager operation 'GetDeployablePatchSnapshotForInstance' in region 'eu-west-1'
Downloading Windows Patching file...
Downloading Windows Patching file, attempt: 1/5...
INFO: Deployable Patch Snapshot downloaded successfully

=====Windows Update Services Status=====
Result: [PASSED]
Getting Services Status and types for Windows Update...
The service 'Application Identity' is currently 'Stopped' and is set to 'Manual'
Starting the service: 'Application Identity'
Service 'Application Identity' started successfully
The service 'Background Intelligent Transfer Service' is currently 'Stopped' and is set to 'Manual'
Starting the service: 'Background Intelligent Transfer Service'
Service 'Background Intelligent Transfer Service' started successfully
INFO: The service 'Cryptographic Services' status is currently 'Running'
The service 'Windows Installer' is currently 'Stopped' and is set to 'Manual'
Starting the service: 'Windows Installer'
Service 'Windows Installer' started successfully
INFO: The service 'Windows Modules Installer' status is currently 'Running'
INFO: The service 'Windows Update' status is currently 'Running'

=====Windows Proxy Settings=====
Result: [PASSED]
No WinInet Proxy is set on the system
No Winhttp Proxy is set on the system
There is no proxy setting for SSM Agent
System Wide Environment HTTP Proxy is not set.
System Wide Environment HTTPS Proxy is not set.
System Wide Environment NO PROXY is not set.
There is no HTTP Proxy configured at local system account user environment.

=====Windows Update Settings=====
Result: [PASSED]
INFO: Windows Update (Policies): Never check for updates
INFO: To modify this setting is in Computer Configuration\Administrative Template\Windows Component\Windows
Update\Configure Automatic Updates. For more details please check this document: https://learn.microsoft.com/de-
de/security-updates/windowsupdateservices/18127451

=====Windows Update Global Settings=====
Result: [PASSED]
Windows Update Client has no restrictions

=====Copy of Windows Update and CBS logs=====
Result: [PASSED]
No errors found in Microsoft-Windows-WindowsUpdateClient events.
INFO: Logs copied to the C:\Windows\TEMP\c176a507-d074-4402-8a5b-631dd643f33a folder
"
```

참조

Systems Manager Automation

- [이 자동화 실행\(콘솔\)](#)
- [자동화 실행](#)
- [Automation 설정](#)
- [Support Automation Workflows 랜딩 페이지](#)

AWS 서비스와 관련된 설명서

- 자세한 내용은 [Troubleshoot Windows Update](#) 문서를 참조하세요.

AWSSupport-UpgradeWindowsAWSDrivers

설명

AWSSupport-UpgradeWindowsAWSDrivers 실행서는 지정된 EC2 인스턴스의 스토리지 및 네트워크 AWS 드라이버를 업그레이드하거나 복구합니다. 실행서는 SSM 에이전트를 호출하여 최신 버전의 AWS 드라이버를 온라인으로 설치하려고 시도합니다. SSM 에이전트에 연결할 수 없는 경우 명시적으로 요청하면 실행서는 AWS 드라이버의 오프라인 설치를 수행할 수 있습니다.

이 실행서는 다음 운영 체제를 지원합니다.

- Windows Server 2016
- Windows Server 2019
- Windows Server 2022
- Windows Server 2025

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 AWS Systems Manager 사용하여 연결되면 us-east-1 리전에서 사용하지 않는 한이 실행서는 실패합니다. 이 실행서는 도메인 컨트롤러에서도 실패합니다. 도메인 컨트롤러에서 AWS PV 드라이버를 업데이트하려면 [도메인 컨트롤러 업그레이드 \(AWS PV 업그레이드\)](#)를 참조하세요.

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 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.

다. 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 InstanceId와 동일한 가용 영역이어야 하며 SSM 엔드포인트와의 통신을 허용해야 합니다.

필수 IAM 권한

실행서를 성공적으로 사용하려면 AutomationAssumeRole 파라미터에 다음 작업이 필요합니다.

명령을 수신하는 EC2 인스턴스는 ssm:StartAutomationExecution 및 ssm:SendCommand가 자동화를 실행하고 인스턴스에 명령을 보낼 수 있는 권한과 ssm:GetAutomationExecution이 자동화 출력을 읽을 수 있는 권한을 포함하는 IAM 역할을 최소한으로 가지고 있어야 합니다.

AmazonSSManagedInstanceCore 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 구성](#)을 참조하세요.

오프라인 업그레이드를 수행하려는 경우 [AWSSupport-StartEC2RescueWorkflow](#)에 필요한 권한을 참조하세요.

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` - ENA 네트워크 드라이버를 설치합니다.
 - iv. `aws:runCommand` - NVMe 드라이버를 설치합니다.
 - v. `aws:runCommand` - AWS PV 드라이버를 설치합니다.
 - b. (오프라인 업그레이드) 입력 인스턴스가 관리형 인스턴스가 아닌 경우:
 - i. `aws:assertAwsResourceProperty` - AllowOffline 플래그가 true로 설정되어 있는지 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` - ForceUpgrade 플래그를 단정합니다.
 - viii. (강제 오프라인 업그레이드) ForceUpgrade = true인 경우 드라이버 강제 업그레이드 스크립트와 함께 `aws:executeAutomation`를 실행하여 `AWSSupport-StartEC2RescueWorkflow`를 호출하십시오. 그러면 설치된 현재 버전과 관계 없이 드라이버가 설치됩니다.

- ix. (오프라인 업그레이드) ForceUpgrade = false인 경우 드라이버 업그레이드 스크립트와 함께 `aws:executeAutomation`를 실행하여 `AWSSupport-StartEC2RescueWorkflow`을 호출하십시오.

출력

`preUpgradeBackup.ImageId`

`preOfflineUpgradeBackup.ImageId`

`installAwsEnaNetworkDriverOnInstance.Output`

`installAWSNVMeOnInstance.Output`

`installAWSPVDriverOnInstance.Output`

`upgradeDriversOffline.Output`

`forceUpgradeDriversOffline.Output`

Amazon ECS

AWS Systems Manager 자동화는 Amazon Elastic Container Service에 사전 정의된 실행서를 제공합니다. 실행서에 대한 자세한 내용은 [실행서 작업](#)을 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 실행서는 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스로부터 운영 체제 및 Amazon Elastic Container Service(Amazon ECS) 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 파라미터 값을 지정하는 경우 대상 인스턴스에는 Linux 인스턴스용 AWS 명령줄 인터페이스(AWS CLI) 또는 Windows PowerShell for Windows 인스턴스용 AWS 도구가 설치되어 있어야 합니다. 자동화는 지정한 Amazon Simple Storage Service(Amazon S3) 버킷의 정책 상태를 평가합니다. Amazon EC2 인스턴스로부터 수집한 로그의 보안을 돕기 위해, 정책 상태 isPublic(이)가 true(으)로 설정되어 있거나 액세스 제어 목록(ACL)이 All Users Amazon S3의 미리 정의된 그룹에 READ|WRITE 권한을 부여하는 경우, 로그는 업로드되지 않습니다. 또한, 제공된 버킷을 계정에서 사용할 수 없는 경우, 로그가 업로드되지 않습니다. Amazon S3 미리 정의된 groups에 대한 자세한 내용은 [Amazon Simple Storage Service 사용 설명서의 Amazon S3 미리 정의된 그룹](#)을 참조하세요.

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.

- 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 할의 Amazon S3 버킷입니다.

필수 IAM 권한

실행서를 성공적으로 사용하려면 AutomationAssumeRole 파라미터에 다음 작업이 필요합니다.

- ssm:ListCommandInvocations
- ssm:ListCommands
- ssm:SendCommand
- ssm:DescribeInstanceInformation

ECSInstanceId 파라미터에서 지정하는 Amazon EC2 인스턴스가

AmazonSSMManagedInstanceCore Amazon 관리형 정책이 연결된 IAM 역할을 가지고 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` 디렉터리에서 아카이브 파일을 생성합니다.
- `runLogCollectionScriptOnWindows` - Windows 인스턴스에서 운영 체제 및 Amazon ECS 관련 로그 파일을 수집하고 `C:\ProgramData\collectECSlogs` 디렉터리에서 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 지정하는 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스에 Amazon Elastic Container Service(Amazon ECS) 에이전트를 설치합니다. 이 실행서는 Amazon Linux 및 Amazon Linux 2 인스턴스만 지원합니다.

[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.

- InstanceIds

유형: StringList

설명: (필수) Amazon ECS 에이전트를 설치하려는 Amazon EC2 인스턴스의 ID입니다.

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 지정하는 Amazon EC2 인스턴스에 Amazon ECS 에이전트를 설치합니다.

출력

InstallAmazonECSAgent.SuccessfullInstances - Amazon ECS 에이전트 설치가 성공한 인스턴스의 ID입니다.

InstallAmazonECSAgent.FailedInstances - Amazon ECS 에이전트 설치가 실패한 인스턴스의 ID입니다.

InstallAmazonECSAgent.InProgressInstances - Amazon ECS 에이전트 설치가 진행 중인 인스턴스의 ID입니다.

AWS-ECSRunTask

설명

AWS-ECSRunTask 실행서는 지정한 Amazon Elastic Container Service(Amazon ECS) 작업을 실행합니다.

[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.

- capacityProviderStrategy

유형: 문자열

설명: (선택 사항) 작업에 사용할 용량 공급자 전략입니다.

- 클러스터

유형: 문자열

설명: (선택 사항) 작업을 실행할 클러스터의 짧은 이름 또는 ARN입니다. 클러스터를 지정하지 않으면 기본 클러스터가 사용됩니다.

- **count**

유형: 문자열

설명: (선택 사항) 클러스터에 배치할 지정된 작업의 인스턴스화 수입니다. 각 요청에 대해 최대 10개의 작업을 지정할 수 있습니다.

- **enableECSTags**

유형: Boolean

설명: (선택 사항) 작업에 Amazon ECS 관리형 태그를 사용할지 여부를 지정합니다. 자세한 내용을 알아보려면 Amazon Elastic Container Service 개발자 안내서의 [Amazon ECS 리소스 태그 지정](#)을 참조하세요.

- **enableExecuteCommand**

유형: Boolean

설명: (선택 사항)이 작업의 컨테이너에 대해 실행 명령 기능을 활성화할지 여부를 결정합니다. true 인 경우 작업의 모든 컨테이너에서 명령 실행 기능이 활성화됩니다.

- **그룹**

유형: 문자열

설명: (선택 사항) 작업과 연결할 작업 그룹의 이름입니다. 기본값은 작업 정의의 패밀리 이름입니다. 예를 들어 family:my-family-name입니다.

- **launchType**

유형: 문자열

유효한 값: EC2 | FARGATE | EXTERNAL

설명: (선택 사항) 독립 실행형 작업을 실행할 인프라입니다.

- **networkConfiguration**

유형: 문자열

설명: (선택 사항) 작업에 대한 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 컨테이너의 이름을 지정하고 수신해야 하는 재정의의 지정하는 JSON 형식의 컨테이너 재정의 목록입니다. 명령 재정의로 작업 정의 또는 Docker 이미지에 지정된 컨테이너의 기본 명령을 재정의할 수 있습니다. 컨테이너의 작업 정의 또는 Docker 이미지에 지정된 기존 환경 변수를 재정의할 수도 있습니다. 또한 환경 재정의로 새 환경 변수를 추가할 수 있습니다.

- placementConstraints

유형: 문자열

설명: (선택 사항) 작업에 사용할 배치 제약 조건 객체의 배열입니다. 작업 정의의 제약 조건과 런타임에 지정된 제약 조건을 포함하여 각 작업에 대해 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) 작업이 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 작업 정의에서 작업으로 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. 이를 통해 ListTasks API 작업의 결과를 필터링하여 특정 작업에 속하는 작업을 식별할 수 있습니다. 최대 36개의 문자(대문자 및 소문자), 숫자, 하이픈(-), 밑줄(_)이 허용됩니다.

- tags

유형: 문자열

설명: (선택 사항) 작업을 분류하고 구성하는 데 도움이 되도록 작업에 적용할 메타데이터입니다. 각 태그는 사용자 정의 키와 값으로 구성됩니다.

- taskDefinition

유형: 문자열

설명: (선택 사항) 실행할 작업 정의의 family 및 revision (family:revision) 또는 전체 ARN입니다. 개정을 지정하지 않으면 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 클러스터를 통한 등록에 실패한 Amazon Elastic Compute Cloud(Amazon EC2) 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`이어야 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.

- ClusterName

유형: 문자열

설명: (필수) 인스턴스가 등록에 실패한 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 클러스터에서 Amazon Elastic Container Service (Amazon ECS) 작업이 시작되지 않은 이유에 대한 문제를 해결하는 데 도움이 됩니다. 시작에 실패한 작업 AWS 리전 과 동일한에서이 실행서를 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

분석 결과 네트워크 연결을 테스트해야 한다고 판단되면 Lambda 함수와 필수 IAM 역할이 계정에 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.

Lambda IAM 역할이 제공되면 자동화는 새 역할을 생성하는 대신 해당 역할을 사용합니다. 제공된 Lambda IAM 역할에는 AWS 관리형 정책이 포함되어야 AWSLambdaVPCAccessExecutionRole 하며 Lambda 서비스 보안 주체가 수임할 수 있도록 허용하는 신뢰 정책이 있어야 합니다 `lambda.amazonaws.com`.

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.

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

- **LambdaRoleArn**

유형: 문자열

설명: (선택 사항) 함수가 필요한 AWS 서비스 및 리소스에 AWS Lambda 액세스할 수 있도록 허용하는 IAM 역할의 ARN입니다. 역할이 지정되지 않은 경우 이 Systems Manager Automation은 관리형 정책을 `NetworkToolSSMRunbookExecution<ExecutionId>` 포함하는 이름으로 계정에 Lambda에 대한 IAM 역할 1개를 생성합니다 `AWSLambdaVPCAccessExecutionRole`.

- **ClusterName**

유형: 문자열

설명: (필수) 작업이 시작되지 않은 Amazon ECS 클러스터의 이름입니다.

- **CloudwatchRetentionPeriod**

유형: 정수

설명: (선택 사항) Amazon CloudWatch Logs에 Lambda 함수 로그를 저장하는 보존 기간(일 단위)입니다. 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:DescribeDhcpOptions`
- `ec2:DescribeInstances`

- `ec2:DescribeInstanceAttribute`
- `ec2:DescribeIamInstanceProfileAssociations`
- `ec2:DescribeSecurityGroups`
- `ec2:DescribeNetworkAcls`
- `ec2:DescribeNetworkInterfaces`
- `ec2:DescribeRouteTables`
- `ec2:DescribeSubnets`
- `ec2:DescribeVpcEndpoints`
- `ec2:DescribeVpcs`
- `ec2:DescribeVpcAttribute`
- `elasticfilesystem:DescribeFileSystems`
- `elasticfilesystem:DescribeMountTargets`
- `elasticfilesystem:DescribeMountTargetSecurityGroups`
- `elasticfilesystem:DescribeFileSystemPolicy`
- `ecr:DescribeImages`
- `ecr:GetRepositoryPolicy`
- `ecs:DescribeContainerInstances`
- `ecs:DescribeServices`
- `ecs:DescribeTaskDefinition`
- `ecs:DescribeTasks`
- `iam:AttachRolePolicy`
- `iam:CreateRole`
- `iam>DeleteRole`
- `iam:DetachRolePolicy`
- `iam:GetInstanceProfile`
- `iam:GetRole`
- `iam:ListRoles`
- `iam:ListUsers`
- `iam:PassRole`
- `iam:SimulateCustomPolicy`

- iam:SimulatePrincipalPolicy
- kms:DescribeKey
- lambda:CreateFunction
- lambda>DeleteFunction
- lambda:GetFunctionConfiguration
- lambda:InvokeFunction
- lambda:TagResource
- logs:DescribeLogGroups
- logs:PutRetentionPolicy
- secretsmanager:DescribeSecret
- ssm:DescribeParameters
- sts:GetCallerIdentity

LambdaRoleArn이 제공되면 자동화가 역할을 생성할 필요가 없으며 다음 권한을 제외할 수 있습니다.

- iam:CreateRole
- iam>DeleteRole
- iam:AttachRolePolicy
- iam:DetachRolePolicy

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 - 분석 결과 네트워크 연결을 테스트해야 한다고 판단되면 VPC에서 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 실행서는 지정하는 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스의 Amazon Elastic Container Service(Amazon ECS) 에이전트를 업데이트합니다. 이 실행서는 Amazon Linux 및 Amazon Linux 2 인스턴스만 지원합니다.

[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.

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

- ClusterARN

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 지정하는 Amazon ECS 클러스터의 Amazon ECS 에이전트를 업데이트합니다.

출력

UpdateAmazonECSAgent.UpdatedContainers - Amazon ECS 에이전트 업데이트가 성공한 인스턴스의 ID입니다.

UpdateAmazonECSAgent.FailedContainers - Amazon ECS 에이전트 업데이트가 실패한 인스턴스의 ID입니다.

UpdateAmazonECSAgent.InProgressContainers - Amazon ECS 에이전트 업데이트가 진행 중인 인스턴스의 ID입니다.

Amazon EFS

AWS Systems Manager 자동화는 Amazon Elastic File System에 사전 정의된 실행서를 제공합니다. 실행서에 대한 자세한 내용은 [실행서 작업](#)을 참조하세요. 실행서 콘텐츠를 보는 방법에 대한 자세한 내용은 [실행서 콘텐츠 보기](#)(을)를 참조하세요.

주제

- [AWSSupport-CheckAndMountEFS](#)

AWSSupport-CheckAndMountEFS

설명

AWSSupport-CheckAndMountEFS 실행서는 Amazon Elastic File System(Amazon EFS) 파일 시스템을 탑재하기 위한 사전 요구 사항을 확인하고 지정하는 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스에 파일 시스템을 탑재합니다. 이 실행서는 DNS 이름을 사용하거나 탑재 대상의 IP 주소를 사용하여 Amazon EFS 파일 시스템을 탑재하는 것을 지원합니다.

[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.

- 작업

유형: 문자열

유효한 값: Check | 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) Amazon EFS 탑재 도우미가 지원하는 옵션 중 파일 시스템을 탑재할 때 사용하려는 옵션입니다. tls 옵션을 지정하는 경우 대상 인스턴스에서 stunel이 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 주소를 통한 탑재는 DNS 호스트 이름이 비활성화된 Virtual Private Cloud(VPC)와 같이 DNS가 비활성화된 환경에서 작동합니다. 또한, 사용자 환경에서 Amazon Route 53(Route 53) 이외의 DNS 공급자를 사용하는 경우에도 이 옵션을 사용할 수 있습니다.

• 리전

유형: 문자열

설명: (필수) Amazon EC2 인스턴스 및 파일 시스템이 AWS 리전 있는 입니다.

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 지정하는 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 파라미터에서 지정하는 Amazon EC2 인스턴스의 포트 2049를 통한 트래픽을 허용하는지 확인합니다.
- `aws:assertAwsResourceProperty` - InstanceId 파라미터에서 지정하는 Amazon EC2 인스턴스가 Systems Manager에서 관리되고 있으며 상태가 Online인지 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 파라미터에서 지정하는 파일 시스템을 탑재하기 위한 사전 요구 사항을 확인하고 InstanceId 파라미터에서 지정하는 Amazon EC2 인스턴스에 파일 시스템을 탑재합니다.

Amazon EKS

AWS Systems Manager Automation은 Amazon Elastic Kubernetes Service에 대한 사전 정의된 실행서를 제공합니다. 실행서에 대한 자세한 내용은 [실행서 작업](#)을 참조하세요. 실행서 콘텐츠를 보는 방법에 대한 자세한 내용은 [실행서 콘텐츠 보기](#)(을)를 참조하세요.

주제

- [AWS-CreateEKSClusterWithFargateProfile](#)
- [AWS-CreateEKSClusterWithNodegroup](#)
- [AWS-DeleteEKSCluster](#)
- [AWS-MigrateToNewEKSSelfManagedNodeGroup](#)
- [AWSPremiumSupport-TroubleshootEKSCluster](#)
- [AWSsupport-TroubleshootEKSWorkerNode](#)

- [AWS-UpdateEKSCluster](#)
- [AWS-UpdateEKSMangedNodeGroup](#)
- [AWS-UpdateEKSSelfManagedLinuxNodeGroups](#)
- [AWSSupport-CollectEKSLinuxNodeStatistics](#)
- [AWSSupport-CollectEKSInstanceLogs](#)
- [AWSSupport-SetupK8sApiProxyForEKS](#)
- [AWSSupport-TroubleshootEbsCsiDriversForEks](#)
- [AWSSupport-TroubleshootEKSSALBControllerIssues](#)
- [AWSSupport-TroubleshootEKSDNSFailure](#)

AWS-CreateEKSClusterWithFargateProfile

설명

AWS-CreateEKSClusterWithFargateProfile 실행서늘을 사용하여 Amazon Elastic Kubernetes Service(Amazon EKS) 클러스터를 생성합니다 AWS Fargate.

[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

다. 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 컨트롤 플레인 사용자가 대신하여 AWS API 작업을 호출할 수 있는 권한을 제공하는 IAM 역할의 ARN입니다.

- **FargateProfileName**

유형: 문자열

설명: (필수) Fargate 프로파일의 이름입니다.

- **FargateProfileRoleArn**

유형: 문자열

설명: (필수) Amazon EKS Pod 실행 IAM 역할의 ARN입니다.

- **FargateProfileSelectors**

유형: 문자열

설명: (필수) 포드를 Fargate 프로파일과 일치시키는 선택기입니다.

- **SubnetIds**

유형: StringList

설명: (필수) Amazon EKS 클러스터에 사용할 서브넷의 IDs입니다. Amazon EKS는 노드와 Kubernetes 컨트롤 플레인 간의 통신을 위해 이러한 서브넷에 탄력적 네트워크 인터페이스를 생성합니다. 2개 이상의 서브넷 ID를 지정해야 합니다.

- **EKSEndpointPrivateAccess**

유형: Boolean

기본값: True

설명: (선택 사항) 클러스터의 Kubernetes API 서버 엔드포인트에 대한 프라이빗 액세스를 허용 True하려면 이 값을 로 설정합니다. 프라이빗 액세스를 활성화하면 클러스터의 VPC 내에서 Kubernetes API 요청이 프라이빗 VPC 엔드포인트를 사용합니다. 프라이빗 액세스를 비활성화하고 클러스터에 노드 또는 AWS Fargate 포드가 있는 경우 노드 또는 Fargate 포드와의 통신에 필요한 CIDR 블록이 `publicAccessCidrs` 포함되어 있는지 확인합니다.

- `EKSEndpointPublicAccess`

유형: Boolean

기본값: False

설명: (선택 사항) 클러스터의 Kubernetes API 서버 엔드포인트에 대한 퍼블릭 액세스를 비활성화 False하려면 이 값을 로 설정합니다. 퍼블릭 액세스를 비활성화하면 클러스터의 Kubernetes API 서버가 시작된 VPC 내에서만 요청을 수신할 수 있습니다.

- `PublicAccessCIDRs`

유형: StringList

설명: (선택 사항) 클러스터의 퍼블릭 Kubernetes API 서버 엔드포인트에 대한 액세스가 허용되는 CIDR 블록입니다. 지정한 CIDR 블록 외부의 주소에서 엔드포인트로의 통신은 거부됩니다. 프라이빗 엔드포인트 액세스를 비활성화하고 클러스터에 노드 또는 Fargate 포드가 있는 경우 필요한 CIDR 블록을 지정해야 합니다.

- `SecurityGroupIds`

유형: StringList

설명: (선택 사항) Amazon EKS에서 계정에 생성한 탄력적 네트워크 인터페이스와 연결할 보안 그룹을 하나 이상 지정합니다.

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 확인합니다ACTIVE.
- `CreateFargateProfile(aws:executeAwsApi)` - 클러스터에 대한 Fargate를 생성합니다.
- `VerifyFargateProfileIsActive(aws:waitForAwsResourceProperty)` - Fargate 프로파일 상태가 인지 확인합니다ACTIVE.

출력

`CreateEKSCluster.CreateClusterResponse`

설명: `CreateCluster` API 호출에서 받은 응답입니다.

`CreateFargateProfile.CreateFargateProfileResponse`

설명: `CreateFargateProfile` API 호출에서 받은 응답입니다.

AWS-CreateEKSClusterWithNodegroup

설명

AWS-CreateEKSClusterWithNodegroup 실행서는 용량에 대한 노드 그룹을 사용하여 Amazon Elastic Kubernetes Service(Amazon EKS) 클러스터를 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.

- ClusterName

유형: 문자열

설명: (필수) 클러스터의 고유한 이름입니다.

- ClusterRoleArn

유형: 문자열

설명: (필수) Kubernetes 컨트롤 플레인 사용자가 사용자를 대신하여 AWS API 작업을 호출할 수 있는 권한을 제공하는 IAM 역할의 ARN입니다.

- NodegroupName

유형: 문자열

설명: (필수) 노드 그룹의 고유한 이름입니다.

- NodegroupRoleArn

유형: 문자열

설명: (필수) 노드 그룹과 연결할 IAM 역할의 ARN입니다. Amazon EKS 작업자 노드 kubelet 데몬은 사용자를 대신하여 API를 AWS 호출합니다. API는 노드는 IAM 인스턴스 프로파일 및 연결 정책을 통해 이 API 직접 호출에 대한 권한을 수신합니다. 노드를 시작해 클러스터에 등록하려면 시작할 때 노드에서 사용할 IAM 역할을 생성해야 합니다.

- SubnetIds

유형: StringList

설명: (필수) Amazon EKS 클러스터에 사용할 서브넷의 IDs입니다. Amazon EKS는 노드와 Kubernetes 컨트롤 플레인 간의 통신을 위해 이러한 서브넷에 탄력적 네트워크 인터페이스를 생성합니다. 2개 이상의 서브넷 ID를 지정해야 합니다.

- EKSEndpointPrivateAccess

유형: Boolean

기본값: True

설명: (선택 사항) 클러스터의 Kubernetes API 서버 엔드포인트에 대한 프라이빗 액세스를 허용True하려면이 값을 로 설정합니다. 프라이빗 액세스를 활성화하면 클러스터의 VPC 내에서 Kubernetes API 요청이 프라이빗 VPC 엔드포인트를 사용합니다. 프라이빗 액세스를 비활성화하고 클러스터에 노드 또는 AWS Fargate 포드가 있는 경우 노드 또는 Fargate 포드와의 통신에 필요한 CIDR 블록이 publicAccessCidrs 포함되어 있는지 확인합니다.

- EKSEndpointPublicAccess

유형: Boolean

기본값: False

설명: (선택 사항) 클러스터의 Kubernetes API 서버 엔드포인트에 대한 퍼블릭 액세스를 비활성화False하려면이 값을 로 설정합니다. 퍼블릭 액세스를 비활성화하면 클러스터의 Kubernetes API 서버가 시작된 VPC 내에서만 요청을 수신할 수 있습니다.

- PublicAccessCIDRs

유형: StringList

설명: (선택 사항) 클러스터의 퍼블릭 Kubernetes API 서버 엔드포인트에 대한 액세스가 허용되는 CIDR 블록입니다. 지정한 CIDR 블록 외부의 주소에서 엔드포인트로의 통신은 거부됩니다. 프라

이빗 엔드포인트 액세스를 비활성화하고 클러스터에 노드 또는 Fargate 포드가 있는 경우 필요한 CIDR 블록을 지정해야 합니다.

- SecurityGroupIds

유형: StringList

설명: (선택 사항) Amazon EKS에서 계정에 생성한 탄력적 네트워크 인터페이스와 연결할 보안 그룹을 하나 이상 지정합니다.

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 확인합니다ACTIVE.
- CreateNodegroup(aws:executeAwsApi) - 클러스터에 대한 노드 그룹을 생성합니다.
- VerifyNodegroupsIsActive(aws:waitForAwsResourceProperty) - 노드 그룹 상태가 인지 확인합니다ACTIVE.

출력

- `CreateEKSCluster.CreateClusterResponse`: `CreateCluster` API 호출에서 수신된 응답입니다.
- `CreateNodegroup.CreateNodegroupResponse`: `CreateNodegroup` API 호출에서 수신된 응답입니다.

AWS-DeleteEKSCluster

설명

이 실행서는 노드 그룹 및 Fargate 프로파일을 포함하여 Amazon EKS 클러스터와 연결된 리소스를 삭제합니다. 선택적으로 모든 자체 관리형 노드, 노드를 생성하는 데 사용되는 CloudFormation 스택, 클러스터의 VPC CloudFormation 스택을 삭제하도록 선택할 수 있습니다. 클러스터 삭제에 대한 자세한 내용은 Amazon EKS 사용 설명서의 [클러스터 삭제](#)를 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 설치](#)를 참조하세요.
2. 다음 명령을 실행하여 클러스터에서 실행 중인 모든 서비스를 나열합니다.

```
kubectl get svc --all-namespaces
```

3. 다음 명령을 실행하여 연결된 EXTERNAL-IP 값이 있는 모든 서비스를 삭제합니다. 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

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.

- EKSClusterName

유형: 문자열

설명: (필수) 삭제할 Amazon EKS 클러스터의 이름입니다.

- VPCCloudFormationStack

유형: 문자열

설명: 삭제 중인 EKS 클러스터의 VPC에 대한 (선택 사항) CloudFormation 스택 이름입니다. 그러면 VPC의 CloudFormation 스택과 스택에서 생성한 모든 리소스가 삭제됩니다.

- VPCCloudFormationStackRole

유형: 문자열

설명: (선택 사항)가 VPC CloudFormation 스택을 삭제하도록 CloudFormation 수임하는 IAM 역할의 ARN입니다.는 역할의 자격 증명을 CloudFormation 사용하여 사용자를 대신하여 호출합니다.

- SelfManagedNodeStacks

유형: 문자열

설명: (선택 사항) 자체 관리형 노드의 CloudFormation 스택 이름 목록을 쉼표로 구분하면 자체 관리형 노드의 CloudFormation 스택이 삭제됩니다.

- SelfManagedNodeStacksRole

유형: 문자열

설명: (선택 사항)가 자체 관리형 노드 스택을 삭제하도록 CloudFormation 수임하는 IAM 역할의 ARN입니다.는 역할의 자격 증명을 CloudFormation 사용하여 사용자를 대신하여 호출합니다.

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 클러스터에서 모든 노드 그룹을 찾아 삭제합니다.
- aws:executeScript - DeleteFargateProfiles: EKS 클러스터에서 모든 Fargate 프로파일을 찾아 삭제합니다.

- `aws:executeScript - DeleteSelfManagedNodes`: 노드를 생성하는 데 사용되는 모든 자체 관리형 노드와 CloudFormation 스택을 삭제합니다.
- `aws:executeScript - DeleteEKSCluster`: EKS 클러스터를 삭제합니다.
- `aws:executeScript - DeleteVPCCloudFormationStack`: VPC CloudFormation 스택을 삭제합니다.

AWS-MigrateToNewEKSSelfManagedNodeGroup

설명

AWS-MigrateToNewEKSSelfManagedNodeGroup 실행서는 기존 애플리케이션을 마이그레이션할 새 Amazon Elastic Kubernetes Service(Amazon EKS) Linux 노드 그룹을 생성하는 데 도움이 됩니다. 자세한 내용은 Amazon EKS 사용 설명서의 [새 노드 그룹으로 마이그레이션](#)을 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.

- OldStackName

유형: 문자열

설명: (필수) 기존 CloudFormation 스택의 이름 또는 스택 ID입니다.

- NewStackName

유형: 문자열

설명: (선택 사항) 새 노드 그룹에 대해 생성된 새 CloudFormation 스택의 이름입니다. 이 파라미터의 값을 지정하지 않으면 스택 이름은 형식을 사용하여 생성됩니다. `NewNodeGroup-ClusterName-AutomationExecutionID`.

- ClusterControlPlaneSecurityGroup

유형: 문자열

설명: (선택 사항) 노드가 Amazon EKS 컨트롤 플레인과 통신하는 데 사용할 보안 그룹의 ID입니다. 이 파라미터의 값을 지정하지 않으면 기존 CloudFormation 스택에 지정된 보안 그룹이 사용됩니다.

- NodeInstanceType

유형: 문자열

설명: (선택 사항) 새 노드 그룹에 사용할 인스턴스 유형입니다. 이 파라미터의 값을 지정하지 않으면 기존 CloudFormation 스택에 지정된 인스턴스 유형이 사용됩니다.

- NodeGroupName

유형: 문자열

설명: (선택 사항) 새 노드 그룹의 이름입니다. 이 파라미터의 값을 지정하지 않으면 기존 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 CloudFormation 스택에 지정된 노드 그룹의 원하는 용량이 사용됩니다.

- NodeAutoScalingGroupMaxSize

유형: 문자열

설명: (선택 사항) 노드 그룹이 확장할 수 있는 최대 노드 수입니다. 이 파라미터의 값을 지정하지 않으면 기존 CloudFormation 스택에 지정된 노드 그룹 최대 크기가 사용됩니다.

- NodeAutoScalingGroupMinSize

유형: 문자열

설명: (선택 사항) 노드 그룹이 축소할 수 있는 최소 노드 수입니다. 이 파라미터의 값을 지정하지 않으면 기존 CloudFormation 스택에 지정된 노드 그룹 최소 크기가 사용됩니다.

- NodeImageId

유형: 문자열

설명: (선택 사항) 노드 그룹에서 사용하려는 Amazon Machine Image(AMI)의 ID입니다.

- NodeImageIdSSMParam

유형: 문자열

설명: (선택 사항) 노드 그룹에서 사용하려는 AMI에 대한 공용 Systems Manager 파라미터입니다.

- NodeVolumeSize

유형: 문자열

설명: (선택 사항) GiB의 노드에 대한 루트 볼륨 크기입니다. 이 파라미터의 값을 지정하지 않으면 기존 CloudFormation 스택에 지정된 노드 볼륨 크기가 사용됩니다.

- NodeVolumeType

유형: 문자열

설명: (선택 사항) 노드의 루트 볼륨에 사용할 Amazon EBS 볼륨의 유형입니다. 이 파라미터의 값을 지정하지 않으면 기존 CloudFormation 스택에 지정된 볼륨 유형이 사용됩니다.

- KeyName

유형: 문자열

설명: (선택 사항) 노드에 할당하려는 키 페어입니다. 이 파라미터의 값을 지정하지 않으면 기존 CloudFormation 스택에 지정된 키 페어가 사용됩니다.

- 서브넷

유형: StringList

설명: (선택 사항) 새 노드 그룹에 사용할 서브넷 IDs의 쉼표로 구분된 목록입니다. 이 파라미터의 값을 지정하지 않으면 기존 CloudFormation 스택에 지정된 서브넷이 사용됩니다.

- `DisableIMDSv1`

유형: Boolean

설명: (선택 사항)를 지정 `true` 하여 인스턴스 메타데이터 서비스 버전 1(IMDSv1)을 비활성화합니다. 기본적으로 노드는 IMDSv1 및 IMDSv2를 지원합니다.

- `BootstrapArguments`

유형: 문자열

설명: (선택 사항) 노드 부트스트랩 스크립트에 전달할 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:DescribeInstanceState`
- `ec2:DescribeInstances`
- `ec2:DescribeKeyPairs`
- `ec2:DescribeLaunchTemplateVersions`
- `ec2:DescribeLaunchTemplates`
- `ec2:DescribeSecurityGroups`
- `ec2:DescribeSubnets`
- `ec2:DescribeVpcs`
- `ec2:RevokeSecurityGroupEgress`
- `ec2:RevokeSecurityGroupIngress`
- `ec2:RunInstances`
- `ec2:TerminateInstances`
- `iam:AddRoleToInstanceProfile`
- `iam:AttachRolePolicy`
- `iam:CreateInstanceProfile`
- `iam:CreateRole`
- `iam:GetInstanceProfile`

- iam:GetRole
- iam:PassRole

문서 단계

- DetermineParameterValuesForNewNodeGroup(aws:executeScript) - 새 노드 그룹에 사용할 파라미터 값을 수집합니다.
- CreateStack(aws:createStack) - 새 노드 그룹에 대한 CloudFormation 스택을 생성합니다.
- GetNewStackNodeInstanceRole(aws:executeAwsApi) - 노드 인스턴스 역할을 가져옵니다.
- GetNewStackSecurityGroup(aws:executeAwsApi) - 이 단계는 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 CloudFormation 스택 이름입니다.

CreateStack.StackId - 새 노드 그룹의 CloudFormation 스택 ID입니다.

AWSPremiumSupport-TroubleshootEKSCluster

설명

AWSPremiumSupport-TroubleshootEKSCluster 실행서는 Amazon Elastic Kubernetes Service(Amazon EKS) 클러스터와 관련된 일반적인 문제를 진단하고 권장 해결 단계를 제공합니다.

⚠ Important

AWSPremiumSupport-* 실행서에 액세스하려면 Business + Support, Enterprise Support 또는 통합 운영 구독이 필요합니다. 자세한 내용은 [AWS Support 플랜 비교](#)를 참조하세요.

S3BucketName 파라미터에 대한 값을 지정하는 경우, 지정하는 Amazon Simple Storage Service(Amazon S3) 버킷의 정책 상태를 자동화에서 평가합니다. EC2 인스턴스로부터 수집한 로그의 보안을 돕기 위해, 정책 상태 isPublic(이)가 true(으)로 설정되어 있거나 액세스 제어 목록(ACL)이 All Users Amazon S3의 미리 정의된 그룹에 READ|WRITE 권한을 부여하는 경우, 로그는 업로드되지 않습니다. Amazon S3의 미리 정의된 그룹에 대한 자세한 내용은 Amazon Simple Storage Service 사용 설명서에서 [Amazon S3의 미리 정의된 그룹](#)을 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.

- ClusterName

유형: 문자열

설명: (필수) 문제를 해결하려는 Amazon EKS 클러스터의 이름입니다.

- S3BucketName

유형: 문자열

설명: (필수) 실행서에서 생성된 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 작업자 노드에 대한 최신 권장 Amazon EKS Amazon Machine Image(AMI)를 가져오려면 다음 퍼블릭 AWS Systems Manager 파라미터에 대한 ssm:GetParameter 작업을 허용해야 합니다.

- `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(Amazon EC2) 인스턴스, Auto Scaling 그룹, AMI, Amazon EC2 GPU 그래픽 인스턴스 유형에 대한 세부 정보를 수집합니다.
- `aws:executeScript` - Amazon EKS 클러스터의 Virtual Private Cloud(VPC), 서브넷, Network Address Translation(NAT) 게이트웨이, 서브넷 경로, 보안 그룹 및 네트워크 액세스 제어 목록(ACL)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 서브넷에서 Amazon EKS 클러스터의 일부로 필요한 태그가 있는지 확인합니다.
- `aws:executeScript` - Amazon VPC 서브넷에서 Elastic Load Balancing 서브넷에 필요한 태그를 확인합니다.

- `aws:executeScript` - 워커 노드 Amazon EC2 인스턴스가 최신 Amazon EKS 최적화 AMI 인스턴스를 사용하는지 확인합니다.
- `aws:executeScript` - 워커 노드에 연결된 Amazon VPC 보안 그룹이 필요한 태그를 제공하는지 확인합니다.
- `aws:executeScript` - Amazon EKS 클러스터와 워커 노드 Amazon VPC 보안 그룹 규칙에서 Amazon EKS 클러스터에 권장되는 수신 규칙을 확인합니다.
- `aws:executeScript` - Amazon EKS 클러스터 및 워커 노드 Amazon VPC 보안 그룹 규칙에서 Amazon EKS 클러스터의 권장 송신 규칙을 확인합니다.
- `aws:executeScript` - Amazon VPC 서브넷의 네트워크 ACL 구성을 확인합니다.
- `aws:executeScript` - 워커 노드 Amazon EC2 인스턴스에 필요한 관리형 정책이 있는지 확인합니다.
- `aws:executeScript` - Auto Scaling 그룹에 클러스터 자동 스케일링에 필요한 태그가 있는지 확인합니다.
- `aws:executeScript` - 워커 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-TroubleshootEKSTaskWorkerNode

설명

이 `AWSSupport-TroubleshootEKSTaskWorkerNode` 실행서는 Amazon Elastic Compute Cloud(Amazon EC2) 워커 노드와 Amazon Elastic Kubernetes Service(Amazon EKS) 클러스터를 분석하여 워커 노드가 클러스터에 가입하지 못하게 하는 일반적인 원인을 식별하고 문제를 해결하는 데 도움이 됩니다. 실행서는 식별된 문제를 해결하는 데 도움이 되는 지침을 출력합니다.

Important

이 자동화를 성공적으로 실행하려면, Amazon EC2 워커 노드의 상태가 `running`이고 Amazon EKS 클러스터 상태가 `ACTIVE`이어야 합니다.

[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.

- ClusterName

유형: 문자열

설명: (필수) Amazon EKS 클러스터의 이름입니다.

- WorkerID

유형: 문자열

설명: (필수) 클러스터에 가입하지 못한 Amazon EC2 워커 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` 파라미터에서 지정하는 Amazon EKS 워커 노드가 존재하고 ACTIVE 상태인지 확인합니다.
- `aws:assertAwsResourceProperty - WorkerID` 파라미터에서 지정하는 Amazon EC2 워커 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(Amazon EKS) 클러스터를 사용하려는 Kubernetes 버전으로 업데이트하는 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.

- 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 될 때까지 기다립니다Successful.

AWS-UpdateEKSMangedNodeGroup

설명

AWS-UpdateEKSMangedNodeGroup 실행서는 Amazon Elastic Kubernetes Service(Amazon EKS) 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

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.

- 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) 사용하려는 Amazon EKS 최적화 AMI 버전입니다. 기본적으로 최신 버전이 사용됩니다.

- ForceUpgrade

유형: Boolean

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 심표로 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 지정하는 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(Amazon EKS) 클러스터의 자체 관리 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 Amazon EKS 사용 설명서의 [kubectl 설치](#)를 참조하세요.
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

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.

- 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.

- DisableIMDSv1

유형: Boolean

설명: (선택 사항) 인스턴스 메타데이터 서비스 버전 1(IMDSv1) 및 IMDSv2를 허용할지 결정합니다.

- 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) 노드 그룹에서 사용하려는 Amazon Machine Image(AMI)의 ID입니다.

- NodeImageIdSSMParam

유형: 문자열

기본값: /aws/service/eks/optimized-ami/1.21/amazon-linux-2/recommended/image_id

설명: (선택 사항) 노드 그룹에서 사용하려는 AMI에 대한 공용 Systems Manager 파라미터입니다.

- StackName

유형: 문자열

설명: (필수) 노드 그룹을 업데이트하는 데 사용되는 CloudFormation 스택의 이름입니다.

- 서브넷

유형: 문자열

설명: (필수) 클러스터에서 사용하려는 서브넷의 씬포로 구분된 목록입니다.

- VpcId

유형: 문자열

기본값: Default

설명: (필수) 클러스터가 배포된 Virtual Private Cloud(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 지정하는 값에 따라 Amazon EKS 클러스터 노드 그룹을 업데이트합니다.
- aws:waitForAwsResourceProperty - CloudFormation 스택 업데이트 상태가 반환될 때까지 기다립니다.

AWSsupport-CollectEKSLinuxNodeStatistics

설명

AWSSupport-CollectEKSLinuxNodeStatistics 실행서는 Amazon EKS 클러스터의 일부인 Amazon EC2 인스턴스와 컨테이너 ID가 지정된 경우 인스턴스에서 실행되는 containerd 컨테이너에서 Linux 통계를 수집합니다. Amazon EC2 인스턴스에서 관리해야 합니다 AWS Systems Manager.

수집되는 호스트 수준 Linux 통계는 다음과 같습니다.

- OS 정보.
- 네트워크 인터페이스 통계 - ethtool 및 /sys/class/net/interface/statistics 디렉터리에서.
- 파일 설명자 수입입니다.
- 임시 포트 수입입니다.
- iptables 규칙의 덤프입니다.
- 전체 conntrack 테이블을 확인합니다.

컨테이너 수준 Linux 통계에는 다음이 포함됩니다.

- 식별자 정보 - 이미지 URI 및 레이블.
- 네트워크 인터페이스 통계 - ethtool 및 /sys/class/net/interface/statistics 디렉터리에서.
- NetworkTargets 파라미터가 채워진 경우 Traceroute 및 DNS 결과입니다.
- 패킷 캡처 분석 수 - TCP 재전송, 순서에 맞지 않는 패킷 등

실행서는 Amazon Linux 2, Amazon Linux 2023 및 Debian/Ubuntu를 포함한 다양한 Linux 배포판에서 데이터를 수집합니다. Amazon ECR 퍼블릭 갤러리에서 다음 이미지의 최신 버전을 사용합니다.

- amazon-ecs-network-sidecar 문제 해결 도구에 액세스할 수 있는 이미지입니다.
- aws-cli 통계 보고서 JSON 파일 및 패킷 캡처 파일을 지정된 Amazon S3 버킷에 업로드하는 이미지입니다.

Important

이 실행서는 Fargate 인스턴스를 지원하지 않습니다. 실행 중에 인스턴스가 종료되거나 연결이 끊어지면 이 실행서가 실패할 수 있습니다.

어떻게 작동하나요?

실행서는 다음 작업을 수행합니다.

- 대상 Amazon S3 버킷이 퍼블릭 읽기 또는 쓰기 액세스 권한을 부여하지 않는지 확인합니다.
- 대상 Amazon EC2 인스턴스가 Systems Manager에서 관리되고 실행 중인 상태인지 확인합니다.
- 인스턴스가 Linux 운영 체제를 실행 중인지 확인합니다.
- Amazon EC2 인스턴스 및 선택적으로 지정된 컨테이너에서 포괄적인 Linux 통계를 수집합니다.
- 수집된 통계를 지정된 Amazon S3 버킷에 업로드합니다.

[이 자동화 실행\(콘솔\)](#)

필수 IAM 권한

실행서를 성공적으로 사용하려면 AutomationAssumeRole 파라미터에 다음 작업이 필요합니다.

AutomationAssumeRole 파라미터에는 다음 작업이 필요합니다.

- s3:GetAccountPublicAccessBlock
- s3:GetBucketPublicAccessBlock
- s3:GetBucketAcl
- s3:GetBucketPolicyStatus
- s3:GetBucketLocation
- s3:GetEncryptionConfiguration
- s3:PutObject
- ssm:DescribeInstanceInformation
- ssm:SendCommand
- ssm:GetCommandInvocation
- ec2:DescribeInstances

IAM 정책 예제:

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



```

{
  "Effect": "Allow",
  "Action": [
    "s3:GetAccountPublicAccessBlock"
  ],
  "Resource": "*"
},
{
  "Effect": "Allow",
  "Action": [
    "s3:GetBucketPublicAccessBlock",
    "s3:GetBucketAcl",
    "s3:GetBucketPolicyStatus",
    "s3:GetBucketLocation",
    "s3:GetEncryptionConfiguration"
  ],
  "Resource": "arn:aws:s3:::S3_BUCKET_NAME"
},
{
  "Effect": "Allow",
  "Action": [
    "s3:PutObject"
  ],
  "Resource": "arn:aws:s3:::S3_BUCKET_NAME/*"
},
{
  "Effect": "Allow",
  "Action": [
    "ssm:DescribeInstanceInformation"
  ],
  "Resource": "*"
},
{
  "Effect": "Allow",
  "Action": [
    "ssm:SendCommand"
  ],
  "Resource": [
    "arn:aws:ssm:*:*:document/AWS-RunShellScript",
    "arn:aws:ec2:*:111122223333:instance/*"
  ]
},
{
  "Effect": "Allow",

```

```

        "Action": [
            "ssm:GetCommandInvocation"
        ],
        "Resource": "*"
    },
    {
        "Effect": "Allow",
        "Action": [
            "ec2:DescribeInstances"
        ],
        "Resource": "*"
    }
]
}

```

지침

다음 단계에 따라 자동화를 구성합니다.

1. Systems Manager [AWSsupport-CollectEKSLinuxNodeStatistics](#)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 IAM 역할의 Amazon 리소스 이름(ARN)입니다. 역할을 지정하지 않은 경우, Systems Manager Automation에서는 이 실행서를 시작하는 사용자의 권한을 사용합니다.

- InstanceId(필수):

통계를 수집할 Amazon EC2 인스턴스의 ID입니다.

- S3BucketName(필수):

Amazon EC2 인스턴스의 JSON 출력을 파일로 내보낼 Amazon S3 버킷의 이름입니다. Amazon EC2

- S3KeyPrefix(선택 사항):

Amazon EC2 인스턴스의 JSON 출력을 파일로 내보내는 Amazon S3 키 접두사(하위 폴더)입니다. Amazon EC2 기본값: AWSsupport-CollectEKSLinuxNodeStatistics.

- S3BucketOwnerRoleArn(선택 사항):

Amazon S3 버킷 및 계정을 가져올 수 있는 권한이 있는 IAM 역할의 ARN은 퍼블릭 액세스 설정, 버킷 암호화 구성, 버킷 ACLs, 버킷 정책 상태 및 버킷에 객체 업로드를 차단합니다. 이 파라미터를 지정하지 않으면 실행서는 이 실행서를 시작하는 AutomationAssumeRole (지정된 경우) 또는 사용자(지정되지 않은 경우) AutomationAssumeRole를 사용합니다.

- **S3BucketOwnerAccount**(선택 사항):

Amazon S3 버킷을 소유한 AWS 계정입니다. 이 파라미터를 지정하지 않으면 실행서는 버킷이 이 계정에 있다고 가정합니다.

- **ContainerId**(선택 사항):

지정된 Amazon EC2 인스턴스에서 실행되는 컨테이너의 ID입니다.

- **NetworkTargets**(선택 사항):

DNS 확인 및 traceroute를 사용한 연결을 테스트하기 위한 IPv4 주소 및/또는 DNS 이름의 쉼표로 구분된 목록입니다.

4. 실행을 선택합니다.

5. 자동화가 시작됩니다.

6. 문서는 다음 단계를 수행합니다.

- **CheckBucketAccess**:

대상 Amazon S3 버킷이 객체에 대한 읽기 및/또는 쓰기 퍼블릭 액세스 권한을 부여할 가능성이 있는지 확인합니다.

- **AssertInstanceIsSSMManaged**:

Systems Manager에서 대상 Amazon EC2 인스턴스를 관리하는지 확인합니다. 그렇지 않으면 자동화가 종료됩니다.

- **VerifyInstanceState**:

통계 수집을 시도하기 전에 Amazon EC2 인스턴스가 실행 중인 상태인지 확인합니다.

- **BranchOnVerifyLinuxInstance**:

계속하기 전에 인스턴스가 Linux 인스턴스인지 확인합니다.

- **BranchOnVerifyInstanceRunning**:

계속하기 전에 인스턴스가 실행 중인 상태인지 확인합니다.

- **CollectEKSLinuxNodeStatistics**:

OS 정보, 네트워크 인터페이스 통계, 파일 설명자, 임시 포트, 방화벽 규칙 및 선택적으로 컨테이너 수준 통계를 포함하여 Amazon EC2 인스턴스에서 포괄적인 Linux 통계를 수집합니다.

- **GenerateStatisticsOutputS3Uri:**

자동화 문서의 출력으로 사용할 Linux 통계 파일에 대한 전체 Amazon S3 URI를 생성합니다.

7. 완료 후에는 Outputs 섹션에서 실행의 세부 결과를 검토합니다.

참조

Systems Manager Automation

- [이 자동화 실행\(콘솔\)](#)
- [자동화 실행](#)
- [Automation 설정](#)
- [자동화 워크플로 지원](#)

AWSSupport-CollectEKSIInstanceLogs

설명

AWSSupport-CollectEKSIInstanceLogs 실행서는 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스로부터 운영 체제 및 Amazon Elastic Kubernetes Service(Amazon EKS) 관련 로그 파일을 수집하여 일반적인 문제를 해결하는 데 도움을 줍니다. 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 활동으로 인해 Amazon EC2 인스턴스에서 CPUUtilization 증가를 초래할 수 있습니다. CPUUtilization에 대한 자세한 내용은 Amazon CloudWatch 사용 설명서의 [인스턴스 지표](#)를 참조하세요.

LogDestination 파라미터에 대한 값을 지정하는 경우, 지정하는 Amazon Simple Storage Service(Amazon S3) 버킷의 정책 상태를 자동화에서 평가합니다. Amazon EC2 인스턴스로부터 수집한 로그의 보안을 돕기 위해, 정책 상태 isPublic(이)가 true(으)로 설정되어 있거나 액세스 제어 목록(ACL)이 All Users Amazon S3의 미리 정의된 그룹에 READ|WRITE 권한을 부여하는 경우, 로그는 업로드되지 않습니다. Amazon S3의 미리 정의된 그룹에 대한 자세한 내용은 Amazon Simple Storage Service 사용 설명서에서 [Amazon S3의 미리 정의된 그룹](#)을 참조하세요.

Note

이 자동화에는 Amazon EC2 인스턴스에 연결된 루트 Amazon Elastic Block Store(Amazon EBS) 볼륨에서 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

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.

- EKSInstanceId

유형: 문자열

설명: (필수) 로그를 수집할 Amazon EKS Amazon EC2 인스턴스의 ID입니다.

- LogDestination

유형: 문자열

설명: (선택 사항) 보관된 로그를 업로드할 계정의 Amazon Simple Storage Service(Amazon S3) 버킷입니다.

필수 IAM 권한

실행서를 성공적으로 사용하려면 AutomationAssumeRole 파라미터에 다음 작업이 필요합니다.

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- ssm:SendCommand

Amazon EC2 인스턴스 프로파일에 필요한 IAM 권한

에서 사용하는 인스턴스 프로파일에는 AmazonSSMManagedInstanceCore Amazon 관리형 정책이 연결되어 EKSInstanceId 있어야 합니다.

또한 수집된 로그를 업로드할 수 있도록 LogDestination Amazon S3 버킷에 액세스할 수 있어야 합니다. 다음은 해당 인스턴스 프로파일에 연결할 수 있는 IAM 정책의 예입니다.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "s3:PutObject",
        "s3:GetBucketPolicyStatus",
        "s3:GetBucketAcl"
      ],
      "Resource": [
        "arn:aws:s3:::LogDestination/*",
        "arn:aws:s3:::LogDestination"
      ]
    }
  ]
}
```

가 AWS KMS 암호화를 LogDestination 사용하는 경우 IAM 정책에 추가 문을 추가하여 암호화에 사용되는 AWS KMS 키에 대한 액세스 권한을 부여해야 합니다.

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

```

```

    "Effect": "Allow",
    "Action": [
        "s3:PutObject",
        "s3:GetBucketPolicyStatus",
        "s3:GetBucketAcl"
    ],
    "Resource": [
        "arn:aws:s3:::LogDestination/*",
        "arn:aws:s3:::LogDestination"
    ]
},
{
    "Effect": "Allow",
    "Action": [
        "kms:Decrypt",
        "kms:GenerateDataKey"
    ],
    "Resource": "arn:aws:kms:REGION:ACCOUNT:key/KMS-KEY-ID"
}
]
}

```

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 지정한 Amazon S3 버킷에 로그 아카이브를 업로드합니다.

AWSSupport-SetupK8sApiProxyForEKS

설명

AWSSupport-SetupK8sApiProxyForEKS 자동화 실행서는 Amazon Elastic Kubernetes Service 클러스터 엔드포인트에 대한 컨트롤 플레인 API 호출을 수행하는 프록시 역할을 하는 AWS Lambda 함수를 생성하는 방법을 제공합니다. Amazon EKS 클러스터의 작업을 자동화하고 문제를 해결하기 위해 컨트롤 플레인 API를 호출해야 하는 런북의 빌딩 블록 역할을 합니다.

⚠ Important

이 자동화로 생성된 모든 리소스에는 태그를 지정하여 쉽게 찾을 수 있습니다. 사용되는 태그는 다음과 같습니다.

- `AWSSupport-SetupK8sApiProxyForEKS: true`

ℹ Note

- 자동화는 헬퍼 런북이며 독립 실행형 런북으로 실행할 수 없습니다. Amazon EKS 클러스터에 대한 컨트롤 플레인 API 호출이 필요한 런북의 하위 자동화로 호출됩니다.
- 원치 않는 비용이 발생하지 않도록 사용 후 Cleanup 작업을 실행해야 합니다.

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.

- `ClusterName`

유형: 문자열

설명: (필수) Amazon Elastic Kubernetes Service 클러스터의 이름입니다.

- 연산

유형: 문자열

설명: (필수) 수행할 작업: Cleanup는 계정에 Lambda 함수를 Setup 프로비저닝하고 설정 단계의 일부로 생성된 리소스를 프로비저닝 해제합니다.

허용된 값: Setup | Cleanup

기본값: 설정

- LambdaRoleArn

유형: 문자열

설명: (선택 사항) 함수가 필요한 AWS 서비스 및 리소스에 AWS Lambda 액세스할 수 있도록 허용하는 IAM 역할의 ARN입니다. 역할이 지정되지 않은 경우 Systems Manager Automation은 관리형 정책인 AWSLambdaBasicExecutionRole 및 Automation-K8sProxy-Role-`<ExecutionId>` 포함된 이름으로 계정에 Lambda에 대한 IAM 역할 하나를 생성합니다. AWSLambdaVPCLambdaAccessExecutionRole.

어떻게 작동하나요?

실행서는 다음 단계를 수행합니다.

- 자동화가 하위 실행으로 실행되고 있는지 확인합니다. 런북은 자체적으로 의미 있는 작업을 수행하지 않으므로 독립 실행형 런북으로 호출될 때는 작동하지 않습니다.
- 지정된 클러스터에 대한 프록시 Lambda 함수의 기존 CloudFormation 스택을 확인합니다.
 - 스택이 있는 경우 기존 인프라가 다시 생성되는 대신 다시 사용됩니다.
 - 동일한 클러스터에 대해 다른 실행서에서 인프라를 재사용하는 경우 런북이 인프라를 삭제하지 않도록 참조 카운터는 태그를 사용하여 유지됩니다.
- 호출에 지정된 작업 유형(Setup/Cleanup)을 수행합니다.
 - 설정: 기존 리소스를 생성하거나 설명합니다.

정리: 다른 실행서에서 인프라를 사용하지 않는 경우 프로비저닝된 리소스를 제거합니다.

필요한 IAM 권한

AutomationAssumeRole 파라미터에는 지정된 다음 권한이 필요합니다 LambdaRoleArn.

- cloudformation:CreateStack
- cloudformation:DescribeStacks
- cloudformation>DeleteStack
- cloudformation:UpdateStack
- ec2:CreateNetworkInterface
- ec2:DescribeNetworkInterfaces
- ec2:DescribeRouteTables
- ec2:DescribeSecurityGroups
- ec2:DescribeSubnets
- ec2:DescribeVpcs
- ec2>DeleteNetworkInterface
- eks:DescribeCluster
- lambda:CreateFunction
- lambda>DeleteFunction
- lambda:ListTags
- lambda:GetFunction
- lambda:ListTags
- lambda:TagResource
- lambda:UntagResource
- lambda:UpdateFunctionCode
- logs:CreateLogGroup
- logs:PutRetentionPolicy
- logs:TagResource
- logs:UntagResource
- logs:DescribeLogGroups
- logs:DescribeLogStreams
- logs:ListTagsForResource
- iam:CreateRole
- iam:AttachRolePolicy

- iam:DetachRolePolicy
- iam:PassRole
- iam:GetRole
- iam>DeleteRole
- iam:TagRole
- iam:UntagRole
- tag:GetResources
- tag:TagResources

LambdaRoleArn이 제공되면 자동화가 역할을 생성할 필요가 없으며 다음 권한을 제외할 수 있습니다.

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

다음은가 전달되지 않은 AutomationAssumeRole 경우에 필요한 권한을 보여주는 정책의 예LambdaRoleArn입니다.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": [
        "tag:GetResources",
        "tag:TagResources",
        "ec2:CreateNetworkInterface",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSecurityGroups",
```

```

        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:DeleteNetworkInterface",
        "eks:DescribeCluster",
        "iam:GetRole",
        "cloudformation:DescribeStacks",
        "logs:DescribeLogGroups",
        "logs:DescribeLogStreams",
        "lambda:GetFunction",
        "lambda:ListTags",
        "logs:ListTagsForResource"
    ],
    "Resource": "*",
    "Effect": "Allow",
    "Sid": "AllowActionsWithoutConditions"
},
{
    "Condition": {
        "StringEquals": {
            "aws:RequestTag/AWSSupport-SetupK8sApiProxyForEKS": "true"
        }
    },
    "Action": "iam:CreateRole",
    "Resource": [
        "arn:aws:iam::111122223333:role/Automation-K8sProxy*"
    ],
    "Effect": "Allow",
    "Sid": "AllowCreateRoleWithRequiredTag"
},
{
    "Condition": {
        "StringEquals": {
            "aws:ResourceTag/AWSSupport-SetupK8sApiProxyForEKS": "true"
        }
    },
    "Action": [
        "iam:DeleteRole",
        "iam:TagRole",
        "iam:UntagRole"
    ],
    "Resource": [
        "arn:aws:iam::111122223333:role/Automation-K8sProxy*"
    ],
    "Effect": "Allow",

```

```

        "Sid": "IAMActions"
    },
    {
        "Condition": {
            "StringEquals": {
                "aws:ResourceTag/AWSSupport-SetupK8sApiProxyForEKS": "true"
            },
            "StringLike": {
                "iam:PolicyARN": [
                    "arn:aws:iam::111122223333:policy/service-role/
AWSLambdaBasicExecutionRole",
                    "arn:aws:iam::111122223333:policy/service-role/
AWSLambdaVPCLambdaAccessExecutionRole"
                ]
            }
        },
        "Action": [
            "iam:AttachRolePolicy",
            "iam:DetachRolePolicy"
        ],
        "Resource": [
            "arn:aws:iam::111122223333:role/Automation-K8sProxy*"
        ],
        "Effect": "Allow",
        "Sid": "AttachRolePolicy"
    },
    {
        "Condition": {
            "StringEquals": {
                "aws:ResourceTag/AWSSupport-SetupK8sApiProxyForEKS": "true"
            }
        },
        "Action": [
            "lambda:CreateFunction",
            "lambda:DeleteFunction",
            "lambda:TagResource",
            "lambda:UntagResource",
            "lambda:UpdateFunctionCode"
        ],
        "Resource": "arn:aws:lambda:us-east-1:111122223333:function:Automation-K8sProxy*",
        "Effect": "Allow",
        "Sid": "LambdaActions"
    },

```

```

    {
      "Condition": {
        "StringEquals": {
          "aws:ResourceTag/AWSSupport-SetupK8sApiProxyForEKS": "true"
        }
      },
      "Action": [
        "cloudformation:CreateStack",
        "cloudformation>DeleteStack",
        "cloudformation:UpdateStack"
      ],
      "Resource": "arn:aws:cloudformation:us-east-1:111122223333:stack/AWSSupport-SetupK8sApiProxyForEKS*",
      "Effect": "Allow",
      "Sid": "CloudFormationActions"
    },
    {
      "Condition": {
        "StringEquals": {
          "aws:ResourceTag/AWSSupport-SetupK8sApiProxyForEKS": "true"
        }
      },
      "Action": [
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents",
        "logs:PutRetentionPolicy",
        "logs:TagResource",
        "logs:UntagResource"
      ],
      "Resource": [
        "arn:aws:logs:us-east-1:111122223333:log-group:/aws/lambda/Automation-K8sProxy*",
        "arn:aws:logs:us-east-1:111122223333:log-group:/aws/lambda/Automation-K8sProxy*:*"
      ],
      "Effect": "Allow",
      "Sid": "LogsActions"
    },
    {
      "Condition": {
        "StringLikeIfExists": {
          "iam:PassedToService": "lambda.amazonaws.com"
        }
      }
    }
  ]
}

```

```

    },
    "Action": [
        "iam:PassRole"
    ],
    "Resource": [
        "arn:aws:iam::111122223333:role/Automation-K8sProxy-Role*"
    ],
    "Effect": "Allow",
    "Sid": "PassRoleToLambda"
  }
]
}

```

LambdaRoleArn이 전달되는 경우 퍼블릭 클러스터의 경우 [AWSLambdaBasicExecutionRole](#) 정책이 연결되어 있고 프라이빗 클러스터의 경우 [AWSLambdaVPCLambdaAccessExecutionRole](#) 정책이 연결되어 있는지 확인하세요.

생성된 리소스

Setup 작업 중에 다음 리소스가 생성됩니다.

1. AWS Lambda 함수
2. IAM 역할: 제공되지 않은 경우 Lambda 실행 역할입니다.
3. CloudWatch 로그 그룹(Lambda 로그)

Lambda 함수 및 실행 역할은 *Cleanup* 작업이 실행될 때까지 유지됩니다. Lambda 로그 그룹은 30일 동안 또는 수동으로 삭제할 때까지 보존됩니다.

지침

실행서는 다른 실행서 내에서 하위 자동화로 실행되도록 설계된 헬퍼 유틸리티입니다. 이를 통해 상위 런북이 Amazon EKS K8s 컨트롤 플레인 API 호출을 수행할 수 있는 인프라를 쉽게 생성할 수 있습니다. 런북을 사용하려면 상위 자동화의 컨텍스트에서 아래 단계를 수행할 수 있습니다.

1. 설정 단계: `aws:executeAutomation` 작업이 로 설정된 Amazon EKS K8s 컨트롤 플레인 API 호출을 수행하려는 실행서의 작업 작업을 사용하여 자동화를 호출합니다Setup.

입력 파라미터의 예:

```
{
```

```

    "AutomationAssumeRole": "<role-arn>",
    "ClusterName": "<eks-cluster-name>",
    "Operation": "Setup"
  }

```

aws:executeAutomation 단계의 출력에는 프록시 Lambda 함수의 ARN이 포함됩니다.

2. Lambda 프록시 사용: API 호출 경로 및 보유자 토큰 목록과 boto3

Lambda.Client.invoke(...) 함께의를 사용하여 aws:executeScript 작업 내에서 Lambda 함수를 호출합니다. Lambda 함수는 보유자 토큰을 권한 부여 헤더의 일부로 전달하여 지정된 경로에 대한 HTTP GET 호출을 수행합니다.

Lambda 호출 이벤트의 예:

```

{
  "ApiCalls": ["/api/v1/pods/", ...],
  "BearerToken": "..."
}

```

Note

보유자 토큰은 상위 자동화 스크립트의 일부로 생성되어야 합니다. 상위 실행서를 실행하는 보안 주체에게 지정된 Amazon EKS 클러스터에 대한 읽기 전용 권한이 있는지 확인해야 합니다.

3. 정리 단계: aws:executeAutomation 작업이 로 설정된 Amazon EKS K8s 컨트롤 플레인 API 호출을 수행하려는 실행서의 작업 작업을 사용하여 자동화를 호출합니다Cleanup.

입력 파라미터의 예:

```

{
  "AutomationAssumeRole": "<role-arn>",
  "ClusterName": "<eks-cluster-name>",
  "Operation": "Cleanup"
}

```

자동화 단계

1. ValidateExecution

- 자동화가 독립 실행형 실행으로 실행되고 있는지 확인합니다.

2. CheckForExistingStack

- 지정된 클러스터 이름에 대해 CloudFormation 스택이 이미 프로비저닝되었는지 확인합니다.
- 스택 존재 상태와 삭제해도 안전한지 여부를 반환합니다.

3. BranchOnIsStackExists

- 스택 존재 여부에 따라 분기되는 결정 단계입니다.
- 기존 스택 이름을 업데이트하거나 작업 분기를 진행하기 위한 경로입니다.

4. UpdateStackName

- StackName 변수를 기존 스택의 이름으로 업데이트합니다.
- 스택이 이미 있는 경우에만 실행됩니다.

5. BranchOnOperation

- Operation 파라미터(Setup /)를 기반으로 자동화를 라우팅합니다Cleanup.
- 의 경우Setup: 새 스택을 생성하거나 기존 리소스를 설명하는 라우팅입니다.
- 의 경우Cleanup: 안전하게 삭제할 수 있는 경우 스택 삭제를 진행합니다.

6. GetClusterNetworkConfig

- VPC 구성을 가져올 Amazon EKS 클러스터에 대해 설명합니다.
- 엔드포인트, VPC ID, 서브넷 IDs, 보안 그룹 ID 및 CA 데이터를 검색합니다.

7. ProvisionResources

- 필요한 리소스가 포함된 CloudFormation 스택을 생성합니다.
- 필요한 네트워킹 구성으로 Lambda 함수를 프로비저닝합니다.
- 추적 및 관리를 위해 모든 리소스에 태그를 지정합니다.

8. DescribeStackResources

- 생성된 스택/기존 스택에 대한 정보를 검색합니다.
- 프로비저닝된 Lambda 함수의 ARN을 가져옵니다.

9. BranchOnIsLambdaDeploymentRequired

- Lambda 코드 배포가 필요한지 여부를 결정합니다.
- 는 새로 생성된 스택에 대해서만 배포를 진행합니다.

10DeployLambdaFunctionCode

- 배포 패키지를 사용하여 Lambda 함수 코드를 배포합니다.

11AssertLambdaAvailable

- Lambda 함수 코드 업데이트가 성공했는지 확인합니다.
- 함수가 Successful 상태가 될 때까지 기다립니다.

12PerformStackCleanup

- CloudFormation 스택 및 연결된 리소스를 삭제합니다.
- Cleanup 작업 중 또는 Setup 작업 실패 시 실행됩니다.

출력

LambdaFunctionArn: 프록시 Lambda 함수의 ARN

참조

Systems Manager Automation

- [자동화 실행](#)
- [Automation 설정](#)
- [자동화 워크플로 지원](#)

AWSSupport-TroubleshootEbsCsiDriversForEks

설명

AWSSupport-TroubleshootEbsCsiDriversForEks 실행서는 Amazon Elastic Kubernetes Service(Amazon EKS)의 Amazon Elastic Block Store 볼륨 마운트 문제와 Amazon EBS 컨테이너 스토리지 인터페이스(CSI) 드라이버 문제를 해결하는 데 도움이 됩니다.

Important

현재에서 실행되는 Amazon EBS CSI 드라이버 AWS Fargate 는 지원되지 않습니다.

어떻게 작동하나요?

실행서는 다음과 같은 상위 수준 단계를 AWSSupport-TroubleshootEbsCsiDriversForEks 수행합니다.

- 대상 Amazon EKS 클러스터가 존재하고 활성 상태인지 확인합니다.

- 추가 기능이 Amazon EKS 관리형인지 자체 관리형인지에 따라 Kubernetes API 호출을 수행하는 데 필요한 인증 리소스를 배포합니다.
- Amazon EBS CSI 컨트롤러 상태 확인 및 진단을 수행합니다.
- 노드 역할 및 서비스 계정 역할에 대한 IAM 권한 검사를 실행합니다.
- 지정된 애플리케이션 포드에 대한 영구 볼륨 생성 문제를 진단합니다.
- node-to-pod 스케줄링을 확인하고 포드 이벤트를 검사합니다.
- 관련 Kubernetes 및 애플리케이션 로그를 수집하여 지정된 Amazon S3 버킷에 업로드합니다.
- 노드 상태 확인을 수행하고 Amazon EC2 엔드포인트와의 연결을 확인합니다.
- 영구 볼륨 블록 디바이스 연결 및 탑재 상태를 검토합니다.
- 문제 해결 중에 생성된 인증 인프라를 정리합니다.
- 모든 진단 결과를 결합하는 포괄적인 문제 해결 보고서를 생성합니다.

Note

- Amazon EKS 클러스터의 인증 모드는 API 또는 로 설정해야 합니다. API_AND_CONFIG_MAP. Amazon EKS Access 항목을 사용하는 것이 좋습니다. 실행서는 필요한 API 호출을 수행하는 데 Kubernetes 역할 기반 액세스 제어(RBAC) 권한이 필요합니다.
- Lambda 함수(LambdaRoleArn 파라미터)에 대한 IAM 역할을 지정하지 않으면 자동화가 Automation-K8sProxy-Role-<ExecutionId> 계정에 라는 역할을 생성합니다. 이 역할에는 관리형 정책 AWSLambdaBasicExecutionRole 및가 포함됩니다. AWSLambdaVPCLAccessExecutionRole.
- 일부 진단 단계에서는 Amazon EKS 작업자 노드가 Systems Manager 관리형 인스턴스여야 합니다. 노드가 Systems Manager 관리형 인스턴스가 아닌 경우 Systems Manager 액세스가 필요한 단계는 건너뛰지만 다른 검사는 계속됩니다.
- 자동화에는 인증 인프라 리소스를 제거하는 정리 단계가 포함됩니다. 이 정리 단계는 이전 단계가 실패하더라도 실행되므로 AWS 계정에서 분리된 리소스를 방지하는 데 도움이 됩니다.

[이 자동화 실행\(콘솔\)](#)

문서 유형

자동화

소유자

Amazon

플랫폼

/

필수 IAM 권한

실행서를 성공적으로 사용하려면 AutomationAssumeRole 파라미터에 다음 작업이 필요합니다.

- ec2:DescribeIamInstanceProfileAssociations
- ec2:DescribeInstanceStatus
- ec2:GetEbsEncryptionByDefault
- eks:DescribeAddon
- eks:DescribeAddonVersions
- eks:DescribeCluster
- iam:GetInstanceProfile
- iam:GetOpenIDConnectProvider
- iam:GetRole
- iam:ListOpenIDConnectProviders
- iam:SimulatePrincipalPolicy
- s3:GetBucketLocation
- s3:GetBucketPolicyStatus
- s3:GetBucketPublicAccessBlock
- s3:GetBucketVersioning
- s3:ListBucket
- s3:ListBucketVersions
- ssm:DescribeInstanceInformation
- ssm:GetAutomationExecution
- ssm:GetDocument
- ssm:ListCommandInvocations

- `ssm:ListCommands`
- `ssm:SendCommand`
- `ssm:StartAutomationExecution`

지침

다음 단계에 따라 자동화를 구성합니다.

1. 계정 `TroubleshootEbsCsiDriversForEks-SSM-Role`에서 SSM 자동화 역할을 생성합니다. 신뢰 관계에 다음 정책이 포함되어 있는지 확인합니다.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "",
      "Effect": "Allow",
      "Principal": {
        "Service": "ssm.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

2. 아래 정책을 IAM 역할에 연결하여 지정된 리소스에서 지정된 작업을 수행하는 데 필요한 권한을 부여합니다.

- 실행 및 리소스 로그를 동일한 AWS 리전의 Amazon S3 버킷에 업로드하려는 경우에서 `arn: {partition}:s3::BUCKET_NAME/*` 로 바꿉니다 `OptionalRestrictPutObjects`.
- SSM 실행 `S3BucketName`에서 선택할 경우 Amazon S3 버킷은 올바른 Amazon S3 버킷을 가리켜야 합니다.
- 지정하지 않으면 이 권한은 선택 사항입니다. `S3BucketName`
- Amazon S3 버킷은 프라이빗이어야 하며 SSM 자동화를 실행하는 리전과 동일한 AWS 리전에 있어야 합니다.

JSON

```
{
```

```

"Version": "2012-10-17",
"Statement": [
  {
    "Sid": "OptionalRestrictPutObjects",
    "Effect": "Allow",
    "Action": [
      "s3:PutObject"
    ],
    "Resource": [
      "arn:aws:s3:::amzn-s3-demo-bucket/*"
    ]
  },
  {
    "Effect": "Allow",
    "Action": [
      "ec2:DescribeIamInstanceProfileAssociations",
      "ec2:DescribeInstanceStatus",
      "ec2:GetEbsEncryptionByDefault",
      "eks:DescribeAddon",
      "eks:DescribeAddonVersions",
      "eks:DescribeCluster",
      "iam:GetInstanceProfile",
      "iam:GetOpenIDConnectProvider",
      "iam:GetRole",
      "iam:ListOpenIDConnectProviders",
      "iam:SimulatePrincipalPolicy",
      "s3:GetBucketLocation",
      "s3:GetBucketPolicyStatus",
      "s3:GetBucketPublicAccessBlock",
      "s3:GetBucketVersioning",
      "s3:ListBucket",
      "s3:ListBucketVersions",
      "ssm:DescribeInstanceInformation",
      "ssm:GetAutomationExecution",
      "ssm:GetDocument",
      "ssm:ListCommandInvocations",
      "ssm:ListCommands",
      "ssm:SendCommand",
      "ssm:StartAutomationExecution"
    ],
    "Resource": "*"
  },
  {
    "Sid": "SetupK8sApiProxyForEKSActions",

```

```

    "Effect": "Allow",
    "Action": [
        "cloudformation:CreateStack",
        "cloudformation>DeleteStack",
        "cloudformation:DescribeStacks",
        "cloudformation:UpdateStack",
        "ec2:CreateNetworkInterface",
        "ec2>DeleteNetworkInterface",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeRouteTables",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "eks:DescribeCluster",
        "iam:CreateRole",
        "iam>DeleteRole",
        "iam:GetRole",
        "iam:TagRole",
        "iam:UntagRole",
        "lambda:CreateFunction",
        "lambda>DeleteFunction",
        "lambda:GetFunction",
        "lambda:InvokeFunction",
        "lambda:ListTags",
        "lambda:TagResource",
        "lambda:UntagResource",
        "lambda:UpdateFunctionCode",
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:DescribeLogGroups",
        "logs:DescribeLogStreams",
        "logs:ListTagsForResource",
        "logs:PutLogEvents",
        "logs:PutRetentionPolicy",
        "logs:TagResource",
        "logs:UntagResource",
        "ssm:DescribeAutomationExecutions",
        "tag:GetResources",
        "tag:TagResources"
    ],
    "Resource": "*"
},
{
    "Sid": "PassRoleToAutomation",

```

```

    "Effect": "Allow",
    "Action": "iam:PassRole",
    "Resource": [
        "arn:aws:iam::*:role/TroubleshootEbsCsiDriversForEks-SSM-Role",
        "arn:aws:iam::*:role/Automation-K8sProxy-Role-*"
    ],
    "Condition": {
        "StringLikeIfExists": {
            "iam:PassedToService": [
                "lambda.amazonaws.com",
                "ssm.amazonaws.com"
            ]
        }
    }
},
{
    "Sid": "AttachRolePolicy",
    "Effect": "Allow",
    "Action": [
        "iam:AttachRolePolicy",
        "iam:DetachRolePolicy"
    ],
    "Resource": "*",
    "Condition": {
        "StringLikeIfExists": {
            "iam:ResourceTag/AWSSupport-SetupK8sApiProxyForEKS": "true"
        }
    }
}
]
}

```

3. Amazon EKS 클러스터 RBAC(역할 기반 액세스 제어)에 필요한 권한을 부여합니다. 권장 접근 방식은 Amazon EKS 클러스터에서 액세스 항목을 생성하는 것입니다.

Amazon EKS 콘솔에서 클러스터로 이동합니다. Amazon EKS 액세스 항목의 경우 액세스 구성이 API_AND_CONFIG_MAP 또는 로 설정되어 있는지 확인합니다 API. 액세스 항목에 대한 인증 모드를 구성하는 단계는 [액세스 항목 설정을](#) 참조하세요.

액세스 항목 생성을 선택합니다.

- IAM 보안 주체 ARN의 경우 이전 단계에서 SSM 자동화를 위해 생성한 IAM 역할을 선택합니다.
- 유형에서 Standard를 선택합니다.

4. 액세스 정책 추가:

- 액세스 범위에서를 선택합니다Cluster.
- 정책 이름에서를 선택합니다AmazonEKSAAdminViewPolicy.

정책 추가를 선택합니다.

액세스 항목을 사용하여 Kubernetes API 권한을 관리하지 않는 경우 aws-auth ConfigMap을 업데이트하고 IAM 사용자 또는 역할 간에 역할 바인딩을 생성해야 합니다. IAM 엔터티에 다음과 같은 읽기 전용 Kubernetes API 권한이 있는지 확인합니다.

- GET /apis/apps/v1/namespaces/{namespace}/deployments/{name}
- GET /apis/apps/v1/namespaces/{namespace}/replicasets/{name}
- GET /apis/apps/v1/namespaces/{namespace}/daemonsets/{name}
- GET /api/v1/nodes/{name}
- GET /api/v1/namespaces/{namespace}/serviceaccounts/{name}
- GET /api/v1/namespaces/{namespace}/persistentvolumeclaims/{name}
- GET /api/v1/persistentvolumes/{name}
- GET /apis/storage.k8s.io/v1/storageclasses/{name}
- GET /api/v1/namespaces/{namespace}/pods/{name}
- GET /api/v1/namespaces/{namespace}/pods
- GET /api/v1/namespaces/{namespace}/pods/{name}/log
- GET /api/v1/events

5. 자동화 [AWSSupport-TroubleshootEbsCsiDriversForEks 실행\(콘솔\)](#)

6. Execute automation(자동화 실행)을 선택합니다.

7. 입력 파라미터에 다음을 입력합니다.

- AutomationAssumeRole(선택 사항):
 - 설명: (선택 사항) SSM Automation이 사용자를 대신하여 작업을 수행하도록 허용하는 (IAM) 역할의 AWS Identity and Access Management Amazon 리소스 이름(ARN)입니다. Kubernetes API 호출을 허용하려면 Amazon EKS 클러스터 액세스 항목 또는 RBAC 권한에 역할을 추가해야 합니다.
 - 유형: AWS::IAM::Role::Arn
 - 예시: TroubleshootEbsCsiDriversForEks-SSM-Role

- 설명: 대상 Amazon Elastic Kubernetes Service(Amazon EKS) 클러스터의 이름입니다.
- 유형: String
- ApplicationPodName:
 - 설명: Amazon EBS CSI 드라이버에 문제가 있는 Kubernetes 애플리케이션 포드의 이름입니다.
 - 유형: String
- ApplicationNamespace:
 - 설명: Amazon EBS CSI 드라이버에 문제가 있는 애플리케이션 포드의 Kubernetes 네임스페이스입니다.
 - 유형: String
- EbsCsiControllerDeploymentName(선택 사항):
 - 설명: (선택 사항) Amazon EBS CSI 컨트롤러 포드의 배포 이름입니다.
 - 유형: String
 - 기본값: ebs-csi-controller
- EbsCsiControllerNamespace(선택 사항):
 - 설명: (선택 사항) Amazon EBS CSI 컨트롤러 포드의 Kubernetes 네임스페이스입니다.
 - 유형: String
 - 기본값: kube-system
- S3BucketName(선택 사항):
 - 설명: (선택 사항) 문제 해결 로그가 업로드될 대상 Amazon S3 버킷 이름입니다.
 - 유형: AWS::S3::Bucket::Name
- LambdaRoleArn(선택 사항):
 - 설명: (선택 사항) AWS Lambda 함수가 필요한 AWS 서비스 및 리소스에 액세스할 수 있도록 허용하는 IAM 역할의 ARN입니다.
 - 유형: AWS::IAM::Role::Arn

실행을 선택합니다.

8. 완료되면 출력 섹션에서 실행의 자세한 결과를 검토합니다.

참조

Systems Manager Automation

- [이 자동화 실행\(콘솔\)](#)

- [자동화 실행](#)
- [Automation 설정](#)
- [자동화 워크플로 지원](#)

Amazon EBS CSI 드라이버에 대한 자세한 내용은 [Amazon EBS CSI 드라이버](#)를 참조하세요.

AWSSupport-TroubleshootEKSALBControllerIssues

설명

AWSSupport-TroubleshootEKSALBControllerIssues 자동화 실행서는 AWS Load Balancer 컨트롤러가 Kubernetes 수신 및 서비스에 대해 Application Load Balancer(ALB) 및 Network Load Balancer(NLB)를 올바르게 프로비저닝하고 관리하지 못하게 하는 일반적인 문제를 진단하는 데 도움이 됩니다.

이 실행서는 OIDC 자격 증명 공급자 설정, IRSA 구성, 네트워킹 사전 조건, 수신/서비스 구성 및 리소스 할당량을 비롯한 필수 구성 요소의 end-to-end 검증을 수행합니다. 또한 컨트롤러 로그 및 관련 Kubernetes 리소스 구성을 캡처하여 잘못된 구성 또는 운영 문제를 식별하는 데 도움이 됩니다.

Important

이 자동화 실행서는 Amazon Elastic Compute Cloud(Amazon EC2) 노드 그룹을 사용하는 Amazon EKS 클러스터용으로 설계되었으며 현재 실행 중인 클러스터를 지원하지 않습니다. AWS Fargate.

어떻게 작동하나요?

실행서는 다음과 같은 상위 수준 단계를 AWSSupport-TroubleshootEKSALBControllerIssues 수행합니다.

- Amazon EKS 클러스터 상태, 액세스 항목 구성 및 OIDC 공급자 설정을 검증합니다.
- Kubernetes API 통신을 위한 임시 Lambda 프록시를 생성합니다.
- Checks AWS Load Balancer Controller 배포 및 서비스 계정 구성.
- 포드 자격 증명 웹훅 및 IAM 역할 주입을 확인합니다.
- Application Load Balancer 및 Network Load Balancer 프로비저닝에 대한 서브넷 구성 및 태그 지정을 검증합니다.

- Application Load Balancer 및 Network Load Balancer 계정 할당량을 현재 사용량과 비교하여 확인합니다.
- 수신 및 서비스 리소스 주석을 검증합니다.
- 작업자 노드 보안 그룹 태그 지정에서 로드 밸런서 통합을 확인합니다.
- 진단을 위한 컨트롤러 포드 로그를 수집합니다.
- 임시 인증 리소스를 정리합니다.
- 조사 결과 및 수정 단계가 포함된 진단 보고서를 생성합니다.

Note

- Amazon EKS 클러스터에는이 자동화를 실행하는 IAM 엔터티에 대해 구성된 액세스 항목이 있어야 합니다. 클러스터의 인증 모드는 API 또는 로 설정해야 합니다 API_AND_CONFIG_MAP. 적절한 액세스 항목 구성이 없으면 초기 검증 중에 자동화가 종료됩니다.
- LambdaRoleArn 파라미터는 필수이며 AWS 관리형 정책이 AWSLambdaBasicExecutionRole 있어야 하며 프록시 함수가 Kubernetes API와 통신할 수 있도록 AWSLambdaVPCAccessExecutionRole 연결되어야 합니다.
- AWS Load Balancer 컨트롤러는 버전 v2.1.1 이상이어야 합니다.
- 자동화에는 임시 인증 인프라 리소스를 제거하는 정리 단계가 포함됩니다. 이 정리 단계는 이전 단계가 실패하더라도 실행되므로 분리된 리소스가 AWS 계정에 남아 있지 않습니다.

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`
- `cloudformation:DescribeStacks`
- `cloudformation:UpdateStack`
- `ec2:CreateNetworkInterface`
- `ec2>DeleteNetworkInterface`
- `ec2:DescribeInstances`
- `ec2:DescribeNetworkInterfaces`
- `ec2:DescribeRouteTables`
- `ec2:DescribeSecurityGroups`
- `ec2:DescribeSubnets`
- `ec2:DescribeVpcs`
- `eks:DescribeCluster`
- `eks:ListAssociatedAccessPolicies`
- `elasticloadbalancing:DescribeAccountLimits`
- `elasticloadbalancing:DescribeLoadBalancers`
- `iam:GetRole`
- `iam:ListOpenIDConnectProviders`
- `iam:PassRole`
- `lambda:CreateFunction`
- `lambda>DeleteFunction`
- `lambda:GetFunction`
- `lambda:InvokeFunction`
- `lambda:ListTags`
- `lambda:TagResource`
- `lambda:UntagResource`
- `lambda:UpdateFunctionCode`
- `logs:CreateLogGroup`
- `logs:CreateLogStream`

- logs:DescribeLogGroups
- logs:DescribeLogStreams
- logs:ListTagsForResource
- logs:PutLogEvents
- logs:PutRetentionPolicy
- logs:TagResource
- logs:UntagResource
- ssm:DescribeAutomationExecutions
- ssm:GetAutomationExecution
- ssm:StartAutomationExecution
- tag:GetResources
- tag:TagResources

지침

다음 단계에 따라 자동화를 구성하고 실행합니다.

Note

자동화를 실행하기 전에 다음 단계에 따라 필요한 IAM 역할을 구성합니다. 하나는 Systems Manager Automation이 실행서를 실행하기 위한 것이고 다른 하나는 Lambda가 Kubernetes API와 통신하기 위한 것입니다.

1. 계정TroubleshootEKSALBController-SSM-Role에서 SSM 자동화 역할을 생성합니다. 신뢰 관계에 다음 정책이 포함되어 있는지 확인합니다.

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "",
      "Effect": "Allow",
      "Principal": {
        "Service": "ssm.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

```
    ]
  }
}
```

2. 다음 IAM 정책을 연결하여 필요한 권한을 부여합니다.

```
{
  "Version": "2012-10-17",
  "Statement": [{
    "Sid": "TroubleshootEKSSALBControllerIssuesActions",
    "Effect": "Allow",
    "Action": [
      "eks:DescribeCluster",
      "eks:ListAssociatedAccessPolicies",
      "iam:GetRole",
      "iam:ListOpenIDConnectProviders",
      "ssm:StartAutomationExecution",
      "ssm:GetAutomationExecution",
      "ssm:DescribeAutomationExecutions",
      "ec2:DescribeSubnets",
      "ec2:DescribeRouteTables",
      "elasticloadbalancing:DescribeLoadBalancers",
      "elasticloadbalancing:DescribeAccountLimits",
      "ec2:DescribeInstances",
      "ec2:DescribeNetworkInterfaces",
      "ec2:DescribeSecurityGroups"
    ],
    "Resource": "*"
  },
  {
    "Sid": "SetupK8sApiProxyForEKSActions",
    "Effect": "Allow",
    "Action": [
      "cloudformation:CreateStack",
      "cloudformation>DeleteStack",
      "cloudformation:DescribeStacks",
      "cloudformation:UpdateStack",
      "ec2:CreateNetworkInterface",
      "ec2>DeleteNetworkInterface",
      "ec2:DescribeNetworkInterfaces",
      "ec2:DescribeRouteTables",
      "ec2:DescribeSecurityGroups",
      "ec2:DescribeSubnets",
      "ec2:DescribeVpcs",
      "eks:DescribeCluster",
```

```

        "iam:GetRole",
        "lambda:CreateFunction",
        "lambda:DeleteFunction",
        "lambda:GetFunction",
        "lambda:InvokeFunction",
        "lambda:ListTags",
        "lambda:TagResource",
        "lambda:UntagResource",
        "lambda:UpdateFunctionCode",
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:DescribeLogGroups",
        "logs:DescribeLogStreams",
        "logs:ListTagsForResource",
        "logs:PutLogEvents",
        "logs:PutRetentionPolicy",
        "logs:TagResource",
        "logs:UntagResource",
        "ssm:DescribeAutomationExecutions",
        "tag:GetResources",
        "tag:TagResources"
    ],
    "Resource": "*"
  },
  {
    "Sid": "PassRoleToAutomation",
    "Effect": "Allow",
    "Action": "iam:PassRole",
    "Resource": "*",
    "Condition": {
      "StringLikeIfExists": {
        "iam:PassedToService": [
          "lambda.amazonaws.com",
          "ssm.amazonaws.com"
        ]
      }
    }
  }
]
}

```

3. Amazon EKS 클러스터에 대한 액세스 항목을 구성합니다. 이는 자동화를 위한 필수 요구 사항입니다. 액세스 항목에 대한 인증 모드를 구성하는 단계는 [액세스 항목 설정을](#) 참조하세요.

Amazon EKS 콘솔에서 클러스터로 이동하여 다음 단계를 따릅니다.

- 액세스 섹션에서 인증 구성이 API 또는 로 설정되어 있는지 확인합니다 API_AND_CONFIG_MAP.
 - 액세스 항목 생성을 선택하고 다음을 구성합니다.
 - IAM 보안 주체 ARN에서 생성한 IAM 역할()을 선택합니다 TroubleshootEKSALBController-SSM-Role.
 - 유형에서 Standard를 선택합니다.
 - 액세스 정책 추가:
 - 정책 이름에서를 선택합니다 AmazonEKSAAdminViewPolicy.
 - 액세스 범위에서를 선택합니다 Cluster.
 - 정책 추가를 선택합니다.
 - 세부 정보를 확인하고 생성을 선택합니다.
4. Lambda 함수에 대한 IAM 역할을 생성합니다(입력 파라미터 LambdaRoleArn에서 참조).
- 다음 신뢰 정책을 사용하여 새 IAM 역할을 생성합니다.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Principal": {
                "Service": "lambda.amazonaws.com"
            },
            "Action": "sts:AssumeRole"
        }
    ]
}
```

- 이 역할에 다음 AWS 관리형 정책을 연결합니다.
 - AWSLambdaBasicExecutionRole
 - AWSLambdaVPCLAccessExecutionRole
- LambdaRoleArn 입력 파라미터에 필요하므로 이 역할의 ARN을 기록해 둡니다.

1. AWS Systems Manager 콘솔에서 [AWSSupport-TroubleshootEKSALBControllerIssues](#)로 이동합니다.
2. 자동화 실행(Execute automation)을 선택합니다.
3. 입력 파라미터의 경우, 다음 내용을 입력합니다.

- AutomationAssumeRole(선택 사항):

유형: AWS::IAM::Role::Arn

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

허용된 패턴: ^arn:(?:aws|aws-cn|aws-us-gov):iam::\d{12}:role/?[a-zA-Z_0-9+=,.\@_-/_]+/\$

- EksClusterName(필수):

유형: 문자열

설명: (필수) Amazon Elastic Kubernetes Service(Amazon EKS) 클러스터의 이름입니다.

허용된 패턴: ^[0-9A-Za-z][A-Za-z0-9_-]{0,99}\$

- ALBControllerDeploymentName(선택 사항):

유형: 문자열

설명: (선택 사항) Amazon EKS 클러스터에서 AWS Load Balancer 컨트롤러 배포의 이름입니다. 설치 중에 사용자 지정하지 않은 한 일반적으로 'aws-load-balancer-controller'입니다.

허용된 패턴: ^[a-z0-9]([-a-z0-9]{0,251}[a-z0-9])?\$

기본값: aws-load-balancer-controller

- ALBControllerNamespace(선택 사항):

유형: 문자열

설명: (선택 사항) AWS Load Balancer 컨트롤러가 배포되는 Kubernetes 네임스페이스입니다. 기본적으로 'kube-system'이지만 사용자 지정 네임스페이스에 컨트롤러를 설치한 경우 다를 수 있습니다.

허용된 패턴: ^[a-z0-9]([-a-z0-9]{0,61}[a-z0-9])?\$

기본값: kube-system

- ServiceAccountName(선택 사항):

유형: 문자열

설명: (선택 사항) AWS Load Balancer 컨트롤러와 연결된 Kubernetes 서비스 계정의 이름입니다. 설치 중에 사용자 지정되지 않는 한 일반적으로 'aws-load-balancer-controller'입니다.

허용된 패턴: `^[a-z0-9]([-a-z0-9]{0,251}[a-z0-9])?$`

기본값: aws-load-balancer-controller

- ServiceAccountNamespace(선택 사항):

유형: 문자열

설명: (선택 사항) AWS Load Balancer 컨트롤러의 서비스 계정이 있는 Kubernetes 네임스페이스입니다. 이는 일반적으로 'kube-system'이지만 사용자 지정 네임스페이스를 사용한 경우 다를 수 있습니다.

허용된 패턴: `^[a-z0-9]([-a-z0-9]{0,61}[a-z0-9])?$`

기본값: kube-system

- IngressName(선택 사항):

유형: 문자열

설명: (선택 사항) 검증할 수신 리소스의 이름(Application Load Balancer). 지정하지 않으면 수신 검증을 건너뜁니다.

허용된 패턴: `^$|^[a-z0-9][a-z0-9-]{0,251}[a-z0-9]$`

기본값: ""(빈 문자열)

- IngressNamespace(선택 사항):

유형: 문자열

설명: (선택 사항) 수신 리소스의 네임스페이스입니다. IngressName를 지정한 경우 필수입니다.

허용된 패턴: `^$|^[a-z0-9][a-z0-9-]{0,61}[a-z0-9]$`

기본값: ""(빈 문자열)

- ServiceName(선택 사항):

유형: 문자열

설명: (선택 사항) Network Load Balancer(Network Load Balancer) 주석을 검증하기 위한 특정 서비스 리소스의 이름입니다. 지정하지 않으면 서비스 리소스 검증을 건너뛵니다.

허용된 패턴: ^\$|^([a-z0-9][a-z0-9-]{0,251}[a-z0-9])\$

기본값: ""(빈 문자열)

- ServiceNamespace(선택 사항):

유형: 문자열

설명: (선택 사항) 서비스 리소스의 네임스페이스입니다. ServiceName를 지정한 경우 필수입니다.

허용된 패턴: ^\$|^([a-z0-9][a-z0-9-]{0,61}[a-z0-9])\$

기본값: ""(빈 문자열)

- LambdaRoleArn(필수):

유형: AWS::IAM::Role::Arn

설명: (필수) AWS Lambda (Lambda) 함수가 필요한 AWS 서비스 및 리소스에 액세스할 수 있도록 허용하는 IAM 역할의 ARN입니다. AWS 관리형 정책: AWSLambdaBasicExecutionRole 및 AWSLambdaVPCLambdaAccessExecutionRole를 Lambda 함수 실행 IAM 역할에 연결합니다.

허용된 패턴: ^arn:(?:aws|aws-cn|aws-us-gov):iam::\d{12}:role/?[a-zA-Z_0-9+=,.\@!-_/]+\$

4. 실행을 선택합니다.

5. 자동화가 시작됩니다.

6. 문서는 다음 단계를 수행합니다.

- a. ValidateAccessEntryAndOIDCProvider:

액세스 항목 권한 및 OIDC 공급자 구성을 확인하여 Amazon EKS 클러스터 IAM 설정을 검증합니다.

- b. SetupK8sAuthenticationClient:

SAW 문서 `AWSSupport-SetupK8sApiProxyForEKS`를 실행하여 클러스터에서 Amazon EKS API 호출을 실행하도록 Lambda 함수를 설정합니다.

c. `VerifyALBControllerAndIRSASetup`:

지정된 서비스 계정 및 Application Load Balancer 컨트롤러가 해당 네임스페이스에 존재하는지 확인합니다. 또한 Application Load Balancer 컨트롤러의 서비스 계정 역할 주석 및 신뢰 정책을 확인합니다.

d. `VerifyPodIdentityWebhookAndEnv`:

`pod-identity-webhook`가 실행 중인지 확인합니다. 또한 IRSA가 포드의 ENV 변수에 주입되는지 확인합니다.

e. `ValidateSubnetRequirements`:

사용 가능한 IP가 8개인 두 AZ의 서브넷을 2개 이상 확인합니다. 퍼블릭/프라이빗 로드 밸런서에 적절한 서브넷 태그 지정이 있습니다.

f. `CheckLoadBalancerLimitsAndUsage`:

계정 제한을 Application Load Balancer 및 Network Load Balancer 수와 비교합니다.

g. `CheckIngressOrServiceAnnotations`:

수신 및 서비스 리소스에서 올바른 주석과 사양을 확인하여 Application Load Balancer 및 Network Load Balancer 사용에 맞게 올바르게 구성되었는지 확인합니다.

h. `CheckWorkerNodeSecurityGroupTags`:

작업자 노드에 연결된 정확히 하나의 보안 그룹에 필요한 클러스터 태그가 있는지 확인합니다.

i. `CaptureALBControllerLogs`:

Amazon EKS 클러스터에서 실행 중인 AWS Load Balancer 컨트롤러 포드에서 최신 진단 로그를 검색합니다.

j. `CleanupK8sAuthenticationClient`:

'정리' 작업을 사용하여 SAW 문서 '`AWSSupport-SetupK8sApiProxyForEKS`'를 실행하여 자동화의 일부로 생성된 리소스를 정리합니다.

k. `GenerateReport`:

자동화 보고서를 생성합니다.

7. 실행이 완료되면 출력 섹션에서 실행의 자세한 결과를 검토합니다.

a. 보고서:

Amazon EKS 클러스터 상태, Application Load Balancer Controller 설정, IRSA 구성, 서브넷 요구 사항, 로드 밸런서 제한, 수신/서비스 주석, 작업자 노드 보안 그룹 태그 및 Application Load Balancer Controller 로그를 포함하여 수행된 모든 검사에 대한 포괄적인 요약を提供합니다. 여기에는 식별된 문제와 권장 해결 단계도 포함됩니다.

참조

Systems Manager Automation

- [이 자동화 실행\(콘솔\)](#)
- [자동화 실행](#)
- [자동화 설정](#)
- [자동화 워크플로 지원](#)

AWS Load Balancer 컨트롤러와 관련된 설명서

- [AWS Load Balancer서 컨트롤러](#)
- [액세스 항목 설정](#)

AWSsupport-TroubleshootEKSDNSFailure

설명

AWSsupport-TroubleshootEKSDNSFailure 실행서는 애플리케이션 또는 포드에 DNS 해결 실패가 발생할 때 Amazon Elastic Kubernetes Service(Amazon EKS)의 CoreDNS 포드 및 구성 문제를 해결하는 데 도움이 됩니다. 실행서는 VPC DNS 설정을 검증하고, CoreDNS 배포 및 ConfigMap을 검사하고, Horizontal Pod Autoscaler(HPA) 구성을 확인하고, CoreDNS 로그를 수집하고, 작업자 노드에서 DNS 확인 검사를 수행합니다. 선택적으로 문제가 있는 작업자 노드와 동일한 서브넷에 Amazon Elastic Compute Cloud 인스턴스를 검색하여 노드에 직접 액세스할 필요 없이 DNS 확인 검사를 수행할 수 있습니다.

⚠ Important

Amazon EKS 클러스터의 인증 모드는 API 또는 로 설정해야 합니다 API_AND_CONFIG_MAP. 이 실행서는 AWS Lambda (Lambda) 함수를 프록시로 배포하여 인증된 Kubernetes API 호출을 수행하고 실행이 끝날 때 생성된 모든 리소스를 정리합니다.

이 자동화 실행(콘솔)

문서 유형

자동화

소유자

Amazon

플랫폼

Linux, macOS, Windows

파라미터

- AutomationAssumeRole

유형: AWS::IAM::Role::Arn

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.

- EksClusterName

유형: 문자열

설명: (필수) 대상 Amazon EKS 클러스터의 이름입니다.

- DnsName

유형: 문자열

기본값: amazon.com

설명: (선택 사항) 애플리케이션 또는 포드가 확인하지 못한 도메인 이름의 스텝 도메인 접미사입니다.

- ProblematicNodeInstanceId

유형: AWS::EC2::Instance::Id

설명: (선택 사항) DNS 확인 오류가 발생한 애플리케이션이 실행 중인 작업자 노드의 인스턴스 ID입니다. 제공된 경우 실행서는 동일한 서브넷에 탐색 Amazon EC2 인스턴스를 생성하여 DNS 확인 검사를 수행합니다. 작업자 노드가 퍼블릭 서브넷에 있지 않거나 작업자 노드 bind-utils에 설치가 허용되지 않는 경우 이 파라미터를 사용합니다.

- CoreDnsNamespace

유형: 문자열

기본값: kube-system

설명: (선택 사항) CoreDNS 포드의 Kubernetes 네임스페이스입니다.

- S3BucketName

유형: AWS::S3::Bucket::Name

설명: (선택 사항) CoreDNS 문제 해결 로그가 업로드되는 Amazon Simple Storage Service 버킷의 이름입니다.

- LambdaRoleArn

유형: AWS::IAM::Role::Arn

설명: (선택 사항) Lambda 프록시 함수에 대한 IAM 역할의 ARN입니다. 제공되지 않은 경우 실행서는 AWSLambdaBasicExecutionRole 및 AWSLambdaVPCLAccessExecutionRole 관리형 정책을 Automation-K8sProxy-Role-<ExecutionId> 사용하여 라는 역할을 생성합니다. 자체 역할을 제공하는 것이 좋습니다.

필수 IAM 권한

실행서를 성공적으로 사용하려면 AutomationAssumeRole 파라미터에 다음 작업이 필요합니다.

- eks:DescribeCluster
- ec2:DescribeVpcs

- `ec2:DescribeInstances`
- `ec2:DescribeSubnets`
- `ec2:DescribeSecurityGroups`
- `cloudformation:CreateStack`
- `cloudformation:DescribeStacks`
- `cloudformation>DeleteStack`
- `lambda:InvokeFunction`
- `s3:GetBucketPublicAccessBlock`
- `s3:GetBucketAcl`
- `s3:PutObject`
- `ssm:DescribeInstanceInformation`
- `ssm:SendCommand`
- `ssm:GetCommandInvocation`
- `ssm:StartAutomationExecution`
- `ssm:GetAutomationExecution`

문서 단계

1. `AssertIfTargetClusterExists` -에 지정된 Amazon EKS 클러스터가 `EksClusterName` 존재하고 ACTIVE 상태인지 확인합니다. 클러스터를 찾을 수 없거나 활성화되지 않은 경우 실행서는 로 건너뛰니다 `GenerateReport`.
2. `UpdateEksClusterExists` - 보고서 생성에 사용할 내부 `eksClusterExists` 변수를 `true`로 설정합니다.
3. `GetVpcDnsSettings` - Amazon EKS 클러스터와 연결된 Amazon Virtual Private Cloud에 대한 `enableDnsSupport` 및 `enableDnsHostnames` 설정을 검색합니다.
4. `BranchOnVpcDnsSettings` - 두 VPC DNS 설정이 모두 활성화되어 있는지 확인합니다. 둘 중 하나가 비활성화되면 실행서는 로 건너뛰니다 `GenerateReport`. 그렇지 않으면가 로 진행합니다 `DeployK8sAuthApisResources`.
5. `DeployK8sAuthApisResources` - Lambda 함수를 실행 `AWSSupport-SetupK8sApiProxyForEKS`하여 Amazon EKS 클러스터에 인증된 Kubernetes API 호출을 수행하기 위한 프록시로 배포합니다.

6. RetrieveCoreDNSDeployment - 포트 준비, 컨테이너 상태, CoreDNS 포드를 호스팅하는 노드의 준비 등 CoreDNS 배포에 대한 정보를 검색합니다. 또한 CoreDNS 클러스터 IP를 검색합니다.
7. RetrieveAndInspectCoreDNSConfigMap - Amazon EKS 클러스터에서 CoreDNS ConfigMap 을 검색하고에 지정된 도메인에 대한 스텝 도메인 설정을 포함하여 구성 문제를 확인합니다DnsName.
8. ValidateHpaConfiguration - 지정된 네임스페이스에서 CoreDNS 배포를 위해 Horizontal Pod Autoscaler(HPA)가 구성되어 있는지 확인합니다.
9. CheckS3BucketPublicStatus -에 지정된 Amazon S3 버킷이 퍼블릭 또는 익명 읽기 또는 쓰기 액세스를 허용하지 S3BucketName 않는지 확인합니다.
- 10CollectLogToS3 - CoreDNS 포트 로그를 수집하여 지정된 Amazon S3 버킷에 업로드합니다.
- 11BranchOnProblematicNodeInstanceId - ProblematicNodeInstanceId가 제공되고 CoreDNS 호스트 노드가 존재하는지 확인합니다. 두 조건이 모두 충족되면가 로 진행합니다VerifyThatProblematicNodeInstanceBelongsToCluster. 그렇지 않으면가 로 분기합니다BranchOnCoreDnsDeployment.
- 12.VerifyThatProblematicNodeInstanceBelongsToCluster -에 지정된 인스턴스가 Amazon EKS 클러스터의 작업자 노드ProblematicNodeInstanceId인지 확인합니다.
- 13.UpdateProblematicNodeInstanceStanding - 내부 problematicNodeInstanceStanding 변수를 로 설정합니다true.
- 14.GetProblematicInstanceDetails - 탐색 Amazon EC2 인스턴스를 생성할 때 사용할 문제가 있는 작업자 노드의 AMI ID, 인스턴스 유형, 서브넷 ID 및 보안 그룹 IDs를 검색합니다.
- 15.CreateProbingInfrastructure - 인스턴스 프로파일을 생성하고 문제가 있는 작업자 노드와 동일한 서브넷의 AWS CloudFormation 스택을 통해 Amazon EC2 인스턴스를 탐색합니다. 스택의 이름은입니다AWSSupport-TroubleshootEKSDNSFailure-<ExecutionId>.
- 16.GetProbingInstanceId - CloudFormation 스택 출력에서 탐색 Amazon EC2 인스턴스 ID를 검색합니다.
- 17.WaitForProbingInstanceSSMAgentStateToBeOnline - 계속하기 전에 탐색 중인 Amazon EC2 인스턴스의 Amazon EC2 Systems Manager 에이전트가 Online 상태를 보고할 때까지 기다립니다. Amazon EC2
- 18.RetrieveCoreDNSPodsIPFromProblematicNode - 문제가 있는 작업자 노드에서 볼 수 있는 CoreDNS 포트 IP 주소를 검색합니다.
- 19.PerformDNSResolutionOnProbingEC2Instance - 클러스터 IP 및 CoreDNS 포트 IP를 사용하여 탐색 Amazon EC2 인스턴스에서 DNS 확인 검사를 실행합니다.

- 20DeleteCloudFormationStack - 탐색 Amazon EC2 인스턴스 및 인스턴스 프로파일을 생성한 CloudFormation 스택을 삭제합니다.
- 21UpdateCfnStackDeleted - 내부 cfnStackDeleted 변수를 로 설정합니다true.
- 22BranchOnCoreDnsDeployment - ProblematicNodeInstanceId가 제공되지 않았고 CoreDNS 호스트 노드가 존재하는지 확인합니다. 두 조건이 모두 충족되면가 로 진행합니다PerformDNSResolutionOnCoreDnsWorkerNodes. 그렇지 않으면가 로 진행합니다CleanupK8sAuthenticationInfrastructure.
- 23BranchOnCoreDnsNodesExistForRunCommandSteps - aws:runCommand 단계를 실행하기 전에 CoreDNS 호스트 노드가 존재하는지 확인합니다. 노드가 없는 경우(예: CoreDNS에 복제본이 없는 경우)는 로 건너뛵니다CleanupK8sAuthenticationInfrastructure.
- 24PerformDNSResolutionOnCoreDnsWorkerNodes - 클러스터 IP 및 CoreDNS 포드 IP를 사용하여 CoreDNS 작업자 노드에서 DNS 확인 검사를 직접 실행합니다.
- 25.VerifyNameserverMatchAndKubeProxyLogsAndIPTableEntries - 네임서버 IP가 클러스터 IP와 일치하는지 확인하고, API 서버에 대한 kube-proxy 포드 액세스를 확인하고, CoreDNS 작업자 노드의 kube-dns iptables 항목을 검증합니다.
- 26.VerifyPPSThrottlingOnENIs - CoreDNS 작업자 노드에서 탄력적 네트워크 인터페이스(ENI)당 packets-per-second 수(PPS) 제한을 확인하여 잠재적 제한을 식별합니다. CoreDNS
- 27UpdateChecksOnNodes - 노드 수준 검사가 수행되었음을 나타내기 true 위해 내부 checksOnNodes 변수를 로 설정합니다.
- 28CleanupK8sAuthenticationInfrastructure - AWSSupport-SetupK8sApiProxyForEKS Cleanup 작업을 실행하여 자동화 중에 생성된 Lambda 프록시 함수 및 관련 리소스를 제거합니다.
- 29UpdateK8sInfrastructreDeleted - 내부 K8sInfrastructreDeleted 변수를 로 설정합니다true.
- 30CleanUpAllResources - 이전 정리 단계가 성공적으로 완료되지 않은 경우 CloudFormation 스택 및 Lambda 프록시 함수를 포함하여 나머지 리소스를 포괄적으로 정리합니다.
- 31CollectOutputFromAllRunCommandSteps - 자동화 중에 실행된 모든 aws:runCommand 단계의 출력을 수집하고 통합합니다.
- 32GenerateReport - 모든 이전 단계의 결과를 VPC DNS 설정, CoreDNS 배포 상태, ConfigMap 구성, HPA 구성, 로그 수집 상태 및 DNS 확인 검사 결과를 포함하는 포괄적인 평가 보고서로 컴파일합니다.

출력

GenerateReport.EvalReport - 조사 결과 및 권장 문제 해결 단계를 포함하여 수행된 모든 DNS 문제 해결 검사에 대한 포괄적인 보고서입니다.

Elastic Beanstalk

AWS Systems Manager 자동화에는 대한 사전 정의된 실행서를 제공합니다 AWS Elastic Beanstalk. 실행서에 대한 자세한 내용은 [실행서 작업](#)을 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(Amazon EC2) Windows Server 인스턴스에서 AWS Elastic Beanstalk 관련 로그 파일을 수집하여 일반적인 문제를 해결하는 데 도움을 줍니다. 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 활동으로 인해 Amazon EC2 인스턴스에서 CPUUtilization 증가를 초래할 수 있습니다. CPUUtilization에 대한 자세한 내용은 Amazon CloudWatch 사용 설명서의 [인스턴스 지표](#)를 참조하세요.

S3BucketName 파라미터에 대한 값을 지정하는 경우, 지정하는 Amazon Simple Storage Service(Amazon S3) 버킷의 정책 상태를 자동화에서 평가합니다. Amazon EC2 인스턴스로부터 수집한 로그의 보안을 돕기 위해, 정책 상태 isPublic(이)가 true(으)로 설정되어 있거나 액세스 제어 목록(ACL)이 All Users Amazon S3의 미리 정의된 그룹에 READ|WRITE 권한을 부여하는 경우, 로그는 업로드되지 않습니다. Amazon S3의 미리 정의된 그룹에 대한 자세한 내용은 Amazon Simple Storage Service 사용 설명서에서 [Amazon S3의 미리 정의된 그룹](#)을 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. *region* 및 *accountID*

값은 자동화를 실행하는 리전 및 AWS 계정 에 따라 달라집니다. 로그 번들은 `resources/environments/logs/bundle/ environmentID / instanceID` 디렉터리에 저장됩니다. *environmentID* 및 *instanceID* 값은 Elastic Beanstalk 환경 및 로그를 수집하는 Amazon EC2 인스턴스에 따라 달라집니다.

기본적으로 Elastic Beanstalk 환경의 Amazon EC2 인스턴스에 연결된 AWS Identity and Access Management (IAM) 인스턴스 프로파일에는 번들을 환경의 기본 Elastic Beanstalk Amazon S3 버킷에 업로드하는 데 필요한 권한이 있습니다. S3BucketName 파라미터 값을 지정하는 경우, Amazon EC2 인스턴스에 연결된 인스턴스 프로파일은 지정된 Amazon S3 버킷 및 경로에 대한 `s3:GetBucketAcl`, `s3:GetBucketPolicy`, `s3:GetBucketPolicyStatus` 및 `s3:PutObject` 작업을 허용해야 합니다.

Note

이 자동화를 수행하려면 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

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.

다. 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 수집하려는 Elastic Beanstalk 환경의 Amazon EC2 인스턴스의 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 파라미터에서 지정하는 Amazon EC2 인스턴스가 AWS Systems Manager에 의해 관리되는지 확인합니다.

- `aws:assertAwsResourceProperty` - InstanceId 파라미터에서 지정하는 Amazon EC2 인스턴스가 Windows Server 인스턴트인지 확인합니다.
- `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 실행서는 지정한 AWS Elastic Beanstalk (Elastic Beanstalk) 환경에 대한 로깅을 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.

- 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 Ready로 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

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.

- EnvironmentId

유형: 문자열

설명: (필수) 일림을 활성화하려는 Elastic Beanstalk 환경의 ID입니다.

- TopicArn

유형: 문자열

설명: (필수) 알림을 보내려는 Amazon Simple Notification Service(Amazon SNS) 주제의 ARN입니다.

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 Ready로 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 Virtual Private Cloud(VPC)에 대한 구성 세부 정보입니다.
- 서브넷과 연결된 보안 그룹 규칙, 라우팅 테이블, 네트워크 액세스 제어 목록(ACL)과 연결된 네트워크 구성 문제.
- 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 파일에 업로드합니다 지원.

[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.

- `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 로그 번들을 업로드 지원 하기 위해에서 제공하는 URL입니다. 이 옵션은 지원 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 주체에 실행서에 정의된 모든 작업을 수행하는 데 필요한 권한이 있는지 확인합니다.
- aws:branch - 이전 단계의 결과를 기반으로 워크플로를 분기합니다.
- aws:executeScript - 로드 밸런서, CloudFormation 스택, Auto Scaling 그룹, Amazon EC2 인스턴스 및 VPC 구성을 포함한 Elastic Beanstalk 환경에 대한 정보를 수집합니다.
- aws:executeScript - VPC의 서브넷과 연결된 라우팅 테이블 및 ACL의 네트워크 연결 문제를 확인합니다.
- aws:executeScript - Amazon EC2 인스턴스와 연결된 보안 그룹 규칙의 네트워크 연결 문제를 확인합니다.
- aws:executeScript - Amazon EC2 인스턴스의 상태를 확인합니다.
- aws:executeScript - Elastic Beanstalk 환경의 로그 번들에 대한 링크를 생성합니다.
- aws:executeScript - 로그 번들들에 업로드합니다 지원.
- 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 Balancing을 위한 사전 정의된 실행서를 제공합니다. 실행서에 대한 자세한 내용은 [실행서 작업](#)을 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](#)
- [AWSSupport-TroubleshootELBHealthChecks](#)

AWSConfigRemediation-DropInvalidHeadersForALB

설명

AWSConfigRemediation-DropInvalidHeadersForALB 실행서는 유효하지 않은 헤더가 있는 HTTP 헤더를 제거하도록 사용자가 지정하는 Application Load Balancer를 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.

- LoadBalancerArn

유형: 문자열

설명: (필수) 유효하지 않은 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 Balancer에 대한 액세스 로그를 활성화합니다.

[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.

- EmitInterval

유형: 정수

유효한 값: 5 | 60

기본값: 60

설명: (선택 사항) 액세스 로그를 분 단위로 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 구조입니다. 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 파라미터에서 지정한 Classic Load Balancer에 대한 액세스 로그를 활성화합니다.

출력

EnableCLBAccessLogs.SuccessesLoadBalancers - 액세스 로그가 성공적으로 활성화된 로드 밸런서 이름 목록입니다.

EnableCLBAccessLogs.FailedLoadBalancers - 액세스 로그 활성화가 실패한 로드 밸런서 이름의 MapList 및 실패 이유.

AWS-EnableCLBConnectionDraining

설명

AWS-EnableCLBConnectionDraining 실행서는 Classic Load Balancer(CLB)에서 지정된 제한 시간 값으로 연결 드레이닝을 활성화합니다. 연결 드레이닝을 사용하면 CLB가 등록 취소 중이거나 비정상인 인스턴스에 대한 진행 중인 요청을 완료할 수 있습니다. 이때 지정된 제한 시간은 인스턴스를 등록 취소된 것으로 보고하기 전에 연결을 유지한 시간입니다. CLB의 연결 드레이닝에 대한 자세한 내용은 [Classic Load Balancer 사용 설명서의 Classic Load Balancer의 연결 드레이닝 구성을 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.

- 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 1초에서 3,600초 사이로 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 지정된 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 실행서는 지정하는 Classic Load Balancer(CLB)에 대한 교차 영역 로드 밸런싱을 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.

- `LoadBalancerName`

유형: 문자열

설명: (필수) 교차 영역 로드 밸런싱을 활성화하려는 CLB의 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 파라미터에서 사용자가 지정하는 CLB에 대해 교차 영역 로드 밸런싱을 활성화합니다.
- aws:assertAwsResourceProperty - CLB에서 교차 영역 로드 밸런싱이 활성화되었는지 확인합니다.

AWSConfigRemediation-EnableELBDeletionProtection

설명

AWSConfigRemediation-EnableELBDeletionProtection 실행서는 지정하는 Elastic Load Balancer(ELB)에 대한 삭제 보호를 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.

- LoadBalancerArn

유형: 문자열

설명: (필수) 삭제 보호를 활성화하려는 ELB의 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 파라미터에서 지정하는 ELB에서 삭제 보호를 활성화합니다.

AWSConfigRemediation-EnableLoggingForALBAndCLB

설명

AWSConfigRemediation-EnableLoggingForALBAndCLB 실행서는 지정된 AWS Application Load Balancer 또는 Classic Load Balancer(CLB)에 대한 로깅을 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.

- LoadBalancerId

유형: 문자열

설명: (필수) Classic Load Balancer 이름 또는 Application Load Balancer ARN입니다.

- 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 Clastic Load Balancer(CLB)와 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스 간의 연결 문제를 해결하는 데 도움이 됩니다. 또한, 클라이언트와 CLB 간의 연결 문제를 검토합니다. 또한 이 실행서는 CLB의 상태 점검을 검토하고, 모범 사례가 준수되고 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 요금](#)을 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.

- InvestigationType

유형: 문자열

유효한 값: Best Practices | Connectivity Issues | Troubleshooting Dashboard

설명: (필수) 실행서에서 수행하려는 작업입니다.

- LoadBalancerName

유형: 문자열

설명: (필수) CLB의 이름입니다.

- 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/*S3LocationPrefix*/*{{InvestigationType}}*_*{{automation:EXECUTION_ID}}*.txt 형식으로 저장됩니다.

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` 파라미터에서 지정하는 CLB가 존재하는지 확인합니다.
- `aws:branch` - `InvestigationType` 파라미터에 대해 지정된 값을 기반으로 분기합니다.
- `aws:executeScript` - CLB에 대한 연결 검사를 수행합니다.
- `aws:executeScript` - CLB 구성이 Elastic Load Balancing 모범 사례를 준수하는지 확인합니다.
- `aws:executeScript` - CLB를 위한 Amazon CloudWatch 대시보드를 생성합니다.
- `aws:executeScript` - 자동화 결과가 포함된 텍스트 파일을 생성하여 `S3Location` 파라미터에서 지정하는 Amazon S3 버킷에 업로드합니다.

출력

`RunBestPractices.Summary`

`RunConnectivityChecks.Summary`

`CreateTroubleshootingDashboard.Output`

`UploadOutputToS3.Output`

AWSConfigRemediation-EnableNLBCrossZoneLoadBalancing

설명

`AWSConfigRemediation-EnableNLBCrossZoneLoadBalancing` 실행서는 지정하는 Network Load Balancer(NLB)에 대한 교차 영역 로드 밸런싱을 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.

- LoadBalancerArn

유형: 문자열

설명: (필수) 교차 영역 로드 밸런싱을 활성화하려는 NLB의 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 지정하는 NLB에 대해 교차 영역 로드 밸런싱을 활성화합니다.
- aws:executeScript - NLB에서 교차 영역 로드 밸런싱이 활성화되었는지 확인합니다.

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

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.

- LoadBalancerArn

유형: 문자열

설명: (필수) 비동기화 완화 모드를 수정하려는 ALB의 Amazon 리소스 이름(ARN)입니다.

- DesyncMitigationMode

유형: 문자열

유효한 값: 모니터 | 방어 | 가장 엄격

설명: (필수) ALB에서 사용할 완화 모드입니다. 비동기화 완화 모드에 대한 자세한 내용은 Application Load Balancer 사용 설명서의 [비동기화 완화 모드](#)를 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)` - 지정된를 사용하도록 ALB를 업데이트합니다 `DesyncMitigationMode`.
- `VerifyLoadBalancerDesyncMitigationMode(aws:executeScript)` - 대상 ALB에 대해 비동기 완화 모드가 업데이트되었는지 확인합니다.

출력

`VerifyLoadBalancerDesyncMitigationMode.ModificationResult` - ALB 수정을 확인하는 스크립트의 메시지 페이로드입니다.

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

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.

- LoadBalancerName

유형: 문자열

설명: (필수) 비동기 완화 모드를 수정하려는 CLB의 이름입니다.

- DesyncMitigationMode

유형: 문자열

유효한 값: 모니터 | 방어 | 가장 엄격

설명: (필수) CLB가 사용할 완화 모드입니다. 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) - 지정된를 사용하도록 CLB를 업데이트합니다DesyncMitigationMode.

- VerifyLoadBalancerDesyncMitigationMode(aws:executeScript) - 대상 CLB에 대해 비동기 완화 모드가 업데이트되었는지 확인합니다.

출력

VerifyLoadBalancerDesyncMitigationMode.ModificationResult - CLB에 대한 수정을 확인하는 스크립트의 메시지 페이로드입니다.

AWSSupport-TroubleshootELBHealthChecks

설명

AWSSupport-TroubleshootELBHealthChecks 실행서는 관련 Amazon CloudWatch(CloudWatch) 지표를 분석하고, 네트워크 연결을 확인하고, 대상 인스턴스에서 진단 명령을 실행하여 AWS Elastic Load Balancing(Elastic Load Balancing) 상태 확인 문제를 해결하는 데 도움이 됩니다.

이 실행서는 다음 사용 사례를 다룹니다.

- 로드 밸런서 또는 대상 그룹의 대상 인스턴스 내에 비정상 인스턴스가 있습니다.
- 비정상 인스턴스는 없지만 CloudWatch 지표에는 대한 데이터 포인트를 나타냅니다.
UnHealthyHostCounts

Important

중요 고려 사항:

- 자동화는 인스턴스 유형 대상 문제 해결에 중점을 둡니다.
- 문제 해결에 허용되는 최대 인스턴스 수는 50개입니다.
- 인스턴스 수준에서 진단 명령을 실행하려면 Systems Manager에서 대상 인스턴스를 관리해야 합니다.
- S3BucketName 파라미터는 선택 사항이지만 특정 진단 결과는 지정된 Amazon S3 버킷에 직접 업로드되며 자동화 출력에 표시되지 않습니다.
- IPv6 네트워크 연결 문제 해결은 지원되지 않습니다.

[이 자동화 실행\(콘솔\)](#)

문서 유형

자동화

소유자

Amazon

플랫폼

/

필수 IAM 권한

실행서를 성공적으로 사용하려면 AutomationAssumeRole 파라미터에 다음 작업이 필요합니다.

- elasticloadbalancing:DescribeLoadBalancers
- elasticloadbalancing:DescribeTargetGroups
- elasticloadbalancing:DescribeTargetHealth
- elasticloadbalancing:DescribeInstanceHealth
- ec2:DescribeInstances
- ec2:DescribeNetworkInterfaces
- ec2:DescribeSecurityGroups
- ec2:DescribeSubnets
- cloudwatch:GetMetricStatistics
- ssm:SendCommand
- ssm:GetCommandInvocation
- ssm:DescribeInstanceInformation
- s3:GetBucketLocation
- s3:GetBucketAcl
- s3:PutObject

정책 예제:

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

```

    {
      "Effect": "Allow",
      "Action": [
        "elasticloadbalancing:DescribeLoadBalancers",
        "elasticloadbalancing:DescribeTargetGroups",
        "elasticloadbalancing:DescribeTargetHealth",
        "elasticloadbalancing:DescribeInstanceHealth",
        "ec2:DescribeInstances",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeSubnets",
        "cloudwatch:GetMetricStatistics",
        "ssm:SendCommand",
        "ssm:GetCommandInvocation",
        "ssm:DescribeInstanceInformation",
        "s3:GetBucketLocation",
        "s3:GetBucketAcl",
        "s3:PutObject"
      ],
      "Resource": "*"
    }
  ]
}

```

지침

다음 단계에 따라 자동화를 구성합니다.

1. Systems Manager [AWSSupport-TroubleshootELBHealthChecks](#)의 문서로 이동합니다.
2. Execute automation(자동화 실행)을 선택합니다.
3. 입력 파라미터에 다음을 입력합니다.
 - AutomationAssumeRole(선택 사항):
 - 설명: (선택 사항) SSM Automation이 사용자를 대신하여 작업을 수행하도록 허용하는 (IAM) 역할의 AWS Identity and Access Management Amazon 리소스 이름(ARN)입니다. 역할이 지정되지 않은 경우 SSM Automation은 이 실행서를 시작하는 사용자의 권한을 사용합니다.
 - 유형: `AWS::IAM::Role::Arn`
 - LoadBalancerOrTargetGroupName(필수):
 - 설명: (필수) Classic Load Balancer의 이름 또는 Application Load Balancer 또는 Network Load Balancer와 연결된 대상 그룹의 이름입니다.

- 유형: String
- 허용된 패턴: `^[a-zA-Z0-9-]+$`
- ExecutionMode(필수):
 - 설명: (필수) 자동화 실행 모드를 제어합니다. Complete는 Amazon EC2 인스턴스에서 runCommands를 포함한 모든 단계를 실행합니다.는 인스턴스에서 명령 실행을 제외한 모든 단계를 SkipRunCommands 실행합니다.
 - 유형: String
 - 허용된 값: [Complete, SkipRunCommands]
- S3BucketName(선택 사항):
 - 설명: (선택 사항) 문제 해결 로그를 업로드하려는 계정의 Amazon S3 버킷 이름입니다.
 - 유형: String
 - 기본값: ""

4. 실행을 선택합니다.

5. 자동화가 시작됩니다.

6. 문서는 다음 단계를 수행합니다.

- getBucketPublicStatus:

대상 Amazon S3 버킷이 객체에 대한 읽기 또는 쓰기 퍼블릭 액세스 권한을 부여할 가능성이 있는지 확인합니다.

- getLoadBalancerDetails:

로드 밸런서 유형을 식별하고 통합 로드 밸런서 세부 정보 객체를 반환합니다.

- checkLoadBalancerType:

로드 밸런서가 존재하는지 확인합니다.

- getTargets:

쿼리는 다양한 유형의 로드 밸런서를 기반으로 정상 및 비정상 대상 세부 정보의 맵을 반환하는 APIs를 설명합니다.

- checkCloudWatchMetrics:

CloudWatch 지표HealthyHostCountsUnHealthyHostCounts를 확인하고 CloudWatch 링크를 생성합니다.

- checkUnhealthyReasons:

비정상 원인을 확인하고 대상을 필터링합니다.

- `checkConnectivity`:

로드 밸런서와 해당 인스턴스 간의 연결을 확인합니다.

- `runCommands`:

인스턴스에서 문제 해결 명령을 실행하고 버킷 이름이 제공된 경우 출력을 업로드합니다.

- `generateReport`:

이전 단계의 출력을 기반으로 최종 보고서를 생성하고 지정된 경우 Amazon S3 버킷에 보고서를 업로드합니다.

7. 완료되면 출력 섹션에서 실행의 자세한 결과를 검토합니다.

진단 명령

실행서는 인스턴스에서 다음 진단 명령을 실행합니다.

- Linux 셸: `top`, `free`, `ss`, `curl`, `iptables`, `tcpdump`
- Windows PowerShell: `Get-CimInstance`, `Get-NetFirewallProfile`, `Get-NetFirewallRule`, `Invoke-WebRequest`, `netstat`, `netsh`, `pktmon`

참조

Systems Manager Automation

- [이 자동화 실행\(콘솔\)](#)
- [자동화 실행](#)
- [Automation 설정](#)
- [자동화 워크플로 지원](#)

Amazon EMR

AWS Systems Manager Automation은 Amazon EMR용 사전 정의된 실행서를 제공합니다. 실행서에 대한 자세한 내용은 [실행서 작업](#)을 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 발생하는 오류를 식별하는 데 도움이 됩니다. 실행서는 파일 시스템에 정의된 로그 목록을 분석하고 미리 정의된 키워드 목록을 찾습니다. 이러한 로그 항목은 Amazon CloudWatch Events 이벤트를 생성하는 데 사용되므로 이벤트를 기반으로 필요한 조치를 취할 수 있습니다. 선택적으로, 실행서는 사용자가 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 컨테이너의 메모리가 부족하여 실행 중인 작업이 실패할 수 있습니다.
- `yarn_nodemanager_health`: CORE 또는 TASK 노드의 디스크 공간이 부족하여 작업을 실행할 수 없습니다.
- `node_state_change`: MASTER 노드에서 CORE 또는 TASK 노드에 연결할 수 없습니다.
- `step_failure`: EMR 단계가 실패했습니다.
- `no_core_nodes_running`: 현재 실행 중인 CORE 노드가 없고 클러스터가 비정상입니다.
- `hdfs_missing_blocks`: HDFS 블록이 누락되어 데이터가 손실될 수 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`: YARN이 실행 중인 작업에서 CORE 또는 TASK 노드를 블랙리스트에 올렸습니다.
- `yarn_node_lost`: CORE 또는 TASK 노드가 YARN에 의해 손실된 것으로 표시되었습니다. 연결 문제가 있을 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 실행서는 Amazon EMR 릴리스 버전 5.20~6.30을 지원합니다.

[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.

- ClusterID

유형: 문자열

설명: (필수) 분석하려는 노드 로그가 있는 클러스터의 ID입니다.

- 연산

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 파라미터에 대해 yes 값을 지정하면 자동화가 CloudWatchLogGroup 파라미터에서 지정된 이름을 가진 CloudWatch Logs 로그 그룹을 생성하여 일치하는 로그 항목을 저장합니다.

- CloudWatchLogGroup

유형: 문자열

설명: (선택 사항) 일치하는 로그 항목을 모두 저장하려는 CloudWatch Logs 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(을)를 지정하면, 해당 내용이 아직 없는 경우 CloudWatch 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 Logs 로그 그룹에 대한 지표 필터를 생성하려는 경우 yes(을)를 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` 파라미터에서 지정된 Amazon EMR 클러스터에 대한 정보를 수집합니다.
- `aws:branch` - 입력을 기반으로 분기합니다.
 - 제공된 작업이 `Run Once` 또는 `Schedule`인 경우:
 - `aws:assertAwsResourceProperty` - 클러스터를 사용할 수 있는지 확인합니다.
 - `aws:executeAwsApi` - 클러스터에서 실행 중인 모든 인스턴스의 ID를 수집합니다.
 - `aws:assertAwsResourceProperty` - 클러스터의 모든 인스턴스에서 SSM 에이전트가 실행되고 있는지 확인합니다.
 - `aws:branch` - 자동화를 한 번 실행하도록 지정했는지, 또는 일정에 따라 실행하도록 지정했는지에 따라 분기합니다.
 - 제공된 작업이 `Run Once`인 경우:
 - `aws:branch` - `LogToCloudWatchLogs` 파라미터에서 지정된 값을 기반으로 분기합니다.
 - `LogToCloudWatchLogs` 값이 `yes`인 경우:
 - `aws:executeScript` - `CloudWatchLogGroup` 파라미터에서 지정된 이름을 가진 `CloudWatch Logs` 로그 그룹이 이미 존재하는지 확인합니다. 그렇지 않은 경우, 지정된 이름으로 그룹이 생성됩니다.
 - `aws:branch` - `CreateMetricFilters` 파라미터에서 지정된 값을 기반으로 분기합니다.
 - `CreateMetricFilters` 값이 `yes`인 경우:
 - `aws:executeAwsApi` - 각 지표 필터에 대해 12단계가 실행됩니다.
 - `aws:branch` - `CreateLogInsightsDashboard` 파라미터에서 지정된 값을 기반으로 분기합니다.

- CreateLogInsightsDashboard 값이 yes인 경우:
 - aws:executeAwsApi - CloudWatchLogGroup 파라미터에서 지정된 동일한 이름을 사용하여 CloudWatch 대시보드를 생성합니다(해당 내용이 아직 없는 경우).
- CreateLogInsightsDashboard 값이 no인 경우:
 - aws:runCommand - 셸 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 - CloudWatchLogGroup 파라미터에서 지정된 동일한 이름을 사용하여 CloudWatch 대시보드를 생성합니다(해당 내용이 아직 없는 경우).
- CreateLogInsightsDashboard 값이 no인 경우:
 - aws:runCommand - 셸 스크립트를 실행하여 클러스터의 각 인스턴스에서 로그 패턴을 찾습니다.
- LogToCloudWatchLogs 값이 no인 경우:
 - aws:executeAwsApi - 셸 스크립트를 실행하여 클러스터의 각 인스턴스에서 로그 패턴을 찾습니다.
- 제공된 작업이 Schedule인 경우:
 - aws:createStack - 이 실행서를 대상으로 하는 Amazon EventBridge 이벤트를 생성합니다.
- 제공된 작업이 Remove Schedule인 경우:
 - aws:executeAwsApi - 클러스터에 일정이 있는지 확인합니다.
 - aws:deleteStack - 일정을 삭제합니다.

출력

GetClusterInformation.ClusterName

GetClusterInformation.ClusterState

ListingClusterInstances.InstanceIDs

CreatingScheduleCloudFormationStack.StackStatus

RemovingScheduleByDeletingScheduleCloudFormationStack.StackStatus

CheckIfLogGroupExists.output

FindLogPatternOnEMRNode.CommandId

AWSSupport-DiagnoseEMRLogsWithAthena

설명

실행AWSSupport-DiagnoseEMRLogsWithAthena서는 AWS Glue Data Catalog와 통합된 Amazon Athena를 사용하여 Amazon EMR 로그를 진단하는 데 도움이 됩니다. Amazon Athena는 특정 날짜 범위 또는 키워드 기반 검색에 대한 선택적 파라미터를 사용하여 컨테이너, 노드 로그 또는 둘 다에 대한 Amazon EMR 로그 파일을 쿼리하는 데 사용됩니다.

실행서는 기존 클러스터의 Amazon EMR 로그 위치를 자동으로 검색하거나 Amazon S3 로그 위치를 지정할 수 있습니다. 로그를 분석하려면 실행서는 다음과 같습니다.

- AWS Glue 데이터베이스를 생성하고 Amazon EMR Amazon S3 로그 위치에서 Amazon Athena Data Definition Language(DDL) 쿼리를 실행하여 클러스터 로그 및 알려진 문제 목록에 대한 테이블을 생성합니다. Amazon S3
- 데이터 조작 언어(DML) 쿼리를 실행하여 Amazon EMR 로그에서 알려진 문제 패턴을 검색합니다. 쿼리는 감지된 문제 목록, 발생 횟수 및 Amazon S3 파일 경로별로 일치하는 키워드 수를 반환합니다.
- 결과는 접두사 아래에 지정한 Amazon S3 버킷에 업로드됩니다. `saw_diagnose_EMR_known_issues`.
- 실행서는 사전 정의된 하위 집합에서 가져온 Amazon 지식 센터(KC) 문서에 대한 조사 결과, 권장 사항 및 참조를 강조 표시하여 Amazon Athena 쿼리 결과를 반환합니다.
- 완료 또는 실패 시 Amazon S3 버킷에 업로드된 AWS Glue 데이터베이스 및 알려진 문제 파일이 삭제됩니다.

어떻게 작동하나요?

는 Amazon Athena를 사용하여 Amazon EMR 로그를 AWSSupport-DiagnoseEMRLogsWithAthena 분석하여 오류를 감지하고 조사 결과, 권장 사항 및 관련 지식 센터 문서를 강조 표시합니다.

실행서는 다음 단계를 수행합니다.

- 클러스터 ID를 사용하여 Amazon EMR 클러스터 로그 위치를 가져오거나 Amazon S3 위치를 입력하여 로그 위치 및 크기를 검색합니다.
- 로그 위치 크기를 기준으로 Athena 예상 비용을 제공합니다.
- Athena 쿼리를 실행하고 다음 단계를 계속하기 전에 지정된 IAM 보안 주체에게 승인을 요청하여 승인을 받습니다.
- 알려진 문제를 지정된 Amazon S3 버킷에 업로드하고 AWS Glue 데이터베이스와 테이블을 생성합니다.
- Amazon EMR 로그 데이터에 대해 Athena 쿼리를 실행합니다. 쿼리는 날짜 범위, 키워드, 두 기준을 기준으로 검색하거나 제공된 입력을 기반으로 필터 없이 실행할 수 있습니다.
- 결과를 분석하여 조사 결과, 권장 사항 및 관련 KC 문서를 강조 표시합니다.
- Amazon Athena DML 쿼리 결과에 대한 출력 링크입니다.
- 생성된 데이터베이스, 테이블 및 업로드된 알려진 문제를 제거하여 환경을 정리합니다.

문서 유형

자동화

소유자

Amazon

플랫폼

/

AutomationAssumeRole 파라미터를 실행서를 성공적으로 사용하려면 다음 작업이 필요합니다.

- athena:GetQueryExecution
- athena:StartQueryExecution
- athena:GetPreparedStatement
- athena:CreatePreparedStatement
- glue:GetDatabase
- glue:CreateDatabase
- glue>DeleteDatabase
- glue:CreateTable

- glue:GetTable
- glue:DeleteTable
- elasticmapreduce:DescribeCluster
- s3:ListBucket
- s3:GetBucketVersioning
- s3:ListBucketVersions
- s3:GetBucketPublicAccessBlock
- s3:GetBucketPolicyStatus
- s3:GetObject
- s3:GetBucketLocation
- 요금:GetProducts
- 요금:GetAttributeValues
- 요금:DescribeServices
- 요금:ListPriceLists

Important

이 자동화에 필요한 리소스에 대한 액세스를 제한하려면 SSM 서비스를 신뢰하는 IAM 역할에 다음 정책을 연결합니다. 파티션, 리전 및 계정을 실행서가 실행되는 파티션, 리전 및 계정 번호의 적절한 값으로 바꿉니다.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "elasticmapreduce:DescribeCluster",
        "glue:GetDatabase",
        "athena:GetQueryExecution",
        "athena:StartQueryExecution",
        "athena:GetPreparedStatement",

```

```

        "athena:CreatePreparedStatement",
        "s3:ListBucket",
        "s3:GetBucketVersioning",
        "s3:ListBucketVersions",
        "s3:GetBucketPublicAccessBlock",
        "s3:GetBucketPolicyStatus",
        "s3:GetObject",
        "s3:GetBucketLocation",
        "pricing:GetProducts",
        "pricing:GetAttributeValues",
        "pricing:DescribeServices",
        "pricing:ListPriceLists"
    ],
    "Resource": "*"
},
{
    "Sid": "RestrictPutObjects",
    "Effect": "Allow",
    "Action": [
        "s3:PutObject"
    ],
    "Resource": [
        "arn:aws:s3:::*/*/results/*",
        "arn:aws:s3:::*/*/saw_diagnose_emr_known_issues/*"
    ]
},
{
    "Sid": "RestrictDeleteAccess",
    "Effect": "Allow",
    "Action": [
        "s3:DeleteObject",
        "s3:DeleteObjectVersion"
    ],
    "Resource": [
        "arn:aws:s3:::*/*/saw_diagnose_emr_known_issues/*"
    ]
},
{
    "Effect": "Allow",
    "Action": [
        "glue:GetDatabase",
        "glue:CreateDatabase",
        "glue:DeleteDatabase"
    ],

```

```

        "Resource": [
            "arn:aws:glue:us-east-1:111122223333:database/
saw_diagnose_emr_database_*",
            "arn:aws:glue:us-east-1:111122223333:table/
saw_diagnose_emr_database_*/*",
            "arn:aws:glue:us-east-1:111122223333:userDefinedFunction/
saw_diagnose_emr_database_*/*",
            "arn:aws:glue:us-east-1:111122223333:catalog"
        ]
    },
    {
        "Effect": "Allow",
        "Action": [
            "glue:CreateTable",
            "glue:GetTable",
            "glue>DeleteTable"
        ],
        "Resource": [
            "arn:aws:glue:us-east-1:111122223333:table/
saw_diagnose_emr_database_*/saw_diagnose_emr_known_issues",
            "arn:aws:glue:us-east-1:111122223333:table/
saw_diagnose_emr_database_*/saw_diagnose_emr_logs_table",
            "arn:aws:glue:us-east-1:111122223333:table/
saw_diagnose_emr_database_*/j_*",
            "arn:aws:glue:us-east-1:111122223333:database/
saw_diagnose_emr_database_*",
            "arn:aws:glue:us-east-1:111122223333:catalog"
        ]
    }
]
}

```

지침

다음 단계에 따라 자동화를 구성합니다.

1. AWS Systems Manager 문서의에서 [AWSSupport-DiagnoseEMRLogsWithAthena](#)를 탐색합니다.
2. Execute automation(자동화 실행)을 선택합니다.
3. 입력 파라미터의 경우, 다음 내용을 입력합니다.
 - AutomationAssumeRole(선택 사항):

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

- ClusterID(필수):

Amazon EMR 클러스터 ID입니다.

- S3LogLocation(선택 사항):

Amazon S3 Amazon EMR 로그 위치입니다. 경로 스타일 URL Amazon S3 위치를 입력합니다.

예: s3://amzn-s3-demo-bucket/myfolder/j-1K48XXXXXXHCB/. Amazon EMR 클러스터가 30 일 이상 종료된 경우이 파라미터를 제공합니다.

- S3BucketName(필수):

알려진 문제 목록과 Amazon Athena 쿼리 출력을 업로드하는 Amazon 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 보안 주체의 목록입니다. 사용자 이름, 사용자 ARN, IAM 역할 ARN 또는 IAM 수임 역할 ARN 형식 중 하나를 사용하여 보안 주체를 지정할 수 있습니다. 최대 승인자 수 수는 10명입니다.

- FetchNodeLogsOnly(선택 사항):

로 설정하면 자동화true가 Amazon EMR 애플리케이션 컨테이너 로그를 진단합니다. 기본값은 false입니다.

- FetchContainersLogsOnly(선택 사항):

로 설정하면 자동화true가 Amazon EMR 컨테이너 로그를 진단합니다. 기본값은 false입니다.

- EndSearchDate(선택 사항):

로그 검색의 종료 날짜입니다. 제공된 경우 자동화는 지정된 날짜까지 YYYY-MM-DD 형식으로 생성된 로그만 검색합니다(예: 2024-12-30).

- DaysToCheck(선택 사항):

EndSearchDate이 제공된 경우이 파라미터는 지정된에서 로그를 소급해서 검색할 일수를 결정하는 데 필요합니다EndSearchDate. 최대값은 30 일입니다. 기본값은 1입니다.

- SearchKeywords(선택 사항):

로그에서 검색할 키워드 목록으로, 쉼표로 구분됩니다. 키워드에는 작은따옴표나 큰따옴표를 사용할 수 없습니다.

Input parameters

AutomationAssumeRole
(Optional) The Amazon Resource Name (ARN) of the AWS Identity and Access Management (IAM) role that allows Systems Manager Automation to perform the actions on your behalf. If no role is specified, Systems Manager Automation uses the permissions of the user that starts this runbook.

SSMAutomation

ClusterID
(Required) The Amazon EMR cluster ID.

j-1K48XXXXXXHCB

S3LogLocation
(Optional) The Amazon S3 URL that contains the Amazon EMR logs. Provide this parameter if the Amazon EMR cluster has been terminated for more than 30 days. Provide the full Amazon S3 path prefix for the EMR logs. Example `s3://mybucket/myfolder/j-1K48XXXXXXHCB/`.

String

S3BucketName
(Required) The Amazon S3 bucket name to upload a list of known issues, and the output of Amazon Athena queries. The bucket should have `Block Public Access Enabled` (<https://docs.aws.amazon.com/AmazonS3/latest/userguide/access-control-block-public-access.html>) and be in the same AWS region as the Amazon EMR cluster provided.

Approvers
(Required) The list of AWS authenticated principals who are able to either approve or reject the action. The maximum number of approvers is 10. You can specify principals by using any of these formats, 1) An AWS Identity and Access Management (IAM) user name 2) An IAM user ARN 3) An IAM role ARN 4) An IAM assume role user ARN.

arn:aws:iam:::role/Approver

FetchNodeLogsOnly
(Optional) If set to "true", the automation diagnoses the Amazon EMR node logs.

false

FetchContainersLogsOnly
(Optional) When "true", the automation diagnoses the Amazon EMR containers logs related to applications on the cluster.

false

EndSearchDate
(Optional) The end date for log searches. If provided, the automation will exclusively search for logs generated up to the specified date in the format YYYY-MM-DD (for example: "2024-12-30").

String

DaysToCheck
(Optional) When "EndSearchDate" is provided, this parameter is required to determine the number of days to retrospectively search for logs from the specified "EndSearchDate". The maximum value is "30" days.

1

SearchKeywords
(Optional) The list of keywords to search in the logs, separated by commas. The keywords cannot contain single or double quotes.

StringList

4. 실행을 선택합니다.

5. 자동화가 시작됩니다.

6. 문서는 다음 단계를 수행합니다.

- getLogLocation:

지정된 Amazon EMR 클러스터 ID를 쿼리하여 Amazon S3 로그 위치를 검색합니다. 자동화가 Amazon EMR 클러스터 ID에서 로그 위치를 쿼리할 수 없는 경우 실행서는 S3LogLocation 입력 파라미터를 사용합니다.

- branchOnValidLog:

Amazon EMR 로그 위치를 확인합니다. 위치가 유효한 경우 Amazon EMR 로그에서 쿼리를 실행할 때 Amazon Athena 잠재적 비용을 추정합니다.

- estimateAthenaCosts:

Amazon EMR 로그의 크기를 결정하고 로그 데이터 세트에서 Athena 스캔을 실행하기 위한 예상 비용을 제공합니다. 비상업적 리전(비AWS 파티션)의 경우 이 단계에서는 비용을 추정하지 않고 로그 크기만 제공합니다. 비용은 지정된 리전의 Athena 요금 설명서를 사용하여 계산할 수 있습니다.

- approveAutomation:

지정된 IAM 보안 주체의 승인이 자동화의 다음 단계를 진행할 때까지 기다립니다. 승인 알림에는 Amazon EMR 로그에서 Amazon Athena 스캔의 예상 비용과 자동화에서 프로비저닝되는 리소스에 대한 세부 정보가 포함됩니다.

- `uploadKnownIssuesExecuteAthenaQueries`:

S3BucketName 파라미터에 지정된 Amazon S3 버킷에 미리 정의된 알려진 문제를 업로드합니다. AWS Glue 데이터베이스 및 테이블을 생성합니다. 입력 파라미터를 기반으로 AWS Glue 데이터베이스에서 Amazon Athena 쿼리를 실행합니다.

- `getQueryExecutionStatus`:

Amazon Athena 쿼리 실행이 SUCCEEDED 상태가 될 때까지 기다립니다. Amazon Athena DML 쿼리는 Amazon EMR 클러스터 로그에서 오류 및 예외를 검색합니다.

- `analyzeAthenaResults`:

Amazon Athena 결과를 분석하여 사전 정의된 매핑 세트에서 가져온 조사 결과, 권장 사항 및 지식 센터(KC) 문서를 제공합니다.

- `getAnalyzeResultsQuery1ExecutionStatus`:

쿼리 실행이 SUCCEEDED 상태가 될 때까지 기다립니다. Amazon Athena DML 쿼리는 이전 DML 쿼리의 결과를 분석합니다. 이 분석 쿼리는 해결 방법 및 KC 문서와 일치하는 예외를 반환합니다.

- `getAnalyzeResultsQuery2ExecutionStatus`:

쿼리 실행이 SUCCEEDED 상태가 될 때까지 기다립니다. Amazon Athena DML 쿼리는 이전 DML 쿼리의 결과를 분석합니다. 이 분석 쿼리는 각 Amazon S3 로그 경로에서 감지된 예외/오류 목록을 반환합니다.

- `printAthenaQueriesMessage`:

Amazon Athena DML 쿼리 결과에 대한 링크를 인쇄합니다.

- `cleanupResources`:

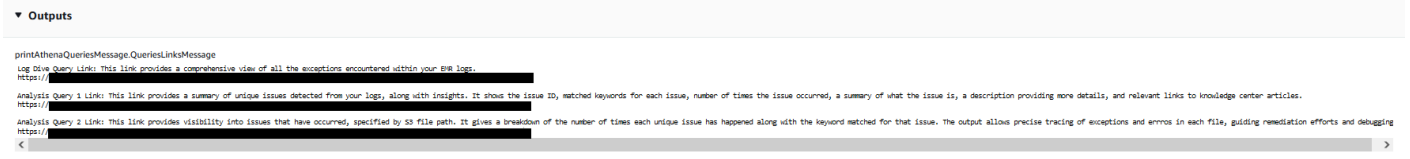
생성된 AWS Glue 데이터베이스를 삭제하고 Amazon EMR 로그 버킷에서 생성된 알려진 문제 파일을 삭제하여 리소스를 정리합니다.

7. 완료되면 출력 섹션에서 실행의 자세한 결과를 검토합니다.

출력은 Athena 쿼리 결과에 대한 세 가지 링크를 제공합니다.

- Amazon EMR 클러스터 로그에서 발견된 모든 오류 및 자주 발생한 예외 목록과 해당 로그 위치 (Amazon S3 접두사).
- 문제 해결에 도움이 되는 권장 해결 방법 및 KC 문서와 함께 Amazon EMR 로그에서 일치하는 고유한 알려진 예외의 요약입니다.

- 추가 진단을 지원하기 위해 Amazon S3 로그 경로에서 특정 오류 및 예외가 나타나는 위치에 대한 세부 정보입니다.



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 참조하세요](#).

Amazon OpenSearch Service

AWS Systems Manager Automation은 Amazon OpenSearch Service에 사전 정의된 실행서를 제공합니다. 실행서에 대한 자세한 내용은 [실행서 작업](#)을 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](#) API를 사용하여 특정 Amazon OpenSearch Service 도메인을 삭제합니다.

[이 자동화 실행\(콘솔\)](#)

문서 유형

자동화

소유자

Amazon

플랫폼

Linux, macOS, Windows

파라미터

- 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) 사용자를 대신하여 Systems Manager Automation을 통해 작업을 수행할 수 있도록 허용하는 AWS Identity and Access Management (IAM) 역할의 Amazon 리소스 이름(ARN)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 입력내용으로 받아 해당 내용을 삭제하고 삭제를 확인합니다.

AWSConfigRemediation-EnforceHTTPSOnOpenSearchDomain

설명

AWSConfigRemediation-EnforceHTTPSOnOpenSearchDomain 실행서는 [UpdateDomainConfig](#) API를 사용하여 특정 Amazon OpenSearch Service 도메인에서 EnforceHTTPS(을)를 활성화합니다.

[이 자동화 실행\(콘솔\)](#)

문서 유형

자동화

소유자

Amazon

플랫폼

Linux, macOS, Windows

파라미터

- `DomainName`

유형: 문자열

유효한 값: `(\d{12})?[a-z]{1}[a-z0-9-]{2,28}`

설명: (필수) HTTPS를 적용하는 데 사용하려는 Amazon OpenSearch Service 도메인의 이름입니다.

- `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.

필수 IAM 권한

실행서를 성공적으로 사용하려면 AutomationAssumeRole 파라미터에 다음 작업이 필요합니다.

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- es:DescribeDomain
- es:UpdateDomainConfig

문서 단계

- aws:executeScript - DomainName 파라미터에서 사용자가 지정하는 Amazon OpenSearch Service 도메인에서 EnforceHTTPS 엔드포인트 옵션을 활성화합니다.

AWSConfigRemediation-UpdateOpenSearchDomainSecurityGroups

설명

AWSConfigRemediation-UpdateOpenSearchDomainSecurityGroups 실행서는 [UpdateDomainConfig](#) API를 사용하여 특정 Amazon OpenSearch Service 도메인의 보안 그룹 구성을 업데이트합니다.

Note

AWS 보안 그룹은 Amazon Virtual Private Cloud(VPC) 액세스를 위해 구성된 Amazon OpenSearch Service 도메인에만 적용할 수 있으며 퍼블릭 액세스를 위해 구성된 Amazon OpenSearch Service 도메인에는 적용할 수 없습니다.

[이 자동화 실행\(콘솔\)](#)

문서 유형

자동화

소유자

Amazon

플랫폼

Linux, macOS, Windows

파라미터

- DomainName

유형: 문자열

설명: (필수) 보안 그룹을 업데이트하기 위해 사용하려는 Amazon OpenSearch Service 도메인의 이름입니다.

- SecurityGroupList

유형: StringList

설명: (필수) Amazon OpenSearch Service 도메인에 할당하려는 보안 그룹 ID입니다.

- 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.

필수 IAM 권한

실행서를 성공적으로 사용하려면 AutomationAssumeRole 파라미터에 다음 작업이 필요합니다.

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- es:DescribeDomain
- es:UpdateDomainConfig

문서 단계

- `aws:executeScript - DomainName` 파라미터에서 사용자가 지정하는 Amazon OpenSearch Service 도메인의 보안 그룹 구성을 업데이트합니다.

AWSSupport-TroubleshootOpenSearchRedYellowCluster

설명

AWSSupport-TroubleshootOpenSearchRedYellowCluster 자동화 실행서는 [빨간색](#) 또는 [노란색](#) 클러스터 상태 원인을 식별하고 클러스터를 다시 녹색으로 변경하는 방법을 안내하는 데 사용됩니다.

어떻게 작동하나요?

실행서는 빨간색 또는 노란색 클러스터의 원인을 해결하는 데 AWSSupport-TroubleshootOpenSearchRedYellowCluster 도움이 되며 클러스터 구성 및 리소스 사용률을 분석하여이 문제를 해결하기 위한 다음 단계를 제공합니다.

실행서는 다음 단계를 수행합니다.

- 대상 도메인에 대해 [DescribeDomain](#) API를 호출하여 클러스터 구성을 가져옵니다.
- OpenSearch Service 도메인이 인터넷 기반(퍼블릭)인지 아니면 [Amazon Virtual Private Cloud\(VPC\) 기반](#)인지 확인합니다.
- 클러스터 구성에 따라 퍼블릭 또는 [Amazon VPC 기반](#) AWS Lambda 함수를 생성합니다. 참고: Lambda 함수에는 클러스터에 대해 OpenSearch Service APIs를 실행하여 클러스터가 빨간색 또는 노란색 상태인 이유를 확인하는 문제 해결 코드가 포함되어 있습니다.
- Lambda 함수를 삭제합니다.
- 수행된 점검과 빨간색 또는 노란색 클러스터 문제를 해결하기 위한 다음 권장 단계를 표시합니다.

문서 유형

자동화

소유자

Amazon

플랫폼

Linux, macOS, Windows

파라미터

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:

다음은이 실행서에 필요한 AWS 서비스 및 리소스에 액세스할 수 있는 권한을 함수에 부여하는 Lambda 함수의 실행 역할(AWS Identity and Access Management (IAM) 역할)의 예입니다. 자세한 내용을 알아보려면 [Lambda 실행 역할](#)을 참조하세요.

Note

ec2:DescribeNetworkInterfaces, ec2>CreateNetworkInterface 및 ec2>DeleteNetworkInterface는 Lambda 함수가 Amazon VPC 네트워크 인터페이스를 생성하고 관리할 수 있도록 OpenSearch Service 클러스터가 Amazon VPC 기반인 경우에만 필요합니다. <https://docs.aws.amazon.com/opensearch-service/latest/developerguide/vpc.html> 자세한 내용은 [Amazon VPC 및 Lambda 실행 역할의 리소스에 아웃바운드 네트워킹 연결을 참조하세요](#). <https://docs.aws.amazon.com/lambda/latest/dg/lambda-intro-execution-role.html>

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "es:ESHttpGet",
      "Resource": [
        "arn:aws:es:us-east-1:111122223333:domain/domain-name/",
        "arn:aws:es:us-east-1:111122223333:domain/domain-name/_cluster/health",
        "arn:aws:es:us-east-1:111122223333:domain/domain-name/_cat/indices",
        "arn:aws:es:us-east-1:111122223333:domain/domain-name/_cat/allocation",
        "arn:aws:es:us-east-1:111122223333:domain/domain-name/_cluster/allocation/explain"
      ]
    }
  ]
}
```



```

    },
    {
      "Condition": {
        "ArnLikeIfExists": {
          "ec2:Vpc": "arn:aws:ec2:us-east-1:111122223333:vpc/vpc_id"
        }
      },
      "Action": [
        "ec2:DeleteNetworkInterface",
        "ec2:CreateNetworkInterface",
        "ec2:DescribeNetworkInterfaces",
        "ec2:UnassignPrivateIpAddresses",
        "ec2:AssignPrivateIpAddresses"
      ],
      "Resource": "*",
      "Effect": "Allow"
    }
  ]
}

```

지침

다음 단계에 따라 자동화를 구성합니다.

1. 콘솔에서 [AWSSupport-TroubleshootOpenSearchRedYellowCluster](#)로 AWS Systems Manager 이 통합합니다.
2. Execute automation(자동화 실행)을 선택합니다.
3. 입력 파라미터의 경우, 다음 내용을 입력합니다.
 - AutomationAssumeRole(선택 사항):

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

- LambdaExecutionRole(필수):

Lambda가 Amazon OpenSearch Service 클러스터에 대한 요청에 서명하는 데 사용할 IAM 역할의 ARN입니다.

- DomainName(필수):

빨간색 또는 노란색 클러스터 상태인 OpenSearch Service 도메인의 이름입니다.

- UtilizationThreshold(선택 사항):

CPUUtilization과 JVMMemoryPressure 지표를 비교하는 데 사용되는 사용률 임계값 백분율입니다. 기본값은 80입니다.

Input parameters

AutomationAssumeRole
(Optional) The Amazon Resource Name (ARN) of the AWS Identity and Access Management (IAM) role that allows Systems Manager Automation to perform the actions on your behalf. If no role is specified, Systems Manager Automation uses the permissions of the user that starts this runbook.

Select an existing IAM Role

AutomationAssumeRole
arn:aws:iam::[redacted]:role/AutomationAssumeRole

DomainName
(Required) The name of the Amazon OpenSearch Service domain is red or yellow status.

opensearch-red-yellow-sample

LambdaExecutionRole
(Required) The ARN of the IAM role that the AWS Lambda will use to sign requests to your Amazon OpenSearch Service cluster.

Select an existing IAM Role

LambdaExecutionRole
arn:aws:iam::[redacted]:role/LambdaExecutionRole

UtilizationThreshold
(Optional) The utilization threshold in percentage used to compare the 'CPUUtilization' and 'JVMMemoryPressure' metrics. Default value is '80'.

80

4. OpenSearch Service 클러스터에서 세분화된 액세스 제어를 활성화한 경우

LambdaExecutionRole 역할 ARN이 최소 cluster_monitor 권한이 있는 역할에 매핑되었는지 확인합니다.

Permissions Mapped users

Cluster permissions (1)
Cluster permissions specify how users in this role can access the cluster. You can specify permissions using both action groups or single permissions. An action group is a list of single permissions. [Learn more](#)

> cluster_monitor

Backend roles
Use a backend role to directly map to roles through an external authentication system. [Learn more](#)

Backend roles

arn:aws:iam::123456789012:role/LambdaExecutionRole Remove

Add another backend role

Cancel Map

5. 실행을 선택합니다.

6. 자동화가 시작됩니다.

7. 자동화 실행서는 다음 단계를 수행합니다.

- GetClusterConfiguration:

OpenSearch Service 클러스터 구성을 가져옵니다.

- CreateAWSLambdaFunctionStack:

를 사용하여 계정에 임시 Lambda 함수를 생성합니다 CloudFormation. Lambda 함수는 OpenSearch Service APIs를 실행하는 데 사용됩니다.

- WaitForAWSLambdaFunctionStack:

CloudFormation 스택이 완료될 때까지 기다립니다.

- GetClusterMetricsFromCloudWatch:

Amazon CloudWatch ClusterStatus, CPUUtilization 및 JVMMemoryPressure OpenSearch Service 클러스터 관련 지표와 생성 날짜를 가져옵니다.

- RunOpenSearchAPIs:

Lambda 함수를 사용하여 OpenSearch Service APIs 호출하고 클러스터 지표 데이터를 분석하여 빨간색 또는 노란색 클러스터 상태의 원인을 진단합니다.

- DeleteAWSLambdaFunctionStack:

계정에서이 자동화로 생성된 Lambda 함수를 삭제합니다.

8. 완료 후에는 Outputs 섹션에서 실행의 세부 결과를 검토합니다.

- RootCause:

클러스터 상태가 빨간색 또는 노란색 상태인 식별된 원인에 대한 개요를 제공합니다.

- IssueDescription:

클러스터가 빨간색 또는 노란색 상태인 이유에 대한 세부 정보와 클러스터를 녹색 상태로 되돌리는 단계를 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 Service 문제 해결을 참조하세요](#).

AWSSupport-TroubleshootOpenSearchHighCPU

설명

AWSSupport-TroubleshootOpenSearchHighCPU 실행서는 Amazon OpenSearch Service 도메인에서 진단 데이터를 수집하여 [높은 CPU](#) 문제를 해결하는 자동화된 솔루션을 제공합니다.

어떻게 작동하나요?

AWSSupport-TroubleshootOpenSearchHighCPU 실행서는 Amazon OpenSearch Service 도메인에서 높은 CPU 사용률 문제를 해결하는 데 도움이 됩니다.

실행서는 다음 단계를 수행합니다.

- 제공된 Amazon OpenSearch Service 도메인에 대해 [DescribeDomain](#) API를 실행하여 클러스터 메타데이터를 가져옵니다.
- Amazon OpenSearch Service 도메인이 퍼블릭인지 또는 Amazon VPC 기반인지 확인하고의 도움을 받아 퍼블릭 또는 [Amazon VPC 기반](#) AWS Lambda 함수를 CloudFormation 생성합니다.
- Lambda 함수는 Amazon OpenSearch Service 도메인에서 진단 데이터를 가져옵니다.
- AWS Step Functions 상태 시스템을 사용하여 여러 Lambda 함수 실행을 오케스트레이션하여 보다 포괄적인 데이터를 수집합니다.
- 수집된 데이터를 기본적으로 24시간 동안 Amazon CloudWatch 로그 그룹에 저장합니다.
- CloudWatch 로그 그룹을 제외하고 생성된 리소스를 삭제합니다.

문서 유형

자동화

소유자

Amazon

플랫폼

Linux, macOS, Windows

파라미터

필수 IAM 권한

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

Note

iam:CreateRole, iam:DeleteRole, iam:PutRolePolicy, 및 iam:GetRole iam:PutRolePolicy iam>DeleteRolePolicy는 LambdaInvocationRoleForStepFunctions 파라미터에 기존 IAM 역할을 사용하지 않는 경우에만 필요합니다.

런북을 성공적으로 사용하려면 LambdaExecutionRole 파라미터에 다음 작업이 필요합니다.

- es:ESHttpGet
- ec2:CreateNetworkInterface
- ec2:DescribeNetworkInterfaces
- ec2>DeleteNetworkInterface
- logs:CreateLogStream
- logs:PutLogEvents

Lambda 실행 역할은 함수에이 실행서에 필요한 AWS 서비스 및 리소스에 액세스할 수 있는 권한을 부여합니다. 자세한 내용을 알아보려면 [Lambda 실행 역할](#)을 참조하세요.

Note

ec2:DescribeNetworkInterfaces, ec2:CreateNetworkInterface 및 ec2>DeleteNetworkInterface는 Lambda 함수가 Amazon VPC 네트워크 인터페이스를 생성하고 관리할 수 있도록 OpenSearch Service 클러스터가 Amazon VPC 기반인 경우에만 필요합니다. <https://docs.aws.amazon.com/opensearch-service/latest/developerguide/vpc.html> 자세한 내용은 [Amazon VPC 및 Lambda 실행 역할의 리소스에 아웃바운드 네트워킹](#)

연결을 참조하세요. <https://docs.aws.amazon.com//lambda/latest/dg/lambda-intro-execution-role.html>

LambdaInvocationRoleForStepFunctions 파라미터는 상태 시스템이 Lambda 함수를 호출할 수 있는 권한을 AWS Step Functions 부여합니다. 다음은 OpenSearch Service 도메인에서 진단 데이터를 가져오는 Lambda 함수를 호출할 수 있는 권한을 Step Functions에 부여하는 IAM 정책의 예입니다. 자세한 내용은 AWS Step Functions 개발자 안내서의 [상태 시스템 IAM 역할 생성을 참조하세요](#).

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": "lambda:InvokeFunction",
      "Resource": [
        "arn:aws:lambda:us-east-1:111122223333:function:AWSSupport-
HighCPU-*"
      ]
    }
  ]
}
```

지침

다음 단계에 따라 자동화를 구성합니다.

1. 콘솔에서 [AWSSupport-TroubleshootOpenSearchHighCPU](#)로 AWS Systems Manager 이동합니다.
2. Execute automation(자동화 실행)을 선택합니다.
3. 입력 파라미터의 경우, 다음 내용을 입력합니다.
 - AutomationAssumeRole(선택 사항):

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

- **DomainName(필수):**

높은 CPU 문제를 해결할 Amazon OpenSearch Service 도메인의 이름입니다.

- **LambdaExecutionRoleForOpenSearch(필수):**

Lambda 함수에 연결할 IAM 역할의 ARN입니다. Lambda 함수는 이 역할의 자격 증명을 사용하여 Amazon OpenSearch Service 도메인에 대한 요청에 서명합니다. Amazon OpenSearch Service 도메인에서 세분화된 액세스 제어가 활성화된 경우 최소 "cluster_monitor" 권한으로 이 역할을 OpenSearch Service Dashboards 백엔드 역할에 매핑해야 합니다.

- **LambdaInvocationRoleForStepFunctions(선택 사항):**

(선택 사항) Step Functions 워크플로에 연결할 IAM 역할의 ARN입니다. 상태 시스템은 이 역할의 자격 증명을 사용하여 OpenSearch Service 도메인에서 진단 데이터를 가져오는 Lambda 함수를 호출합니다. 역할이 지정되지 않은 경우 이 자동화는 계정에서 Step Functions에 대한 IAM 역할을 생성합니다.

- **DataRetentionDays(선택 사항):**

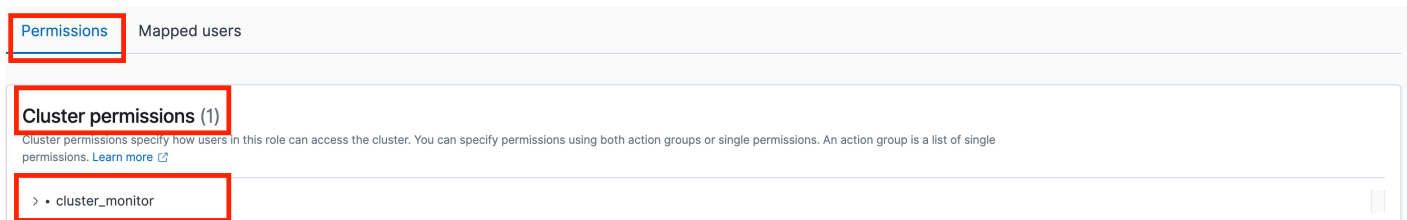
Amazon OpenSearch Service 도메인에서 수집된 진단 데이터를 보존할 일수입니다. 기본적으로 데이터는 24시간(1일) 동안 보존됩니다. 최대 30일 동안 데이터를 보존하도록 선택할 수 있습니다.

- **NumberOfDataSamples(선택 사항):**

Amazon OpenSearch Service 도메인에서 수집할 데이터 샘플 수입니다. 기본적으로 5개의 데이터 샘플이 수집됩니다. 최대 10개의 샘플을 수집할 수 있으며 각 샘플 수집에 대해 Lambda 함수가 호출됩니다.

4. OpenSearch Service 클러스터에서 세분화된 액세스 제어를 활성화한 경우

LambdaExecutionRole 역할 ARN이 최소 cluster_monitor 권한이 있는 역할에 매핑되었는지 확인합니다.



Backend roles
Use a backend role to directly map to roles through an external authentication system. [Learn more](#)

Backend roles

arn:aws:iam::[redacted]:role/LambdaExecutionRole Remove

Add another backend role

Cancel Map

5. 실행을 선택합니다.

6. 자동화가 시작됩니다.

7. 자동화 실행서는 다음 단계를 수행합니다.

- checkConcurrency:

지정된 Amazon OpenSearch Service 도메인을 대상으로 하는 이 실행서의 실행이 하나만 있는지 확인합니다. 실행서가 동일한 도메인 이름을 대상으로 하는 다른 실행을 찾으면 오류가 반환되고 종료됩니다.

- getDomainConfig:

대상 OpenSearch Service 도메인의 구성 세부 정보를 가져옵니다.

- provisionResources:

를 사용하여 데이터 수집을 위한 리소스를 프로비저닝합니다 CloudFormation.

- waitForStackCreation:

CloudFormation 스택이 완료될 때까지 기다립니다.

- describeStackResources:

CloudFormation 스택을 설명하고 상태 시스템의 ARN을 가져옵니다.

- runStateMachine:

Step Functions 상태 시스템을 실행하여 데이터 수집기 Lambda 함수를 한 번 이상 호출합니다.

- describeErrorsFromStackEvents:

CloudFormation 스택의 오류에 대해 설명합니다.

- unstageOpenSearchHighCPUAutomation:

AWSsupport-TroubleshootOpenSearchHighCPU CloudFormation 스택을 삭제합니다.

CloudFormation 스택을 삭제하는 동안 발생한 오류를 설명합니다.

- `finalStatus`:

AWSSupport-TroubleshootOpenSearchHighCPU 실행서의 최종 출력을 반환합니다.

8. 완료 후에는 Outputs 섹션에서 실행의 세부 결과를 검토합니다.

- `finalStatus.FinalOutput`:

진단 데이터가 저장되는 CloudWatch 로그 그룹을 제공합니다.

▼ Outputs
<code>finalStatus.FinalOutput</code> Hot thread data collection completed. Please check the custom CloudWatch log group <code>/aws/lambda/AWSSupport-HighCPU-df52ba5d-8773-4038-a908-b67ecd9c9d11</code> for more information.

참조

Systems Manager Automation

- [이 자동화 실행\(콘솔\)](#)
- [자동화 실행](#)
- [Automation 설정](#)
- [Support Automation Workflows 랜딩 페이지](#)

AWS 서비스 설명서

- 자세한 내용은 [Amazon OpenSearch Service 문제 해결을 참조하세요](#).

EventBridge

AWS Systems Manager Automation은 Amazon EventBridge에 대한 사전 정의된 실행서를 제공합니다. 실행서에 대한 자세한 내용은 [실행서 작업](#)을 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 연결된 모든 AWS Systems Manager OpsItems에 대한 중복 제거 문자열을 추가합니다. 규칙에 이미 적용된 경우, 이 실행서는 중복 제거 문자열을 추가하지 않습니다. 중복 제거 문자열 및 OpsItem에 대해 자세히 알아보려면, AWS Systems Manager 사용 설명서의 [중복 OpsItems 감소](#)를 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.

- 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 지정하는 EventBridge 규칙에 중복 제거 문자열을 추가합니다.

AWS-DisableEventBridgeRule

설명

AWS-DisableEventBridgeRule 실행서는 지정하는 Amazon EventBridge 규칙을 비활성화합니다. EventBridge 규칙에 대해 자세히 알아보려면, Amazon EventBridge 사용 설명서의 [Amazon EventBridge 규칙](#)을 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.

- 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 파라미터에서 지정하는 EventBridge 규칙을 비활성화합니다.

AWS Glue

AWS Systems Manager 자동화에는 대한 사전 정의된 실행서를 제공합니다 AWS Glue. 실행서에 대한 자세한 내용은 [실행서 작업](#)을 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(RDS) 클러스터/인스턴스, Amazon Redshift 클러스터 또는 JDBC를 통해 액세스할 수 있는 기타 대상일 수 있습니다. 처음 두 경우에서 Reachability Analyzer 도구를 사용하여 소스(AWS Glue)와 대상(Amazon RDS 또는 Amazon Redshift) 간의 연결이 부여되는지 확인합니다.

연결 대상이 Amazon RDS 또는 Amazon Redshift가 아닌 경우에도 연결과 동일한 서브넷(네트워크 존재 지점)에 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 인터페이스](#)가 생성됩니다. 이 자동화를 실행하기 전에 해당 서브넷에 충분한 무료 IPs가 있고 한 IP의 소비가 워크로드에 영향을 미치지 않는지 확인하세요.

Important

이 자동화로 생성된 모든 리소스에는 태그를 지정하여 쉽게 찾을 수 있습니다. 사용되는 태그는 다음과 같습니다.

- AWSSupport-TroubleshootGlueConnection: true
- AutomationExecutionId: *Amazon EC2 Systems Manager ## ID*

어떻게 작동하나요?

실행서는 다음 단계를 수행합니다.

- AWS Glue 연결 확인을 위한 소스 정보(서브넷 및 보안 그룹)를 가져오는 연결을 설명합니다.

- JDBC URL에서 참조되는 데이터 소스 또는 존재하는 경우 DatasourceSecurityGroups 및 DatasourceSubnets 파라미터에서 대상 정보(서브넷 및 보안 그룹)를 가져옵니다.
- JDBC URL에 있는 데이터 소스가 Amazon RDS 인스턴스 또는 클러스터이거나 Amazon Redshift 클러스터인 경우 이 자동화는 이전 단계에서 수집된 소스 및 대상 정보를 모두 사용하여 ENIs를 생성하고 Reachability Analyzer를 사용하여 이들 간의 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 수행되도록에는 [AmazonVPCReachabilityAnalyzerFullAccessPolicy](#)가 [연결된 관리형 정책](#)으로 AutomationAssumeRole 있어야 합니다.

다음은에 부여할 수 있는 정책의 예입니다AutomationAssumeRole.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [ {
    "Sid": "TaggedAWSResourcesPermissions",
    "Effect": "Allow",
    "Condition": {
      "StringEquals": {
        "aws:ResourceTag/AWSSupport-TroubleshootGlueConnection":
"true"
      }
    },
    "Action": [
      "iam:AttachRolePolicy",
      "iam:CreateRole",
      "iam>DeleteRole",
      "iam>DeleteRolePolicy",
      "iam:DetachRolePolicy",
      "iam:TagRole",
      "lambda:CreateFunction",
      "lambda>DeleteFunction",
      "lambda:TagResource",

```

```

        "logs:DeleteLogGroup",
        "logs>CreateLogGroup",
        "logs:PutRetentionPolicy",
        "logs:TagResource",
        "cloudformation>CreateStack",
        "cloudformation>DeleteStack"
    ],
    "Resource": "*"
},
{
    "Sid": "TaggedEC2ResourcesPermissions",
    "Effect": "Allow",
    "Condition": {
        "StringEquals": {
            "ec2:ResourceTag/AWSSupport-TroubleshootGlueConnection":
"true"
        }
    },
    "Action": [
        "ec2:DeleteNetworkInterface"
    ],
    "Resource": "*"
},
{
    "Sid": "PutRolePolicy",
    "Effect": "Allow",
    "Condition": {
        "StringEquals": {
            "iam:ResourceTag/AWSSupport-TroubleshootGlueConnection":
"true"
        }
    },
    "Action": [
        "iam:PutRolePolicy",
        "iam>DeleteRolePolicy"
    ],
    "Resource": "*"
},
{
    "Sid": "InvokeFunction",
    "Effect": "Allow",
    "Action": [
        "lambda:InvokeFunction"
    ],

```

```

        "Resource": "arn:*:lambda:*:*:function:point-of-presence-*"
    },
    {
        "Sid": "UnTaggedActions",
        "Effect": "Allow",
        "Action": [
            "ec2:CreateNetworkInsightsPath",
            "ec2:DeleteNetworkInsightsAnalysis",
            "ec2:DeleteNetworkInsightsPath",
            "ec2:CreateNetworkInterface",
            "ec2:CreateTags",
            "ec2:StartNetworkInsightsAnalysis",
            "glue:GetConnection",
            "glue:GetDataCatalogEncryptionSettings",
            "cloudformation:DescribeStacks",
            "cloudformation:DescribeStackEvents",
            "ec2:DescribeDhcpOptions",
            "ec2:DescribeNetworkInsightsPaths",
            "ec2:DescribeNetworkInsightsAnalyses",
            "ec2:DescribeSecurityGroupRules",
            "ec2:DescribeSecurityGroups",
            "ec2:DescribeSubnets",
            "ec2:DescribeVpcs",
            "ec2:DescribeVpcAttribute",
            "iam:GetRole",
            "iam:ListAttachedRolePolicies",
            "iam:SimulatePrincipalPolicy",
            "kms:DescribeKey",
            "lambda:GetFunction",
            "s3:GetEncryptionConfiguration"
        ],
        "Resource": "*"
    },
    {
        "Effect": "Allow",
        "Action": [
            "iam:PassRole"
        ],
        "Resource": "arn:*:iam:*:role/point-of-presence-*",
        "Condition": {
            "StringLikeIfExists": {
                "iam:PassedToService": "lambda.amazonaws.com"
            }
        }
    }
}

```

```

    }
  ]
}
```

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 사용자를 대신하여 작업을 수행하도록 허용하는 (IAM) 역할의 Amazon 리소스 이름 AWS AWS Identity and Access Management (ARN)입니다. 역할이 지정되지 않은 경우 Systems Manager Automation은 이 실행서를 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 알리는 플래그입니다. 기본값: false.

- PointOfPresenceLogRetentionPeriod(선택 사항)

현재 위치 Lambda에 대한 로그가 저장되는 일수입니다. 기본값: 7.

- DatasourceSubnets(선택 사항)

원래 데이터 소스를 사용할 수 없는 경우이 파라미터를 사용하여 연결 테스트가 계속 수행되도록 사용한 서브넷을 제공합니다. 와 함께 사용해야 합니다 DatasourceSecurityGroups. 예시: subnet-1, subnet-2.

- DatasourceSecurityGroups(선택 사항)

원래 데이터 소스를 사용할 수 없는 경우이 파라미터를 사용하여 연결 테스트가 계속 수행되도록 사용한 보안 그룹을 제공합니다. 와 함께 사용해야 합니다 `DatasourceSubnets`. 예시: `sg-1, sg-2`.

Input parameters

AutomationAssumeRole
(Optional) The Amazon Resource Name (ARN) of the AWS Identity and Access Management (IAM) role that allows Systems Manager Automation to perform the actions on your behalf. If no role is specified, Systems Manager Automation uses the permissions of the user that starts this runbook.

TestConnectionRole
(Required) The Amazon Resource Name (ARN) of the AWS Identity and Access Management (IAM) role that is used during the connection test.

PointOfPresenceLogRetentionPeriod
(Optional) The amount of days the logs for the point of presence AWS Lambda will be stored for. Default: 7.

DatasourceSecurityGroups
(Optional) If the original datasource is not available, use this parameter to provide the security groups it used so that the connectivity tests are still performed. ****Must**** be used with `DatasourceSubnets`. Example: `sg-1,sg-2`.

ConnectionString
(Required) The name of the AWS Glue Connection you want to troubleshoot the failed test connection attempt.

PersistReachabilityAnalyzerResults
(Optional) The flag informing if the results of the VPC Reachability Analyzer execution should be kept or not. Default: false.

DatasourceSubnets
(Optional) If the original datasource is not available, use this parameter to provide the subnets that it used so that the connectivity tests are still performed. ****Must**** be used with `DatasourceSecurityGroups`. Example: `subnet-1,subnet-2`.

4. 실행을 선택합니다.

5. 자동화가 시작됩니다.

6. 자동화 실행서는 다음 단계를 수행합니다.

- ParseInputs:

이 단계에서는 입력 조합을 검증합니다. `DatasourceSecurityGroups` 및 `DatasourceSubnets`가 모두 제공되면 유효하며 그대로 반환됩니다. 아무 것도 제공되지 않으면 두 개의 빈 목록이 반환됩니다. 이 중 하나만 제공되면 단계에서가 발생합니 다 `ValueException`.

- GetConnectionDetails:

이 단계에서는 제공된 AWS Glue 연결의 세부 정보를 반환합니다.

- ParseSecurityGroupList:

이 단계는 이 자동화 `SecurityGroupIdList`에서 나중에 사용할 String 수 있도록 의를 연결하는 데 사용됩니다.

- GetConnectionData:

JDBC URL을 기반으로 , RedShift RdsInstance RdsCluster 및 간의 연결 유형을 결정합니다. 또한는 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.

- CreateENITemplate:

연결을 테스트하는 데 사용되는 네트워크 인터페이스를 생성하는 데 사용되는 AWS CloudFormation 템플릿을 생성합니다. Reachability Analyzer 도구를 실행하는 데 필요합니다.

- CreateENIStack:

이전 단계에서 생성한 템플릿에서 CloudFormation 스택을 생성합니다.

- GetStackDetails:

이전 CloudFormation 스택에서 생성된 스택을 설명하고 SourceNetworkInterface TargetNetworkInterfaces 정보를 검색합니다.

- RunSourceToTargetCheck:

Reachability Analyzer 도구를 사용하여 이전 단계에서 생성된 소스 및 대상 ENIs 간에 검사를 실행합니다.

- DeleteENIStack:

네트워크 인터페이스를 생성하는 CloudFormation 스택을 삭제합니다.

- CreateNetworkPointOfPresence:

CloudFormation 는 네트워크 존재 지점으로 사용되는 Lambda 함수를 생성합니다.

- GetFunctionName:

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 연결할 수 있는지 확인합니다.

- CheckS3Connectivity:

Amazon S3 서비스에 대한 AWS Glue 연결에서 네트워크 연결을 확인합니다.

- DeletePointOfPresence:

네트워크 존재 지점 Lambda를 생성하는 CloudFormation 스택을 삭제합니다.

- TestIAMRolePermissions:

테스트에 사용되는 IAM 역할에 이를 실행하는 데 필요한 권한이 있는지 확인합니다.

- CheckConnectionSecurityGroupReferencingRule:

AWS Glue 연결에 사용되는 보안 그룹이 자체로부터의 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 단원에서는 테스트 연결 작업이 실패할 수 있는 원인(조사 결과)과 이를 해결하는 방법(다음 단계)을 설명하는 시나리오를 살펴봅니다. 자동화가 테스트 실패의 원인을 찾을 수 없는 경우 이 단원에서도 이를 알립니다.

- 성공적인 테스트

이 섹션에서는 이 자동화에서 성공적으로 테스트한 내용을 알려주는 시나리오를 확인할 수 있습니다. 성공한 테스트는 테스트 연결 실패의 원인을 식별할 수 없는 경우 문제의 원인을 알려 조사 범위를 줄일 수 있으므로 유용합니다.

- 자동화 오류

이 섹션에서는 자동화가 수행할 수 있는 테스트 수를 제한했을 수 있는 자동화 중에 발생한 문제를 설명하는 시나리오를 살펴봅니다. 시나리오에 대한 설명은 실패한 단계를 알려줍니다.

```

TroubleshootGlueConnection
-----
Automation Results
Below are possible causes for the issue being troubleshoot and their fixes.
-----

# Scenario: AWS Glue connection's VPC using Amazon Provided DNS
🔍 Findings:
- The JDBC URL's endpoint dummy-instance.c3c3tj8ogvmj.us-east-1.rds.amazonaws.com could not be resolved from the AWS Glue connection's subnet subnet-
- Glue connection's VPC (vpc- ) is using AWS DNS Resolver but no issue could be found.
➔ Next steps:
- Please check the following links for further DNS troubleshooting:
- https://repost.aws/knowledge-center/vpc-find-cause-of-failed-dns-queries.
- https://repost.aws/knowledge-center/vpc-peering-troubleshoot-dns-resolution
- https://docs.aws.amazon.com/vpc/latest/userguide/vpc-dns.html#vpc-dns-support

# Scenario: Checking AWS Glue connection IAM role trust relationship
🔍 Findings:
- The IAM role arn:aws:iam:: :role/SAW-Core-Test-AWSSupport-Trou-IncorrectGlueTestRole-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:: :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:: :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:: :role/SAW-Core-Test-AWSSupport-Trou-IncorrectGlueTestRole-lLu7FYAp9bfi.

-----
✓ Successful Tests
Below are the successful tests performed by the automation, for further troubleshooting.
-----

# Scenario: Datasource security group
✓ The target's security group(s) allow(s) inbound connections from the Glue connection.

# Scenario: Checking connection security group self referencing rule
✓ The AWS Glue connection has a self referencing inbound rule allowing all traffic.

```

참조

Systems Manager Automation

- [이 자동화 실행\(콘솔\)](#)
- [자동화 실행](#)
- [Automation 설정](#)
- [Support Automation Workflows 랜딩 페이지](#)

Amazon FSx

AWS Systems Manager Automation은 Amazon FSx용 사전 정의된 실행서를 제공합니다. 실행서에 대한 자세한 내용은 [실행서 작업](#)을 참조하세요. 실행서 콘텐츠를 보는 방법에 대한 자세한 내용은 [실행서 콘텐츠 보기](#)(을)를 참조하세요.

주제

- [AWSsupport-ValidateFSxWindowsADConfig](#)

AWSSupport-ValidateFSxWindowsADConfig

설명

AWSSupport-ValidateFSxWindowsADConfig 실행서는 Amazon FSx for Windows File Server의 자체 관리형 Active Directory(AD) 구성을 검증하는 데 사용됩니다.

어떻게 작동하나요?

실행서는 Amazon FSx 서브넷의 실행서에서 시작한 임시 Amazon Elastic Compute Cloud(Amazon EC2) Windows 인스턴스에서 Amazon FSx 검증 스크립트를 AWSSupport-ValidateFSxWindowsADConfig 실행합니다. 스크립트는 여러 검사를 수행하여 자체 관리형 AD/DNS 서버에 대한 네트워크 연결과 Amazon FSx 서비스 계정의 권한을 검증합니다. 실행서는 실패하거나 잘못 구성된 Amazon FSx for Windows File Server를 검증하거나 자체 관리형 AD를 사용하여 새 Amazon FSx for Windows File Server를 생성할 수 있습니다.

기본적으로 실행서는 Amazon FSx 서브넷에서 사용하여 Amazon EC2 Windows 인스턴스, (SSM) 액세스를 위한 AWS Systems Manager 보안 그룹, AWS Identity and Access Management (IAM) 역할 및 정책을 생성합니다. CloudFormation FSx 기존 Amazon EC2 인스턴스에서 스크립트를 실행하려면 파라미터에 ID를 입력합니다 InstanceId. 실행에 성공하면 CloudFormation 리소스가 삭제됩니다. 그러나 리소스를 유지하려면 RetainCloudFormationStack 파라미터를 로 설정합니다 true.

CloudFormation 템플릿은 사용자를 대신하여 Amazon EC2 인스턴스에 연결하여 Amazon FSx 검증 스크립트를 실행하는 데 필요한 권한을 가진 IAM 역할을 생성합니다. 임시 인스턴스에 대한 기존 IAM 인스턴스 프로파일을 지정하려면 InstanceProfileName 파라미터를 사용합니다. 연결된 IAM 역할에는 다음 권한이 포함되어야 합니다.

- ec2:DescribeSubnets 및 ec2:DescribeVpcs 권한과 Amazon 관리형 정책 AmazonSSMManagedInstanceCore.
- GetSecretValue API를 호출하여 Systems Manager에서 Amazon FSx 서비스 계정 사용자 이름과 암호를 가져올 수 있는 권한.
- 스크립트 출력을 위해 Amazon Simple Storage Service(Amazon S3) 버킷에 객체를 넣을 수 있는 권한.

사전 조건

SSM Run Command를 사용하여 AmazonFSxADValidation 스크립트를 실행하려면 임시 Amazon EC2 인스턴스가 생성되는 서브넷(또는 InstanceId 파라미터에 제공된 기존 인스턴스)에서 AWS

Systems Manager AWS Secrets Manager, 및 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 보안 암호 생성](#)의 단계에 따라 새 Secrets Manager 보안 암호를 생성합니다. 형식의 키/값 페어를 사용하여 사용자 이름과 암호를 저장해야 합니다{"username":"EXAMPLE-USER", "password":"EXAMPLE-PASSWORD"}. [보안 암호에 대한 액세스 보안에 대한 자세한 내용은의 인증 및 액세스 제어를 AWS Secrets Manager 참조하세요.](#)

도구에 대한 자세한 내용은 [AmazonFSxADValidation](#) README.md 파일의 TROUBLESHOOTING.md 및 파일을 참조하세요.

런북 실행

Amazon FSx ID 또는 AD 파라미터를 사용하여 실행서를 실행합니다. 다음은 실행서 워크플로입니다.

- Amazon FSx ID에서 파라미터를 가져오거나 입력 AD 파라미터를 사용합니다.
- CloudFormation을 사용하여 Amazon FSx 서브넷, SSM 액세스를 위한 보안 그룹, IAM 역할 및 정책 (조건부)에서 임시 검증 Amazon EC2 Windows 인스턴스를 생성합니다. FSx InstanceId 파라미터를 지정하면 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

파라미터

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 수임 역할에 대한 IAM 정책 예시

JSON

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "AllowDescribe",
      "Effect": "Allow",
      "Action": [
        "ec2:DescribeSubnets",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeImages",
        "ec2:DescribeInstances",
        "ec2:DescribeLaunchTemplates",
        "ec2:DescribeLaunchTemplateVersions",
        "ssm:DescribeInstanceInformation",
        "ssm:DescribeAutomationExecutions",
        "ssm:DescribeAutomationStepExecutions",
        "fsx:DescribeFileSystems",
        "ds:DescribeDirectories"
      ],
      "Resource": "*"
    },
    {
      "Sid": "CloudFormation",
      "Effect": "Allow",
      "Action": [
        "cloudformation:DescribeStacks",
        "cloudformation:DescribeStackResources",
        "cloudformation:DescribeStackEvents",
        "cloudformation:CreateStack",
        "cloudformation>DeleteStack"
      ],
      "Resource": "arn*:cloudformation:*:*:stack/
AWSsupport-ValidateFSxWindowsADConfig-*"
    },
    {
      "Sid": "AllowCreateLaunchTemplate",
      "Effect": "Allow",
      "Action": [
        "ec2:CreateLaunchTemplate",
        "ec2:CreateTags"
      ]
    }
  ]
}

```

```

    ],
    "Resource": [
        "arn:aws:ec2:*:*:launch-template/*"
    ]
},
{
    "Sid": "AllowEC2RunInstances",
    "Effect": "Allow",
    "Action": [
        "ec2:RunInstances",
        "ec2:CreateTags"
    ],
    "Resource": [
        "arn:aws:ec2:*:*:image/*",
        "arn:aws:ec2:*:*:snapshot/*",
        "arn:aws:ec2:*:*:subnet/*",
        "arn:aws:ec2:*:*:network-interface/*",
        "arn:aws:ec2:*:*:security-group/*",
        "arn:aws:ec2:*:*:key-pair/*",
        "arn:aws:ec2:*:*:launch-template/*"
    ]
},
{
    "Sid": "AllowEC2RunInstancesWithTags",
    "Effect": "Allow",
    "Action": [
        "ec2:RunInstances",
        "ec2:CreateTags"
    ],
    "Resource": [
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ec2:*:*:volume/*"
    ]
},
{
    "Sid": "EC2SecurityGroup",
    "Effect": "Allow",
    "Action": [
        "ec2:CreateSecurityGroup",
        "ec2:RevokeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:CreateTags"
    ],
    "Resource": [

```

```

        "arn:*:ec2:*:*:security-group/*",
        "arn:*:ec2:*:*:vpc/*"
    ],
},
{
    "Sid": "EC2Remove",
    "Effect": "Allow",
    "Action": [
        "ec2:TerminateInstances",
        "ec2>DeleteLaunchTemplate",
        "ec2>DeleteSecurityGroup"
    ],
    "Resource": [
        "arn:aws:ec2:*:*:instance/*",
        "arn:aws:ec2:*:*:launch-template/*",
        "arn:*:ec2:*:*:security-group/*"
    ]
},
{
    "Sid": "IAMInstanceProfile",
    "Effect": "Allow",
    "Action": [
        "iam:CreateInstanceProfile",
        "iam>DeleteInstanceProfile",
        "iam:GetInstanceProfile",
        "iam:AddRoleToInstanceProfile",
        "iam:RemoveRoleFromInstanceProfile"
    ],
    "Resource": "arn:*:iam:*:*:instance-profile/*"
},
{
    "Sid": "IAM",
    "Effect": "Allow",
    "Action": [
        "iam:CreateRole",
        "iam>DeleteRole",
        "iam:AttachRolePolicy",
        "iam:DetachRolePolicy",
        "iam:getRolePolicy",
        "iam:PutRolePolicy",
        "iam>DeleteRolePolicy",
        "iam:GetRole",
        "iam:TagRole"
    ],
},

```

RunPowerShellScript

```

        "Resource": "arn:*:iam:*:*:role/*"
    },
    {
        "Sid": "SSM",
        "Effect": "Allow",
        "Action": [
            "ssm:StartAutomationExecution",
            "ssm:GetDocument",
            "ssm:GetAutomationExecution",
            "ssm:ListCommandInvocations",
            "ssm:GetParameters",
            "ssm:ListCommands",
            "ssm:GetCommandInvocation"
        ],
        "Resource": "*"
    },
    {
        "Sid": "SSMSendCommand",
        "Effect": "Allow",
        "Action": [
            "ssm:SendCommand"
        ],
        "Resource": "arn:aws:ssm:*:*:document/AWS-

RunPowerShellScript"
    },
    {
        "Sid": "SSMSendCommandOnlyFsxInstance",
        "Effect": "Allow",
        "Action": [
            "ssm:SendCommand"
        ],
        "Resource": [
            "arn:aws:ec2:*:*:instance/*"
        ],
        "Condition": {
            "StringLike": {
                "ssm:resourceTag/CreatedBy": [
                    "AWSSupport-ValidateFSxWindowsADConfig"
                ]
            }
        }
    },
    {
        "Sid": "AllowPassRoleToEC2",

```



```

        "Effect": "Allow",
        "Action": "iam:PassRole",
        "Resource": "arn:*:iam:*:role/AWSSupport-
ValidateFSxWindowsADConfig-*",
        "Condition": {
            "StringEquals": {
                "iam:PassedToService": [
                    "ec2.amazonaws.com"
                ]
            }
        }
    },
    {
        "Effect": "Allow",
        "Action": [
            "s3:GetEncryptionConfiguration",
            "s3:GetBucketPublicAccessBlock",
            "s3:GetAccountPublicAccessBlock",
            "s3:GetBucketPolicyStatus",
            "s3:GetBucketAcl",
            "s3:GetBucketLocation"
        ],
        "Resource": "*"
    }
]
}

```

지침

다음 단계에 따라 자동화를 구성합니다.

1. Systems Manager [AWSSupport-ValidateFSxWindowsADConfig](#)의 문서로 이동합니다.
2. Execute automation(자동화 실행)을 선택합니다.
3. 장애가 발생하거나 잘못 구성된 기존 Amazon FSx를 사용하여 자체 관리형 AD를 검증하려면 다음 파라미터를 입력합니다.
 - AutomationAssumeRole(선택 사항):

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

지 않은 경우 Systems Manager Automation은 이 실행서를 시작하는 사용자의 권한을 사용합니다.

- FSxId(조건부):

Amazon FSx for Windows File Server ID입니다. 이는 장애가 발생하거나 잘못 구성된 기존 Amazon FSx를 검증하는 데 필요합니다.

- SecretArn(필수):

Amazon FSx 서비스 계정 사용자 이름 및 암호가 포함된 Secrets Manager 보안 암호의 ARN입니다. 형식의 키/값 페어를 사용하여 사용자 이름과 암호를 저장해야 합니다{"username": "EXAMPLE-USER", "password": "EXAMPLE-PASSWORD"}. CloudFormation 스택은 이 ARN에 대해 수행할 권한이 있는 검증 인스턴스 GetSecretValue를 생성합니다.

- FSxSecurityGroupId(필수):

Amazon FSx for Windows File Server의 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 확인합니다. 또한 Amazon EC2 Windows 인스턴스에 Amazon S3 버킷에 대한 필수 액세스 권한이 있는지 확인합니다.

Input parameters

InstanceId

(Optional) The ID of an existing AWS Systems Manager managed Windows Server Amazon EC2 instance where you intend to run the validation script. The instance requires the [AWS Tools for PowerShell](https://docs.aws.amazon.com/powershell/) to be installed. ****Caution****: The script will temporarily modify the DNS configuration of the instance, which may result in loss of network connectivity. To avoid disruptions, ****do not use a production instance****. Ensure the selected instance is designated for testing purposes only. Please ensure that access to the contents of the instance's volume is not exposed to parties that do not need to access the logs.

☒ Show interactive instance picker

AWS::EC2::Instance::Id

AutomationAssumeRole

(Optional) The Amazon Resource Name (ARN) of the AWS Identity and Access Management (IAM) role that allows Systems Manager Automation to perform the actions on your behalf. If no role is specified, Systems Manager Automation uses the permissions of the user that starts this runbook.

fsx-test

BucketName

(Required) The Amazon S3 bucket to upload the validation results to. Please make sure the bucket is configured with server-side encryption (SSE), and the bucket policy does not grant unnecessary read/write permissions to parties that do not need to access the logs. Also please make sure EC2 Windows instance has necessary access to the S3 Bucket.

test-for-customer

RetainCloudFormationStack

(Optional) Set it to `true` if you want to retain the AWS CloudFormation Stack created by this runbook.

false

SecretArn

(Required) The ARN of your AWS Secrets Manager secret containing the FSx service account username and password. Make sure that the username and password are stored using a key/value pair in the format {"username": "EXAMPLE-USER", "password": "EXAMPLE-PASSWORD"}.

arn:aws:secretsmanager:us-west-2:123456789012:secret:fsx-test

FSxSecurityGroupId

(Required) The security group ID of the Amazon FSx for Windows File Server.

sg-examplesg1234

FSxId

(Optional) The Amazon FSx for Windows File Server ID. Required for getting the configuration of an existing Amazon FSx for Windows File Server. If this parameter is provided, the other Amazon FSx input parameters are ignored.

fs-abcdef123456789

4. 새 Amazon FSx 생성에 대한 자체 관리형 AD 구성을 검증하려면 다음 파라미터를 입력합니다.

- AutomationAssumeRole(선택 사항):

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

- SecretArn(필수):

Amazon FSx 서비스 계정 사용자 이름 및 암호가 포함된 Secrets Manager 보안 암호의 ARN입니다. 형식의 키/값 페어를 사용하여 사용자 이름과 암호를 저장해야 합니다{"username": "EXAMPLE-USER", "password": "EXAMPLE-PASSWORD"}. CloudFormation 스택은 이 ARN에 대해 수행할 권한이 있는 검증 인스턴스GetSecretValue를 생성합니다.

- FSxSecurityGroupId(필수):

Amazon FSx for Windows File Server의 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 확인합니다. 또한 Amazon EC2 Windows 인스턴스에 Amazon S3 버킷에 대한 필수 액세스 권한이 있는지 확인합니다.

- FSxPreferredSubnetId(조건부):

Amazon FSx for Windows File Server 기본 설정 서브넷입니다.

- DomainName(조건부):

자체 관리형 Microsoft AD 도메인의 정규화된 도메인 이름입니다.

- DnsIpAddresses(조건부):

자체 관리형 AD 도메인에서 최대 2개의 DNS 서버 또는 도메인 컨트롤러 IP 주소 목록입니다. 최대 2개의 IPs 쉼표로 구분하여 입력합니다.

- FSxAdminsGroup(조건부):

Amazon FSx for Windows File Server 위임된 파일 시스템 관리자 그룹입니다. 기본 이름은 Domain Admins입니다.

- FSxOrganizationalUnit(조건부):

파일 시스템에 조인할 조직 단위(OU)입니다. OU의 고유 경로 이름을 제공합니다. 예시:
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 객체에 대한 읽기 및/또는 쓰기 퍼블릭 액세스 권한을 부여할 가능성이 있는지 확인합니다.

- BranchOnInputParameters(aws:branch):

Amazon FSx ID 또는 Amazon FSx 파라미터와 같은 제공된 입력 파라미터를 분기합니다.

- AssertFileSystemTypeIsWindows(aws:assertAwsResourceProperty):

Amazon FSx ID가 제공된 경우는 파일 시스템 유형이 Amazon FSx for Windows File Server인지 확인합니다.

- GetValidationInputs(aws:executeScript):

Amazon EC2 인스턴스를 생성하기 위해 CloudFormation 템플릿에 필요한 자체 관리형 Microsoft AD 구성을 반환합니다.

- `BranchOnInstanceId(aws:branch)`:

제공된 입력에 분기합니다 `InstanceId`. 이 제공되면 검증 스크립트 `InstanceId`는 자동화의 대상 Amazon EC2 인스턴스에서 실행됩니다 `step:RunValidationScript`.

- `CreateEC2InstanceStack(aws:createStack)`:

`AmazonFSxADValidation` 도구가 실행될 CloudFormation 를 사용하여 기본 서브넷에 Amazon EC2 인스턴스를 생성합니다.

- `DescribeStackResources(aws:executeAwsApi)`:

임시 Amazon EC2 인스턴스 ID를 가져오는 CloudFormation 스택에 대해 설명합니다.

- `WaitForEC2InstanceToBeManaged(aws:waitForAwsResourceProperty)`:

SSM Run Command를 사용하여 검증 스크립트를 실행하기 위해 Systems Manager에서 Amazon EC2 인스턴스를 관리할 때까지 기다립니다.

- `GetAmazonFSxADValidationAttachment(aws:executeAwsApi)`:

실행서 첨부 파일에서 `AmazonFSxADValidation` 도구 URL을 가져옵니다.

- `RunValidationScript(aws:runCommand)`:

임시 Amazon EC2 인스턴스에서 `AmazonFSxADValidation` 도구를 실행하고 `BucketName` 파라미터에 지정된 Amazon S3 버킷에 결과를 저장합니다.

- `DescribeErrorsFromStackEvents(aws:executeScript)`:

실행서가 스택을 생성하지 못하는 경우 CloudFormation 스택 이벤트를 설명합니다.

- `BranchOnRetainCloudFormationStack(aws:branch)`:

`RetainCloudFormationStack` 및 `InstanceId` 파라미터를 분기하여 CloudFormation 스택을 삭제해야 하는지 여부를 결정합니다.

- `DeleteCloudFormationStack(aws:deleteStack)`:

CloudFormation 스택을 삭제합니다.

8. 완료되면 출력 섹션에서 실행 결과를 검토합니다.

▼ Outputs

```
DescribeInstanceAndSubnet.InstanceId
i-06: [REDACTED]

CreateEC2InstanceStack.CloudFormationStackId
arn:aws:cloudformation:us-east-1:[REDACTED]:stack/AWSSupport-ValidateFSxWindowsADConfig-3428bd96-f8ca-4c8d-9b02-57d81560bac8/67c23cc0-3585-11ef-868f-0efb7b77b54b

RunValidationScript.Output
AmazonFSxADValidation tool downloaded and extracted successfully.
RSAT-AD-PowerShell installed successfully.

Running Test-FSxADConfiguration with parameters:
DomainDNSRoot: self.msfc.com
DnsIpAddresses: 10.10.1.191
SubnetIds: subnet-[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.
```

실행서는 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

- [What is Amazon FSx for Windows File Server?](#)
- [Amazon FSx for Windows File Server에 대한 자체 관리형 AD 구성 검증](#)

GuardDuty

AWS Systems Manager 자동화는 Amazon GuardDuty에 대한 사전 정의된 실행서를 제공합니다. 실행서에 대한 자세한 내용은 [실행서 작업](#)을 참조하세요. 실행서 콘텐츠를 보는 방법에 대한 자세한 내용은 [실행서 콘텐츠 보기\(을\)](#)를 참조하세요.

주제

- [AWSConfigRemediation-CreateGuardDutyDetector](#)

AWSConfigRemediation-CreateGuardDutyDetector

설명

AWSConfigRemediation-CreateGuardDutyDetector 실행서는 자동화를 AWS 리전 실행하는 데 Amazon GuardDuty(GuardDuty) 감지기를 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.

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 Status가 ENABLED인지 확인합니다.

IAM

AWS Systems Manager 자동화에는 대한 사전 정의된 실행서를 제공합니다 AWS Identity and Access Management. 실행서에 대한 자세한 내용은 [실행서 작업](#)을 참조하세요. 실행서 콘텐츠를 보는 방법에 대한 자세한 내용은 [실행서 콘텐츠 보기](#)(을)를 참조하세요.

주제

- [AWSSupport-TroubleshootIAMAccessDeniedEvents](#)
- [AWS-AttachIAMToInstance](#)
- [AWS-DeleteIAMInlinePolicy](#)
- [AWSConfigRemediation-DeleteIAMRole](#)
- [AWSConfigRemediation-DeleteIAMUser](#)
- [AWSConfigRemediation-DeleteUnusedIAMGroup](#)
- [AWSConfigRemediation-DeleteUnusedIAMPolicy](#)
- [AWSConfigRemediation-DetachIAMPolicy](#)
- [AWSConfigRemediation-EnableAccountAccessAnalyzer](#)
- [AWSSupport-GrantPermissionsToIAMUser](#)
- [AWSConfigRemediation-RemoveUserPolicies](#)
- [AWSConfigRemediation-ReplaceIAMInlinePolicy](#)
- [AWSConfigRemediation-RevokeUnusedIAMUserCredentials](#)
- [AWSConfigRemediation-SetIAMPasswordPolicy](#)
- [AWSSupport-ContainIAMPrincipal](#)
- [AWSSupport-TroubleshootSAMLIssues](#)

AWSSupport - TroubleshootIAMAccessDeniedEvents

설명

AWSSupport-TroubleshootIAMAccessDeniedEvents 자동화 실행서는 AWS Identity and Access Management (IAM) 액세스 거부 문제를 해결하는 데 도움이 됩니다. 실행서는 지정된 IAM 엔터티 및 AWS 서비스 이벤트 소스와 관련된 최근 액세스 거부 이벤트에 대해 CloudTrail을 쿼리합니다. 최대 24시간의 구성 가능한 기간 내에 이벤트를 분석하여 실행당 최대 10개의 이벤트를 처리합니다. 식별된 각 액세스 거부 이벤트는 거부의 컨텍스트와 시도된 작업을 이해하는 데 도움이 되도록 검사됩니다. 자동화는 자격 증명 기반 및 리소스 기반 IAM 정책을 모두 분석합니다. 자격 증명 기반 정책의 경우 IAM 엔터티에 연결된 인라인 및 관리형 정책을 검사합니다. 리소스 기반 정책의 경우 Amazon Simple Storage Service(Amazon S3), AWS Key Management Service (AWS KMS), AWS Lambda Amazon Simple Notification Service(Amazon SNS), Amazon Elastic Container Registry(Amazon ECR), Amazon API Gateway, CodeArtifact, Amazon Elastic File System(Amazon EFS), Amazon Simple Queue Service(Amazon SQS), AWS Cloud9 Amazon OpenSearch Service AWS AWS Serverless Application Repository, Signer 및 등 여러 AWS 서비스의 정책을 평가합니다 AWS Secrets Manager.

실행서는 IAM 정책 시뮬레이션 기능을 활용하여 CloudTrail 이벤트에서 발견된 거부된 작업과 비교하여 이러한 정책을 평가합니다. 실행서는 IAM 사용자용 [SimulatePrincipalPolicy](#)와 IAM 역할용 [SimulateCustomPolicy](#)를 통해 IAM의 정책 시뮬레이션 기능을 활용하여 CloudTrail 이벤트에서 발견된 거부된 작업에 대해 이러한 정책을 평가합니다. 자동화는 거부된 특정 작업을 식별하는 데 도움이 되는 보고서를 출력하여 암시적 거부와 명시적 거부를 구분하고 액세스 거부를 담당하는 정책을 나열하고 각 거부에 대한 설명을 제공합니다. 보고서는 누락된 허용 문 식별 또는 거부 문 충돌과 같은 잠재적 해결 방법도 제안합니다.

어떻게 작동하나요?

실행서는 다음 단계를 수행합니다.

- RequesterARN (역할 또는 사용자)를 설명하고 검증하여 IAM 엔터티 유형 및 IAM ID와 같은 정보를 가져옵니다.
- 제공된 ResourceARN 경우 RequesterARN, EventSource 및와 연결된 CloudTrail 이벤트를 가져옵니다.
- CloudTrail 이벤트를 분석하여 액세스 거부됨 오류가 반환될 때 수행된 작업을 가져온 다음 IAM 엔터티에 연결된 인라인 및 관리형 정책과 리소스 기반 정책과 같은 모든 IAM 정책을 검사합니다. 그런 다음 해당 CloudTrail 이벤트의 액세스 거부 오류에서 발견된 작업에 대해 이러한 정책을 시뮬레이션하여 오류의 원인을 확인합니다.
- 액세스 거부 오류 유형, 오류를 담당하는 정책을 결정하는 보고서를 출력하고 오류에 대한 잠재적 해결 방법을 제안합니다.

[이 자동화 실행\(콘솔\)](#)

문서 유형

자동화

소유자

Amazon

플랫폼

/

필수 IAM 권한

실행서를 성공적으로 사용하려면 AutomationAssumeRole 파라미터에 다음 작업이 필요합니다.

- `apigateway:GetRestApis`
- `cloudtrail:LookupEvents`
- `cloud9:GetEnvironment`
- `codeartifact:GetRepositoryPermissionsPolicy`
- `ecr:GetRepositoryPolicy`
- `elasticfilesystem:GetFileSystemPolicy`
- `es:DescribeDomain`
- `iam:GetPolicy`
- `iam:GetPolicyVersion`
- `iam:GetRole`
- `iam:GetRolePolicy`
- `iam:GetUser`
- `iam:GetUserPolicy`
- `iam:ListAttachedRolePolicies`
- `iam:ListAttachedUserPolicies`
- `iam:ListRolePolicies`
- `iam:ListUserPolicies`
- `iam:SimulatePrincipalPolicy`
- `iam:SimulateCustomPolicy`
- `kms:GetKeyPolicy`

- `lambda:GetPolicy`
- `secretsmanager:GetResourcePolicy`
- `serverlessrepo:GetApplication`
- `signer:GetSigningProfile`
- `sns:GetTopicAttributes`
- `ssm:StartAutomationExecution`
- `ssm:StopAutomationExecution`
- `sqs:GetQueueAttributes`
- `s3:GetBucketPolicy`

예제 정책:

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": [
        "iam:GetUser",
        "iam:GetRole",
        "iam:SimulatePrincipalPolicy",
        "iam:ListUserPolicies",
        "iam:ListRolePolicies",
        "iam:GetRolePolicy",
        "iam:ListAttachedRolePolicies",
        "iam:GetPolicy",
        "iam:GetUserPolicy",
        "iam:GetPolicyVersion",
        "iam:ListAttachedUserPolicies",
        "ssm:StartAutomationExecution",
        "ssm:StopAutomationExecution",
        "cloudtrail:LookupEvents",
        "iam:SimulateCustomPolicy"
      ],
      "Resource": "*",
      "Effect": "Allow"
    }
  ]
}
```

```

    },
    {
      "Action": [
        "s3:GetBucketPolicy",
        "kms:GetKeyPolicy",
        "lambda:GetPolicy",
        "sns:GetTopicAttributes",
        "ecr:GetRepositoryPolicy",
        "apigateway:GET",
        "codeartifact:GetRepositoryPermissionsPolicy",
        "elasticfilesystem:DescribeFileSystemPolicy",
        "sqs:GetQueueAttributes",
        "cloud9:DescribeEnvironmentStatus",
        "es:DescribeDomain",
        "signer:GetSigningProfile",
        "serverlessrepo:GetApplication",
        "secretsmanager:GetResourcePolicy"
      ],
      "Resource": "*",
      "Effect": "Allow"
    }
  ]
}

```

지침

다음 단계에 따라 자동화를 구성합니다.

1. Systems Manager [AWSSupport-TroubleshootIAMAccessDeniedEvents](#)의 문서로 이동합니다.
2. Execute automation(자동화 실행)을 선택합니다.
3. 입력 파라미터에 다음을 입력합니다.
 - AutomationAssumeRole(선택 사항):
 - 설명: (선택 사항) SSM Automation이 사용자를 대신하여 작업을 수행하도록 허용하는 (IAM) 역할의 AWS Identity and Access Management Amazon 리소스 이름(ARN)입니다. Kubernetes API 호출을 허용하려면 Amazon EKS 클러스터 액세스 항목 또는 RBAC 권한에 역할을 추가해야 합니다.
 - 유형: AWS::IAM::Role::Arn

- RequesterARN(필수):
 - 설명: (필수) 특정 AWS 리소스에 대한 액세스 권한을 조사하려는 IAM 사용자 또는 역할의 ARN입니다.
 - 유형: String
 - 패턴 허용: `^arn:(aws|aws-cn|aws-us-gov|aws-iso(-[a-z]))?:iam::[0-9]{12}:(role|user)\\/[\\w+\\/=,\\.@-]+$`
- ResourceARN(선택 사항):
 - 설명: (선택 사항) 액세스가 거부된 리소스 AWS 의 ARN이 평가됩니다. AWS 대상 리소스는 자동화 실행서가 실행되는 리전과 동일한 리전에 있어야 합니다.
 - 유형: String
 - 패턴 허용: `^$|^arn:(aws|aws-cn|aws-us-gov|aws-iso(-[a-z]))?:([a-zA-Z0-9\\-]{1,63}):([a-z0-9\\-]{0,63})?:([\\d]{12})?:([a-zA-Z0-9\\-_/:.]{1,1024})$`
- EventSource(필수):
 - 설명: (필수) CloudTrail 이벤트가 시작된 Amazon API 엔드포인트입니다. 예를 들어 `s3.amazonaws.com`입니다.
 - 유형: String
 - 패턴 허용: `^([a-zA-Z0-9.-]+)\\.amazonaws\\.com$`
- EventName(선택 사항):
 - 설명: (선택 사항) CloudTrail 이벤트와 연결된 Amazon API 작업 이름입니다. 예를 들어 `s3:CreateBucket`입니다.
 - 유형: String
 - 패턴 허용: `^$|^([a-z0-9]+:[A-Za-z0-9])+$`
- LookBackHours(선택 사항):
 - 설명: (선택 사항) 이벤트를 검색할 때 CloudTrail Access Denied 이벤트를 다시 살펴보는 시간입니다. 유효한 범위: 1 ~ 24 시간.
 - 유형: 정수
 - 패턴 허용: `^([1-9]|1[0-9]|2[0-4])$`
 - 기본값: 12
- MaxEvents(선택 사항):
 - 설명: (선택 사항) Access Denied 이벤트를 검색할 때 반환되는 CloudTrail 이벤트의 최대 수입니다. 유효한 범위: 1 ~ 5 이벤트.

- 유형: 정수
- 패턴 허용: $^([1-9]|1[0-9]|2[0-4])\$$
- 기본값: 3
- UseContextEntries(선택 사항):
 - 설명: (선택 사항)를 지정하면 자동화true는 CloudTrail 이벤트에서 API 요청의 컨텍스트에 대한 세부 정보를 추출하여 IAM 정책 시뮬레이션에 포함합니다.
 - 유형: Boolean
 - 패턴 허용: $^([1-9]|1[0-9]|2[0-4])\$$
 - 기본값: 3

4. 실행을 선택합니다.

5. 자동화가 시작됩니다.

6. 문서는 다음 단계를 수행합니다.

- ValidateRequesterArn

대상 IAM 사용자 또는 역할에 대한 정보를 검색하여 RequesterArn ARN을 검증하고 해체합니다.

- GetCloudTrailEventsWithAccessDeniedError

지정된 IAM 엔터티 및 AWS 서비스와 관련된 최근 이벤트에 대해 CloudTrail Access Denied 이벤트를 쿼리합니다EventSource.

- EvaluateIAMRequesterPolicies

CloudTrail 이벤트의 작업에 대해 요청자 IAM 엔터티의 IAM 권한을 평가합니다. 이 평가에는 요청자와 연결된 자격 증명 기반 정책 및 리소스 기반 정책을 모두 분석하는 것이 포함됩니다. 자동화는 IAM의 정책 시뮬레이션 기능을 활용하여 CloudTrail 이벤트에서 식별된 거부된 작업의 컨텍스트에서 이러한 정책을 평가합니다.

7. 완료되면 출력 섹션에서 실행의 자세한 결과를 검토합니다.

- PermissionEvaluationResults

거부된 특정 작업을 식별하는 데 도움이 되는 보고서를 출력하여 암시적 거부와 명시적 거부를 구분합니다. 또한 액세스 거부를 담당하는 정책을 나열하고 각 거부에 대한 설명을 제공합니다. 보고서는 누락된 허용 문 식별 또는 거부 문 충돌과 같은 잠재적 해결 방법도 제안합니다.

Systems Manager Automation

- [이 자동화 실행\(콘솔\)](#)
- [자동화 실행](#)
- [Automation 설정](#)
- [Support Automation Workflows 랜딩 페이지](#)

AWS-AttachIAMToInstance

설명

관리형 인스턴스에 AWS Identity and Access Management (IAM) 역할을 연결합니다.

[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.

- ForceReplace

유형: Boolean

설명: (선택 사항) 플래그를 사용하여 기존 IAM 프로파일을 대체할지 여부를 지정합니다.

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` - EC2 인스턴스에 연결된 IAM 인스턴스 프로파일을 찾습니다.
2. `aws:branch - CheckInstanceProfileAssociations` - EC2 인스턴스에 연결된 IAM 인스턴스 프로파일을 확인합니다.
 - a. IAM 인스턴스 프로파일이 연결되어 있고 `ForceReplace`가 `true`로 설정된 경우:
 - i. `aws:executeAwsApi - DisassociateIamInstanceProfile` - EC2 인스턴스에서 IAM 인스턴스 프로파일의 연결을 해제합니다.
 - b. `aws:executeAwsApi - ListInstanceProfilesForRole` - 제공된 IAM 역할을 위한 인스턴스 프로파일을 표시합니다.
 - c. `aws:branch - CheckInstanceProfileCreated` - 제공된 IAM 역할에 연결된 인스턴스 프로파일이 있는지 확인합니다.
 - i. IAM 역할에 연결된 인스턴스 프로파일이 있는 경우:
 - A. `aws:executeAwsApi - AttachIAMProfileToInstance` - IAM 인스턴스 프로파일 역할을 EC2 인스턴스에 연결합니다.
 - i. IAM 역할에 연결된 인스턴스 프로파일이 없는 경우:
 - A. `aws:executeAwsApi - CreateInstanceProfileForRole` - 지정된 IAM 역할을 위한 인스턴스 프로파일 역할을 생성합니다.
 - B. `aws:executeAwsApi - AddRoleToInstanceProfile` - 인스턴스 프로파일 역할을 지정된 IAM 역할에 연결합니다.

- C. `aws:executeAwsApi - GetInstanceProfile` - 지정된 IAM 역할을 위한 인스턴스 프로파일 데이터를 가져옵니다.
- D. `aws:executeAwsApi - AttachIAMProfileToInstanceWithRetry` - IAM 인스턴스 프로파일 역할을 EC2 인스턴스에 연결합니다.

출력

`AttachIAMProfileToInstanceWithRetry.AssociationId`

`GetInstanceProfile.InstanceProfileName`

`GetInstanceProfile.InstanceProfileArn`

`AttachIAMProfileToInstance.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

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.

- IamArns

유형: 문자열

설명: (필수) 인라인 정책을 삭제하려는 IAM 자격 증명에 대해 심표로 구분된 ARNs 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 실행서는 지정하는 AWS Identity and Access Management (IAM) 역할을 삭제합니다. 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

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.

- 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 - 파라미터에서 지정하는 IAM 역할 이름을 수집합니다.IAMRoleID
- 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 지정하는 AWS Identity and Access Management (IAM) 사용자를 삭제합니다. 이 자동화는 IAM 사용자와 연결된 다음 리소스를 삭제하거나 분리합니다.

- 액세스 키
- 연결된 관리형 정책
- Git 보안 인증
- IAM 그룹 멤버십
- IAM 사용자의 암호
- 인라인 정책
- 다중 인증(MFA) 디바이스 사용
- 인증서 서명
- SSH 퍼블릭 키

[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.

- 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 파라미터에서 지정하는 IAM 사용자의 사용자 이름을 수집합니다.
- aws:executeScript - IAM 사용자와 연결된 액세스 키, 인증서, 보안 인증, MFA 디바이스, SSH 키를 수집합니다.
- aws:executeScript - IAM 사용자의 그룹 멤버십 및 정책을 수집합니다.
- aws:executeScript - IAM 사용자와 연결된 액세스 키, 인증서, 보안 인증, MFA 디바이스, 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 사용자를 포함하지 않는 IAM 그룹을 삭제합니다.

AWSConfigRemediation-DeleteUnusedIAMGroup 실행서는 사용자를 포함하지 않는 IAM 그룹을 삭제합니다.

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.

- 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

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.

- 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 지정하는 AWS Identity and Access Management (IAM) 정책을 분리합니다.

[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.

- 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 실행서는에서 AWS Identity and Access Management (IAM) Access Analyzer를 생성합니다 AWS 계정. Access Analyzer에 대한 자세한 내용은 IAM 사용 설명서의 [AWS Access Analyzer 사용하기](#)를 참조하세요.

이 자동화 실행(콘솔)

문서 유형

자동화

소유자

Amazon

플랫폼

Linux, macOS, Windows

파라미터

- AnalyzerName

유형: 문자열

설명: (필수) 생성할 분석기의 이름입니다.

- 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.

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 ACTIVE가 될 때까지 기다립니다.
- `aws:assertAwsResourceProperty` - Access Analyzer의 상태가 ACTIVE인지 확인합니다.

AWSSupport-GrantPermissionsToIAMUser

설명

이 실행서는 지정된 권한을 IAM 그룹(신규 또는 기존)에 부여하고 기존 IAM 사용자를 이 그룹에 추가합니다. 선택할 수 있는 정책은 [결제](#) 또는 [지원](#)입니다. IAM에 대한 결제 액세스를 활성화하려면 [Billing and Cost Management 페이지에 대한 IAM 사용자 및 연합된 사용자 액세스](#)도 활성화해야 합니다.

Important

기존 IAM 그룹을 제공할 경우 해당 그룹의 모든 현재 IAM 사용자가 새 권한을 받게 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.

다. 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) Lambda에서 수입하는 역할의 ARN입니다.

- 권한

유형: 문자열

유효한 값: SupportFullAccess | BillingFullAccess | SupportAndBillingFullAccess

기본값: SupportAndBillingFullAccess

설명: (필수) 다음 중 하나 선택: SupportFullAccess에서 지원 센터에 대한 모든 액세스 권한 부여. BillingFullAccess에서 결제 대시보드에 대한 모든 액세스 권한 부여.

SupportAndBillingFullAccess에서 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

연결된 AmazonSSMAutomationRole Amazon 관리형 정책과, Lambda 함수를 생성하고 IAM 역할을 Lambda로 전달할 수 있는 다음 추가 권한을 보유하는 것이 좋습니다.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": [
        "lambda:InvokeFunction",
        "lambda:CreateFunction",
        "lambda>DeleteFunction",
        "lambda:GetFunction"
      ],
      "Resource": "arn:aws:lambda:*:111122223333:function:AWSSupport-*",
      "Effect": "Allow"
    },
    {
      "Effect": "Allow",
      "Action": [
        "iam:CreateGroup",
        "iam:AddUserToGroup",
        "iam:ListAttachedGroupPolicies",
        "iam:GetGroup",
        "iam:GetUser"
      ],
      "Resource": [
        "arn:aws:iam::*:user/*",
        "arn:aws:iam::*:group/*"
      ]
    },
    {
      "Effect": "Allow",
      "Action": [
        "iam:AttachGroupPolicy"
      ],
      "Resource": "*",
      "Condition": {
        "ArnEquals": {
          "iam:PolicyArn": [
            "arn:aws:iam::aws:policy/job-function/Billing",
            "arn:aws:iam::aws:policy/AWSSupportAccess"
          ]
        }
      }
    }
  ]
}
```

```

    ]
  }
},
{
  "Effect": "Allow",
  "Action": [
    "iam:ListAccountAliases",
    "iam:GetAccountSummary"
  ],
  "Resource": "*"
}
]
}

```

AutomationAssumeRole 및 LambdaAssumeRole 사용

사용자는 실행서에서 `ssm:StartAutomationExecution` 권한이 있어야 하며, `AutomationAssumeRole` 및 `LambdaAssumeRole`로 전달된 IAM 역할에 대한 `iam:PassRole` 권한이 있어야 합니다. 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` - CloudFormation 템플릿을 실행하여 Lambda 함수를 생성합니다.
2. `aws:invokeLambdaFunction` - Lambda를 실행하여 IAM 권한을 설정합니다.
3. `aws:deleteStack` - CloudFormation 템플릿을 삭제합니다.

출력

`configureIAM.Payload`

AWSConfigRemediation-RemoveUserPolicies

설명

AWSConfigRemediation-RemoveUserPolicies 실행서는 AWS Identity and Access Management (IAM) 인라인 정책을 삭제하고 지정하는 사용자에게 연결된 모든 관리형 정책을 분리합니다.

[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.

- **IAMUserID**

유형: 문자열

설명: (필수) 정책을 제거하려는 사용자의 ID입니다.

- **PolicyType**

유형: 문자열

유효한 값: All | Inline | Managed

기본값: All

설명: (필수) 사용자로부터 제거하려는 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 파라미터에서 지정하는 사용자로부터 IAM 정책을 삭제하고 분리합니다.

AWSConfigRemediation-ReplaceIAMInlinePolicy

설명

AWSConfigRemediation-ReplaceIAMInlinePolicy 실행서는 인라인 AWS Identity and Access Management (IAM) 정책을 복제된 관리형 IAM 정책으로 대체합니다. 사용자, 그룹 또는 역할에 연결된

인라인 정책의 경우, 인라인 정책 권한이 관리형 IAM 정책에 복제됩니다. 관리형 IAM 정책이 리소스에 추가되고 인라인 정책이 제거됩니다. 이 자동화를 실행하는 AWS 리전 에서 활성화해야 AWS Config 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.

- InlinePolicyName

유형: StringList

설명: (필수) 대체하려는 인라인 IAM 정책입니다.

- ResourceId

유형: 문자열

설명: (필수) 대체하려는 인라인 정책이 있는 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 지정하는 리소스의 AWS 복제된 정책으로 대체합니다.

AWSConfigRemediation-RevokeUnusedIAMUserCredentials

설명

AWSConfigRemediation-RevokeUnusedIAMUserCredentials 실행서는 미사용 AWS Identity and Access Management (IAM) 암호와 활성 액세스 키를 취소합니다. 또한 이 실행서는 만료된 액세스 키를 비활성화하고 만료된 로그인 프로필을 삭제합니다. 이 자동화를 실행하는 AWS 리전 에서 활성화해야 AWS Config 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.

- IAMResourceId

유형: 문자열

설명: (필수) 사용하지 않은 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 보안 인증을 취소합니다. 만료된 액세스 키는 비활성화되고 만료된 로그인 프로파일은 삭제됩니다.

Note

이 작업을 트리거하는 데 사용하는 AWS Config 규칙의 MaxCredentialUsageAge파라미터인 [access-keys-rotated](#)와 일치하도록 수정 작업의 maxAccessKeyAge 파라미터를 구성해야 합니다.

AWSConfigRemediation-SetIAMPASSWORDPolicy

설명

AWSConfigRemediation-SetIAMPASSWORDPolicy 실행서는 AWS 계정에 대해 AWS Identity and Access Management (IAM) 사용자 암호 정책을 설정합니다.

[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.

- AllowUsersToChangePassword

유형: Boolean

기본값: false

설명: (선택 사항) true로 설정하면 모든 IAM 사용자가 AWS Management Console를 사용하여 암호를 변경할 AWS 계정 수 있습니다.

- HardExpiry

유형: Boolean

기본값: false

설명: (선택 사항) true로 설정된 경우, IAM 사용자는 암호가 만료된 후 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 암호의 수입니다.

- RequireLowercaseCharacters

유형: Boolean

기본값: false

설명: (선택 사항) true로 설정된 경우, IAM 사용자의 암호에는 ISO 기본 라틴 알파벳(a~z)의 소문자가 포함되어야 합니다.

- RequireNumbers

유형: Boolean

기본값: false

설명: (선택 사항) true로 설정된 경우, IAM 사용자의 암호는 숫자(0-9)를 포함해야 합니다.

- RequireSymbols

유형: Boolean

기본값: false

설명: (선택 사항) true로 설정된 경우, IAM 사용자의 암호는 영숫자 이외의 문자(! @ # \$ % ^ * () _ + - = [] { } | ')를 포함해야 합니다.

- RequireUppercaseCharacters

유형: Boolean

기본값: false

설명: (선택 사항) true로 설정된 경우, IAM 사용자의 암호에는 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 - AWS 계정에 대해 실행서 파라미터에서 지정하는 값을 기반으로 IAM 사용자의 암호 정책을 설정합니다.

AWSSupport-ContainIAMPrincipal

설명

보안 인시던트가 발생하거나 AWS Identity and Access Management (IAM) 사용자/역할 또는 AWS Identity Center(IDC) 사용자의 침해가 의심되는 경우 조사를 위한 구성을 유지하면서 영향을 받는 자격 증명을 신속하게 격리하는 것이 중요합니다. AWSSupport-ContainIAMPrincipal 실행서는 손상된 IAM 또는 IDC 자격 증명을 억제하여 AWS 리소스에 대한 액세스를 효과적으로 차단하고 손상의 잠재적 확산을 방지하는 구조화되고 되돌릴 수 있는 접근 방식을 제공합니다.

이 자동화된 프로세스를 통해 자격 증명 구성을 영구적으로 변경하지 않고도 조사를 수행할 수 있으므로 적절한 것으로 간주되면 일반 액세스를 복원할 수 있습니다. 억제 프로세스는 IAM 내에서 사용자 또는 역할을 유지하거나 IDC 내에서 사용자를 유지 관리하는 동시에 모든 네트워크 활동에서 효과적으로 격리합니다. 이 격리는 포함된 자격 증명 리소스가 Amazon Virtual Private Cloud 내의 리소스와 통신하거나 인터넷 리소스에 액세스하는 것을 방지합니다. 격납은 되돌릴 수 있도록 설계되어 적절한 것으로 간주될 때 일반 액세스를 복원할 수 있습니다.

어떻게 작동하나요?

AWSSupport-ContainIAMPrincipal 실행서는 IAM 사용자, 역할 및 Identity Center 사용자를 위한 포괄적인 격리 프로세스를 구현합니다. Contain 모드에서 실행되면 먼저 모든 입력 파라미터를 검증하고 지정된 Amazon S3 버킷에 대한 보안 검사를 수행합니다. 그런 다음 대상 IAM 보안 주체에 대한 세부 정보를 수집하고 보안 주체 유형에 따라 적절한 억제 조치를 적용합니다. IAM 사용자의 경우 액세스 키를 비활성화하고 콘솔 액세스를 제거하며 거부 정책을 연결합니다. IAM 역할의 경우 격리 전에 생성된 세션에 대한 권한을 취소하는 거부 정책을 연결합니다. Identity Center 사용자의 경우 권한 세트, 그룹 멤버십을 제거하고 거부 정책을 적용합니다. 전체 프로세스에서 실행서는 잠재적 복원을 위해 원본 구성을 Amazon S3 버킷에 백업합니다. Restore 모드에서 실행되면 백업된 구성을 사용하여 보안 주체를 컨테이너 전 상태로 되돌리려고 시도합니다. 실행서에는 변경 사항을 적용하지 않고 미리 볼 수 있는 DryRun 옵션이 포함되어 있으며, 성공적인 운영 및 실패 시나리오 모두에 대한 포괄적인 보고를 제공합니다.

⚠ Important

- **승격된 권한 사용:** 이 SSM 문서는 IAM 및 IDC 자격 증명 정책 수정, 격리 구성 적용 등 승격된 권한이 필요한 다양한 작업을 수행합니다. 이러한 작업은 잠재적으로 권한 상승으로 이어지거나 대상 자격 증명에 의존하는 다른 워크로드에 영향을 미칠 수 있습니다. AutomationAssumeRole 파라미터에 지정된 역할에 부여된 권한을 검토하고 의도된 사용 사례에 적합한지 확인해야 합니다. IAM 권한에 대한 자세한 내용은 다음 AWS 설명서를 참조하세요.
 - [Identity and Access Management\(IAM\) 권한](#)
 - [AWS Systems Manager Automation 권한](#)
- **워크로드 사용 불가 위험:** 이 Systems Manager 문서는 워크로드를 사용할 수 없거나 중단시킬 수 있는 격리 작업을 수행합니다. 보안 이벤트 중에 실행되면 지정된 IAM 및 IDC 자격 증명에서 AWS API 권한을 취소하여 영향을 받는 리소스에 대한 액세스를 제한하여 API 호출 또는 작업을 수행하지 AWS 못하도록 합니다. 이는 이러한 자격 증명에 의존하는 모든 애플리케이션 또는 서비스에 영향을 미칠 수 있습니다.
- **추가 리소스 생성:** 자동화 문서는 실행 파라미터에 따라 Amazon Simple Storage Service(Amazon S3) 버킷 및 여기에 저장된 Amazon S3 객체와 같은 추가 리소스를 조건부로 생성할 수 있습니다. 이러한 리소스에는 AWS 사용량에 따라 추가 요금이 발생합니다.
- **복원 위험:** 작업 파라미터가 로 설정된 경우 Restore이 SSM 문서는 IAM 또는 IDC 자격 증명 구성을 원래 상태로 복원하려고 시도합니다. 그러나 복원 프로세스가 실패하여 IAM 또는 IDC 자격 증명이 일관되지 않은 상태로 유지될 위험이 있습니다. 이 문서는 이러한 실패 시 수동 복원에 대한 지침을 제공하지만 복원 프로세스 중에 잠재적 문제를 처리할 준비가 되어 있어야 합니다.

프로덕션 환경에서 실행하기 전에 실행서를 철저히 검토하고, 실행서의 잠재적 영향을 이해하고, 비프로덕션 환경에서 테스트하는 것이 좋습니다.

이 자동화 실행(콘솔)

문서 유형

자동화

소유자

Amazon

플랫폼

/

필수 IAM 권한

런북을 성공적으로 사용하려면 AutomationAssumeRole 파라미터에 다음 권한이 필요합니다.

- s3:GetBucketLocation
- s3:GetBucket
- s3:ListBucket
- s3:GetBucketPublicAccessBlocks
- s3:GetAccountPublicAccessBlocks
- s3:GetBucketPolicyStatus
- s3:GetBucketAcl
- s3:GetObject
- s3:CreateBucket
- s3:PutObject
- iam:GetUser
- iam:GetUserPolicy
- iam:GetRole
- iam:ListUserPolicies
- iam:ListAttachedUserPolicies
- iam:ListAccessKeys
- iam:ListMfaDevices
- iam:ListVirtualMFADevices
- iam:GetLoginProfile
- iam:GetPolicy
- iam:GetRolePolicy
- iam:ListPolicies
- iam:ListAttachedRolePolicies
- iam:ListRolePolicies
- iam:UpdateAccessKey

- iam:CreateAccessKey
- iam>DeleteLoginProfile
- iam>DeleteAccessKey
- iam:PutUserPolicy
- iam>DeleteUserPolicy
- iam:DeactivateMFADevice
- iam:AttachRolePolicy
- iam:AttachUserPolicy
- iam>DeleteRolePolicy
- iam:TagMFADevice
- iam:PutRolePolicy
- iam:TagPolicy
- iam:TagRole
- iam:TagUser
- iam:UntagUser
- iam:UntagRole
- organizations:ListAccounts
- sso:ListPermissionSetsProvisionedToAccount
- sso:GetInlinePolicyForPermissionSet
- sso:ListInstances
- sso-directory:SearchUsers
- sso:ListPermissionSets
- sso:ListAccountAssignments
- sso-directory:DescribeUser
- identitystore:ListUsers
- identitystore:ListGroups
- identitystore:IsMemberInGroups
- identitystore:ListGroupMemberships
- secretsmanager:CreateSecret
- secretsmanager>DeleteSecret

- sso:DeleteAccountAssignment
- sso:PutInlinePolicyToPermissionSet
- sso:CreateAccountAssignment
- sso:DeleteInlinePolicyFromPermissionSet
- sso:TagResource
- sso:UntagResource
- identitystore:DeleteGroupMembership
- identitystore:CreateGroupMembership

다음은에 필요한 권한을 부여하는 IAM 정책의 예입니다. AutomationAssumeRole

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "S3Permissions",
      "Effect": "Allow",
      "Action": [
        "s3:GetBucketLocation",
        "s3:ListBucket",
        "s3:GetBucketPublicAccessBlock",
        "s3:GetBucketPolicyStatus",
        "s3:GetBucketAcl",
        "s3:GetObject",
        "s3:CreateBucket",
        "s3:PutObject"
      ],
      "Resource": "*"
    },
    {
      "Sid": "IAMPermissions",
      "Effect": "Allow",
      "Action": [
        "iam:GetUser",
        "iam:GetUserPolicy",
        "iam:GetRole",
        "iam:ListUserPolicies",
```

```

        "iam:ListAttachedUserPolicies",
        "iam:ListAccessKeys",
        "iam:ListMfaDevices",
        "iam:ListVirtualMFADevices",
        "iam:GetLoginProfile",
        "iam:GetPolicy",
        "iam:GetRolePolicy",
        "iam:ListPolicies",
        "iam:ListAttachedRolePolicies",
        "iam:ListRolePolicies",
        "iam:UpdateAccessKey",
        "iam:CreateAccessKey",
        "iam:DeleteLoginProfile",
        "iam:DeleteAccessKey",
        "iam:PutUserPolicy",
        "iam:DeleteUserPolicy",
        "iam:DeactivateMFADevice",
        "iam:AttachRolePolicy",
        "iam:AttachUserPolicy",
        "iam:DeleteRolePolicy",
        "iam:TagMFADevice",
        "iam:PutRolePolicy",
        "iam:TagPolicy",
        "iam:TagRole",
        "iam:TagUser",
        "iam:UntagUser",
        "iam:UntagRole"
    ],
    "Resource": "*"
},
{
    "Sid": "OrganizationsPermissions",
    "Effect": "Allow",
    "Action": [
        "organizations:ListAccounts"
    ],
    "Resource": "*"
},
{
    "Sid": "SSOPermissions",
    "Effect": "Allow",
    "Action": [
        "sso:ListPermissionSetsProvisionedToAccount",
        "sso:GetInlinePolicyForPermissionSet",

```

```

        "sso:ListInstances",
        "sso-directory:SearchUsers",
        "sso:ListPermissionSets",
        "sso:ListAccountAssignments",
        "sso-directory:DescribeUser",
        "sso:DeleteAccountAssignment",
        "sso:PutInlinePolicyToPermissionSet",
        "sso:CreateAccountAssignment",
        "sso:DeleteInlinePolicyFromPermissionSet",
        "sso:TagResource",
        "sso:UntagResource"
    ],
    "Resource": "*"
},
{
    "Sid": "IdentityStorePermissions",
    "Effect": "Allow",
    "Action": [
        "identitystore:ListUsers",
        "identitystore:ListGroups",
        "identitystore:IsMemberInGroups",
        "identitystore:ListGroupMemberships",
        "identitystore:DeleteGroupMembership",
        "identitystore:CreateGroupMembership"
    ],
    "Resource": "*"
},
{
    "Sid": "SecretsManagerPermissions",
    "Effect": "Allow",
    "Action": [
        "secretsmanager:CreateSecret",
        "secretsmanager:DeleteSecret"
    ],
    "Resource": "*"
}
]
}

```

지침

다음 단계에 따라 자동화를 구성합니다.

1. AWS Systems Manager 콘솔에서 [AWSSupport-ContainIAMPrincipal](#)로 이동합니다.
2. Execute automation(자동화 실행)을 선택합니다.
3. 입력 파라미터에 다음을 입력합니다.
 - AutomationAssumeRole(선택 사항):
 - 설명: (선택 사항) Systems Manager Automation이 사용자를 대신하여 작업을 수행하도록 허용하는 AWS Identity and Access Management(IAM) 역할의 Amazon 리소스 이름(ARN)입니다. 역할이 지정되지 않은 경우 Systems Manager Automation은 이 실행서를 시작하는 사용자의 권한을 사용합니다.
 - 유형: `AWS::IAM::Role::Arn`
 - PrincipalType(필수):
 - 설명: (필수) AWS IAM 보안 주체 유형: IAM 사용자, IAM 역할 또는 Identity Center 사용자.
 - 유형: String
 - 허용되는 값: `IAM user|IAM role|Identity Center user`
 - PrincipalName(필수):
 - 설명: (필수) IAM 보안 주체의 이름입니다. Identity Center 사용자의 경우 사용자 이름을 입력합니다.
 - 유형: 문자열
 - 허용된 패턴: `^[a-zA-Z0-9\\.\-_\!*\'()/+=,@]{1,1024}$`
 - 작업(필수):
 - 설명: (필수) 대상 IAM 보안 주체를 Contain 격리Restore하거나 이전 백업에서 원래 구성으로 IAM 보안 주체를 복원하려고 합니다.
 - 유형: String
 - 허용되는 값: `Contain|Restore`
 - DryRun(선택 사항):
 - 설명: (선택 사항) 로 설정하면 true자동화는 대상 IAM 보안 주체를 변경하지 않고, 대신 각 단계에 대해 자세히 설명하면서 변경하려고 시도한 내용을 출력합니다. 기본값: true.
 - 유형: Boolean
 - 허용되는 값: `true|false`
 - ActivateDisabledKeys(조건부):
 - 설명: (조건부) 입력 파라미터 Action이 로 설정Restore되고 PrincipalType이 IAM 사용자로 설정된 경우 이 옵션을 비활성화한 경우 이 자동화가 연결된 액세스 키를 활성화해야 하는지 여부

를 결정합니다. 손상된 액세스 키의 무결성은 확인할 수 없습니다. AWS 는 손상된 키를 다시 활성화하지 않도록 강력히 권장합니다. 대신 새 키를 생성하는 것이 좋습니다. 기본값: false.

- 유형: Boolean
- 허용된 값: true|false
- BackupS3BucketName(조건부):
 - 설명: (조건부) 작업이 로 설정된 경우 IAM 보안 주체 구성을 백업하거나 작업이 인 경우 구성을 복원Contain하는 Amazon S3 버킷입니다Restore. 지정된 작업이 Contain 이고 실행서가 버킷에 액세스할 수 없거나 값이 제공되지 않은 경우 계정에 이름이 인 새 버킷이 생성됩니다awssupport-containiamprincipal-<random-string>. DryRun이 로 설정된 경우 true이 파라미터가 필요합니다.
 - 유형: AWS::S3::Bucket::Name
- BackupS3KeyName(조건부):
 - 설명: (조건부) 작업이 로 설정된 경우 자동화가 IAM 보안 주체 구성을 복원하는 데 사용할 Amazon S3 키를 Restore지정합니다. Amazon S3 키는 일반적으로 형식을 따릅니다{year}/{month}/{day}/{hour}/{minute}/{automation_execution_id}.json. 키는 이전 억제 자동화 실행의 출력에서 가져올 수 있습니다.
 - 유형: 문자열
 - 허용된 패턴: ^[a-zA-Z0-9\\._-\\\\!*'()/{0,1024}\$
- BackupS3BucketAccess(조건부):
 - 설명: (조건부) 억제 작업을 실행한 후 백업 Amazon S3 버킷에 대한 액세스가 허용되는 IAM 사용자 또는 역할의 ARN입니다. 이 파라미터는 작업이 일 때 필요합니다Contain. AutomationAssumeRole 또는 Automation이 실행 중인 컨텍스트의 사용자가 없는 경우 목록에 자동으로 추가됩니다.
 - 유형: StringList
 - 허용된 패턴: ^\$|^arn:(aws|aws-cn|aws-us-gov|aws-iso(-[a-z]))?:iam::[0-9]{12}:(role|user)\\/[\\w+\\/=,\\.@-]+\$
- TagIdentifier(선택 사항):
 - 설명: (선택 사항) 형식을 사용하여 선택한 태그로 IAM 보안 주체에 태그를 지정합니다Key=<EXAMPLE_KEY>,Value=<EXAMPLE_VALUE>. 이 옵션을 사용하면이 실행서의 대상이 된 IAM 보안 주체를 추적할 수 있습니다. 참고: 태그 키와 값은 대/소문자를 구분합니다.
 - 유형: 문자열
 - 허용된 패턴: ^\$|^([Kk][Ee][Yy]=[\\+\\-\\=\\._\\:\\\\/@a-zA-Z0-9]{1,128},[Vv][Aa][Rr][I][I][Uu][Ee]=[\\+\\-\\=\\._\\:\\\\/@a-zA-Z0-9]{0,128})\$

4. 실행을 선택합니다.

5. 자동화가 시작됩니다.

6. 문서는 다음 단계를 수행합니다.

- `ValidateRequiredInputs`

Action 지정된를 기반으로 필요한 자동화 입력 파라미터를 검증합니다.

- `CheckBackupS3BucketName`

대상 Amazon S3 버킷이 객체에 read 대한 또는 write 퍼블릭 액세스 권한을 부여할 가능성이 있는지 확인합니다. 격리 워크플로의 경우 버킷이 없으면 새 Amazon S3 BackupS3BucketName 버킷이 생성됩니다.

- `BranchOnAction`

지정된의 값을 기반으로 자동화를 분기합니다Action.

- `BranchOnPrincipalTypeAndDryRun`

IAM 보안 주체 유형(IAM 사용자, IAM 역할 또는 Identity Center 사용자)과 DryRun 모드에서 실행 중인지 여부에 따라 자동화를 분기합니다.

- `BranchOnPrincipalTypeForContain`

Contain 작업 기반 및 입력에 지정된 IAM 보안 주체 유형(IAM 사용자, IAM 역할 또는 Identity Center 사용자)에 대한 자동화를 분기합니다.

- `GetIAMUser`

대상 IAM 사용자의 생성 시간과 사용자 이름을 가져옵니다.

- `GetIAMUserDetails`

인라인 정책, 관리형 정책, 액세스 키, MFA 디바이스 및 로그인 프로필을 포함하여 대상 IAM 사용자의 구성을 가져오고 저장합니다.

- `UpdateS3KeyForUser`

자동화 'S3Key' 변수를 단계의 출력에서 업데이트합니다GetIAMUserDetails.

- `GetIAMRole`

대상 IAM 역할의 생성 시간, 역할 이름 및 경로를 가져옵니다.

- `GetIAMRoleDetails`

역할에 연결된 인라인 정책 및 관리형 정책을 포함하여 대상 IAM 역할의 구성을 가져오고 저장합니다.

- UpdateS3KeyForRole

자동화 'S3Key' 변수를 단계의 출력에서 업데이트합니다GetIAMRoleDetails.

- GetIdentityStoreId

AWS 계정과 연결된 AWS IAM Identity Center 인스턴스의 ID를 가져옵니다.

- GetIDCUser

Identity Store ID를 사용하여 대상 Identity Center 사용자의 사용자 ID를 가져옵니다.

- GatherIDCUserDetails

계정 할당, 연결된 권한 세트 및 인라인 정책을 포함하여 대상 Identity Center 사용자의 구성을 가져오고 저장합니다.

- UpdateS3KeyForIDCUser

자동화 'S3Key' 변수를 단계의 출력에서 업데이트합니다GatherIDCUserDetails.

- BranchOnIdentityContain

Contain 작업의 값과 IAM 보안 주체 유형을 기반으로 자동화DryRun를 분기합니다.

- BranchOnDisableAccessKeys

IAM 사용자에게 비활성화해야 하는 액세스 키가 있는지 여부에 따라 자동화를 분기합니다.

- DisableAccessKeys

활성 IAM 사용자 액세스 키를 비활성화합니다.

- BranchOnDisableConsoleAccess

IAM 사용자에게 AWS Management Console 액세스가 활성화되어 있는지 여부에 따라 분기합니다.

- DisableConsoleAccess

AWS 관리 콘솔에 대한 IAM 사용자의 암호 기반 액세스를 제거합니다.

- AttachInlineDenyPolicyToUser

이전 세션 토큰에 대한 권한을 취소하는 거부 정책을 IAM 사용자에게 연결합니다.

- `AttachInlineDenyPolicyToRole`

IAM 역할에 거부 정책을 연결하여 이전 세션 토큰에 대한 권한을 취소합니다.

- `RemovePermissionSets`

Identity Center 사용자와 연결된 권한 세트를 제거합니다.

- `RemoveIDCUserFromIDCGroups`

Identity Center 그룹에서 Identity Center 사용자를 제거합니다.

- `AttachInlineDenyPolicyToPermissionSet`

Identity Center 사용자와 연결된 권한 세트에 거부 정책을 연결합니다.

- `BranchOnReactivateKeys`

복원 프로세스 중에 `ActivateDisabledKeys` 파라미터를 기반으로 자동화를 분기합니다.

- `DetachInlineDenyPolicy`

억제 프로세스 중에 IAM 역할에 연결된 거부 정책을 제거합니다.

- `DetachInlineDenyPolicyFromPermissionSet`

억제 프로세스 중에 권한 세트에 연결된 거부 정책을 제거합니다.

- `ReportContain`

가 로 `DryRun` 설정된 경우 수행할 억제 작업에 대한 세부 정보를 출력합니다 `True`.

- `ReportRestore`

가 로 `DryRun` 설정된 경우 수행할 복원 작업에 대한 세부 정보를 출력합니다 `True`.

- `ReportContainFailure`

억제 워크플로 실패 시나리오 중에 IAM 보안 주체의 원래 구성을 수동으로 복원하는 포괄적인 지침을 제공합니다.

- `ReportRestoreFailure`

복원 워크플로 실패 시나리오 중에 IAM 보안 주체의 원래 구성 복원을 수동으로 완료하기 위한 자세한 지침을 제공합니다.

7. 실행이 완료되면 출력 섹션에서 실행의 자세한 결과를 검토합니다.

작업이 포함으로 설정되고 DryRun이 거짓으로 설정될 때 수행되는 억제 작업에 대한 자세한 정보를 제공합니다. 백업 위치, 적용된 거부 정책 및 수정된 구성에 대한 정보를 포함합니다.

- RestoreIAMPrincipal.Output

작업이 복원으로 설정되고 DryRun이 거짓으로 설정될 때 수행되는 복원 작업에 대한 자세한 정보를 제공합니다. 복원된 구성 및 복원 중에 발생하는 모든 문제에 대한 정보를 포함합니다.

- ReportContain.Output

작업이 포함으로 설정되고 DryRun이 True로 설정될 때 수행할 억제 작업에 대한 세부 정보를 출력합니다. 현재 및 컨테이너 후 구성의 비교를 포함합니다.

- ReportRestore.Output

작업이 복원으로 설정되고 DryRun이 True로 설정될 때 수행되는 복원 작업에 대한 세부 정보를 출력합니다. 복원할 현재 구성과 원래 구성을 표시합니다.

- ReportContainFailure.Output

억제 워크플로 실패 시나리오 중에 IAM 보안 주체의 원래 구성을 수동으로 복원하는 포괄적인 지침을 제공합니다.

- ReportRestoreFailure.Output

복원 워크플로 실패 시나리오 중에 IAM 보안 주체의 원래 구성 복원을 수동으로 완료하기 위한 자세한 지침을 제공합니다.

출력

실행이 완료되면 출력 섹션에서 자세한 결과를 검토합니다.

- ContainIAMPrincipal.Output

작업이 포함으로 설정되고 DryRun이 거짓으로 설정될 때 수행되는 억제 작업에 대한 자세한 정보를 제공합니다. 백업 위치, 적용된 거부 정책 및 수정된 구성에 대한 정보를 포함합니다.

- RestoreIAMPrincipal.Output

작업이 복원으로 설정되고 DryRun이 거짓으로 설정될 때 수행되는 복원 작업에 대한 자세한 정보를 제공합니다. 복원된 구성 및 복원 중에 발생하는 모든 문제에 대한 정보를 포함합니다.

- ReportContain.Output

작업이 포함으로 설정되고 DryRun이 True로 설정될 때 수행할 억제 작업에 대한 세부 정보를 출력합니다. 현재 및 컨테이너 후 구성의 비교를 포함합니다.

- ReportRestore.Output

작업이 복원으로 설정되고 DryRun이 True로 설정될 때 수행되는 복원 작업에 대한 세부 정보를 출력합니다. 복원할 현재 구성과 원래 구성을 표시합니다.

- ReportContainFailure.Output

억제 워크플로 실패 시나리오 중에 IAM 보안 주체의 원래 구성을 수동으로 복원하는 포괄적인 지침을 제공합니다.

- ReportRestoreFailure.Output

복원 워크플로 실패 시나리오 중에 IAM 보안 주체의 원래 구성 복원을 수동으로 완료하기 위한 자세한 지침을 제공합니다.

참조

Systems Manager Automation

- [이 자동화 실행\(콘솔\)](#)
- [단순한 자동화 실행](#)
- [자동화 설정](#)
- [자동화 워크플로 지원](#)

AWSSupport-TroubleshootSAMLIssues

설명

AWSSupport-TroubleshootSAMLIssues 자동화 실행서는 Amazon Simple Storage Service(Amazon S3)에 저장된 SAML 응답 파일을 분석하여 SAML(Security Assertion Markup Language) 관련 문제를 진단하는 데 도움이 됩니다. 스키마 확인, 서명 검증, 대상 제한 확인 및 만료 시간 확인을 포함한 포괄적인 검증을 수행합니다. 실행서는 SAML 응답에서 발급자, 어설션, 주체, 조건, 서명 및 속성을 포함한 주요 SAML 요소를 디코딩하고 추출합니다. SAML을 사용하여 IAM 자격 증명 공급자를 통해 AWS 리소스(예: Amazon Connect 또는 Amazon WorkSpaces 애플리케이션)에 액세스하는 환경의 경우 SAML 응답 서명의 인증서가 IAM 자격 증명 공급자에 구성된 인증서와 일치하는지 확인합니다.

어떻게 작동하나요?

실행서는 다음 단계를 수행합니다.

- SAML 응답 형식 및 필수 요소를 검증합니다.
- SAML 응답 구성 요소(발급자, 어설션, 제목, 조건, 서명, 속성)를 디코딩하고 추출합니다.
- 제공된 경우 IAM 자격 증명 공급자 인증서와 비교하여 디지털 서명을 확인합니다.
- 대상 제한 및 시간 유효성을 확인합니다.
- 구문 분석된 SAML 구조 및 검증 결과를 보여주는 자세한 진단 정보를 제공합니다.

[이 자동화 실행\(콘솔\)](#)

문서 유형

자동화

소유자

Amazon

플랫폼

/

필수 IAM 권한

실행서를 성공적으로 사용하려면 AutomationAssumeRole 파라미터에 다음 작업이 필요합니다.

- s3:GetBucketLocation
- s3:ListBucket
- s3:GetBucketPublicAccessBlock
- s3:GetAccountPublicAccessBlock
- s3:GetObject
- s3:GetBucketPolicyStatus
- s3:GetEncryptionConfiguration
- s3:GetBucketOwnershipControls
- s3:GetBucketAcl
- s3:GetBucketPolicy
- s3:PutObject

- iam:GetSAMLProvider
- sts:AssumeRole

정책 예제:

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": [
        "s3:GetBucketLocation",
        "s3:ListBucket",
        "s3:GetBucketPublicAccessBlock",
        "s3:GetAccountPublicAccessBlock",
        "s3:GetObject",
        "s3:GetBucketPolicyStatus",
        "s3:GetEncryptionConfiguration",
        "s3:GetBucketOwnershipControls",
        "s3:GetBucketAcl",
        "s3:GetBucketPolicy",
        "s3:PutObject",
        "iam:GetSAMLProvider",
        "sts:AssumeRole"
      ],
      "Resource": "*",
      "Effect": "Allow"
    }
  ]
}
```

지침

다음 단계에 따라 자동화를 구성합니다.

1. 이 실행서를 사용하기 전에 Base64-encoded SAML 응답(txt 파일)을 캡처하여 S3 버킷에 저장해야 합니다. SAML 응답 캡처 지침은 [이 문서에서](#) 확인할 수 있습니다.

2. Systems Manager [AWSsupport-TroubleshootSAMLIssues](#)의 문서로 이동합니다.

3. Execute automation(자동화 실행)을 선택합니다.

4. 입력 파라미터에 다음을 입력합니다.

- AutomationAssumeRole(선택 사항):
 - 설명: (선택 사항) SSM Automation이 사용자를 대신하여 작업을 수행하도록 허용하는 (IAM) 역할의 AWS Identity and Access Management Amazon 리소스 이름(ARN)입니다. 역할을 지정하지 않은 경우, Systems Manager Automation에서는 이 실행서를 시작하는 사용자의 권한을 사용합니다.
 - 유형: AWS::IAM::Role::Arn
- InputFileS3URI(필수):
 - 설명: (필수) SAML 응답 txt 파일의 Amazon Simple Storage Service(Amazon S3) URI(예: s3://bucket-name/path/to/file.txt).
 - 유형: 문자열
 - 패턴 허용: ^s3://[a-z0-9][a-z0-9.-][a-z0-9](/.)?\$
- S3OutputPrefix(선택 사항):
 - 설명: (선택 사항) 분석 출력 파일은 입력 버킷에 'saml_analysis_<executionID of the runbook>.json' 이름으로 저장됩니다. 특정 접두사가 있는 파일을 출력하려는 경우 이 파라미터를 사용할 수 있습니다. 기본값은 'output'이며, 이 경우 결과를 출력하는 파일 URI는 's3://bucket-name/output/saml_analysis_<executionID of the runbook>.json'이 됩니다.
 - 유형: 문자열
 - 패턴 허용: ^[a-zA-Z0-9+ =, . @ \ - _ /] * / \$
- ExpectedAudience(선택 사항):
 - 설명: (선택 사항) SAML 응답의 예상 대상 값입니다. 지정하지 않으면를 사용합니다. urn:amazon:webservices. IdP 및 SP 설정에서 특정 대상 값을 구성한 경우 정확한 형식 (예: , urn:amazon:webserviceshttps://signin.aws.amazon.com/saml)을 제공하세요.
 - 유형: 문자열
 - 기본값: urn:amazon:webservices
- IdProviderArn(선택 사항):
 - 설명: (선택 사항) IAM ID 공급자 엔터티를 사용하여 IdP를 AWS IAM과 직접 연결하는 경우 해당 ARN(예: arn:aws:iam::<account-id>:saml-provider/<provider-name>)을 제공하세요.

- 유형: 문자열
- 패턴 허용: `^$|^arn:aws:iam::[0-9]{12}:saml-provider/[a-zA-Z0-9_-]+$`
- SAMLAuthenticationTime(선택 사항):
 - 설명: (선택 사항) SAML 인증이 수행된 날짜 및 시간입니다. 시간대는 UTC여야 합니다. YYYY-MM-DDThh:mm:ss 형식이어야 합니다(예: 2025-02-01T10:00:00). 이 파라미터를 제공하지 않으면 현재 타임스탬프에 대해 만료 검사가 수행됩니다.
 - 유형: 문자열
 - 패턴 허용: `^$|^\\d{4}-(?:0[1-9]|1[0-2])-(?:0[1-9]|[12]\\d|3[01])T(?:[01]\\d|2[0-3]):[0-5]\\d:[0-5]\\d$`
- S3BucketOwnerRoleArn(선택 사항):
 - 설명: (선택 사항) Amazon S3 버킷에 액세스하기 위한 IAM 역할 ARN입니다. Amazon S3 버킷 및 계정을 가져올 수 있는 권한이 있는 IAM 역할의 ARN은 퍼블릭 액세스 설정, 버킷 암호화 구성, 버킷 ACLs, 버킷 정책 상태 및 버킷에 객체 업로드를 차단합니다. 이 파라미터를 지정하지 않으면 실행서는 'AutomationAssumeRole'(지정된 경우) 또는 이 실행서를 시작하는 사용자('AutomationAssumeRole'이 지정되지 않은 경우)를 사용합니다.
 - 유형: AWS::IAM::Role::Arn

5. 실행을 선택합니다.

6. 자동화가 시작됩니다.

7. 문서는 다음 단계를 수행합니다.

- ValidateIAMIDProvider

제공된 IAM ID 공급자 ARN이 존재하고 액세스할 수 있는지 확인하여 검증합니다. ARN이 제공되지 않으면 검증을 건너뛰고 단계가 성공적으로 완료됩니다.

- CheckS3BucketPublicStatus

Amazon S3 버킷이 익명 또는 퍼블릭 읽기 또는 쓰기 액세스 권한을 허용하는지 확인합니다. 버킷이 이러한 권한을 허용하는 경우 이 단계에서 자동화가 중지됩니다.

- CheckS3ObjectExistence

Amazon S3 버킷에 대한 액세스를 검증합니다. 버킷과 객체가 있는지, 자동화에 소스에서 읽고 대상에 쓰는 데 필요한 권한이 있는지 확인합니다.

- AnalyzeSAMLResponse

검사(스키마 검증, 서명 확인, 대상 검증, 만료 확인)를 수행하여 SAML 응답 파일을 분석합니다. 세부 JSON 보고서를 생성하여 지정된 Amazon S3 위치에 저장합니다.

8. 완료되면 출력 섹션에서 실행의 자세한 결과를 검토합니다.
 - 출력 섹션에는 분석 결과가 설명된 Amazon S3 객체에 대한 정보가 포함되어 있습니다.
9. 분석 결과의 Amazon S3 객체는 다음 정보가 포함된 Json 파일입니다.
 - validation_result: SAML 응답의 기본 검증 결과를 포함합니다.
 - saml_info: 발급자, 서명 및 어설션을 포함한 주요 SAML 정보입니다.
 - schema_validation: SAML 스키마 검증 결과입니다.
 - verification_result: 보다 자세한 진단 결과를 제공합니다.
 - 서명: 서명 확인 결과입니다.
 - audience: 대상 제한 검증의 결과입니다.
 - expiration: 만료 시간 확인 결과입니다.

참조

Systems Manager Automation

- [이 자동화 실행\(콘솔\)](#)
- [자동화 실행](#)
- [Automation 설정](#)
- [Support Automation Workflows 랜딩 페이지](#)

인시던트 감지 및 대응

AWS Systems Manager Automation은 AWS 인시던트 감지 및 대응을 위한 사전 정의된 실행서를 제공합니다. 실행서에 대한 자세한 내용은 [실행서 작업](#)을 참조하세요. 실행서 콘텐츠를 보는 방법에 대한 자세한 내용은 [실행서 콘텐츠 보기](#)(을)를 참조하세요.

주제

- [AWSPremiumSupport-OnboardWorkloadToIDR](#)

AWSPremiumSupport-OnboardWorkloadToIDR

설명

AWSPremiumSupport-OnboardWorkloadToIDR 실행서는 AWS Enterprise Support 고객이 AWS 인시던트 감지 및 대응을 사용하여 모니터링 및 중요한 인시던트 관리를 위한 워크로드를 온보딩하는

데 도움이 됩니다. 워크로드는 AWS Resource Group 또는 AWS Service Catalog AppRegistry 애플리케이션과 연결된 AWS 리소스 모음으로 정의할 수 있습니다. AWS Resource Group 또는 AWS Service Catalog AppRegistry 애플리케이션을 지정하지 않으면 실행서는 태그 필터 또는 그룹에 포함하려는 리소스의 AWS CloudFormation 스택 ID를 사용하여 사용자를 대신하여 리소스 그룹을 생성합니다. 파라미터를 CreateApplicationInsights로 설정하면 자동화Yes는를 사용하여 Amazon CloudWatch Application Insights 애플리케이션을 프로비저닝합니다 AWS CloudFormation. CloudWatch Application Insights는 감지된 문제에 대한 알림을 위해 Amazon CloudWatch 지표, 로그 및 이벤트를 사용하여 선택한 애플리케이션 리소스에 대한 권장 지표 및 로그를 설정합니다.

Important

이 실행서는 제공된 입력 파라미터에 따라 계정에서 다음 작업을 수행합니다.

- ResourceGroupName 또는 지정AppRegistryApplication되지 않은 AWS CloudFormation 경우를 사용하여 새 AWS 리소스 그룹을 생성합니다. 스택이 생성된 후 실행서는 종료 방지 설정을 시도합니다.
- 태그를 포함하여 워크로드 관련 AWS 리소스 그룹에 aws_idr 태그를 지정합니다.
- CreateApplicationInsights 입력 파라미터가 로 설정된 경우 Amazon CloudWatch Application Insights 리소스 그룹 기반 애플리케이션을 생성합니다Yes. 스택이 생성된 후 실행서는 스택에 대한 종료 방지 설정을 시도합니다.
- AWSServiceRoleForHealth_EventProcessor 서비스 연결 역할(SLR)을 설치하여 InstallServiceLinkedRole 입력 파라미터가 로 설정된 경우 인시던트 감지 및 대응에 대한 알림 수집 액세스를 프로비저닝합니다Yes.
- AWS 인시던트 감지 및 대응을 사용하여 AWS 지원 사례를 생성합니다.

Important

이 실행서를 사용하고 AWS 인시던트 감지 및 대응에 온보딩하려면 AWS 엔터프라이즈 지원 (추가 요금 부과) 또는 통합 운영 구독이 필요합니다. 자세한 내용은 [지원 플랜 비교](#)를 참조하세요.

어떻게 작동하나요?

실행서는 다음과 같은 상위 수준 단계를 수행합니다.

- 현재 AWS 계정 지원 플랜이 Enterprise인지 확인합니다. 그렇지 않으면 자동화가 종료됩니다.
- 제공된 파라미터를 기반으로 기존 AWS 리소스 그룹을 사용할지 아니면 새 리소스 그룹을 생성할지 결정합니다.
- 새 리소스 그룹을 생성하는 경우는 AWS CloudFormation 템플릿을 생성하고 적절한 태그가 있는 스택을 생성합니다.
- 필요한 AWS 인시던트 감지 및 대응 태그로 리소스 그룹에 태그를 지정합니다.
- 선택적으로 AWS 인시던트 감지 및 대응을 위한 서비스 연결 역할을 설치합니다.
- 선택적으로 향상된 모니터링을 위해 Amazon CloudWatch Application Insights 애플리케이션을 생성합니다.
- 온보딩 프로세스를 완료하기 위한 AWS 지원 사례를 생성합니다.

[이 자동화 실행\(콘솔\)](#)

문서 유형

자동화

소유자

Amazon

플랫폼

/

필수 IAM 권한

실행서를 성공적으로 사용하려면 AutomationAssumeRole 파라미터에 다음 작업이 필요합니다.

- `cloudformation:CreateStack`
- `cloudformation:DescribeStackResource`
- `cloudformation:DescribeStacks`
- `cloudformation:UpdateTerminationProtection`
- `iam:CreateServiceLinkedRole`
- `resource-groups:CreateGroup`

- resource-groups:GetGroup
- resource-groups:TagResource
- servicecatalog-appregistry:GetApplication
- support:CreateCase
- support:DescribeSeverityLevels
- support:DescribeServices
- support:DescribeSupportLevel

정책 예제:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "cloudformation:CreateStack",
        "cloudformation:DescribeStackResource",
        "cloudformation:DescribeStacks",
        "cloudformation:UpdateTerminationProtection",
        "iam:CreateServiceLinkedRole",
        "resource-groups:CreateGroup",
        "resource-groups:GetGroup",
        "resource-groups:TagResource",
        "servicecatalog-appregistry:GetApplication",
        "support:CreateCase",
        "support:DescribeSeverityLevels",
        "support:DescribeServices",
        "support:DescribeSupportLevel"
      ],
      "Resource": "*"
    }
  ]
}
```

지침

다음 단계에 따라 자동화를 구성합니다.

1. Systems Manager [AWSPremiumSupport-OnboardWorkloadToIDR](#)의 문서로 이동합니다.

2. Execute automation(자동화 실행)을 선택합니다.

3. 입력 파라미터에 다음을 입력합니다.

- AutomationAssumeRole(선택 사항):

- 설명: (선택 사항) Systems Manager Automation이 사용자를 대신하여 작업을 수행하도록 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.

- 유형: AWS::IAM::Role::Arn

- WorkloadName(필수):

- 설명: (필수) 워크로드의 이름입니다. ResourceGroupName이 제공되지 않은 경우 워크로드 이름은 이름으로 새 AWS 리소스 그룹을 설정하는 데 사용됩니다 IDR-AWS-
<WorkloadName>.

- 유형: String

- 패턴 허용: `^[a-zA-Z0-9_-]{1,128}$`

- WorkloadDescription(필수):

- 설명: (필수) 워크로드 설명입니다. 이 워크로드의 사용 사례를 자세히 설명하는 간단한 설명을 입력합니다. 기본 최종 사용자와 이 워크로드의 기능을 포함하세요.

- 유형: String

- 패턴 허용: `^[a-zA-Z0-9.:;,-_&() ]{1,1024}$`

- AppRegistryApplication(선택 사항):

- 설명: (선택 사항) AWS Service Catalog AppRegistry 애플리케이션의 이름 또는 ID입니다. 제공되지 않은 경우에 대한 입력을 제공해야 합니다 ResourceGroupName.

- 유형: String

- 패턴 허용: `^$|^[a-zA-Z0-9.-_]{1,128}$`

- 기본값: ""

- ResourceGroupName(선택 사항):

- 설명: (선택 사항)이 제공되지 않은 경우 기존 AWS 리소스 그룹의 이름 AppRegistryApplication입니다. 리소스 그룹을 생성하려면 TagFilters 및 선택적으로에 대한 입력을 제공하여 새 AWS 리소스 그룹을 생성 ResourceTypeFilters해야 합니다.

- 유형: String

- 패턴 허용: `^$|^[a-zA-Z0-9_-]{1,128}$`

- 기본값: ""

- TagFilters(조건부):
 - 설명: (조건부) AWS 리소스에 연결된 태그와 비교되는 키/값(문자열/문자열 목록) 페어 목록입니다. 이 파라미터는 기존 ResourceGroupName 또는를 지정하지 않은 경우 새 AWS 리소스 그룹을 생성하는 데 사용됩니다AppRegistryApplication.
 - 유형: StringMap
- ResourceTypeFilters(조건부):
 - 설명: (조건부) Resource Groups에서 지원하는 리소스 유형 목록입니다.
 - 유형: StringList
 - 최대 항목: 10
 - 기본값: AWS::AllSupported
- InstallServiceLinkedRole(선택 사항):
 - 설명: (선택 사항) Yes를 선택하여 AWSServiceRoleForHealth_EventProcessor 서비스 연결 역할(SLR)을 설치합니다.
 - 유형: String
 - 허용된 값: [Yes, No]
 - 기본값: No
- CreateApplicationInsights(선택 사항):
 - 설명: (선택 사항) Amazon CloudWatch Application Insights 리소스 그룹 기반 애플리케이션을 생성Yes하려면 선택합니다.
 - 유형: String
 - 허용된 값: [Yes, No]
 - 기본값: No
- ComplianceAndRegulatoryRequirements(필수):
 - 설명: (필수)이 워크로드에 적용되는 규정 준수 및/또는 규제 요구 사항과 인시던트 AWS 발생 후에서 필요한 모든 조치입니다.
 - 유형: String
 - 패턴 허용: `^[a-zA-Z0-9.:;,\-\_&() ]{1,1024}$`
- NonAWSComponents(선택 사항):
 - 설명: (선택 사항)이 워크로드에 대한 온프레미스 또는 비AWS 구성 요소를 자세히 설명하시겠습니까? 그렇다면 해당 함수는 무엇이고 어떤 함수를 수행하나요?

- 패턴 허용: `^$|^[a-zA-Z0-9.~;,\-_\&() ]{1,1024}$`
 - 기본값: ""
 - UpstreamDownstreamDependencies(선택 사항):
 - 설명: (선택 사항) 온보딩되지 않은 업스트림/다운스트림 구성 요소의 세부 정보로, 중단이 발생할 경우 이 워크로드에 영향을 미칠 수 있습니다.
 - 유형: String
 - 패턴 허용: `^$|^[a-zA-Z0-9.~;,\-_\&() ]{1,1024}$`
 - 기본값: ""
 - FailoverDisasterRecoveryPlan(선택 사항):
 - 설명: (선택 사항) AZ 및 리전 수준에서 수동 또는 자동 장애 조치/재해 복구 계획에 대한 세부 정보를 제공합니다.
 - 유형: String
 - 패턴 허용: `^$|^[a-zA-Z0-9.~;,\-_\&() ]{1,1024}$`
 - 기본값: ""
 - BridgeDetails(선택 사항):
 - 설명: (선택 사항) 회사에서 설정한 정적 인시던트/위기 관리 브리지입니다. 비정적 브리지를 사용하는 경우 원하는 애플리케이션을 지정하면 인시던트 발생 시 AWS 에서 이러한 세부 정보를 요청합니다.
 - 유형: String
 - 허용되는 값: [Amazon Chime bridge, Non-Static bridge, Static bridge]
 - 기본값: Amazon Chime bridge
 - SubscriptionStartDate(필수):
 - 설명: (필수) AWS Incident Detection and Response 구독을 시작하려는 YYYY-MM-DD 형식의 날짜입니다.
 - 유형: String
 - 패턴 허용: `^(202[4-9]|20[3-9][0-9])-(0[1-9]|1[0-2])-(0[1-9]|[12][0-9]|3[01])$`
4. 실행을 선택합니다.
 5. 자동화가 시작됩니다.
 6. 문서는 다음 단계를 수행합니다.

현재 AWS 계정 지원 플랜이 Enterprise인지 확인합니다. 그렇지 않으면 자동화가 종료됩니다.

- BranchOnResourceGroup:

기존 AWS 리소스 그룹이 제공되었는지 여부에 대한 자동화를 분기합니다. 제공되지 않으면 자동화가 새 AWS 리소스 그룹을 생성합니다.

- GetAppRegistryApplication:

제공된 경우 AWS Service Catalog AppRegistry 애플리케이션에 대한 메타데이터 정보를 가져옵니다.

- GenerateResourceGroupTemplate:

지정된 태그 필터를 사용하여 AWS 리소스 그룹에 대한 AWS CloudFormation 템플릿을 생성합니다.

- CreateResourceGroup:

를 사용하여 새 AWS 리소스 그룹을 생성합니다 AWS CloudFormation.

- TagResourceGroup:

AWS Incident Detection and Response(IDR) 필수 태그로 리소스 그룹에 태그를 지정합니다.

- InstallServiceLinkedRole:

요청 시 AWS Incident Detection and Response(IDR) 서비스 연결 역할을 설치합니다.

- CreateApplicationInsightsApplication:

요청 시 Amazon CloudWatch Application Insights 애플리케이션을 생성합니다.

- CreateAwsSupportCase:

AWS 인시던트 감지 및 대응을 사용하여 AWS 지원 사례를 생성합니다.

7. 완료 후 출력 섹션에서 실행의 자세한 결과를 검토합니다.

참조

Systems Manager Automation

- [이 자동화 실행\(콘솔\)](#)
- [자동화 실행](#)
- [Automation 설정](#)

- [자동화 워크플로 지원](#)
- [AWS 인시던트 감지 및 대응 시작하기](#)
- [인시던트 감지 및 대응의 워크로드 검색](#)

Amazon Kinesis Data Streams

AWS Systems Manager Automation은 Amazon Kinesis Data Streams에 사전 정의된 실행서를 제공합니다. 실행서에 대한 자세한 내용은 [실행서 작업](#)을 참조하세요. 실행서 콘텐츠를 보는 방법에 대한 자세한 내용은 [실행서 콘텐츠 보기](#)(을)를 참조하세요.

주제

- [AWS-EnableKinesisStreamEncryption](#)

AWS-EnableKinesisStreamEncryption

설명

AWS-EnableKinesisStreamEncryption 실행서는 Amazon Kinesis Data Streams(Kinesis Data Streams)에서 암호화를 활성화합니다. 암호화된 스트림에 쓰는 생산자 애플리케이션은 AWS Key Management Service (AWS KMS) 키에 액세스할 수 없는 경우 오류가 발생합니다.

[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.

- KinesisStreamName

유형: 문자열

설명: (필수) 암호화를 활성화하려는 스트림의 이름입니다.

- KeyId

유형: 문자열

기본값: alias/aws/kinesis

설명: (필수) 암호화에 사용할 고객 관리형 AWS KMS 키입니다. 이 값은 전역 고유 식별자, 별칭 또는 키에 대한 ARN 또는 "alias/" 접두사가 붙은 별칭 이름일 수 있습니다. 파라미터의 기본값을 사용하여 AWS 관리형 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 Data Streams의 상태를 확인합니다.
- EnableKinesisStreamEncryption(aws:executeAwsApi) - Kinesis Data Streams에 대한 암호화를 활성화합니다.

- `VerifyKinesisStreamUpdateComplete(aws:waitForAwsResourceProperty)` - Kinesis Data Streams 상태가 `로` 돌아갈 때까지 기다립니다 `ACTIVE`.
- `VerifyKinesisStreamEncryption(aws:assertAwsResourceProperty)` - Kinesis Data Streams에 암호화가 활성화되어 있는지 확인합니다.

AWS KMS

AWS Systems Manager 자동화에는 대한 사전 정의된 실행서를 제공합니다 AWS Key Management Service. 실행서에 대한 자세한 내용은 [실행서 작업](#)을 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

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.

- 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 키에 대한 자동 키 교체를 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.

- 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 자동화하는에 대한 사전 정의된 실행서를 제공합니다 AWS Lambda. 실행서에 대한 자세한 내용은 [실행서 작업](#)을 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 실행서는 FunctionName 파라미터에서 지정한 AWS Lambda 함수에 대한 AWS X-Ray 라이브 추적을 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.

- FunctionName

유형: 문자열

설명: (필수) 추적을 활성화하는 Lambda 함수의 이름 또는 ARN입니다.

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

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.

- 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 () 고객 관리형 키를 사용하여 지정하는 AWS Lambda (Lambda AWS Key Management Service AWS KMS) 함수의 환경 변수를 저장 시 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

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.

- FunctionName

유형: 문자열

설명: (필수) 환경 변수를 암호화하려는 Lambda 함수의 이름 또는 ARN입니다.

- KMSKeyArn

유형: 문자열

설명: (필수) Lambda 함수의 환경 변수를 암호화하는 데 사용할 AWS KMS 고객 관리형 키의 ARN입니다.

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 AWS Lambda (Lambda) 함수를 Amazon Virtual Private Cloud(Amazon VPC)로 이동시킵니다.

[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.

- FunctionName

유형: 문자열

설명: (필수) Amazon VPC로 이동시킬 Lambda 함수의 이름입니다.

- SecurityGroupIds

유형: 문자열

설명: (필수) Lambda 함수와 연결된 탄력적 네트워크 인터페이스(ENI)를 할당하려는 보안 그룹 ID입니다.

- SubnetIds

유형: 문자열

설명: (필수) Lambda 함수와 연결된 탄력적 네트워크 인터페이스(ENI)를 생성하려는 서브넷 ID입니다.

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 지정하는 Lambda 함수의 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

AWSSupport-TroubleshootLambdaS3Event 실행서는 AWS 지식 센터 문서 [내 Amazon S3 이벤트 알림이 Lambda 함수를 트리거하지 않는 이유는 무엇입니까?](#)에 설명된 절차에 대한 자동화된 솔루션을 제공합니다. 및 [Lambda 함수를 트리거하는 Amazon S3 이벤트 알림을 생성할 때 “다음 대상 구성을 검증할 수 없음” 오류가 발생하는 이유는 무엇입니까?](#) 이 실행서는 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 조정](#)을 참조하세요.

Note

잘못된 Amazon Simple Notification Service(Amazon SNS) 및 Amazon Simple Queue Service(Amazon SQS) Amazon S3 이벤트 구성으로 인해 “다음 대상 구성의 유효성을 검사할 수 없습니다.” 오류가 발생할 수도 있습니다. 이 실행서는 Lambda 함수 구성만 검사합니다. 실행서를 사용한 후에도 “다음 대상 구성의 유효성을 검사할 수 없습니다” 오류가 계속 표시되면 기존 Amazon SNS 및 Amazon SQS Amazon S3 이벤트 구성을 검토하십시오.

[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.

- LambdaFunctionArn

유형: 문자열

설명: (필수) Lambda 함수의 ARN입니다.

- 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 Troubleshoot인 경우:

- `aws:executeAutomation` - `AWSSupport-TroubleshootLambdaS3Event` 실행서를 실행합니다.
- `aws:executeAwsApi` - 이전 단계에서 실행한 `AWSSupport-TroubleshootLambdaS3Event` 실행서의 출력을 확인합니다.

지정된 값이 Remediate인 경우:

- `aws:executeScript` - 스크립트를 실행하여 [Amazon S3 이벤트 알림이 Lambda 함수를 트리거하지 않는 이유는 무엇입니까?](#) 및 [Lambda 함수를 트리거하는 Amazon S3 이벤트를 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 VPC)에서 시작된 AWS Lambda 함수의 인터넷 액세스 문제를 해결하는 데 도움이 됩니다.

니다. 서브넷 경로, 보안 그룹 규칙, 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

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.

- 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 VPC의 다양한 리소스 구성을 확인합니다.
- `aws:branch` - 지정된 Lambda 함수가 VPC에 있는지 여부를 기반으로 분기합니다.
- `aws:executeScript` - Lambda 함수가 시작된 서브넷의 라우팅 테이블 경로를 검토하고 Network Address Translation(NAT) 게이트웨이 및 인터넷 게이트웨이로 가는 경로가 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` - `destinationIp` 및 `destinationPort` 파라미터에 대해 지정된 값을 기반으로 Lambda 함수의 서브넷과 연결된 ACL 규칙 및 NAT 게이트웨이가 아웃바운드 인터넷 액세스를 허용하는지 확인합니다.

출력

`checkVpc.vpc` - Lambda 함수가 시작된 VPC의 ID입니다.

`checkVpc.subnet` - Lambda 함수가 시작된 서브넷의 ID입니다.

`checkVpc.securityGroups` - Lambda 함수와 연결된 보안 그룹입니다.

`checkNACL.NACL` - 리소스 이름이 포함된 분석 메시지. `LambdaIp`는 Lambda 함수의 탄력적 네트워크 인터페이스의 프라이빗 IP 주소를 나타냅니다. `LambdaIpRules` 객체는 NAT 게이트웨이로 연결되는 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 / destination port in Ingress rule",
    "LambdaIpRules":{
      "{LambdaIp}":{
        "Egress":"notAllowed",
        "Ingress":"notAllowed",
        "Analysis":"This is a NAT subnet NACL. It does not have ingress or egress
rule allowed in it for Lambda's corresponding private ip {LambdaIp} Please allow this
IP in your egress and ingress NACL rules"
      }
    }
  },
  "subnet-0987654321":{
    "NACL":"acl-0987654321",
    "destinationIp_Egress":"Allowed",
    "destinationIp_Ingress":"notAllowed",
    "Analysis":"This NACL has an allow rule for Egress traffic but there is no
Ingress rule. Please allow the destination IP / destination port in Ingress rule"
  }
}
```

checkSecurityGroups.secgrps - 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 연결된 VPC의 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

AWSSupport-TroubleshootLambdaS3Event 실행서는 AWS 지식 센터 문서 내 [Amazon S3 이벤트 알림이 Lambda 함수를 트리거하지 않는 이유는 무엇입니까?](#)에 설명된 절차에 대한 자동화된 솔루션을 제공합니다. 및 [Lambda 함수를 트리거하는 Amazon S3 이벤트 알림을 생성할 때 “다음 대상 구성을 검증할 수 없음” 오류가 발생하는 이유는 무엇입니까?](#) 이 실행서는 Amazon Simple Storage Service(Amazon S3) 이벤트 알림이 지정한 AWS Lambda 함수를 트리거하지 못한 이유를 식별하는데 도움이 됩니다. 실행서 출력에서 Lambda 함수 동시성의 유효성을 검사하고 구성하도록 제안하는 경우, [비동기 호출](#) 및 [AWS Lambda 함수 크기 조정](#)을 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.

- LambdaFunctionArn

유형: 문자열

설명: (필수) Amazon S3 이벤트 알림이 트리거하는 Lambda 함수의 ARN입니다.

- 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 필요한 권한이 정책에서 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 Automation은 Amazon Managed Workflows for Apache Airflow에 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

- [AWSSupport-TroubleshootMWAAEnvironmentCreation](#)

AWSSupport-TroubleshootMWAAEnvironmentCreation

설명

AWSSupport-TroubleshootMWAAEnvironmentCreation 실행서는 Amazon Managed Workflows for Apache Airflow(Amazon MWAA) 환경 생성 문제를 디버깅하고 오류를 식별하는 데 도움이 되도록 문서화된 이유와 함께 검사를 수행하는 정보를 제공합니다.

어떻게 작동하나요?

실행서는 다음 단계를 수행합니다.

- Amazon MWAA 환경의 세부 정보를 검색합니다.
- 실행 역할 권한을 확인합니다.
- 환경에 로깅에 제공된 AWS KMS 키를 사용할 수 있는 권한이 있는지, 필요한 CloudWatch 로그 그룹이 있는지 확인합니다.
- 제공된 로그 그룹의 로그를 구문 분석하여 오류를 찾습니다.
- 네트워크 구성을 확인하여 Amazon MWAA 환경에 필요한 엔드포인트에 대한 액세스 권한이 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 Manager [AWSSupport-TroubleshootMWAAEnvironmentCreation](#)의 문서로 이동합니다.
2. Execute automation(자동화 실행)을 선택합니다.
3. 입력 파라미터에 다음을 입력합니다.
 - AutomationAssumeRole(선택 사항):

Systems Manager Automation이 사용자를 대신하여 작업을 수행하도록 허용하는 (IAM) 역할의 Amazon 리소스 이름 AWS AWS Identity and Access Management (ARN)입니다. 역할이 지정되지 않은 경우 Systems Manager Automation은 이 실행서를 시작하는 사용자의 권한을 사용합니다.

- EnvironmentName(필수):

평가하려는 Amazon MWAA 환경의 이름입니다.

Input parameters	
AutomationAssumeRole (Optional) The Amazon Resource Name (ARN) of the AWS Identity and Access Management (IAM) role that allows Systems Manager Automation to perform the actions on your behalf. If no role is specified, Systems Manager Automation uses the permissions of the user that starts this runbook.	EnvironmentName (Required) Name of the MWAA environment you wish to evaluate.

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

- **GetMWAAEnvironmentDetails:**

Amazon MWAA 환경의 세부 정보를 검색합니다. 이 단계가 실패하면 자동화 프로세스가 중지되고 로 표시됩니다Failed.

- **CheckIAMPermissionsOnExecutionRole:**

실행 역할에 Amazon MWAA, Amazon S3, CloudWatch Logs, CloudWatch 및 Amazon SQS 리소스에 필요한 권한이 있는지 확인합니다. 고객 관리형 AWS Key Management Service (AWS KMS) 키를 감지하면 자동화는 키의 필수 권한을 검증합니다. 이 단계에서는 `iam:SimulateCustomPolicy` API를 사용하여 자동화 실행 역할이 필요한 모든 권한을 충족하는지 확인합니다.

- **CheckKMSPolicyOnKMSKey:**

AWS KMS 키 정책이 Amazon MWAA 환경에서 CloudWatch Logs 암호화에 키를 사용하도록 허용하는지 확인합니다. AWS KMS 키가 AWS관리형이면 자동화는 이 검사를 건너뜁니다.

- **CheckIfRequiredLogGroupsExists:**

Amazon MWAA 환경에 필요한 CloudWatch 로그 그룹이 있는지 확인합니다. 그렇지 않은 경우 자동화는 CloudTrail에서 CreateLogGroup 및 DeleteLogGroup 이벤트를 확인합니다. 이 단계에서는 CreateLogGroup 이벤트도 확인합니다.

- **BranchOnLogGroupsFindings:**

Amazon MWAA 환경과 관련된 CloudWatch 로그 그룹의 존재 여부에 따라 분기합니다. 하나 이상의 로그 그룹이 있는 경우 자동화는 이를 구문 분석하여 오류를 찾습니다. 로그 그룹이 없는 경우 자동화는 다음 단계를 건너뜁니다.

- **CheckForErrorsInLogGroups:**

CloudWatch 로그 그룹을 구문 분석하여 오류를 찾습니다.

- **GetRequiredEndpointsDetails:**

Amazon MWAA 환경에서 사용하는 서비스 엔드포인트를 검색합니다.

- **CheckNetworkConfiguration:**

Amazon MWAA 환경의 네트워크 구성이 보안 그룹, 네트워크 ACLs, 서브넷 및 라우팅 테이블 구성에 대한 검사를 포함하여 요구 사항을 충족하는지 확인합니다.

- **CheckEndpointsConnectivity:**

AWSsupport-ConnectivityTroubleshooter 하위 자동화를 호출하여 필요한 엔드포인트에 대한 Amazon MWAA의 연결을 검증합니다.

- **CheckS3BlockPublicAccess:**

Amazon MWAA 환경의 Amazon S3 버킷이 Block Public Access 활성화되었는지 확인하고 계정의 전체 Amazon S3 퍼블릭 액세스 차단 설정을 검토합니다.

- **GenerateReport:**

자동화에서 정보를 수집하고 각 단계의 결과 또는 출력을 인쇄합니다.

7. 완료되면 출력 섹션에서 실행의 자세한 결과를 검토합니다.

- **Amazon MWAA 환경 실행 역할 권한 확인.**

실행 역할에 Amazon MWAA, Amazon S3, CloudWatch Logs, CloudWatch 및 Amazon SQS 리소스에 필요한 권한이 있는지 확인합니다. 고객 관리형 AWS KMS 키가 감지되면 자동화는 키의 필수 권한을 검증합니다.

- Amazon MWAA 환경 AWS KMS 키 정책 확인:

실행 역할에 Amazon MWAA, Amazon S3, CloudWatch Logs, CloudWatch 및 Amazon SQS 리소스에 필요한 권한이 있는지 확인합니다. 또한 고객 관리형 AWS KMS 키가 감지되면 자동화는 키의 필수 권한을 확인합니다.

- Amazon MWAA 환경 CloudWatch 로그 그룹 확인:

Amazon MWAA 환경에 필요한 CloudWatch 로그 그룹이 있는지 확인합니다. 그렇지 않은 경우 자동화는 CloudTrail을 확인하여 CreateLogGroup 및 DeleteLogGroup 이벤트를 찾습니다.

- Amazon MWAA 환경 라우팅 테이블 확인:

Amazon MWAA 환경의 Amazon VPC 라우팅 테이블이 제대로 구성되었는지 확인합니다.

- Amazon MWAA 환경 보안 그룹 확인:

Amazon MWAA 환경 Amazon VPC 보안 그룹이 올바르게 구성되어 있는지 확인합니다.

- Amazon MWAA 환경 네트워크 ACLs 확인:

Amazon MWAA 환경의 Amazon VPC 보안 그룹이 올바르게 구성되었는지 확인합니다.

- Amazon MWAA 환경 서브넷 확인:

Amazon MWAA 환경의 서브넷이 프라이빗인지 확인합니다.

- Amazon MWAA 환경 필수 엔드포인트 연결 확인:

Amazon MWAA 환경이 필요한 엔드포인트에 액세스할 수 있는지 확인합니다. 이를 위해 자동화는 AWSsupport-ConnectivityTroubleshooter 자동화를 호출합니다.

- Amazon MWAA 환경 Amazon 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 확인합니다.

Amazon MWAA 환경의 기존 CloudWatch 로그 그룹을 구문 분석하여 오류를 찾습니다.

▼ Outputs

GenerateReportAutomationReport
Troubleshooting report for MWAA environment

🔍 The automation found no issues with the MWAA environment configuration ✓

🔍 Checking the MWAA environment execution role permissions
All the required permissions for the MWAA environment execution role are in place ✓

🔍 Checking the MWAA environment KMS key policy
KMS key is an AWS managed key ✓

🔍 Checking the MWAA environment CloudWatch logs groups
The number of CloudWatch log groups found is 5 and the number of enabled log groups for the MWAA environment is 5. This suggests that all log groups were created successfully ✓

🔍 Checking the MWAA environment Route Tables
NAT GW has Internet route: subnet- → nat- → igw- ✓
NAT GW has Internet route: subnet- → nat- → igw- ✓

🔍 Checking the MWAA environment Security Groups
Security group has self-referencing rules for all traffic. ✓

🔍 Checking the MWAA environment Network ACLs
NACL: allows port 5432 on egress ✓ and allows port 5432 on ingress ✓

🔍 Checking the MWAA environment Subnets
Subnet: subnet- is private ✓
Subnet: subnet- is private ✓

🔍 Checking the MWAA environment required endpoints connectivity

✓ Testing connectivity with sqs.eu-west-1.amazonaws.com:
Connectivity test between ENI- and sqs.eu-west-1.amazonaws.com on port 443 was successful, this means that the MWAA environment has access to the sqs.eu-west-1.amazonaws.com service ✓
To check the SSM automation execution click here: https://eu-west-1.console.aws.amazon.com/systems-manager/automation/execution- region=eu-west-1

✓ Testing connectivity with api.ecr.eu-west-1.amazonaws.com:
Connectivity test between ENI- and api.ecr.eu-west-1.amazonaws.com on port 443 was successful, this means that the MWAA environment has access to the api.ecr.eu-west-1.amazonaws.com service ✓
To check the SSM automation execution click here: https://eu-west-1.console.aws.amazon.com/systems-manager/automation/execution- region=eu-west-1

✓ Testing connectivity with monitoring.eu-west-1.amazonaws.com:
Connectivity test between ENI- and monitoring.eu-west-1.amazonaws.com on port 443 was successful, this means that the MWAA environment has access to the monitoring.eu-west-1.amazonaws.com service ✓
To check the SSM automation execution click here: https://eu-west-1.console.aws.amazon.com/systems-manager/automation/execution- region=eu-west-1

✓ Testing connectivity with kms.eu-west-1.amazonaws.com:
Connectivity test between ENI- and kms.eu-west-1.amazonaws.com on port 443 was successful, this means that the MWAA environment has access to the kms.eu-west-1.amazonaws.com service ✓
To check the SSM automation execution click here: https://eu-west-1.console.aws.amazon.com/systems-manager/automation/execution- region=eu-west-1

✓ Testing connectivity with s3.eu-west-1.amazonaws.com:
Connectivity test between ENI- and s3.eu-west-1.amazonaws.com on port 443 was successful, this means that the MWAA environment has access to the s3.eu-west-1.amazonaws.com service ✓
To check the SSM automation execution click here: https://eu-west-1.console.aws.amazon.com/systems-manager/automation/execution- region=eu-west-1

✓ Testing connectivity with env.airflow.eu-west-1.amazonaws.com:
Connectivity test between ENI- and env.airflow.eu-west-1.amazonaws.com on port 443 was successful, this means that the MWAA environment has access to the env.airflow.eu-west-1.amazonaws.com service ✓
To check the SSM automation execution click here: https://eu-west-1.console.aws.amazon.com/systems-manager/automation/execution- region=eu-west-1

✓ Testing connectivity with env.airflow.eu-west-1.amazonaws.com:
Connectivity test between ENI- and env.airflow.eu-west-1.amazonaws.com on port 5432 was successful, this means that the MWAA environment has access to the env.airflow.eu-west-1.amazonaws.com service ✓
To check the SSM automation execution click here: https://eu-west-1.console.aws.amazon.com/systems-manager/automation/execution- region=eu-west-1

✓ Testing connectivity with api.airflow.eu-west-1.amazonaws.com:
Connectivity test between ENI- and api.airflow.eu-west-1.amazonaws.com on port 443 was successful, this means that the MWAA environment has access to the api.airflow.eu-west-1.amazonaws.com service ✓
To check the SSM automation execution click here: https://eu-west-1.console.aws.amazon.com/systems-manager/automation/execution- region=eu-west-1

✓ Testing connectivity with logs.eu-west-1.amazonaws.com:
Connectivity test between ENI- and logs.eu-west-1.amazonaws.com on port 443 was successful, this means that the MWAA environment has access to the logs.eu-west-1.amazonaws.com service ✓
To check the SSM automation execution click here: https://eu-west-1.console.aws.amazon.com/systems-manager/automation/execution- region=eu-west-1

✓ Testing connectivity with ops.airflow.eu-west-1.amazonaws.com:
Connectivity test between ENI- and ops.airflow.eu-west-1.amazonaws.com on port 443 was successful, this means that the MWAA environment has access to the ops.airflow.eu-west-1.amazonaws.com service ✓
To check the SSM automation execution click here: https://eu-west-1.console.aws.amazon.com/systems-manager/automation/execution- region=eu-west-1

🔍 Checking the MWAA environment S3 bucket
Environment's S3 bucket and/or account block public access ✓

🔍 Checking the MWAA environment CloudWatch logs groups errors

Parsed log group	DAGProcessing - no errors found ✓
Parsed log group	Scheduler - no errors found ✓
Parsed log group	Task - no errors found ✓
Parsed log group	WebServer - no errors found ✓
Parsed log group	Worker - no errors found ✓

참조

Systems Manager Automation

- [이 자동화 실행\(콘솔\)](#)
- [자동화 실행](#)
- [Automation 설정](#)
- [Support Automation Workflows 랜딩 페이지](#)

Neptune

AWS Systems Manager 자동화는 Amazon Neptune에 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 실행서는 Amazon Neptune DB 클러스터에 대한 감사 로그를 Amazon CloudWatch Logs로 전송하는 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.

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

- `DbClusterResourceId`

유형: 문자열

설명: (필수) 감사 로그를 활성화하려는 Neptune DB 클러스터의 리소스 ID입니다.

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`.
- `EnableNeptuneDbAuditLogs(aws:executeAwsApi)` - CloudWatch Logs를 전송할 Neptune DB 클러스터에 대한 감사 로그를 활성화합니다.
- `VerifyNeptuneDbStatus(aws:waitAwsResourceProperty)` - Neptune DB 클러스터 상태가 인지 확인합니다 `available`.
- `VerifyNeptuneDbAuditLogs(aws:executeScript)` - 감사 로그가 CloudWatch Logs로 전송되도록 성공적으로 구성되었는지 확인합니다.

AWS-EnableNeptuneDbBackupRetentionPeriod

설명

AWS-EnableNeptuneDbBackupRetentionPeriod 실행서는 Amazon Neptune DB 클러스터의 백업 보존 기간이 7~35일인 자동 백업을 활성화하는 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.

- DbClusterResourceId

유형: 문자열

설명: (필수) 백업을 활성화하려는 Neptune DB 클러스터의 리소스 ID입니다.

- BackupRetentionPeriod

유형: 정수

유효한 값: 7~35

설명: (필수) 백업이 유지되는 일수입니다.

- PreferredBackupWindow

유형: 문자열

설명: (선택 사항) 백업이 수행되는 최소 30분의 일일 기간입니다. 값은 UTC(Universal Time Coordinated)여야 하며 형식을 사용해야 합니다 hh24:mm-hh24:mm. 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 확인합니다neptune.
- VerifyNeptuneDbStatus(aws:waitAwsResourceProperty) - Neptune DB 클러스터 상태가 인지 확인합니다available.
- ModifyNeptuneDbRetentionPeriod(aws:executeAwsApi) - Neptune DB 클러스터의 보존 기간을 설정합니다.
- VerifyNeptuneDbBackupsEnabled(aws:executeScript) - 보존 기간과 백업 기간이 성공적으로 설정되었는지 확인합니다.

AWS-EnableNeptuneClusterDeletionProtection

설명

AWS-EnableNeptuneClusterDeletionProtection 실행서는 지정한 Amazon Neptune 클러스터에 대한 삭제 보호를 활성화합니다.

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.

- DbClusterResourceId

유형: 문자열

설명: (필수) 삭제 방지를 활성화하려는 Neptune 클러스터의 ID입니다.

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)` - 지정된 DB 클러스터의 엔진 유형이 인지 확인합니다neptune.
- `VerifyNeptuneStatus(aws:waitForAwsResourceProperty)` - 클러스터의 상태가 인지 확인합니다available.
- `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 Automation은 Amazon Relational Database Service에 대한 사전 정의된 실행서를 제공합니다. 실행서에 대한 자세한 내용은 [실행서 작업](#)을 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-EnableMinorVersionUpgradeOnRDSDBInstance](#)

- [AWSConfigRemediation-EnableMultiAZOnRDSInstance](#)
- [AWSConfigRemediation-EnablePerformanceInsightsOnRDSInstance](#)
- [AWSConfigRemediation-EnableRDSClusterDeletionProtection](#)
- [AWSConfigRemediation-EnableRDSInstanceBackup](#)
- [AWSConfigRemediation-EnableRDSInstanceDeletionProtection](#)
- [AWSConfigRemediation-ModifyRDSInstancePortNumber](#)
- [AWSSupport-ModifyRDSSnapshotPermission](#)
- [AWSPremiumSupport-PostgreSQLWorkloadReview](#)
- [AWS-RebootRdsInstance](#)
- [AWSSupport-ShareRDSSnapshot](#)
- [AWS-StartRdsInstance](#)
- [AWS-StartStopAuroraCluster](#)
- [AWS-StopRdsInstance](#)
- [AWSSupport-TroubleshootConnectivityToRDS](#)
- [AWSSupport-TroubleshootRDSIAMAuthentication](#)
- [AWSSupport-ValidateRdsNetworkConfiguration](#)

AWS-CreateEncryptedRdsSnapshot

설명

AWS-CreateEncryptedRdsSnapshot 실행서는 암호화되지 않은 Amazon Relational Database Service(RDS) 인스턴스에서 암호화된 스냅샷을 생성합니다.

[이 자동화 실행\(콘솔\)](#)

문서 유형

자동화

소유자

Amazon

플랫폼

데이터베이스 수

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.

- 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 *DBInstanceIdentifier-yyyymmddhhmmss###*.

- EncryptedDBSnapshotIdentifier

유형: 문자열

설명: (선택 사항) 암호화된 스냅샷의 이름입니다. 기본 이름은에 추가된 DBSnapshotIdentifier 파라미터에 대해 지정하는 값입니다-encrypted.

- 인스턴스 태그

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 ARN, 키 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 지정하는 DB 인스턴스의 스냅샷을 생성합니다.
- aws:executeScript - 이전 단계에서 생성된 스냅샷이 존재하고 인지 확인합니다available.
- aws:executeScript - 이전에 생성한 스냅샷을 암호화된 스냅샷에 복사합니다.
- aws:executeScript - 이전 단계에서 생성된 암호화된 스냅샷이 존재하는지 확인합니다.

출력

CopyRdsSnapshotToEncryptedRdsSnapshot.EncryptedSnapshotId - 암호화된 Amazon RDS 스냅샷의 ID입니다.

AWS-CreateRdsSnapshot

설명

Amazon RDS 인스턴스용 Amazon Relational Database Service(Amazon RDS) 스냅샷을 생성합니다.

이 자동화 실행(콘솔)

문서 유형

자동화

소유자

Amazon

플랫폼

데이터베이스 수

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.

- DBInstanceIdentifier

유형: 문자열

설명: (필수) 스냅샷을 생성할 RDS 인스턴스의 DBInstanceID ID입니다.

- DBSnapshotIdentifier

유형: 문자열

설명: (선택 사항) 생성할 RDS 스냅샷의 DBSnapshotIdentifier ID입니다.

- 인스턴스 태그

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 생성한 스냅샷이 존재하는지 확인합니다.

출력

createRDSSnapshot.SnapshotId – 생성된 스냅샷의 ID입니다.

AWSConfigRemediation-DeleteRDSCluster

설명

AWSConfigRemediation-DeleteRDSCluster 실행서는 지정한 Amazon Relational Database Service(RDS) 클러스터를 삭제합니다.이 자동화를 AWS 리전 실행하는에서 활성화해야 AWS Config 합니다.

[이 자동화 실행\(콘솔\)](#)

문서 유형

자동화

소유자

Amazon

플랫폼

데이터베이스 수

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.

- 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 특정 Amazon Relational Database Service(Amazon RDS) 클러스터 스냅샷을 삭제합니다.

[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.

- DBClusterSnapshotId

유형: 문자열

설명: (필수) 삭제해야 하는 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) 클러스터 스냅샷 식별자를 사용하여 특정 Amazon RDS 클러스터 스냅샷을 삭제합니다.
- aws:executeScript - 특정 Amazon RDS 클러스터 스냅샷이 삭제되었는지 확인합니다.

AWSConfigRemediation-DeleteRDSInstance

설명

AWSConfigRemediation-DeleteRDSInstance 실행서는 지정하는 Amazon Relational Database Service(Amazon RDS) 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

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.

- DbiResourceId

유형: 문자열

설명: (필수) 삭제하려는 DB 인스턴스의 리소스 식별자입니다.

- SkipFinalSnapshot

유형: Boolean

기본값: false

설명: (선택 사항) true로 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 - DbResourceId 파라미터에서 지정하는 값에서 DB 인스턴스 이름을 수집합니다.
- aws:branch - SkipFinalSnapshot 파라미터에서 지정하는 값을 기반으로 분기합니다.
- aws:executeAwsApi - DbResourceId 파라미터에서 지정하는 DB 인스턴스를 삭제합니다.
- aws:executeAwsApi - 최종 스냅샷이 생성된 후, DbResourceId 파라미터에서 지정하는 DB 인스턴스를 삭제합니다.
- aws:assertAwsResourceProperty - DB 인스턴스가 삭제되었는지 확인합니다.

AWSConfigRemediation-DeleteRDSInstanceSnapshot

설명

AWSConfigRemediation-DeleteRDSInstanceSnapshot 실행서는 지정하는 Amazon Relational Database Service(Amazon RDS) 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

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.

- 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 available인지 확인합니다.

- `aws:executeAwsApi` - `DbSnapshotId` 파라미터에서 지정된 스냅샷을 삭제합니다.
- `aws:executeScript` - 스냅샷이 삭제되었는지 확인합니다.

AWSConfigRemediation-DisablePublicAccessToRDSInstance

설명

AWSConfigRemediation-DisablePublicAccessToRDSInstance 실행서는 지정하는 Amazon Relational Database Service(Amazon RDS) 데이터베이스(DB) 인스턴스에 대한 퍼블릭 액세스를 비활성화합니다.

[이 자동화 실행\(콘솔\)](#)

문서 유형

자동화

소유자

Amazon

플랫폼

데이터베이스 수

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.

- `DbResourceId`

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 지정하는 Amazon Relational Database Service(Amazon RDS) 클러스터의 CopyTagsToSnapshot 설정을 활성화합니다. 이 설정을 활성화하면 모든 태그를 DB 클러스터에서 DB 클러스터의 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

파라미터

- `ApplyImmediately`

유형: Boolean

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) 사용자를 대신하여 Systems Manager Automation을 통해 작업을 수행할 수 있도록 허용하는 AWS Identity and Access Management (IAM) 역할의 Amazon 리소스 이름(ARN)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 지정하는 Amazon Relational Database Service(Amazon RDS) 인스턴스의 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

파라미터

- `ApplyImmediately`

유형: Boolean

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) 사용자를 대신하여 Systems Manager Automation을 통해 작업을 수행할 수 있도록 허용하는 AWS Identity and Access Management (IAM) 역할의 Amazon 리소스 이름(ARN)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 지정하는 Amazon RDS 데이터베이스 인스턴스의 확장 모니터링을 활성화합니다. 확장 모니터링에 대한 자세한 내용은 Amazon RDS 사용 설명서의 [확장 모니터링](#)을 참조하세요.

[이 자동화 실행\(콘솔\)](#)

문서 유형

자동화

소유자

Amazon

플랫폼

데이터베이스 수

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.

- 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) Amazon RDS에서 Amazon CloudWatch Logs로 확장 모니터링 지표를 전송할 수 있도록 하는 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-EnableMinorVersionUpgradeOnRDSDBInstance

설명

AWSConfigRemediation-EnableMinorVersionUpgradeOnRDS 실행서는 지정하는 Amazon RDS 데이터베이스 인스턴스의 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

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.

- 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(Amazon RDS) 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

파라미터

- `ApplyImmediately`

유형: Boolean

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

- DbResourceId

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 available인지 확인합니다.
- aws:branch - DbResourceId 파라미터에서 지정하는 DB 인스턴스에 MultiAZ(이)가 이미 true로 설정되어 있는지 확인합니다.
- aws:executeAwsApi - DbResourceId 파라미터에서 지정하는 DB 인스턴스에서 MultiAZ 설정을 true로 변경합니다.
- aws:assertAwsResourceProperty - DbResourceId 파라미터에서 지정하는 DB 인스턴스에 MultiAZ(이)가 true로 설정되어 있는지 확인합니다.

AWSConfigRemediation-EnablePerformanceInsightsOnRDSInstance

설명

AWSConfigRemediation-EnablePerformanceInsightsOnRDSInstance 실행서는 지정하는 Amazon RDS DB 인스턴스에 대한 Performance Insights를 활성화합니다.

[이 자동화 실행\(콘솔\)](#)

문서 유형

자동화

소유자

Amazon

플랫폼

데이터베이스 수

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.

- DbiResourceId

유형: 문자열

설명: (필수) Performance Insights를 활성화하려는 DB 인스턴스의 리소스 식별자입니다.

- PerformanceInsightsKMSKeyId

유형: 문자열

기본값: alias/aws/rds

설명: (선택 사항) 성능 개선 도우미가 잠재적으로 민감한 모든 데이터를 암호화하는 데 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 키가 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 키의 ARN을 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(RDS) 클러스터에서 삭제 방지를 활성화합니다. 이 자동화를 실행하는 AWS 리전 에서 활성화해야 AWS Config 합니다.

[이 자동화 실행\(콘솔\)](#)

문서 유형

자동화

소유자

Amazon

플랫폼

데이터베이스 수

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.

- 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(Amazon RDS) 데이터베이스 인스턴스에 대한 백업을 지원합니다. 이 실행서는 Amazon Aurora 데이터베이스 인스턴스에 대한 백업 활성화를 지원하지 않습니다.

[이 자동화 실행\(콘솔\)](#)

문서 유형

자동화

소유자

Amazon

플랫폼

데이터베이스 수

파라미터

- `ApplyImmediately`

유형: Boolean

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) 사용자를 대신하여 Systems Manager Automation을 통해 작업을 수행할 수 있도록 허용하는 AWS Identity and Access Management (IAM) 역할의 Amazon 리소스 이름(ARN)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 일일 시간 범위(UTC)입니다.

제약 조건:

- hh24:mi-hh24:mi 형식이어야 합니다.
- 협정 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 지정하는 Amazon RDS 데이터베이스 인스턴스에 대한 삭제 보호를 지원합니다.

[이 자동화 실행\(콘솔\)](#)

문서 유형

자동화

소유자

Amazon

플랫폼

데이터베이스 수

파라미터

- ApplyImmediately

유형: Boolean

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) 사용자를 대신하여 Systems Manager Automation을 통해 작업을 수행할 수 있도록 허용하는 AWS Identity and Access Management (IAM) 역할의 Amazon 리소스 이름(ARN)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(Amazon RDS) 인스턴스가 연결을 허용하는 포트 번호를 수정합니다. 이 자동화를 실행하면 데이터베이스가 다시 시작됩니다.

[이 자동화 실행\(콘솔\)](#)

문서 유형

자동화

소유자

Amazon

플랫폼

데이터베이스 수

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.

- 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-ModifyRDSnapshotPermission

설명

AWSSupport-ModifyRDSnapshotPermission 실행서는 여러 Amazon Relational Database Service(Amazon RDS) 스냅샷에 대한 권한을 수정하는 데 도움이 됩니다. 이 실행서를 사용하여 Public 또는 Private 스냅샷을 만들거나 다른 AWS 계정과 공유할 수 있습니다. 기본 KMS 키로 암호화된 스냅샷은 이 실행서를 사용하는 다른 계정과 공유할 수 없습니다.

[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.

- AccountIds

유형: StringList

기본값: 없음

설명: (선택 사항) 스냅샷을 공유하려는 계정의 ID입니다. 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.

- Private

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` 파라미터에서 제공된 스냅샷의 ID를 확인합니다. ID를 확인한 후, 스크립트는 암호화된 스냅샷을 확인하고 해당 내용이 발견된 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.Result`

`MakePrivate.Result`

`MakePrivate.Commands`

AWSPremiumSupport-PostgreSQLWorkloadReview

설명

AWSPremiumSupport-PostgreSQLWorkloadReview 실행서는 Amazon Relational Database Service(Amazon RDS) PostgreSQL 데이터베이스 사용 통계에 대한 여러 스냅샷을 캡처합니다. 캡처된 통계는 지원 [사전 대응 서비스](#) 전문가가 운영 검토를 수행하는 데 필요합니다. 통계는 일련의 사용자 지정 SQL 및 셸 스크립트를 사용하여 수집됩니다. 이러한 스크립트는 이 실행서에서 생성된 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 실행서는 AWS CloudFormation 스택을 AWS 계정 사용하여 다음 AWS 리소스를 자동으로 생성합니다. CloudFormation 콘솔을 사용하여 스택 생성을 모니터링할 수 있습니다.

- Virtual Private Cloud(VPC) 및 Amazon EC2 인스턴스는 VPC의 프라이빗 서브넷에서 시작되며 NAT 게이트웨이를 사용하여 인터넷에 선택적으로 연결할 수 있습니다.
- Secrets Manager 보안 암호 값을 검색할 수 있는 권한이 있는 임시 Amazon EC2 인스턴스에 연결된 AWS Identity and Access Management (IAM) 역할입니다. 또한 이 역할은 선택한 Amazon Simple Storage Service(Amazon S3) 버킷에 파일을 업로드하고 선택적으로 지원 사례에 파일을 업로드할 수 있는 권한을 제공합니다.
- DB 인스턴스와 임시 Amazon EC2 인스턴스 간의 연결을 허용하는 VPC 피어링 연결.
- 임시 VPC에 연결된 Systems Manager, Secrets Manager, Amazon S3 VPC 엔드포인트.
- 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 권한을 제공하는 유지 관리 기간을 위한 IAM 역할도 생성됩니다.

실행서가 완료되면 필요한 AWS 리소스를 생성하는 데 사용되는 CloudFormation 스택이 삭제되고 보고서가 선택한 Amazon S3 버킷에 업로드되고 선택적으로 지원 사례가 업로드됩니다.

Note

기본적으로, 임시 Amazon EC2 인스턴스의 루트 Amazon EBS 볼륨은 보존됩니다. EbsVolumeDeleteOnTermination 파라미터를 true로 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 실행서를 사용하기 전에 Technical Account Manager(TAM) 또는 Specialist TAM(STAM)에게 지침을 문의하십시오. 자세한 내용은 [지원 사전 대응 서비스](#)를 참조하세요.
- 계정 및 할당량이 AWS 리전 런북을 사용하는 계정 및 리전에서 생성할 수 있는 최대 Amazon EC2 인스턴스 또는 VPCs 수에 도달하지 않았는지 확인합니다. 제한 증가를 요청해야 하는 경우, [서비스 제한 증가 양식](#)을 사용하십시오.
- 데이터베이스 구성

1. DatabaseName 파라미터에서 지정하는 데이터베이스에는 pg_stat_statements 확장 프로그램이 구성되어 있어야 합니다. shared_preload_libraries에서 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 작업](#)을 참조하세요. pg_stat_statements(을)를 shared_preload_libraries에 추가하면 일부 성능 오버헤드가 추가됩니다. 하지만, 이는 개별 명령문의 성능을 추적하는 데 유용합니다. pg_stat_statements 확장에 대한 자세한 내용은 [PostgreSQL 문서](#)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 인스턴스에서 파라미터로 작업하기](#)(을)를 참조하세요.
3. track_io_timing 파라미터를 끄면 I/O 수준 통계는 운영 검토에 포함되지 않습니다. track_io_timing(을)를 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.

결제 및 요금 임시 Amazon EC2 인스턴스, 연결된 Amazon EBS 볼륨, NAT 게이트웨이 및 이 자동화가 실행되는 동안 전송된 데이터와 관련된 비용에 대해 AWS 계정 요금이 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 뷰와 함수](#)를 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. AWS TAM에 문의하여 워크로드 검토를 위한 대체 접근 방식을 논의합니다.

이 자동화에서 수집한 통계 및 메타데이터를 공유하는 데 필요한 승인 및 권한이 있는지 확인합니다 AWS.

보안 고려 사항 UpdateRdsSecurityGroup 파라미터를 yes로 설정하면 실행서에서 DB 인스턴스와 연결된 보안 그룹을 업데이트하여 임시 Amazon EC2 인스턴스의 프라이빗 IP 주소로부터 들어오는 인바운드 트래픽을 허용합니다.

UpdateRdsRouteTable 파라미터를 yes로 설정하면 실행서는 DB 인스턴스가 실행되는 서브넷과 연결된 라우팅 테이블을 업데이트하여 VPC 피어링 연결을 통해 임시 Amazon EC2 인스턴스로의 트래픽을 허용합니다.

사용자 생성 수집 스크립트가 Amazon RDS 데이터베이스에 연결되도록 하려면 통계 보기를 읽을 수 있는 권한을 가진 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_table의 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. 임시 Amazon EC2 인스턴스와 연결된 IAM 역할에 다음과 같은 권한이 추가됩니다. 또한 AmazonSSMManagedInstanceCore 관리형 정책은 IAM 역할과 연결되어 있어 Systems Manager에서 Amazon EC2 인스턴스를 관리할 수 있습니다.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": [
        "ec2:DescribeTags"
      ],
      "Resource": "*",
      "Effect": "Allow"
    },
    {
      "Action": [
        "s3:GetBucketLocation"
      ],
      "Resource": "arn:aws:s3:::amzn-s3-demo-bucket",
      "Effect": "Allow"
    },
    {
      "Action": [
        "s3:PutObject"
      ],
      "Resource": "arn:aws:s3:::amzn-s3-demo-bucket/automation-execution-  
id/*",
      "Effect": "Allow"
    },
    {
      "Action": [
        "secretsmanager:GetSecretValue"
      ],
      "Resource": "arn:aws:secretsmanager:us-  
east-1:111122223333:secret:secret-id",
      "Effect": "Allow"
    },
    {
      "Action": [
```

```

        "support:AddAttachmentsToSet",
        "support:AddCommunicationToCase",
        "support:DescribeCases"
    ],
    "Resource": "*",
    "Effect": "Allow"
}
]
}

```

이 Systems Manager Automation에 의해 임시 유지 관리 기간에 추가된 권한. 다음 권한은 Maintenance Windows 작업과 연결된 IAM 역할에 자동으로 추가됩니다. Maintenance Windows 작업은 시작 및 중지되며 임시 Amazon EC2 인스턴스로 명령을 전송합니다.

JSON

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": [
        "ssm:GetAutomationExecution",
        "ssm:ListCommands",
        "ssm:ListCommandInvocations",
        "ssm:GetCommandInvocation",
        "ssm:GetCalendarState",
        "ssm:CancelCommand",
        "ec2:DescribeInstanceStatus"
      ],
      "Resource": "*",
      "Effect": "Allow"
    },
    {
      "Action": [
        "ssm:SendCommand",
        "ec2:StartInstances",
        "ec2:StopInstances",
        "ssm:StartAutomationExecution"
      ],
      "Resource": [

```

```

        "arn:aws:ec2:us-east-1:111122223333:instance/temporary-instance-
id",
        "arn:aws:ssm:*:*:document/AWS-RunShellScript",
        "arn:aws:ssm:*:*:document/AWS-StopEC2Instance",
        "arn:aws:ssm:*:*:document/AWS-StartEC2Instance",
        "arn:aws:ssm:*:111122223333:automation-execution/*"
    ],
    "Effect": "Allow"
},
{
    "Condition": {
        "StringEquals": {
            "iam:PassedToService": "ssm.amazonaws.com"
        },
        "ArnLike": {
            "iam:AssociatedResourceARN": "arn:aws:ssm:*:*:document/AWS-*"
        }
    },
    "Action": "iam:PassRole",
    "Resource": "arn:aws:iam:*:111122223333:role/SSM-*",
    "Effect": "Allow"
}
]
}

```

[이 자동화 실행\(콘솔\)](#)

문서 유형

자동화

소유자

Amazon

플랫폼

데이터베이스 수

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.

- 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 쌍이 포함된 Secrets Manager 보안 암호의 ARN입니다. CloudFormation 스택은 이 ARN에 대한 GetSecretValue 작업 권한이 있는 IAM 정책을 생성합니다. 보안 인증은 임시 인스턴스가 데이터베이스 통계를 수집할 수 있도록 하는 데 사용됩니다. TAM 또는 STAM에 문의하여 필요한 최소 권한에 대해 논의하십시오.

- 확인

유형: 문자열

설명: (필수) 이 실행서가 계정에 임시 리소스를 생성하여 DB 인스턴스에서 통계를 수집한다는 사실을 확인하면 **yes**를 입력합니다. 이 자동화를 실행하기 전에 TAM 또는 STAM에 문의하는 것이 좋습니다.

- SupportCase

유형: 문자열

설명: (선택 사항) TAM 또는 STAM에서 제공하는 지원 사례 번호입니다. 제공된 경우, 실행서는 케이스를 업데이트하고 수집된 데이터를 첨부합니다. 이 옵션을 사용하려면 임시 Amazon EC2 인스턴스에 인터넷 연결이 있어야 지원 API 엔드포인트에 액세스할 수 있습니다. AllowVpcInternetAccess 파라미터를 true로 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 대한 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 셸 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 VPC에 대한 CIDR 표기법의 IP 주소 범위(예: 172.31.0.0/16). DB 인스턴스에 연결된 기존 VPC와 겹치거나 일치하지 않는 CIDR을 선택해야 합니다. 생성할 수 있는 최소 VPC는 /28 서브넷 마스크를 사용하고, 최대 VPC는 /16 서브넷 마스크를 사용합니다.

기본값: 172.31.0.0/16

- StackResourcesNamePrefix

유형: 문자열

설명: (선택 사항) CloudFormation 스택 리소스 이름 접두사 및 태그입니다. 실행서는 리소스에 적용된 이름 및 태그의 일부로 이 접두사를 사용하여 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 hour입니다.

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) true로 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 임시 Amazon EC2 인스턴스에 인터넷 연결을 제공하여 지원 API 엔드포인트와 통신할 수 있는 NAT 게이트웨이를 생성합니다. 실행서가 Amazon S3 버킷에 출력만 업로드하도록 하려는 경우처럼 이 파라미터를 false로 둘 수 있습니다.

유효한 값: true | false

기본값: false

- UpdateRdsSecurityGroup

유형: 문자열

설명: (선택 사항) true로 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 실행서가 CloudFormation 스택 true을 완료하고 삭제한 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 Automation 실행서 첨부 파일에서 CloudFormation 템플릿 콘텐츠를 가져옵니다 AWS 계정.
5. `aws:createStack` - CloudFormation 스택 리소스를 생성합니다.
6. `aws:waitForAwsResourceProperty` - CloudFormation 템플릿으로 생성된 Amazon EC2 인스턴스가 실행될 때까지 기다립니다.
7. `aws:executeAwsApi` - CloudFormation에서 생성한 임시 Amazon EC2 인스턴스 및 VPC 피어링 연결의 ID를 가져옵니다.
8. `aws:executeAwsApi` - DB 인스턴스와의 연결을 구성하기 위한 임시 Amazon EC2 인스턴스의 IP 주소를 가져옵니다.
9. `aws:executeAwsApi` - 임시 Amazon EC2 인스턴스에 연결된 Amazon EBS 볼륨에 태그를 지정합니다.
10. `aws:waitForAwsResourceProperty` - 임시 Amazon EC2 인스턴스가 상태 검사를 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 제한 시간이 초과된 경우 임시 Amazon EC2 인스턴스를 재부팅합니다.
 - b. `aws:waitForAwsResourceProperty` - 재부팅 후 Systems Manager에서 임시 Amazon EC2 인스턴스를 관리할 때까지 기다립니다.

- 12aws:runCommand - 메타데이터 수집기 애플리케이션 요구 사항을 임시 Amazon EC2 인스턴스에 설치합니다.
- 13aws:runCommand - 임시 Amazon EC2 인스턴스에서 구성 파일을 생성하여 DB 인스턴스에 대한 액세스를 구성합니다.
- 14aws:executeAwsApi - Run Command를 사용하여 메타데이터 수집기 애플리케이션을 정기적으로 실행할 수 있는 유지 관리 기간을 생성합니다. 유지 관리 기간은 명령 간에 인스턴스를 시작하고 중지시킵니다.
- 15aws:waitForAwsResourceProperty - CloudFormation 템플릿에서 생성한 유지 관리 기간이 준비될 때까지 기다립니다.
- 16aws:executeAwsApi -에서 생성한 유지 관리 기간 및 변경 달력의 IDs를 가져옵니다 CloudFormation.
- 17aws:sleep - 유지 관리 기간의 종료 날짜가 될 때까지 기다립니다.
- 18aws:executeAwsApi - 유지 관리 기간을 끕니다.
- 19aws:executeScript - 유지 관리 기간 동안 실행된 작업의 결과를 가져옵니다.
- 20aws:waitForAwsResourceProperty - 계속하기 전에 유지 관리 기간이 마지막 작업을 완료할 때까지 기다립니다.
- 21aws:branch - SupportCase 파라미터 값을 제공했는지 여부를 기준으로 워크플로를 분기합니다.
- a. aws:changeInstanceState - 임시 Amazon EC2 인스턴스를 시작하고 상태 확인이 통과될 때까지 기다린 후 보고서를 업로드합니다.
 - 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 제한 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 지원 케이스에 첨부합니다. 스크립트는 보고서를 5MB 파일로 압축하고 분할합니다. 스크립트가 지원 케이스에 첨부할 수 있는 최대 파일 수는 12개입니다.
- 22aws:changeInstanceState - CloudFormation 스택이 삭제되지 않는 경우 임시 Amazon EC2 인스턴스를 중지합니다.
- 23aws:executeAwsApi - 실행서가 CloudFormation 스택을 생성하거나 업데이트하지 못하는 경우 CloudFormation 스택 이벤트를 설명합니다.

24.aws:waitForAwsResourceProperty - CloudFormation 스택이 터미널 상태가 될 때까지 기다렸다가 삭제합니다.

25.aws:executeAwsApi - 유지 관리 기간을 제외한 CloudFormation 스택을 삭제합니다.

EbsVolumeDeleteOnTermination 파라미터 값이 false로 설정된 경우 임시 Amazon EC2 인스턴스와 연결된 루트 Amazon EBS 볼륨은 보존됩니다.

AWS-RebootRdsInstance

설명

AWS-RebootRdsInstance 실행서는 Amazon Relational Database Service(Amazon RDS) DB 인스턴스를 재부팅합니다(아직 재부팅되지 않은 경우).

[이 자동화 실행\(콘솔\)](#)

문서 유형

자동화

소유자

Amazon

플랫폼

데이터베이스 수

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) 재부팅하려는 Amazon RDS DB 인스턴스의 ID입니다.

문서 단계

RebootInstance - DB 인스턴스가 아직 재부팅되지 않은 경우 DB 인스턴스를 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 하나요?](#) 절차에 대한 자동화된 솔루션을 제공합니다. Amazon Relational Database Service(Amazon RDS) 스냅샷이 기본값을 사용하여 암호화된 경우 스냅샷을 공유할 AWS 관리형 키가 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 자동화는 스냅샷을 암호화하는 데 사용되는 새 AWS KMS 고객 관리형 키를 계정에 생성합니다.

[이 자동화 실행\(콘솔\)](#)

문서 유형

자동화

소유자

Amazon

플랫폼

데이터베이스 수

파라미터

- AccountIds

유형: StringList

설명: (필수) 스냅샷을 공유할 계정 ID의 쉼표로 구분된 목록입니다.

- 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.

- 데이터베이스

유형: 문자열

설명: (필수) 스냅샷을 공유하려는 Amazon RDS DB 인스턴스 또는 클러스터의 이름입니다. SnapshotName 파라미터의 값을 지정하는 경우, 이 파라미터는 선택 사항입니다.

- KMSKey

유형: 문자열

설명: (선택 사항) 스냅샷을 암호화하는 데 사용되는 AWS KMS 고객 관리형 키의 전체 Amazon 리소스 이름(ARN)입니다.

- SnapshotName

유형: 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 `AutomationAssumeRole`에서 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 변경](#)을 참조하세요.

`KMSKey` 파라미터 값을 지정하지 않은 경우 실행서를 성공적으로 시작하려면 `AutomationAssumeRole`에서 다음과 같은 추가 작업이 필요합니다.

- `kms:CreateKey`
- `kms:ScheduleKeyDeletion`
- `kms:CreateGrant`
- `kms:DescribeKey`

문서 단계

1. `aws:executeScript` - `KMSKey` 파라미터에 값이 제공되었는지 확인하고 값을 찾을 수 없는 경우 AWS KMS 고객 관리형 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 KMSKey를 사용하여 스냅샷을 복사합니다.
6. `aws:waitForAwsResourceProperty` - 스냅샷 복사 작업이 완료될 때까지 기다립니다.
7. `aws:executeAwsApi` - 새 스냅샷을 지정된 AccountIds와 공유합니다.
8. `aws:executeAwsApi` - 제공된 스냅샷이 DB 클러스터의 내용인지 확인합니다.
9. `aws:executeScript` - 콜론을 하이픈으로 대체하여 SnapshotName 파라미터의 형식을 지정합니다.
10. `aws:executeAwsApi` - 지정된 KMSKey를 사용하여 스냅샷을 복사합니다.
11. `aws:waitForAwsResourceProperty` - 스냅샷 복사 작업이 완료될 때까지 기다립니다.
12. `aws:executeAwsApi` - 새 스냅샷을 지정된 AccountIds와 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 Database의 스냅샷 목록을 검색합니다.
16. `aws:executeScript` - 이전 단계에서 조합한 목록에서 사용 가능한 최신 스냅샷을 결정합니다.
17. `aws:executeAwsApi` - 지정된 KMSKey를 사용하여 DB 인스턴스 스냅샷을 복사합니다.
18. `aws:waitForAwsResourceProperty` - 스냅샷 복사 작업이 완료될 때까지 기다립니다.
19. `aws:executeAwsApi` - 새 스냅샷을 지정된 AccountIds와 공유합니다.
20. `aws:executeAwsApi` - 지정된 Database의 스냅샷 목록을 검색합니다.
21. `aws:executeScript` - 이전 단계에서 조합한 목록에서 사용 가능한 최신 스냅샷을 결정합니다.
22. `aws:executeAwsApi` - 지정된 KMSKey를 사용하여 DB 인스턴스 스냅샷을 복사합니다.
23. `aws:waitForAwsResourceProperty` - 스냅샷 복사 작업이 완료될 때까지 기다립니다.
24. `aws:executeAwsApi` - 새 스냅샷을 지정된 AccountIds와 공유합니다.
25. `aws:executeScript` - KMSKey 파라미터 값을 지정하지 않아 자동화가 실패할 경우 자동화에서 생성된 AWS KMS 고객 관리형 키를 삭제합니다.

AWS-StartRdsInstance

설명

Amazon Relational Database Service(RDS) 인스턴스를 시작합니다.

[이 자동화 실행\(콘솔\)](#)

문서 유형

자동화

소유자

Amazon

플랫폼

데이터베이스 수

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) 시작할 Amazon RDS 인스턴스의 ID입니다.

AWS-StartStopAuroraCluster

설명

이 실행서는 Amazon Aurora 클러스터를 시작하거나 중지합니다.

Note

클러스터를 시작하려면 클러스터가 stopped 상태여야 합니다. 클러스터를 중지하려면 클러스터가 available 상태여야 합니다. 이 실행서는 Aurora Serverless v1 클러스터, Aurora 멀티 마스터 클러스터, Aurora 글로벌 데이터베이스의 일부 또는 Aurora 병렬 쿼리를 사용하는 클러스터인 클러스터를 시작하거나 중지하는 데 사용할 수 없습니다. 실행서는 Aurora Serverless v2 클러스터를 중지하고 시작하는 데 사용할 수 있습니다.

이 자동화 실행(콘솔)

문서 유형

자동화

소유자

Amazon

플랫폼

데이터베이스 수

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.

- 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(RDS) 인스턴스를 중지합니다.

[이 자동화 실행\(콘솔\)](#)

문서 유형

자동화

소유자

Amazon

플랫폼

데이터베이스 수

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) 중지할 Amazon RDS 인스턴스의 ID입니다.

AWSSupport-TroubleshootConnectivityToRDS

설명

AWSSupport-TroubleshootConnectivityToRDS 실행서는 EC2 인스턴스와 Amazon 관계형 데이터베이스 서비스 인스턴스 간의 연결 문제를 진단합니다. 자동화를 통해 DB 인스턴스를 사용할 수 있는지 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.

다. 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 available로 설정되어 있는지 확인합니다.
- aws:executeAwsApi - DB 인스턴스에 대한 정보를 가져옵니다.
- aws:executeAwsApi - DB 인스턴스 네트워크 ACL에 대한 정보를 가져옵니다.
- aws:executeAwsApi - DB 인스턴스 서브넷 CIDR을 가져옵니다.
- aws:executeAwsApi - EC2 인스턴스에 대한 정보를 가져옵니다.
- aws:executeAwsApi - EC2 인스턴스 네트워크 ACL에 대한 정보를 가져옵니다.
- 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 인스턴스를 위해 Amazon VPC와 연결된 기본 라우팅 테이블에 대한 정보를 가져옵니다.
- `aws:executeAwsApi` - DB 인스턴스와 연결된 라우팅 테이블에 대한 정보를 가져옵니다.
- `aws:executeAwsApi` - DB 인스턴스를 위해 Amazon VPC와 연결된 기본 라우팅 테이블에 대한 정보를 가져옵니다.
- `aws:executeScript` - 보안 그룹 규칙을 평가합니다.
- `aws:executeScript` - 네트워크 ACL을 평가합니다.
- `aws:executeScript` - 라우팅 테이블을 평가합니다.
- `aws:sleep` - 자동화를 종료합니다.

출력

`getRDSInstanceProperties.DBInstanceIdentifier` - 자동화에 사용되는 DB 인스턴스입니다.

`getRDSInstanceProperties.DBInstanceStatus` - DBInstance의 현재 상태입니다.

`evalSecurityGroupRules.SecurityGroupEvaluation` - SourceInstance 보안 그룹 규칙을 DB 인스턴스 보안 그룹 규칙과 비교한 결과입니다.

`evalNetworkAclRules.NetworkAclEvaluation` - SourceInstance 네트워크 ACL을 DB 인스턴스 네트워크 ACL과 비교한 결과입니다.

`evalRouteTableEntries.RouteTableEvaluation` - SourceInstance 라우팅 테이블을 DB 인스턴스 라우팅과 비교한 결과입니다.

AWSSupport-TroubleshootRDSIAMAuthentication

설명

는 Amazon RDS for PostgreSQL, Amazon RDS for MySQL, Amazon RDS for MariaDB, Amazon Aurora PostgreSQL 및 Amazon Aurora MySQL 인스턴스에 대한 AWS Identity and Access Management (IAM) 인증 문제를 해결하는 `AWSSupport-TroubleshootRDSIAMAuthentication` 데 도움이 됩니다. PostgreSQL MySQL 이 실행서를 사용하여 Amazon RDS 인스턴스 또는 Aurora 클러스터를 사용한 IAM 인증에 필요한 구성을 확인합니다. 또한 Amazon RDS 인스턴스 또는 Aurora 클러스터에 대한 연결 문제를 해결하는 단계도 제공합니다.

⚠ Important

이 실행서는 Amazon RDS for Oracle 또는 Amazon RDS for Microsoft SQL Server를 지원하지 않습니다.

⚠ Important

소스 Amazon EC2 인스턴스가 제공되고 대상 데이터베이스가 Amazon RDS 인 경우 TCP 연결 문제를 해결하기 위해 하위 자동화가 호출 `AWSSupport-TroubleshootConnectivityToRDS`됩니다. 또한 출력은 Amazon EC2 인스턴스 또는 소스 시스템에서 실행하여 IAM 인증을 사용하여 Amazon RDS 인스턴스에 연결할 수 있는 명령을 제공합니다.

어떻게 작동하나요?

이 실행서는 6단계로 구성됩니다.

- 1단계: `validateInputs`: 자동화에 대한 입력을 검증합니다.
- 2단계: `branchOnSourceEC2Provided`: 입력 파라미터에 소스 Amazon EC2 인스턴스 ID가 제공되었는지 확인합니다.
- 3단계: `validateRDSConnectivity`: 제공된 경우 소스 Amazon EC2 인스턴스에서 Amazon RDS 연결을 검증합니다.
- 4단계: `validateRDSIAMAuthentication`: IAM 인증 기능이 활성화되어 있는지 확인합니다.
- 5단계: `validateIAMPolicies`: 제공된 IAM 사용자/역할에 필요한 IAM 권한이 있는지 확인합니다.
- 6단계: `generateReport`: 이전에 실행된 단계의 결과에 대한 보고서를 생성합니다.

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.

- RDSType

유형: 문자열

설명: (필수): 연결 및 인증하려는 관계형 데이터베이스 유형을 선택합니다.

허용된 값: Amazon RDS 또는 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: 63자

- SourceEc2InstanceIdentifier

유형: `AWS::EC2::Instance::Id`

설명: (선택 사항) 동일한 계정 및 리전에서 실행 중인 Amazon EC2 인스턴스에서 Amazon RDS 데이터베이스 인스턴스에 연결하는 경우의 Amazon EC2 인스턴스 ID입니다. 소스가 Amazon EC2 인스턴스가 아니거나 대상 Amazon RDS 유형이 Aurora 데이터베이스 클러스터인 경우 이 파라미터를 지정하지 마십시오.

기본값: ""

- DBIAMRoleName

유형: 문자열

설명: (선택 사항) IAM 기반 인증에 사용되는 IAM 역할 이름입니다. 파라미터DBIAMUserName가 제공되지 않은 경우에만 제공하고, 그렇지 않으면 비워 둡니다. DBIAMRoleName 또는 DBIAMUserName을 제공해야 합니다.

허용된 패턴: `^[a-zA-Z0-9+=, .@_-]{1,64}$|^$`

최대 문자: 64자

기본값: ""

- DBIAMUserName

유형: 문자열

설명: (선택 사항) IAM 기반 인증에 사용되는 IAM 사용자 이름입니다. DBIAMRoleName 파라미터가 제공되지 않은 경우에만 제공하고, 그렇지 않으면 비워 둡니다. DBIAMRoleName 또는 DBIAMUserName을 제공해야 합니다.

허용된 패턴: `^[a-zA-Z0-9+=, .@_-]{1,64}$|^$`

최대 문자: 64자

기본값: ""

- DBUserName

유형: 문자열

설명: (선택 사항) 데이터베이스 내 IAM 기반 인증을 위해 IAM 역할/사용자에 매핑된 데이터베이스 사용자 이름입니다. 기본 옵션은 데이터베이스의 모든 사용자에게 `rds-db:connect` 권한이 허용되는지 * 평가합니다.

허용된 패턴: `^[a-zA-Z0-9+=, .@*_]{1,64}$`

최대 문자: 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. AWS Systems Manager 콘솔에서 [AWSSupport-TroubleshootRDSIAMAuthentication](#)으로 이동합니다.
2. 자동화 실행을 선택합니다.
3. 입력 파라미터에 다음을 입력합니다.
 - AutomationAssumeRole(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.

- RDSType(필수):

연결 및 인증하려는 Amazon RDS 유형을 선택합니다. 두 개의 허용되는 값 중에서 선택합니다. Amazon RDS 또는 Amazon Aurora Cluster.

- DBInstanceIdentifier(필수):

인증에 IAM 자격 증명을 연결하고 사용하려는 대상 Amazon RDS 데이터베이스 인스턴스 또는 Aurora 클러스터의 식별자를 입력합니다.

- SourceEc2InstanceIdentifier(선택 사항):

동일한 계정 및 리전에 있는 Amazon EC2 인스턴스에서 Amazon RDS 데이터베이스 인스턴스에 연결하는 경우 Amazon EC2 인스턴스 ID를 제공합니다. 소스가 Amazon EC2가 아니거나 대상 Amazon RDS 유형이 Aurora 클러스터인 경우 비워 둡니다.

- DBIAMRoleName(선택 사항):

IAM 기반 인증에 사용되는 IAM 역할 이름을 입력합니다. DBIAMUserName가 제공되지 않은 경우에만 제공하고, 그렇지 않으면 비워 둡니다. DBIAMRoleName 또는 DBIAMUserName을 제공해야 합니다.

- DBIAMUserName(선택 사항):

IAM 기반 인증에 사용되는 IAM 사용자를 입력합니다. DBIAMRoleName가 제공되지 않은 경우에만 제공하고, 그렇지 않으면 비워 둡니다. DBIAMRoleName 또는 DBIAMUserName을 제공해야 합니다.

- DBUserName(선택 사항):

데이터베이스 내에서 IAM 기반 인증을 위해 IAM 역할/사용자에 매핑된 데이터베이스 사용자를 입력합니다. 기본 옵션은 평가에 * 사용되며이 필드에는 제공되지 않습니다.

Input parameters

SourceEc2InstanceIdentifier
(Optional) The Amazon EC2 Instance ID if you are connecting to the RDS DB instance from an EC2 Instance running in the same account and region. Do not specify this parameter if the source is not an EC2 instance or if the target RDS type is an Aurora DB cluster.

☒ Show interactive instance picker

Name	Instance ID	State	Availability zone	Platform
There are no managed instances in this account.				

We recommend using [Quick Setup](#) to configure your instances for Systems Manager.

After configuring your instances for Systems Manager, the instances will be displayed here in a few minutes.

AutomationAssumeRole
(Optional) The Amazon Resource Name (ARN) of the role that allows the Automation runbook to perform the actions on your behalf. If no role is specified, Systems Manager Automation uses your current IAM user permissions context to execute this runbook.

RDSType
(Required) The type of Relational Database.

DBInstanceIdentifier
(Required) The identifier of the target Amazon RDS DB instance or Amazon Aurora DB cluster.

DBIAMRoleName
(Optional) The IAM role name being used for IAM-based authentication. Provide only if the parameter 'DBIAMUserName' is not provided, otherwise leave it empty. Either 'DBIAMRoleName' or 'DBIAMUserName' must be provided.

DBIAMUserName
(Optional) The IAM user name used for IAM-based authentication. Provide only if the 'DBIAMRoleName' parameter is not provided, otherwise leave it empty. Either 'DBIAMRoleName' or 'DBIAMUserName' must be provided.

DBUserName
(Optional) The database user name mapped to an IAM role/user for IAM-based authentication within the database. The default option "" evaluates if the 'rds-db:connect' permission is allowed for all users in the DB.

4. 실행을 선택합니다.

5. 자동화가 시작됩니다.

6. 문서는 다음 단계를 수행합니다.

- 1단계: validateInputs:

자동화 - SourceEC2InstanceIdentifier (선택 사항), DBInstanceIdentifier 또는 ClusterID, DBIAMRoleName 또는에 대한 입력을 검증합니다DBIAMUserName. 입력한 입력 파라미터가 계정 및 리전에 있는지 확인합니다. 또한 사용자가 IAM 파라미터 중 하나(예: DBIAMRoleName 또는)를 입력했는지 확인합니다DBIAMUserName. 또한 언급된 데이터베이스가 사용 가능 상태인지 여부와 같은 다른 확인을 수행합니다.

- 2단계: branchOnSourceEC2Provided:

입력 파라미터에 소스 Amazon EC2가 제공되고 데이터베이스가 Amazon RDS인지 확인합니다. 그렇다면 3단계로 진행합니다. 그렇지 않으면 Amazon EC2-Aurora RDS 연결 검증인 3단계를 건너뛰고 4단계로 진행합니다.

- 3단계: validateRDSConnectivity:

소스 Amazon EC2가 입력 파라미터에 제공되고 데이터베이스가 Amazon RDS인 경우 2단계는 3단계를 시작합니다. 이 단계에서AWSSupport-TroubleshootConnectivityToRDS는 하위 자동화가 호출되어 소스 Amazon EC2의 Amazon RDS 연결을 검증합니다. 하위 자동화 실행서는 Amazon EC2 인스턴스에서 Amazon RDS 인스턴스로 연결할 수 있도록 필요한 네트워크 구

성(Amazon Virtual Private Cloud[Amazon VPC], 보안 그룹, 네트워크 액세스 제어 목록[NACL], Amazon RDS 가용성)이 있는지 `AWSSupport-TroubleshootConnectivityToRDS` 확인합니다.

- 4단계: `validateRDSIAMAuthentication`:

Amazon RDS 인스턴스 또는 Aurora 클러스터에서 IAM 인증 기능이 활성화되어 있는지 확인합니다.

- 5단계: `validateIAMPolicies`:

IAM 자격 증명이 지정된 데이터베이스 사용자(있는 경우)의 Amazon RDS 인스턴스에 인증할 수 있도록 전달된 IAM 사용자/역할에 필요한 IAM 권한이 있는지 확인합니다.

- 6단계: `generateReport`:

이전 단계에서 모든 정보를 가져오고 각 단계의 결과 또는 출력을 인쇄합니다. 또한 IAM 자격 증명을 사용하여 Amazon RDS 인스턴스에 연결하기 위해 참조하고 수행하는 단계도 나열됩니다.

7. 자동화가 완료되면 출력 섹션에서 자세한 결과를 검토합니다.

- 데이터베이스에 연결하기 위한 IAM 사용자/역할 권한 확인:

IAM 자격 증명이 지정된 데이터베이스 사용자(있는 경우)의 Amazon RDS 인스턴스에 인증할 수 있도록 전달된 IAM 사용자/역할에 필요한 IAM 권한이 있는지 확인합니다.

- 데이터베이스의 IAM 기반 인증 속성 확인:

지정된 Amazon RDS 데이터베이스/Aurora 클러스터에 대해 IAM 인증 기능이 활성화되어 있는지 확인합니다.

- Amazon EC2 인스턴스에서 Amazon RDS 인스턴스로의 연결 확인:

Amazon EC2 인스턴스에서 Amazon RDS 인스턴스로 연결할 수 있도록 필요한 네트워크 구성(Amazon VPC, 보안 그룹, NACL, Amazon RDS 가용성)이 있는지 확인합니다.

- 다음 단계:

IAM 자격 증명을 사용하여 Amazon RDS 인스턴스에 연결하기 위해 참조하고 수행할 명령과 단계를 나열합니다.

Outputs

ScriptExecutionId

Zel[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 자동화는 ModifyDBInstance 또는 StartDBInstance 작업을 수행하기 전에 기존 Amazon Relational Database Service(RDS)/Amazon Aurora/Amazon DocumentDB 인스턴스의 호환되지 않는 네트워크 상태를 방지하는 데 도움이 됩니다. 인스턴스가 이미 호환되지 않는 네트워크 상태인 경우 실행서에서 이유를 제공합니다.

어떻게 작동하나요?

이 실행서는 Amazon RDS 데이터베이스 인스턴스가 비호환 네트워크 상태가 될지 또는 비호환 네트워크 상태인 이유를 결정합니다.

실행서는 Amazon RDS 데이터베이스 인스턴스에 대해 다음 검사를 수행합니다.

- 리전당 Amazon Elastic Network Interface(ENI) 할당량입니다.
- 데이터베이스 서브넷 그룹의 모든 서브넷이 존재합니다.
- 서브넷에 사용할 수 있는 사용 가능한 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 DBInstanceIdentifier 대신 ClusterIdentifier를 사용해야 합니다. 그렇지 않으면 첫 번째 단계에서 문서가 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:

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "ValidateRdsNetwork",
      "Effect": "Allow",
      "Action": [
        "rds:DescribeDBInstances",
        "servicequotas:GetServiceQuota",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DescribeVpcAttribute",
        "ec2:DescribeSubnets"
      ],
      "Resource": [
        "arn:aws:rds:us-east-1:111122223333:db:db-instance-name"
      ]
    }
  ]
}
```

지침

1. AWS Systems Manager 콘솔에서 [AWSSupport-ValidateRdsNetworkConfiguration](#)으로 이동합니다.
2. 자동화 실행을 선택합니다.
3. 입력 파라미터에 다음을 입력합니다.

- AutomationAssumeRole(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.

- DBInstanceIdentifier(필수):

Amazon Relational Database Service 인스턴스 식별자를 입력합니다.

Input parameters

AutomationAssumeRole
(Optional) The Amazon Resource Name (ARN) of the AWS Identity and Access Management (IAM) role that allows Systems Manager Automation to perform the actions on your behalf. If no role is specified, Systems Manager Automation uses the permissions of the user that starts this runbook.

Select an existing IAM Role

AutomationAssumeRoleSSM
arn:aws:iam::<account-id>:role/AutomationAssumeRoleSSM

DBInstanceIdentifier
(Required) The Amazon Aurora or Amazon DocumentDB instance identifier.

my-rds-instance-01

4. 실행을 선택합니다.

5. 자동화가 시작됩니다.

6. 문서는 다음 단계를 수행합니다.

- 1단계: `assertRdsState`:

제공된 인스턴스 식별자가 존재하고 `available`, `stopped` 또는 상태 중 하나가 있는지 확인합니다. `incompatible-network`.

- 2단계: `gatherRdsInformation`:

자동화의 뒷부분에서 사용할 Amazon RDS 인스턴스에 대한 필수 정보를 수집합니다.

- 3단계: `checkEniQuota`:

리전에 대해 현재 사용 가능한 Amazon ENI 할당량을 확인합니다.

- 4단계: `validateVpcAttributes`:

Amazon VPC의 DNS 파라미터(`enableDnsSupport` 및 `enableDnsHostnames`)가 `true`(Amazon RDS 인스턴스가 인 경우에는 그렇지 않음)로 설정되어 있는지 확인합니다. `PubliclyAccessible`.

- 5단계: `validateSubnetAttributes`:

에 서브넷이 있는지 검증 `DBSubnetGroup`하고 각 서브넷에서 사용 가능한 IPs 확인합니다.

- 6단계: `generateReport`:

이전 단계에서 모든 정보를 가져오고 각 단계의 결과 또는 출력을 인쇄합니다. 또한 IAM 자격 증명을 사용하여 Amazon RDS 인스턴스에 연결하기 위해 참조하고 수행하는 단계도 나열됩니다.

7. 자동화가 완료되면 출력 섹션에서 자세한 결과를 검토합니다.

유효한 네트워크 구성이 있는 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 Existence Check: ✅ [PASSED]
```

```
  ii. Available IP Check: ✅ [PASSED]
```

```
* Availability Zone: ap-south-1a
```

```
  i. Subnet Existence Check: ✅ [PASSED]
```

```
  ii. Available IP Check: ✅ [PASSED]
```

```
### [Next Steps]
```

```
✅ All the checks has passed so the RDS Network configuration is correct.
```

```
Disclaimer: Please note that Check 5 is only valid if you are going to perform a MultiAZ conversion,
if you are not trying to perform a MultiAZ conversion then you can ignore the Check 5.
```

```
If any of the availability zone above has status as FAILED/WARNING then, please check the respective availability zone.
```

네트워크 구성이 잘못된 Amazon RDS 인스턴스(VPC 속성 enableDnsHostnames가 false로 설정됨):

▼ Outputs

```

generateReport.Report
# AWS RDS Network Configuration Checks: test-fail-sazrds-vpcattr (stopped)
### 🚫 Issue(s) Found!!!

### [Troubleshooting Results]
1. Checking ENI Quota for region the RDS Instance is in:
✅ [PASSED] : Quota for Elastic Network Interface (ENIs) (4996) is sufficient at the moment.

2. Checking VPC Attribute ('enableDnsHostname' & 'enableDnsSupport') settings:
❌ [FAILED] : Value for 'enableDnsHostnames' VPC Attribute is 'false'.

3. Checking if subnets required for RDS exists or not:
✅ [PASSED] : All subnets in 'ap-south-1b' availability zone exists.

4. Checking if Available IPs are sufficient per subnets that are required:
! [WARNING] : There are sufficient available IPs in 'ap-south-1b' availability zone, but it is recommended to have more than 9 IPs.

5. Checking if other Availability zone satisfy Check No# 3 & 4:
* Availability Zone: ap-south-1a
  i. Subnet Existence Check: ✅ [PASSED]
  ii. Available IP Check: ! [WARNING]

### [Next Steps]
o Please set the value of 'enableDnsHostnames' VPC attribute to 'true'.
  [+] View and update DNS attributes for your VPC: https://docs.aws.amazon.com/vpc/latest/userguide/vpc-dns.html#vpc-dns-updating
o Please free up some IPs before performing Modify/Stop operation on the instance.
  [+] Learn why a subnet in your VPC has insufficient IP addresses : https://repost.aws/knowledge-center/subnet-insufficient-ips

Disclaimer: Please note that Check 5 is only valid if you are going to perform a MultiAZ conversion,
if you are not trying to perform a MultiAZ conversion then you can ignore the Check 5.
If any of the availability zone above has status as FAILED/WARNING then, please check the respective availability zone.

```

참조

Systems Manager Automation

- [이 자동화 실행\(콘솔\)](#)
- [자동화 실행](#)
- [Automation 설정](#)
- [Support Automation Workflows 랜딩 페이지](#)

AWS 서비스 설명서

- [호환되지 않는 네트워크 상태인 Amazon RDS 데이터베이스 관련 문제를 해결하려면 어떻게 해야 하나요?](#)
- [호환되지 않는 네트워크 상태인 Amazon DocumentDB 인스턴스의 문제를 해결하려면 어떻게 해야 하나요?](#)

Amazon Redshift

AWS Systems Manager Automation은 Amazon Redshift에 대한 사전 정의된 실행서를 제공합니다. 실행서에 대한 자세한 내용은 [실행서 작업](#)을 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

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.

- ClusterIdentifier

유형: 문자열

설명: (필수) 삭제하려는 Amazon Redshift 클러스터의 ID입니다.

- SkipFinalClusterSnapshot

유형: Boolean

기본값: false

설명: (선택 사항) false로 설정하면 Amazon Redshift 클러스터를 삭제하기 전에 자동화가 스냅샷을 생성합니다. true로 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

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.

- 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

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 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

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.

- `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 실행서는 이미 암호화된 클러스터에서 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

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.

- ClusterIdentifier

유형: 문자열

설명: (필수) 암호화를 활성화하려는 클러스터의 고유 식별자입니다.

- KMSKeyARN

유형: 문자열

설명: (필수) 클러스터 데이터를 암호화하는 데 사용하려는 AWS KMS 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 지정하는 Amazon Redshift 클러스터에 대한 향상된 Virtual Private Cloud(VPC) 라우팅을 지원합니다. VPC 라우팅에 대한 자세한 내용은 Amazon Redshift 관리 안내서의 [Amazon Redshift Enhanced VPC Routing](#)(을)를 참조하세요.

[이 자동화 실행\(콘솔\)](#)

문서 유형

자동화

소유자

Amazon

플랫폼

데이터베이스 수

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.

- 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 실행서에서는 지정하는 Amazon Redshift 클러스터에 대해 SSL을 사용하려면 들어오는 연결을 필요로 합니다.

[이 자동화 실행\(콘솔\)](#)

문서 유형

자동화

소유자

Amazon

플랫폼

데이터베이스 수

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.

- 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

파라미터

- AllowVersionUpgrade

유형: Boolean

설명: (필수) true로 설정하면 유지 관리 기간 동안 메이저 버전 업그레이드가 클러스터에 자동으로 적용됩니다.

- 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.

- 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 관리를 실행할 수 있는 주 단위 기간(UTC)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 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

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.

- 클래식

유형: Boolean

설명: (선택 사항) true로 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 실행서를 제공합니다. 실행서에 대한 자세한 내용은 [실행서 작업](#)을 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](#)
- [AWSSupport-ConfigureS3ReplicationSameAndCrossAccount](#)
- [AWSSupport-EmptyS3Bucket](#)
- [AWSSupport-TroubleshootS3EventNotifications](#)
- [AWSSupport-ContainS3Resource](#)

AWS-ArchiveS3BucketToIntelligentTiering

설명

AWS-ArchiveS3BucketToIntelligentTiering 실행서는 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

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.

- BucketName

유형: 문자열

설명: (필수) 지능형 계층화 구성을 생성하려는 S3 버킷의 이름입니다.

- ConfigurationId

유형: 문자열

설명: (필수) 지능형 계층화 구성의 ID입니다. 새 구성 ID 또는 기존 구성의 ID일 수 있습니다.

- NumberOfDaysToArchive

유형: 문자열

유효한 값: 90~730

설명: (필수) 버킷의 객체를 Archive Access 계층으로 전환할 수 있는 연속 일수입니다.

- NumberOfDaysToDeepArchive

유형: 문자열

유효한 값: 180~730

설명: (필수) 버킷의 객체를 Deep Archive Access 계층으로 전환할 수 있는 연속 일수입니다.

- S3Prefix

유형: 문자열

설명: (선택 사항) 구성을 적용할 객체의 키 이름 접두사입니다.

- Tags

유형: MapList

설명: (선택 사항) 구성을 적용할 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.

Important

이 실행서에서 사용하는 Amazon S3 [PutBucketLogging](#) API의 이메일 피부여자 ACL에 대한 다음 중요 정보를 참고하세요.

지원 종료 공지: 2025년 10월 1일부터 Amazon S3는 새 이메일 피부여자 액세스 제어 목록 (ACL) 생성에 대한 지원을 중단할 예정입니다. 이 날짜 이전에 생성된 이메일 피부여자 ACLs 은 계속 작동하며 AWS Management Console, AWS CLI (CLI), SDKs 및 REST API를 통해 액세스할 수 있습니다. 그러나 더 이상 새 이메일 피부여자 ACL을 생성할 수 없습니다. 2025년 7월 15일부터 2025년 10월 1일까지 새 이메일 피부여자 ACLs을 생성하려고 할 때 Amazon S3에 대한 요청에 대해 HTTP 405 오류가 증가하기 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.

- 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.

- Granteeld

유형: 문자열

설명: (선택 사항) 피부여자의 정식 사용자 ID입니다.

- GranteeType

유형: 문자열

유효한 값: CanonicalUser | AmazonCustomerByEmail | Group

설명: (필수) 피부여자의 유형입니다.

- GranteeUri

유형: 문자열

설명: (선택 사항) 피부여자 그룹의 URI입니다.

- 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 파일이 키로 구분되도록 각 소스 버킷마다 다른 TargetPrefix를 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

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.

- BucketName

유형: 문자열

설명: (필수) 버전 관리를 구성하려는 Amazon S3 버킷의 이름입니다.

- VersioningState

유형: 문자열

유효한 값: Enabled | Suspended

기본값: 활성화됨

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. Suspended로 설정된 경우 이 프로세스는 버킷의 객체에 대한 버전 관리를 비활성화합니다. 버킷에 추가된 모든 객체는 버전 ID null을 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

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.

- BlockPublicAcls

유형: Boolean

기본값: true

설명: (선택 사항) true로 설정하면 Amazon S3는 S3 버킷에 대한 퍼블릭 액세스 제어 목록(ACL), 그리고 BucketName 파라미터에서 지정하는 S3 버킷에 저장된 객체를 차단합니다.

- BlockPublicPolicy

유형: Boolean

기본값: true

설명: (선택 사항) true로 설정하면 Amazon S3는 BucketName 파라미터에서 지정하는 S3 버킷에 대한 퍼블릭 버킷 정책을 차단합니다.

- BucketName

유형: 문자열

설명: (필수) 구성하려는 S3 버킷의 이름입니다.

- IgnorePublicAcls

유형: Boolean

기본값: true

설명: (선택 사항) true로 설정하면 Amazon S3는 BucketName 파라미터에서 지정하는 S3 버킷에 대한 모든 퍼블릭 ACL을 무시합니다.

- RestrictPublicBuckets

유형: Boolean

기본값: true

설명: (선택 사항) true로 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

실행서는 AWSConfigRemediation-ConfigureS3PublicAccessBlock 실행서 파라미터에서 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

파라미터

- AccountId

유형: 문자열

설명: (필수) 구성 중인 S3 버킷을 소유 AWS 계정 한의 ID입니다.

- 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.

- BlockPublicAcls

유형: Boolean

기본값: true

설명: (선택 사항) true 로 설정하면 Amazon S3는 AccountId 파라미터에서 AWS 계정 지정한가 소유한 S3 버킷에 대한 퍼블릭 액세스 제어 목록(ACLs)을 차단합니다.

- BlockPublicPolicy

유형: Boolean

기본값: true

설명: (선택 사항) true 로 설정하면 Amazon S3는 AccountId 파라미터에서 AWS 계정 지정한가 소유한 S3 버킷에 대한 퍼블릭 버킷 정책을 차단합니다.

- IgnorePublicAcls

유형: Boolean

기본값: true

설명: (선택 사항) true 로 설정하면 Amazon S3는 AccountId 파라미터에서 AWS 계정 지정한가 소유한 S3 버킷의 모든 퍼블릭 ACLs을 무시합니다.

- RestrictPublicBuckets

유형: Boolean

기본값: true

설명: (선택 사항) true 로 설정하면 Amazon S3는 AccountId 파라미터에서 AWS 계정 지정한가 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 지정된에 대한 PublicAccessBlock 구성을 반환하고 실행서 파라미터에 지정된 값을 기반으로 변경 사항이 성공적으로 적용되었는지 확인합니다.

AWS-CreateS3PolicyToExpireMultipartUploads

설명

AWS-CreateS3PolicyToExpireMultipartUploads 실행서는 정의된 일수 이후에 진행 중인 미완료 멀티파트 업로드가 만료되는 지정된 버킷에 대한 수명 주기 정책을 생성합니다. 이 실행서는 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

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.

- 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 적용할 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 구성되어 있는지 확인합니다.

출력

- VerifyExpireMultipartUploads.VerifyExpireMultipartUploadsResponse
- VerifyExpireMultipartUploads.LifecycleConfigurationRule

AWS-DisableS3BucketPublicReadWrite

설명

Amazon Simple Storage Service(Amazon S3) Block Public Access를 사용하여 퍼블릭 S3 버킷에 대한 읽기 및 쓰기 액세스를 비활성화합니다. 자세한 내용은 Amazon Simple Storage Service 사용 설명서의 [Amazon S3 퍼블릭 액세스 차단 사용](#)을 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.

- 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

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.

- BucketName

유형: 문자열

설명: (필수) 내용을 암호화할 S3 버킷의 이름입니다.

- SSEAlgorithm

유형: 문자열

기본 값: 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) 키를 사용한 이중 계층 서버 측 암호화(DSSE-KMS)에는 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.

- BucketName

유형: 문자열

설명: (필수) 버킷 키를 활성화하려는 S3 버킷의 이름입니다.

- KMSKeyId

유형: 문자열

설명: (선택 사항) 서버 측 암호화에 사용할 (AWS KMS) 고객 관리형 키의 Amazon 리소스 이름 AWS Key Management Service (ARN), 키 ID 또는 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-KMS를 사용할지 결정합니다.
- `PutBucketKeysKMS(aws:executeAwsApi)` - 지정된를 사용하여 지정된 S3 버킷에 `true` 대한 `BucketKeyEnabled` 속성을 로 설정합니다 `KmsKeyId`.
- `PutBucketKeysAES256(aws:executeAwsApi)` - AES256 암호화를 사용하여 지정된 S3 버킷 `true`의 `BucketKeyEnabled` 속성을 로 설정합니다.
- `VerifyS3BucketKeysEnabled(aws:assertAwsResourceProperty)` - 대상 S3 버킷에서 버킷 키가 활성화되었는지 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

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) 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 지정하는 Amazon S3에 대한 HTTP 요청을 명시적으로 거부하는 Amazon Simple Storage Service(Amazon S3) 버킷 정책 설명을 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) 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 - BucketName 파라미터에 지정된 S3 버킷에 대해 HTTP 요청을 명시적으로 거부하는 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 Amazon S3에 대한 액세스가 허용되는지 확인하기 위해 서비스 제어 정책을 평가하지 않습니다.

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.

- CloudWatchLogGroupName

유형: 문자열

설명: (선택 사항) 자동화 출력을 전송하려는 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 전송하려는 CloudWatch Logs 로그 스트림입니다. 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

유형: Boolean

유효한 값: true | false

기본값: true

설명: (선택 사항) 이 파라미터를 true로 설정하면 자동화가 지정하는 S3BucketName의 객체에 부분 HTTP 요청을 보냅니다. Range HTTP 헤더를 사용하면 객체의 첫 번째 바이트만 반환됩니다.

- IgnoreBlockPublicAccess

유형: Boolean

유효한 값: true | false

기본값: false

설명: (선택 사항) 이 파라미터를 true로 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 키](#)를 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

유형: Boolean

유효한 값: true | false

기본값: false

설명: (선택 사항) 자동화 중에 더 자세한 정보를 반환하려면, 이 파라미터를 true로 설정합니다. 파라미터가 false로 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 자동화를 통해 로그 데이터를 CloudWatch 로그로 전송하도록 하려는 경우에만 필요합니다.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": [
        "iam:SimulateCustomPolicy",
        "iam:GetContextKeysForCustomPolicy",
        "s3:ListAllMyBuckets",
        "logs:CreateLogGroup",
        "logs:CreateLogStream",
        "logs:PutLogEvents",
        "logs:PutRetentionPolicy",
        "s3:GetAccountPublicAccessBlock"
      ],
      "Resource": "*",
      "Effect": "Allow"
    },
    {
      "Action": [
        "s3:GetObject",
        "s3:GetObjectAcl",
        "s3:GetObjectTagging"
      ],
      "Resource": "arn:aws:s3:::amzn-s3-demo-bucket1/*",
      "Effect": "Allow"
    }
  ]
}
```

```

    },
    {
      "Action": [
        "s3:ListBucket",
        "s3:GetBucketLocation",
        "s3:GetBucketPublicAccessBlock",
        "s3:GetBucketRequestPayment",
        "s3:GetBucketPolicyStatus",
        "s3:GetBucketPolicy",
        "s3:GetBucketAcl"
      ],
      "Resource": "arn:aws:s3:::amzn-s3-demo-bucket1",
      "Effect": "Allow"
    }
  ]
}

```

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 Pays가 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 의미](#)를 참조하세요.
- `aws:executeAwsApi` - S3 버킷 정책을 반환합니다.
- `aws:executeAwsApi` - S3 버킷 정책에 있는 모든 컨텍스트 키를 반환합니다.
- `aws:assertAwsResourceProperty` - S3 버킷 정책에 GetObject API 작업에 대한 명시적 거부 기능이 있는지 확인합니다.
- `aws:executeAwsApi` - S3 버킷의 액세스 제어 목록(ACL)을 반환합니다.
- `aws:executeScript` - CloudWatchLogGroupName 파라미터 값을 지정하는 경우 CloudWatch Logs 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 true로 설정된 경우 반환된 객체에 대해 부분 HTTP 요청을 수행합니다. Range HTTP 헤더를 사용하면 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.
- 객체의 ACL이 익명 사용자에게 READ 또는 FULL_CONTROL 권한을 부여하는지 확인합니다.
- 객체와 연결된 태그를 반환합니다.
- 시뮬레이션된 IAM 정책을 사용하여 GetObject API 작업에 대한 S3 버킷 정책에 이 객체에 대한 명시적 거부기가 있는지 확인합니다.
- 객체의 메타데이터를 반환하여 스토리지 클래스가 지원되는지 확인합니다.
- 객체의 서버 측 암호화 설정을 확인하여 객체가 AWS Key Management Service (AWS KMS) 고객 관리형 키를 사용하여 암호화되는지 확인합니다.

출력

AnalyzeObjects.bucket

AnalyzeObjects.object

AWSsupport-ConfigureS3ReplicationSameAndCrossAccount

설명

AWSsupport-ConfigureS3ReplicationSameAndCrossAccount 자동화 실행서는 동일한 계정 또는 교차 계정에 대해 소스 버킷과 대상 버킷 간의 Amazon Simple Storage Service(Amazon S3) 버킷 복제를 구성합니다. 이 자동화는 Amazon S3-Managed 키를 사용한 서버 측 암호화(SSE-S3) 및 AWS Key Management Service (SSE-KMS)를 사용한 서버 측 암호화로 암호화된 버킷의 복제를 지원합니다. 또한 접두사 및 태그 기반 선택적 복제 필터링, 15분 SLA를 사용하는 Amazon S3 복제 시간 제어(Amazon S3 RTC) 및 삭제 마커 복제를 지원합니다. 자동화는 다음 작업을 수행합니다.

- 입력 파라미터 및 버킷 구성의 호환성을 검증합니다.

- 소스 버킷과 대상 버킷 모두에 대한 암호화 설정을 확인합니다.
- 입력으로 제공되지 않은 경우 복제에 대한 적절한 권한이 있는 새 AWS Identity and Access Management (IAM) 역할을 생성합니다.
- 지정된 파라미터(접두사, 태그 또는 전체 버킷)를 기반으로 복제 규칙을 구성합니다.
- 아직 활성화되지 않은 경우 버킷 버전 관리를 활성화합니다.
- 복제 시간 제어(RTC) 및 삭제 마커 복제와 같은 선택적 기능을 사용하여 복제 구성을 설정합니다.

Important

- 이 자동화는 기존 복제 규칙이 있는 버킷을 지원하지 않습니다. 소스 버킷에는 기존 복제 구성이 없어야 합니다.
- 이 자동화는 S3ReplicationRole 입력이 제공되지 않은 경우 복제에 대한 적절한 권한이 있는 새 IAM 역할을 생성합니다. S3ReplicationRole
- 이 자동화는 기존 객체를 복제하지 않습니다. Amazon S3 복제는 복제 구성이 활성화된 후 업로드/생성된 객체에만 적용됩니다.
- 교차 계정 복제의 경우 대상 계정의 IAM 역할에 Amazon S3 작업 및 AWS KMS 작업에 대한 적절한 권한을 제공해야 합니다(버킷이 AWS KMS 암호화를 사용하는 경우).
- 이 자동화는 지정된 보안 주체가 구성 변경을 승인할 때까지 실행을 일시적으로 일시 중지하는 `aws:approve` 작업을 사용합니다. 자세한 내용은 [승인자를 사용하여 자동화 실행을 참조하세요](#).

어떻게 작동하나요?

실행서는 다음 단계를 수행합니다.

- `ValidateInputParameters`: 모든 입력 파라미터의 정확성과 호환성을 검증하여 적절한 복제 구성을 보장합니다.
- `PrepareApprovalMessage`: 사용자 검토를 위해 모든 복제 구성 파라미터가 포함된 승인 메시지를 준비합니다.
- `RequestApproval`: 소스 버킷에 Amazon S3 복제 구성을 추가하기 전에 승인된 사용자에게 승인을 요청합니다.
- `CheckBucketEncryption`: 소스 및 대상 Amazon S3 버킷 모두에 대한 암호화 구성을 확인하여 호환되는 복제 설정을 결정합니다.

- BranchOnEncryptionType: Amazon S3 버킷 암호화 유형을 기반으로 실행을 분기하여 SSE-S3 또는 SSE-KMS 암호화 버킷에 적절한 복제 구성을 적용합니다.
- ConfigureSSES3Replication: IAM 역할 및 복제 규칙을 포함하여 Amazon S3 S3-Managed3 복제를 구성합니다.
- ConfigureSSEKMSReplication: IAM 역할, KMS 키 권한 및 복제 규칙을 포함하여 AWS KMS (SSE-KMS)를 사용한 서버 측 암호화로 암호화된 버킷에 대해 Amazon S3 복제를 구성합니다.
- CleanupResources: S3ReplicationRole이 입력으로 제공되지 않을 때 실패한 복제 구성 중에 생성된 IAM 역할을 정리합니다.

[이 자동화 실행\(콘솔\)](#)

필수 IAM 권한

실행서를 성공적으로 사용하려면 AutomationAssumeRole 파라미터에 다음 작업이 필요합니다.

- s3:ListBucket
- s3:GetBucketVersioning
- s3:GetEncryptionConfiguration
- s3:GetBucketLocation
- s3:GetReplicationConfiguration
- s3:PutBucketVersioning
- s3:PutReplicationConfiguration
- iam:ListRoles
- iam:GetRole
- iam:GetRolePolicy
- iam:ListRoleTags
- iam:ListAttachedRolePolicies
- iam:ListRolePolicies
- iam:SimulatePrincipalPolicy
- iam:CreateRole
- iam:TagRole
- iam:PassRole
- iam>DeleteRole

- iam:DeleteRolePolicy
- iam:DetachRolePolicy
- iam:PutRolePolicy
- sts:GetCallerIdentity
- sns:Publish
- kms:GetKeyPolicy(버킷이 SSE-KMS를 사용하는 경우, 동일 계정 복제)
- kms:DescribeKey(버킷이 SSE-KMS, 동일 계정 복제를 사용하는 경우)
- kms:PutKeyPolicy(버킷이 SSE-KMS, 동일 계정 복제를 사용하는 경우)
- sts:AssumeRole(교차 계정 복제용)

CrossAccountReplicationRole(교차 계정 시나리오의 경우):

교차 계정 복제의 경우 대상 계정의 CrossAccountReplicationRole에 다음 권한을 제공해야 합니다.

- s3:ListBucket
- s3:GetBucketVersioning
- s3:GetBucketLocation
- s3:GetBucketPolicy
- s3:GetEncryptionConfiguration
- s3:PutBucketVersioning
- s3:PutBucketPolicy
- kms:GetKeyPolicy(교차 계정 대상 버킷이 SSE-KMS를 사용하는 경우)
- kms:DescribeKey(교차 계정 대상 버킷이 SSE-KMS를 사용하는 경우)
- kms:PutKeyPolicy(교차 계정 대상 버킷이 SSE-KMS를 사용하는 경우)

S3ReplicationRole(고객 제공 역할):

기존 S3ReplicationRole을 제공하는 경우 다음 권한이 있어야 합니다.

- s3:ListBucket
- s3:GetBucketLocation
- s3:GetReplicationConfiguration
- s3:GetObjectVersionAcl

- s3:GetObjectVersionTagging
- s3:GetObjectVersionForReplication
- s3:GetObjectTagging
- s3:ReplicateObject
- s3:ReplicateDelete
- s3:ReplicateTags
- s3:ObjectOwnerOverrideToBucketOwner
- kms:Decrypt(SSE-KMS 시나리오의 경우 소스 KMS 키)
- kms:Encrypt(SSE-KMS 시나리오의 경우 대상 KMS 키)
- kms:GenerateDataKey(SSE-KMS 시나리오의 경우 대상 KMS 키)
- kms:ReEncrypt*(SSE-KMS 시나리오의 경우 대상 KMS 키)

동일 계정 복제를 위한 AutomationAssumeRole 정책 예제:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "S3Permissions",
      "Effect": "Allow",
      "Action": [
        "s3:GetBucketVersioning",
        "s3:GetEncryptionConfiguration",
        "s3:GetBucketLocation",
        "s3:GetReplicationConfiguration",
        "s3:ListBucket",
        "s3:PutBucketVersioning",
        "s3:PutReplicationConfiguration"
      ],
      "Resource": [
        "arn:aws:s3:::SOURCE_BUCKET",
        "arn:aws:s3:::DESTINATION_BUCKET"
      ]
    },
    {
      "Sid": "IAMReadOperations",
      "Effect": "Allow",

```

```

        "Action": [
            "iam:GetRole",
            "iam:GetRolePolicy",
            "iam:ListRoleTags",
            "iam:ListAttachedRolePolicies",
            "iam:ListRolePolicies",
            "iam:SimulatePrincipalPolicy"
        ],
        "Resource": "*"
    },
    {
        "Sid": "IAMListRolesForCleanup",
        "Effect": "Allow",
        "Action": "iam:ListRoles",
        "Resource": "*"
    },
    {
        "Sid": "IAMCreateAndTagRole",
        "Effect": "Allow",
        "Action": [
            "iam:CreateRole",
            "iam:TagRole"
        ],
        "Resource": "arn:aws:iam::ACCOUNT_ID:role/S3RepRole-*",
        "Condition": {
            "StringLike": {
                "aws:RequestTag/AWSSupport-ConfigureS3ReplicationSameAndCrossAccount": "*"
            }
        }
    },
    {
        "Sid": "IAMPassRole",
        "Effect": "Allow",
        "Action": "iam:PassRole",
        "Resource": "arn:aws:iam::ACCOUNT_ID:role/S3RepRole-*",
        "Condition": {
            "StringEquals": {
                "iam:PassedToService": "s3.amazonaws.com"
            }
        }
    },
    {
        "Sid": "TaggedIAMRoleModifyAndDeleteOperations",

```

```

        "Effect": "Allow",
        "Action": [
            "iam:DeleteRole",
            "iam:DeleteRolePolicy",
            "iam:DetachRolePolicy",
            "iam:PutRolePolicy"
        ],
        "Resource": "arn:aws:iam::ACCOUNT_ID:role/S3RepRole-*",
        "Condition": {
            "StringLike": {
                "aws:ResourceTag/AWSSupport-
ConfigureS3ReplicationSameAndCrossAccount": "*"
            }
        }
    },
    {
        "Sid": "STSGetCallerIdentity",
        "Effect": "Allow",
        "Action": "sts:GetCallerIdentity",
        "Resource": "*"
    },
    {
        "Sid": "SNSPublish",
        "Effect": "Allow",
        "Action": "sns:Publish",
        "Resource": "SNS_TOPIC_ARN"
    },
    {
        "Sid": "KMSKeyReadOperations",
        "Effect": "Allow",
        "Action": [
            "kms:GetKeyPolicy",
            "kms:DescribeKey"
        ],
        "Resource": [
            "arn:aws:kms:REGION:ACCOUNT_ID:key/SOURCE_KMS_KEY_ID",
            "arn:aws:kms:REGION:ACCOUNT_ID:key/DESTINATION_KMS_KEY_ID"
        ]
    },
    {
        "Sid": "KMSKeyMutatingOperations",
        "Effect": "Allow",
        "Action": "kms:PutKeyPolicy",
        "Resource": [

```

```

        "arn:aws:kms:REGION:ACCOUNT_ID:key/SOURCE_KMS_KEY_ID",
        "arn:aws:kms:REGION:ACCOUNT_ID:key/DESTINATION_KMS_KEY_ID"
    ],
    "Condition": {
        "StringEquals": {
            "kms:CallerAccount": "ACCOUNT_ID"
        }
    }
}
]
}

```

Note

정책 설명(KMSKeyReadOperations 및 KMSKeyMutatingOperations)은 버킷이 SSE-KMS 암호화를 사용하는 경우에만 필요합니다.

교차 계정 복제를 위한 AutomationAssumeRole 정책 예제:

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "S3SourceBucketOperations",
      "Effect": "Allow",
      "Action": [
        "s3:GetBucketVersioning",
        "s3:GetEncryptionConfiguration",
        "s3:GetBucketLocation",
        "s3:GetReplicationConfiguration",
        "s3:ListBucket",
        "s3:PutBucketVersioning",
        "s3:PutReplicationConfiguration"
      ],
      "Resource": "arn:aws:s3:::SOURCE_BUCKET"
    },
    {
      "Sid": "IAMReadOperations",
      "Effect": "Allow",

```

```

        "Action": [
            "iam:GetRole",
            "iam:GetRolePolicy",
            "iam:ListRoleTags",
            "iam:ListAttachedRolePolicies",
            "iam:ListRolePolicies",
            "iam:SimulatePrincipalPolicy"
        ],
        "Resource": "*"
    },
    {
        "Sid": "IAMListRolesForCleanup",
        "Effect": "Allow",
        "Action": "iam:ListRoles",
        "Resource": "*"
    },
    {
        "Sid": "IAMCreateAndTagRole",
        "Effect": "Allow",
        "Action": [
            "iam:CreateRole",
            "iam:TagRole"
        ],
        "Resource": "arn:aws:iam::SOURCE_ACCOUNT_ID:role/S3RepRole-*",
        "Condition": {
            "StringLike": {
                "aws:RequestTag/AWSSupport-ConfigureS3ReplicationSameAndCrossAccount": "*"
            }
        }
    },
    {
        "Sid": "IAMPassRole",
        "Effect": "Allow",
        "Action": "iam:PassRole",
        "Resource": "arn:aws:iam::SOURCE_ACCOUNT_ID:role/S3RepRole-*",
        "Condition": {
            "StringEquals": {
                "iam:PassedToService": "s3.amazonaws.com"
            }
        }
    },
    {
        "Sid": "TaggedIAMRoleModifyAndDeleteOperations",

```

```

        "Effect": "Allow",
        "Action": [
            "iam:DeleteRole",
            "iam:DeleteRolePolicy",
            "iam:DetachRolePolicy",
            "iam:PutRolePolicy"
        ],
        "Resource": "arn:aws:iam::SOURCE_ACCOUNT_ID:role/S3RepRole-*",
        "Condition": {
            "StringLike": {
                "aws:ResourceTag/AWSSupport-
ConfigureS3ReplicationSameAndCrossAccount": "*"
            }
        }
    },
    {
        "Sid": "CrossAccountRoleAssumption",
        "Effect": "Allow",
        "Action": "sts:AssumeRole",
        "Resource": "CROSS_ACCOUNT_REPLICATION_ROLE_ARN"
    },
    {
        "Sid": "STSGetCallerIdentity",
        "Effect": "Allow",
        "Action": "sts:GetCallerIdentity",
        "Resource": "*"
    },
    {
        "Sid": "SNSPublish",
        "Effect": "Allow",
        "Action": "sns:Publish",
        "Resource": "SNS_TOPIC_ARN"
    },
    {
        "Sid": "KMSSourceKeyReadOperations",
        "Effect": "Allow",
        "Action": [
            "kms:GetKeyPolicy",
            "kms:DescribeKey"
        ],
        "Resource": "arn:aws:kms:SOURCE_REGION:SOURCE_ACCOUNT_ID:key/
SOURCE_KMS_KEY_ID"
    },
    {

```

```

        "Sid": "KMSSourceKeyMutatingOperations",
        "Effect": "Allow",
        "Action": "kms:PutKeyPolicy",
        "Resource": "arn:aws:kms:SOURCE_REGION:SOURCE_ACCOUNT_ID:key/
SOURCE_KMS_KEY_ID",
        "Condition": {
            "StringEquals": {
                "kms:CallerAccount": "SOURCE_ACCOUNT_ID"
            }
        }
    }
]
}

```

Note

- 정책 설명(KMSSourceKeyReadOperations 및 KMSSourceKeyMutatingOperations)은 소스 버킷이 SSE-KMS 암호화를 사용하는 경우에만 필요합니다.
- CROSS_ACCOUNT_REPLICATION_ROLE_ARN을 자동화에 제공한 실제 CrossAccountReplicationRole 파라미터 값으로 바꿉니다.

CrossAccountReplicationRole 정책 예제:

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "S3DestinationBucketReadOperations",
      "Effect": "Allow",
      "Action": [
        "s3:GetBucketVersioning",
        "s3:GetBucketLocation",
        "s3:GetBucketPolicy",
        "s3:GetEncryptionConfiguration",
        "s3:ListBucket",
        "s3:PutBucketVersioning",
        "s3:PutBucketPolicy"
      ],

```



```

        "Resource": "arn:aws:s3:::DESTINATION_BUCKET"
    },
    {
        "Sid": "KMSDestinationKeyReadOperations",
        "Effect": "Allow",
        "Action": [
            "kms:GetKeyPolicy",
            "kms:DescribeKey"
        ],
        "Resource": "arn:aws:kms:DESTINATION_REGION:DESTINATION_ACCOUNT_ID:key/DESTINATION_KMS_KEY_ID"
    },
    {
        "Sid": "KMSDestinationKeyMutatingOperations",
        "Effect": "Allow",
        "Action": "kms:PutKeyPolicy",
        "Resource": "arn:aws:kms:DESTINATION_REGION:DESTINATION_ACCOUNT_ID:key/DESTINATION_KMS_KEY_ID",
        "Condition": {
            "StringEquals": {
                "kms:CallerAccount": "DESTINATION_ACCOUNT_ID"
            }
        }
    }
]
}

```

Note

KMS 문(KMSDestinationKeyReadOperations 및 KMSDestinationKeyMutatingOperations)은 대상 버킷이 SSE-KMS 암호화를 사용하는 경우에만 필요합니다. SSE-S3 시나리오에 대한 다음 문을 제거합니다.

CrossAccountReplicationRole 신뢰 정책 예제:

```

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

```

```

        "Effect": "Allow",
        "Principal": {
            "AWS": "AUTOMATION_ASSUME_ROLE_ARN"
        },
        "Action": "sts:AssumeRole"
    }
]
}

```

Note

AUTOMATION_ASSUME_ROLE_ARN을 자동화에 제공한 실제 AutomationAssumeRole 파라미터 값으로 바꿉니다.

S3ReplicationRole 정책의 예:

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "S3SourceBucketPermissions",
      "Effect": "Allow",
      "Action": [
        "s3:ListBucket",
        "s3:GetBucketLocation",
        "s3:GetReplicationConfiguration",
        "s3:GetObjectVersionAcl",
        "s3:GetObjectVersionTagging",
        "s3:GetObjectVersionForReplication",
        "s3:GetObjectTagging"
      ],
      "Resource": [
        "arn:aws:s3:::SOURCE_BUCKET",
        "arn:aws:s3:::SOURCE_BUCKET/*"
      ]
    },
    {
      "Sid": "S3DestinationBucketPermissions",
      "Effect": "Allow",

```

```

        "Action": [
            "s3:ReplicateObject",
            "s3:ReplicateDelete",
            "s3:ReplicateTags"
        ],
        "Resource": "arn:aws:s3:::DESTINATION_BUCKET/*"
    },
    {
        "Sid": "S3CrossAccountPermissions",
        "Effect": "Allow",
        "Action": "s3:ObjectOwnerOverrideToBucketOwner",
        "Resource": "arn:aws:s3:::DESTINATION_BUCKET/*"
    },
    {
        "Sid": "KMSSourceKeyPermissions",
        "Effect": "Allow",
        "Action": "kms:Decrypt",
        "Resource": "arn:aws:kms:SOURCE_REGION:SOURCE_ACCOUNT_ID:key/
SOURCE_KMS_KEY_ID"
    },
    {
        "Sid": "KMSDestinationKeyPermissions",
        "Effect": "Allow",
        "Action": [
            "kms:Encrypt",
            "kms:GenerateDataKey",
            "kms:ReEncrypt*"
        ],
        "Resource": "arn:aws:kms:DESTINATION_REGION:DESTINATION_ACCOUNT_ID:key/
DESTINATION_KMS_KEY_ID"
    }
]
}

```

Note

- KMS 문(KMSSourceKeyPermissions 및 KMSDestinationKeyPermissions)은 버킷이 SSE-KMS 암호화를 사용하는 경우에만 필요합니다.
- S3CrossAccountPermissions 문은 교차 계정 버킷 복제에만 필요합니다.

S3ReplicationRole 신뢰 정책 예:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "Service": "s3.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

지침

다음 단계에 따라 자동화를 구성합니다.

1. Systems Manager [AWSSupport-ConfigureS3ReplicationSameAndCrossAccount](#)의 문서로 이동합니다.
2. Execute automation(자동화 실행)을 선택합니다.
3. 입력 파라미터에 다음을 입력합니다.
 - AutomationAssumeRole(필수):
 - 설명: (필수) Systems Manager Automation이 사용자를 대신하여 작업을 수행하도록 허용하는 (IAM) 역할의 Amazon 리소스 이름 AWS Identity and Access Management (ARN)입니다. 역할을 지정하지 않은 경우, Systems Manager Automation에서는 이 실행서를 시작하는 사용자의 권한을 사용합니다.
 - 유형: AWS::IAM::Role::Arn
 - SourceBucket(필수):
 - 설명: (필수) 복제 규칙을 생성하거나 업데이트할 소스 Amazon S3 버킷의 이름입니다.
 - 유형: AWS::S3::Bucket::Name
 - DestinationBucket(필수):
 - 설명: (필수) 객체를 복제할 대상 Amazon S3 버킷의 이름입니다.
 - 유형: String

- 허용된 패턴: `^[0-9a-z][a-z0-9\\-\\.]{3,63}$`
- SourceAccountId(필수):
 - 설명: (필수) 소스 버킷이 위치한 AWS 계정 ID입니다.
 - 유형: String
 - 허용된 패턴: `^[0-9]{12,13}$`
- DestinationAccountId(필수):
 - 설명: (필수) 대상 버킷이 위치한 AWS 계정 ID입니다.
 - 유형: String
 - 허용된 패턴: `^[0-9]{12,13}$`
- SnsNotificationArn(필수):
 - 설명: (필수) 자동화 승인을 위한 Amazon Simple Notification Service(Amazon SNS) 주제의 ARN입니다.
 - 유형: String
 - 허용된 패턴: `^arn:(aws|aws-cn|aws-us-gov|aws-iso(-[a-z]))?:sns:[a-z]{2}(-gov)?(-iso[a-z])?-[a-z]{2,10}-[0-9]{1,2}:\d{12}:([0-9a-zA-Z-]{1,256})(.fifo)?$`
- 승인자(필수):
 - 설명: (필수) 자동화 실행을 승인할 권한이 있는 IAM 사용자/역할 ARNs 목록입니다.
 - 유형: StringList
 - 허용된 패턴: `^arn:(aws|aws-cn|aws-us-gov|aws-iso(-[a-z]))?:iam:.\d{12}:(user|role)/[\w+=,.\@\\-/+]+$`
- S3ReplicationRole(선택 사항):
 - 설명: (선택 사항) Amazon S3 복제 작업에 사용할 기존 IAM 역할의 ARN입니다. 이 역할에는 버킷이 SSE-KMS 암호화를 사용하는 경우 KMS 권한을 포함하여 소스 버킷에서 읽고 대상 버킷에 쓸 수 있는 권한이 있어야 합니다. 제공되지 않은 경우 자동화는 적절한 권한이 있는 새 역할을 생성합니다.
 - 유형: String
 - 허용된 패턴: `^$|^arn:(aws|aws-cn|aws-us-gov|aws-iso(-[a-z]))?:iam:.\d{12}:role/[\w+=,.\@\\-/+]+$`
 - 기본값: ""
- CrossAccountReplicationRole(선택 사항):

- 설명: (선택 사항) 자동화가 수임할 수 있는 대상 계정의 IAM 역할 ARN입니다. 이는 교차 계정 복제에 필요합니다. 동일 계정 복제의 경우 비워 둡니다.
- 유형: String
- 허용된 패턴: `^$|^arn:(aws|aws-cn|aws-us-gov|aws-iso(-[a-z]))?:iam::\d{12}:role/[\\w+=,.\@\\-/+]+$`
- 기본값: ""
- ReplicateEntireBucket(선택 사항):
 - 설명: (선택 사항) 로 설정하면 true전체 버킷이 복제되고 접두사와 태그가 모두 비어 있어야 합니다. false인 경우 복제는 지정된 접두사 또는 태그를 기반으로 합니다.
 - 유형: Boolean
 - 허용된 값: [true, false]
 - 기본값: true
- ReplicationRuleStatus(선택 사항):
 - 설명: (선택 사항) 로 설정하면 생성된 true복제 규칙이 활성화됩니다. 로 설정하면 생성된 false복제 규칙이 비활성화됨으로 설정됩니다.
 - 유형: Boolean
 - 허용된 값: [true, false]
 - 기본값: true
- DeleteMarkerReplicationStatus(선택 사항):
 - 설명: (선택 사항) 로 설정하면 자동화true가 삭제 마커 복제를 활성화합니다.
 - 유형: Boolean
 - 허용된 값: [true, false]
 - 기본값: false
- ReplicationTimeControl(선택 사항):
 - 설명: (선택 사항) 로 설정하면 예측 가능한 복제 시간을 위해 15분 SLA로 Amazon S3 Replication Time Control(Amazon S3 RTC)을 true활성화합니다.
 - 유형: Boolean
 - 허용된 값: [true, false]
 - 기본값: false
- ReplicaModifications(선택 사항):

- 설명: (선택 사항) 로 설정하면 복제본 객체에 대한 메타데이터 변경 사항을 true복제할 수 있으므로 복제된 객체에 대한 수정 사항을 소스와 다시 동기화할 수 있습니다.
 - 유형: Boolean
 - 허용된 값: [true, false]
 - 기본값: false
 - 접두사(선택 사항):
 - 설명: (선택 사항) 특정 키 접두사가 있는 객체의 선택적 복제를 위한 접두사 필터입니다. 적절한 Amazon S3 접두사 필터링을 위해 접두사는 후행 슬래시(/)로 끝나야 합니다.
 - 유형: String
 - 허용된 패턴: `^$|^([a-zA-Z0-9!_'\(\)\-\]*/+)$`
 - 기본값: ""
 - 태그(선택 사항):
 - 설명: (선택 사항) 복제할 객체를 필터링하기 위한 태그의 JSON 배열입니다. 단일 태그 형식: [{"Key": "TagKey", "Value": "TagValue"}] 및 여러 태그 형식: [{"Key": "TagKey1", "Value": "TagValue1"}, {"Key": "TagKey2", "Value": "TagValue2"}].
 - 유형: String
 - 허용된 패턴: `^\\[\\(\\{\\\"Key\\\":\\\"[a-zA-Z0-9+\\-\\.:/ @\\s]{1,128}\\\",\\\"Value\\\":\\\"[a-zA-Z0-9+\\-\\.:/@\\s]{0,256}\\\"\\}\\}\\(,\\{\\\"Key\\\":\\\"[a-zA-Z0-9+\\-\\.:/ @\\s]{1,128}\\\",\\\"Value\\\":\\\"[a-zA-Z0-9+\\-\\.:/@\\s]{0,256}\\\"\\}\\}\\)*\\)?\\$`
 - 기본값: []
4. 실행을 선택합니다.
 5. 자동화가 시작됩니다.
 6. 문서는 다음 단계를 수행합니다.
 - ValidateInputParameters:

모든 입력 파라미터의 정확성과 호환성을 검증하여 적절한 복제 구성을 보장합니다.
 - PrepareApprovalMessage:

사용자 검토를 위한 모든 복제 구성 파라미터가 포함된 승인 메시지를 준비합니다.
 - RequestApproval:

- CheckBucketEncryption:

호환되는 복제 설정을 결정하기 위해 소스 및 대상 Amazon S3 버킷 모두에 대한 암호화 구성을 확인합니다.

- BranchOnEncryptionType:

Amazon S3 버킷 암호화 유형을 기반으로 실행을 분기하여 SSE-S3 또는 SSE-KMS 암호화 버킷에 적절한 복제 구성을 적용합니다.

- ConfigureSSES3Replication:

IAM 역할 및 복제 규칙을 포함하여 Amazon S3 S3-Managed3 복제를 구성합니다.

- ConfigureSSEKMSReplication:

IAM 역할, KMS 키 권한 및 복제 규칙을 포함하여 AWS KMS (SSE-KMS)를 사용한 서버 측 암호화로 암호화된 버킷에 대해 Amazon S3 복제를 구성합니다.

- CleanupResources:

고객이 S3ReplicationRole을 제공하지 않은 경우 실패한 복제 구성 중에 생성된 IAM 역할을 정리합니다.

7. 완료되면 ConfigureSSES3Replication 단계(SSE-S3 암호화 버킷의 경우) 또는 ConfigureSSEKMSReplication 단계(SSE-KMS 암호화 버킷의 경우)의 출력을 검토하여 복제에 사용되는 IAM 역할과 함께 복제 구성 상태를 포함한 실행 결과를 확인합니다.

참조

Systems Manager Automation

- [이 자동화 실행\(콘솔\)](#)
- [자동화 실행](#)
- [Automation 설정](#)
- [자동화 워크플로 지원](#)

AWSsupport-EmptyS3Bucket

설명

AWSsupport-EmptyS3Bucket 자동화 실행서는 수명 주기 만료 구성 규칙을 사용하여 기존 Amazon Simple Storage Service(Amazon S3) 버킷을 비웁니다.

⚠ Important

- 다중 인증(MFA)이 활성화된 Amazon S3 버킷은 지원되지 않습니다.
- 이 실행서에 의해 수정된 수명 주기 규칙은 지정된 Amazon S3 버킷의 모든 객체와 해당 버전을 영구적으로 삭제합니다. 영구적으로 삭제된 객체는 복구할 수 없습니다. 자세한 내용은 [만료 중인 객체를 참조하세요](#).

어떻게 작동하나요?

실행서는 다음과 같은 상위 수준 단계를 AWSsupport-EmptyS3Bucket 수행합니다.

- 활성화된 경우 버킷 버전 관리를 일시 중지합니다.
- (비우는 동안 새 업로드를 방지하기 위해) s3:PutObject API 호출을 거부하도록 버킷 정책을 업데이트합니다.
- 입력 파라미터에 지정된 만료 날짜에 따라 모든 객체를 삭제하도록 수명 주기 규칙을 업데이트합니다.

i Note

- Amazon S3 객체 잠금으로 보호되는 객체 버전은 수명 주기 구성에 의해 삭제되거나 덮어쓰여지지 않습니다.
- 삭제 프로세스는 비동기식이며 실행서 실행이 완료된 후 완료하는 데 시간이 걸릴 수 있습니다.

이 자동화 실행(콘솔)

문서 유형

자동화

소유자

Amazon

플랫폼

/

필수 IAM 권한

실행서를 성공적으로 사용하려면 AutomationAssumeRole 파라미터에 다음 작업이 필요합니다.

AutomationAssumeRole 파라미터를 실행서를 성공적으로 사용하려면 다음 작업이 필요합니다.

- ssm:DescribeAutomationExecutions
- ssm:GetAutomationExecution
- s3:GetBucketVersioning
- s3:PutBucketVersioning
- s3:GetBucketPolicy
- s3:GetBucketLifecycleConfiguration
- s3:GetLifecycleConfiguration
- s3:PutBucketPolicy
- s3:PutBucketLifecycleConfiguration
- s3:PutLifecycleConfiguration
- s3>DeleteBucketPolicy
- s3>DeleteBucketLifecycle

지침

다음 단계에 따라 자동화를 구성합니다.

1. Systems Manager [AWSSupport-EmptyS3Bucket](#)의 문서로 이동합니다.
2. Execute automation(자동화 실행)을 선택합니다.
3. 입력 파라미터에 다음을 입력합니다.
 - AutomationAssumeRole(선택 사항):

Systems Manager Automation이 사용자를 대신하여 작업을 수행하도록 허용하는 (IAM) 역할의 Amazon 리소스 이름 AWS AWS Identity and Access Management (ARN)입니다. 역할이 지정되지 않은 경우 Systems Manager Automation은 이 실행서를 시작하는 사용자의 권한을 사용합니다.

- S3BucketName:

비우려는 Amazon S3 버킷의 이름입니다.

- **SNSTopicArn:**

승인 알림을 위해 Amazon SNS 주제의 ARN을 제공합니다. 이 Amazon SNS 주제는 자동화 실행 중에 필요한 동안 승인 알림을 보내는 데 사용됩니다.

- **ApproverIAM:**

작업을 승인하거나 거부할 수 있는 AWS 인증된 보안 주체 목록을 제공합니다. 최대 승인자 수는 10입니다. 이러한 형식, AWS Identity and Access Management (IAM) 사용자 이름, IAM 사용자 ARN, IAM 역할 ARN 또는 IAM 수임 역할 사용자 ARN을 사용하여 보안 주체를 지정할 수 있습니다.

- **MinimumRequiredApprovals(선택 사항):**

자동화를 다시 시작하는 데 필요한 최소 승인 횟수입니다. 값을 지정하지 않으면 시스템의 기본값은 1입니다. 이 파라미터의 값은 양수여야 합니다. 이 파라미터의 값은 ApproverIAM 파라미터에서 정의한 승인자 수를 초과할 수 없습니다.

- **NoncurrentVersionExpirationDays(선택 사항):**

최신이 아닌 객체 버전이 만료되는 일수를 지정합니다. 만료 시 Amazon S3는 최신이 아닌 객체 버전을 영구적으로 삭제합니다.

- 기본값: 1

- 최댓값: 365

- **ExpirationDays(선택 사항):**

객체의 수명 주기 만료를 일 형식으로 지정합니다.

- 기본값: 1

- 최댓값: 365

- **AbortIncompleteMultipartUpload(선택 사항):**

불완전한 멀티파트 업로드를 시작한 이후 Amazon S3가 업로드의 모든 부분을 영구적으로 제거하기 전에 대기할 날짜를 지정합니다.

- 기본값: 1

- 최댓값: 365

- **승인:**

이 자동화 실행서에서 수행하는 작업의 전체 세부 정보를 읽고 단계를 승인하는 Yes, I understand and acknowledge 경우 동의를 제공하세요.

Input parameters

AutomationAssumeRole
(Optional) The Amazon Resource Name (ARN) of the AWS Identity and Access Management (IAM) role that allows Systems Manager Automation to perform the actions on your behalf. If no role is specified, Systems Manager Automation uses the permissions of the user that starts this runbook.

SNSTopicArn
(Required) The ARN of the Amazon Simple Notification Service (Amazon SNS) Topic for approval notification. This SNS topic is used to send the approval notifications required during the automation execution.

MinimumRequiredApprovals
(Optional) The minimum number of approvals required to resume the automation. If you don't specify a value, the system defaults to one. The value for this parameter must be a positive number. The value for this parameter can't exceed the number of approvers defined in the 'ApproverIAM' parameter.

ExpirationDays
(Optional) Specify the expiration for the lifecycle of the object in days. Default value is 1 and max value is 365.

Acknowledgement
(Required) Please read the complete details of the actions performed by this automation runbook and write 'Yes, I understand and acknowledge' if you acknowledge the steps. ****Important:**** You cannot recover permanently removed objects. For more information please review [Expiring objects] (<https://docs.aws.amazon.com/AmazonS3/latest/userguide/lifecycle-expire-general-considerations.html>).

S3BucketName
(Required) The name of the Amazon S3 bucket you want to empty.

ApproverIAM
(Required) The list of AWS authenticated principals who are able to either approve or reject the action. The maximum number of approvers is 10. You can specify principals by using any of these formats, 1) An AWS Identity and Access Management (IAM) user name 2) An IAM user ARN 3) An IAM role ARN 4) An IAM assume role user ARN.

NoncurrentVersionExpirationDays
(Optional) Specify the number of days when noncurrent object versions expire. Upon expiration, Amazon S3 permanently deletes the noncurrent object versions. Default value is 1 and max value is 365.

AbortIncompleteMultipartUpload
(Optional) Specify the days since the initiation of an incomplete multipart upload that Amazon S3 will wait before permanently removing all parts of the upload. Default value is 1 and max value is 365.

- 실행을 선택합니다.
- 자동화가 시작됩니다.
- 문서는 다음 단계를 수행합니다.

- **checkConcurrency:**

지정된 Amazon S3 버킷을 대상으로 하는 이 실행서의 실행이 하나만 있는지 확인합니다. 실행서가 동일한 버킷 이름을 대상으로 진행 중인 다른 실행을 찾으면 오류가 반환되고 종료됩니다.

- **getBucketVersioningConfiguration:**

지정된 Amazon S3 버킷의 버전 관리 상태를 가져옵니다.

- **branchOnStoppingIfMFADeleteEnabled** (조건부):

지정된 Amazon S3 버킷에서 다중 인증(MFA)이 활성화된 경우 자동화를 중지합니다.

- **approvalToMakeChangesToTheProvidedS3Bucket:**

지정된 보안 주체가 버킷 버전 관리를 비활성화하고 지정된 Amazon S3 버킷에 대한 버킷 정책 및 수명 주기 규칙 구성을 업데이트할 때까지 기다립니다.

- **branchOnBucketVersioningStatus** (조건부):

지정된 Amazon S3 버킷에서 버전 관리가 활성화된 경우 비활성화하고, 그렇지 않으면 버킷 정책 및 수명 주기 구성을 계속 업데이트합니다.

- **suspendBucketVersioning**:

지정된 Amazon S3 버킷의 버전 관리 상태를 일시 중지합니다.

- **updateBucketPolicyAndLifecycleConfiguration**:

버킷 정책을 추가하거나 업데이트하여 모든 s3:PutObject 요청을 거부하고 수명 주기 구성을 업데이트하여 사용자가 제공한 입력 파라미터를 기반으로 객체를 만료시킵니다.

- **branchOnFailingIfBucketPropertiesNotUpdated** (조건부):

updateBucketPolicyAndLifecycleConfiguration 단계의 상태를 확인하고 자동화에 의해 변경된 경우 원래 버킷 버전 관리 상태를 되돌리려고 시도합니다.

- **branchOnFailureOriginalVersioningStatus** (조건부):

장애가 발생하면가 분기하여 원래 버전 관리 상태를 결정합니다. 이 자동화에 의해 활성화되고 일시 중지된 경우는이 자동화를 다시 활성화하려고 시도합니다.

- **onFailureRestoreBucketVersioning**

지정된 Amazon S3 버킷의 활성화된 버전 관리 상태를 복원합니다.

7. 완료되면 출력 섹션에서 실행의 자세한 결과를 검토합니다.

✓ Execution has been initiated.
✕

Execution detail: AWSSupport-EmptyS3Bucket Cancel execution Actions ▾

▶ Execution description

▼ Outputs

updateBucketPolicyAndLifecycleConfiguration.Message
 ===== Execution Result =====
 INFO: Getting the configured lifecycle rules for the S3 Bucket: sample-not-empty-bucket
 INFO: Getting bucket policy for S3 Bucket: sample-not-empty-bucket
 INFO: Creating new bucket policy to deny any s3:PutObject API calls (to prevent new uploads while it is being emptied).
 INFO: Creating a new lifecycle rule to delete all the objects according to the expiration days specified in the input parameters
 INFO: The bucket updates have been successfully completed.
 Upon the expiration of items, as specified in the parameters, the bucket will be emptied.
 Meanwhile, S3 'put object' requests are denied by the bucket policy to prevent the upload of new items.

Execution status
 Overall status
✓ Success

 # Failed
 0

All executed steps
 7

 # Cancelled
 0

Succeeded
 7

 # TimedOut
 0

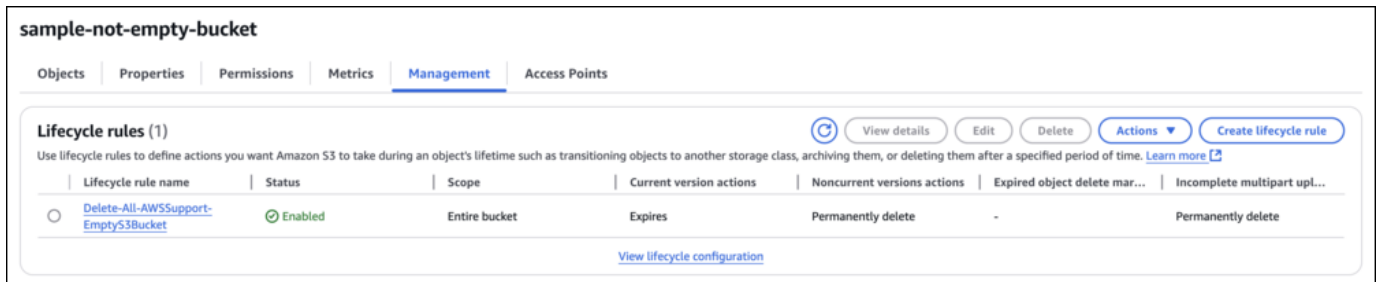
Executed steps (10)

< 1 >

Step ID	Step #	Step name	Action	Status	Start time
17e09354-6a90-4216-9797-a9d6fa18d57c	1	checkConcurrency	aws:executeScript	✓ Success	Wed, 18 Dec 2024 08:01:54 GM
44bc75db-0bd9-44c1-9537-0b9ff9eea87a	2	getBucketVersioningConfiguration	aws:executeAwsApi	✓ Success	Wed, 18 Dec 2024 08:02:08 GM
1e942013-e886-4fce-b685-bc8e578bcb2a	3	branchOnStoppingIfMFADeleteEnabled	aws:branch	✓ Success	Wed, 18 Dec 2024 08:02:09 GM
742066ac-39a8-4699-8aa4-13a7a8b0239f	4	approvalToMakeChangesToTheProvidedS3Bucket	aws:approve	✓ Success	Wed, 18 Dec 2024 08:02:09 GM
34c276bb-f7e3-43f8-a89f-8d457040cc31	5	branchOnBucketVersioningStatus	aws:branch	✓ Success	Wed, 18 Dec 2024 08:03:24 GM
5f3efb16-d6f8-441e-b090-ab6c88ab2a9d	6	updateBucketPolicyAndLifecycleConfiguration	aws:executeScript	✓ Success	Wed, 18 Dec 2024 08:03:25 GM
739dd72a-e7de-42d9-900a-7a0aa5e826d0	7	branchOnFailingIfBucketPropertiesNotUpdated	aws:branch	✓ Success	Wed, 18 Dec 2024 08:03:29 GM
f97fc493-3d62-4884-901f-dcc2a2a3bcd0	8	suspendBucketVersioning	aws:executeAwsApi	⌚ Pending	-
4b02a204-8de7-49c8-b079-e94741c40a37	9	branchOnFailureOriginalVersioningStatus	aws:branch	⌚ Pending	-
92645daf-8587-4947-bc53-b4c440d07f84	10	onFailureRestoreBucketVersioning	aws:executeAwsApi	⌚ Pending	-

• 성공적인 실행

이 워크플로는 버킷의 수명 주기 규칙을 업데이트합니다. 객체는 Delete-All-AWSSupport-EmptyS3-Bucket 수명 주기 정책에 따라 삭제됩니다.



- 실패 실행

부분 삭제는 수행되지 않습니다. 실행이 실패하면 수명 주기 및 기타 버킷 설정이 롤백됩니다.

참조

Systems Manager Automation

- [이 자동화 실행\(콘솔\)](#)
- [자동화 실행](#)
- [Automation 설정](#)
- [자동화 워크플로 지원](#)

Amazon S3 버킷 및 객체 관리에 대한 자세한 내용은 [버킷 비우기](#)를 참조하세요.

AWSSupport-TroubleshootS3EventNotifications

설명

AWSSupport-TroubleshootS3EventNotifications AWS Systems Manager 자동화 실행서는 함수, Amazon Simple Notification Service(Amazon SNS) 버킷 이벤트 알림 문제를 해결하는 데 도움이 됩니다. AWS Lambda Amazon SNS Amazon SQS Amazon S3 버킷을 대상 이벤트 알림으로 사용하여 구성된 다양한 리소스의 구성 설정 보고서를 제공합니다.

어떻게 작동하나요?

실행서는 다음 단계를 수행합니다.

- 가 실행되는 동일한 계정에 Amazon S3 버킷이 존재하는 AWSSupport-TroubleshootS3EventNotifications지 확인합니다.
- [GetBucketNotificationConfiguration](#) API를 사용하여 Amazon S3 버킷에 대한 이벤트 알림으로 구성된 대상 리소스(AWS Lambda 함수 또는 Amazon SNS 주제 또는 Amazon SQS 대기열)를 가져옵니다. Amazon S3

- 대상 리소스가 존재하는지 확인한 다음 대상 리소스의 리소스 기반 정책을 검토하여 Amazon S3가 대상에 게시할 수 있는지 확인합니다.
- AWS Key Management Service (AWS KMS) 키로 대상을 암호화한 경우 키 정책을 확인하여 Amazon S3 액세스가 허용되는지 확인합니다.
- 모든 대상 리소스 검사에 대한 보고서를 생성합니다.

Important

- 이 런북은 Amazon S3 버킷 소유자가 자동화 런북이 실행되는 AWS 계정 소유자와 동일한 경우에만 이벤트 알림 구성을 평가할 수 있습니다.
- 또한 이 실행서는 다른에서 호스팅되는 대상 리소스에 대한 정책을 평가할 수 없습니다 AWS 계정.

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: AWS::S3::Bucket::Name

설명: (필수) 이벤트 알림(들)으로 구성된 Amazon S3 버킷의 이름입니다.

필수 IAM 권한

실행서를 성공적으로 사용하려면 AutomationAssumeRole 파라미터에 다음 작업이 필요합니다.

- s3:GetBucketLocation
- s3:ListAllMyBuckets
- s3:GetBucketNotification
- sqs:GetQueueAttributes
- sqs:GetQueueUrl
- sns:GetTopicAttributes
- kms:GetKeyPolicy
- kms:DescribeKey
- kms:ListAliases
- lambda:GetPolicy
- lambda:GetFunction
- iam:GetContextKeysForCustomPolicy
- iam:SimulateCustomPolicy
- iam:ListRoles
- ssm:DescribeAutomationStepExecutions

자동화 수임 역할에 대한 IAM 정책 예시

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "S3Permission",
```

```

        "Effect": "Allow",
        "Action": [
            "s3:GetBucketLocation",
            "s3:ListAllMyBuckets"
        ],
        "Resource": "*"
    },
    {
        "Sid": "S3PermissionGetBucketNotification",
        "Effect": "Allow",
        "Action": [
            "s3:GetBucketNotification"
        ],
        "Resource": "arn:aws:s3:::amzn-s3-demo-bucket"
    },
    {
        "Sid": "SQSPermission",
        "Effect": "Allow",
        "Action": [
            "sqs:GetQueueAttributes",
            "sqs:GetQueueUrl"
        ],
        "Resource": "arn:aws:sqs:us-east-1:111122223333:*"
    },
    {
        "Sid": "SNSPermission",
        "Effect": "Allow",
        "Action": [
            "sns:GetTopicAttributes"
        ],
        "Resource": "arn:aws:sns:us-east-1:111122223333:*"
    },
    {
        "Sid": "KMSPermission",
        "Effect": "Allow",
        "Action": [
            "kms:GetKeyPolicy",
            "kms:DescribeKey",
            "kms:ListAliases"
        ],
        "Resource": "arn:aws:kms:us-east-1:111122223333:key/key-id"
    }

```

```

    },
    {
      "Sid": "LambdaPermission",
      "Effect": "Allow",
      "Action": [
        "lambda:GetPolicy",
        "lambda:GetFunction"
      ],
      "Resource": "arn:aws:lambda:us-
east-1:111122223333:function:*"
    },
    {
      "Sid": "IAMPermission",
      "Effect": "Allow",
      "Action": [
        "iam:GetContextKeysForCustomPolicy",
        "iam:SimulateCustomPolicy",
        "iam:ListRoles"
      ],
      "Resource": "*"
    },
    {
      "Sid": "SSMPermission",
      "Effect": "Allow",
      "Action": [
        "ssm:DescribeAutomationStepExecutions"
      ],
      "Resource": "*"
    }
  ]
}

```

지침

다음 단계에 따라 자동화를 구성합니다.

1. Systems Manager [AWSSupport-TroubleshootS3EventNotifications](#)의 문서로 이동합니다.
2. Execute automation(자동화 실행)을 선택합니다.
3. 입력 파라미터에 다음을 입력합니다.
 - AutomationAssumeRole(선택 사항):

Systems Manager Automation이 사용자를 대신하여 작업을 수행하도록 허용하는 (IAM) 역할의 Amazon 리소스 이름 AWS AWS Identity and Access Management (ARN)입니다. 역할이 지정되지 않은 경우 Systems Manager Automation은 이 실행서를 시작하는 사용자의 권한을 사용합니다.

- S3BucketName(필수):

이벤트 알림(들)으로 구성된 Amazon S3 버킷의 이름입니다.

Input parameters

AutomationAssumeRole
(Optional) The Amazon Resource Name (ARN) of the AWS Identity and Access Management (IAM) role that allows Systems Manager Automation to perform the actions on your behalf. If no role is specified, Systems Manager Automation uses the permissions of the user that starts this runbook.

AWS-SystemsManager-AutomationAdministrationRole

S3BucketName
(Required) The name of the Amazon S3 bucket configured with event notification(s).

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

- ValidateInputs

제공된 Amazon S3 버킷이 자동화가 실행되는 동일한 계정에 속하는지 확인하고 버킷이 호스팅되는 리전을 가져옵니다.

- GetBucketNotificationConfiguration

GetBucketNotificationConfiguration API를 호출하여 Amazon S3 버킷으로 구성된 이벤트 알림을 검토하고 출력 형식을 지정합니다.

- BranchOnSQSResourcePolicy

이벤트 알림에 Amazon SQS 리소스가 있는지 여부를 분기합니다.

- ValidateSQSResourcePolicy

Amazon SQS 대기열 속성의 리소스 정책에 Amazon S3에 대한 sqs:SendMessage 권한이 있는지 확인합니다. Amazon SQS 리소스가 암호화된 경우는 암호화가 기본 AWS KMS 키, 즉름 사용하고 있지 않은지 aws/sqs 확인하고 AWS KMS 키 정책에 Amazon S3에 대한 권한이 있는지 확인합니다.

- BranchOnSNSResourcePolicy

이벤트 알림에 Amazon SNS 리소스가 있는지 여부를 분기합니다.

- ValidateSNSResourcePolicy

Amazon SNS 주제 속성의 리소스 정책에 Amazon S3에 대한 `sns:Publish` 권한이 있는지 확인합니다. Amazon SNS 리소스가 암호화된 경우는 암호화가 기본 AWS KMS 키, 즉, 사용하고 있지 않은지 `aws/sns` 확인하고 AWS KMS 키 정책에 Amazon S3에 대한 권한이 있는지 확인합니다.

- `BranchOnLambdaFunctionResourcePolicy`

이벤트 알림에 AWS Lambda 함수가 있는지 여부를 분기합니다.

- `ValidateLambdaFunctionResourcePolicy`

AWS Lambda 함수에 대한 리소스 정책이 Amazon S3에 대한 `lambda:InvokeFunction` 권한이 있는지 확인합니다.

- `GenerateReport`

실행서 단계 출력의 세부 정보와 Amazon S3 버킷으로 구성된 이벤트 알림 관련 문제를 해결하기 위한 권장 사항을 반환합니다.

7. 완료되면 출력 섹션에서 실행의 자세한 결과를 검토합니다.

- Amazon SQS 이벤트 알림

Amazon S3 버킷으로 구성된 Amazon SQS 대상 알림이 있는 경우 Amazon SQS 대기열 목록이 검사 결과와 함께 표시됩니다. Amazon S3 보고서에는 Amazon SQS 리소스 확인, Amazon SQS 액세스 정책 확인, AWS KMS 키 확인, AWS KMS 키 상태 확인 및 AWS KMS 키 정책 확인이 포함됩니다.

- Amazon SNS 이벤트 알림

Amazon S3 버킷으로 구성된 Amazon SNS 대상 알림이 있는 경우 Amazon SNS 주제 목록이 검사 결과와 함께 표시됩니다. Amazon S3 보고서에는 Amazon SNS 리소스 확인, Amazon SNS 액세스 정책 확인, AWS KMS 키 확인, AWS KMS 키 상태 확인 및 AWS KMS 키 정책 확인이 포함됩니다.

- AWS Lambda 이벤트 알림

Amazon S3 버킷으로 구성된 AWS Lambda 대상 알림이 있는 경우 Lambda 함수 목록이 검사 결과와 함께 표시됩니다. 보고서에는 Lambda 리소스 검사 및 Lambda 액세스 정책 검사가 포함됩니다.

▼ Outputs

generateReport.Output

```

Amazon S3 Event Notification Troubleshooting Results for S3 Bucket
-----
Amazon SQS Event Notifications
-----
SQS Queue: 1. arn:aws:sqs:us-east-1: :SAW-Core-TroubleshootS3EventNotification-EncryptedQueue | KMS Key: 
SQS resource check [✓][PASSED]: The resource exists in the S3 Bucket Region.
SQS access policy check [✓][PASSED]: The resource policy is properly configured for use with S3 Bucket.
KMS key check [✓][PASSED]: The resource exists in the S3 Bucket Region.
KMS key status check [✗][FAILED]: The KMS key is disabled.
KMS key policy check [✓][PASSED]: The resource policy is properly configured for use with S3 Bucket.
-----
Amazon SNS Event Notifications
-----
SNS Topic: 1. arn:aws:sns:us-east-1: :CoreInfra-TestSNSTopic-IdW0EaySLdmr | KMS Key: alias/aws/sns
SNS resource check [✓][PASSED]: The resource exists in the S3 Bucket Region.
SNS access policy check [✓][PASSED]: The resource policy is properly configured for use with S3 Bucket.
KMS key check [✓][PASSED]: The resource exists in the S3 Bucket Region.
KMS key status check [✓][INFO]: Not Applicable.
KMS key policy check [✗][FAILED]: Amazon S3 Event Notifications does not support using SQS or SNS targets encrypted using AWS managed keys, i.e., aws/sns or aws/sqs respectively.
-----
AWS Lambda Event Notifications
-----
Lambda Function: 1. arn:aws:lambda:us-east-1: :function:SAW-Core-TroubleshootS3EventNotification-LambdaFunction
Lambda resource check [✓][PASSED]: The resource exists in the S3 Bucket Region.
Lambda access policy check [✗][FAILED]: No resource policies found on the resource. Please update the resource with a valid policy using this guide: https://docs.aws.amazon.com/AmazonS3/latest/userguide/grant-destin

```

참조

Systems Manager Automation

- [이 자동화 실행\(콘솔\)](#)
- [자동화 실행](#)
- [Automation 설정](#)
- [Support Automation Workflows 랜딩 페이지](#)

AWSSupport-ContainS3Resource

설명

AWSSupport-ContainS3Resource 실행서는 [Support Automation Workflow\(SAW\) Runbook: Contain a compromised AWS Amazon S3 Bucket](#) 문서에 설명된 절차에 대한 자동화된 솔루션을 제공합니다.

⚠ Important

- 이 실행서는 Amazon S3 버킷 정책, 태그 및 퍼블릭 액세스 구성을 수정하는 등 승격된 권한이 필요한 다양한 작업을 수행합니다. 이러한 작업은 잠재적으로 권한 상승으로 이어지거나 대상 Amazon S3 버킷에 의존하는 다른 워크로드에 영향을 미칠 수 있습니다. AutomationAssumeRole 파라미터에 지정된 역할에 부여된 권한을 검토하고 의도된 사용 사례에 적합한지 확인해야 합니다. IAM 권한에 대한 자세한 내용은 다음 AWS 설명서

를 참조하세요 [Identity and Access Management \(IAM\) Permissions](#) [AWS Systems Manager Automation Permissions](#).

- 이 실행서는 워크로드를 사용할 수 없거나 중단시킬 수 있는 변경 작업을 수행합니다. 특히 Contain 작업은 SecureRoles 파라미터에 지정된 역할을 제외하고 지정된 Amazon S3 버킷에 대한 모든 액세스를 차단합니다. 이는 대상 Amazon S3 버킷에 의존하는 모든 애플리케이션 또는 서비스에 영향을 미칠 수 있습니다.
- Contain 작업 중에 이 실행서는 원본 버킷의 구성 백업이 아직 없는 경우 이를 저장하기 위해 추가 Amazon S3 버킷(BackupS3BucketName 파라미터에 의해 지정됨)을 생성할 수 있습니다.
- Action 파라미터가 로 설정된 경우 Restore 이 실행서는 버킷에 저장된 백업을 기반으로 Amazon S3 BackupS3BucketName 버킷의 구성을 원래 상태로 복원하려고 시도합니다. 그러나 복원 프로세스가 실패하여 Amazon S3 버킷이 일관되지 않은 상태로 유지될 위험이 있습니다. 실행서는 이러한 장애가 발생할 경우 수동 복원에 대한 지침을 제공하지만 복원 프로세스 중에 잠재적 문제를 처리할 준비가 되어 있어야 합니다.

프로덕션 환경에서 실행하기 전에 런북을 철저히 검토하고, 런북의 잠재적 영향을 이해하고, 비프로덕션 환경에서 테스트하는 것이 좋습니다.

어떻게 작동하나요?

이 실행서는 리소스 유형 및 작업에 따라 다르게 작동합니다.

- Amazon S3 범용 버킷의 경우 Containment: 자동화는 버킷에 대한 퍼블릭 액세스를 차단하고, ACL 구성을 비활성화하고, 버킷 소유자 객체 소유권을 적용하고, 나열된 IAM 역할 허용을 제외한 모든 Amazon S3 작업을 버킷에 거부하는 제한적인 버킷 정책을 적용합니다.
- Amazon S3 범용 객체의 경우 Containment: 자동화는 버킷에 대한 퍼블릭 액세스를 차단하고, ACL 구성을 비활성화하고, 버킷 소유자 객체 소유권을 적용하고, 나열된 IAM 역할 허용을 제외한 객체에 대한 모든 Amazon S3 작업을 거부하는 제한적인 버킷 정책을 적용합니다.
- Amazon S3 디렉터리 버킷의 경우 Containment: 자동화는 나열된 IAM 역할 허용을 제외한 모든 Amazon S3 작업을 버킷에 거부하는 제한적인 버킷 정책을 적용합니다.
- Amazon S3 범용 버킷의 경우 Restore: 자동화는 격리 전에 퍼블릭 액세스 차단 구성, 버킷 ACL 구성, 버킷 소유자 객체 소유권 및 버킷 정책을 초기 구성으로 복원합니다.
- Amazon S3 범용 객체의 경우 Restore: 자동화는 퍼블릭 액세스 차단 구성, 버킷 ACL 구성, 객체 ACL 구성, 버킷 소유자 객체 소유권 및 버킷 정책을 격리 전 초기 구성으로 복원합니다.

- Amazon S3 디렉터리 버킷의 경우 Restore: 자동화는 격리 전에 버킷 정책을 초기 구성으로 복원합니다.

[이 자동화 실행\(콘솔\)](#)

문서 유형

자동화

소유자

Amazon

플랫폼

/

필요한 IAM 권한

실행서를 성공적으로 사용하려면 AutomationAssumeRole 파라미터에 다음 작업이 필요합니다.

- s3:CreateBucket
- s3:DeleteBucketPolicy
- s3:DeleteObjectTagging
- s3:GetAccountPublicAccessBlock
- s3:GetBucketAcl
- s3:GetBucketLocation
- s3:GetBucketOwnershipControls
- s3:GetBucketPolicy
- s3:GetBucketPolicyStatus
- s3:GetBucketTagging
- s3:GetEncryptionConfiguration
- s3:GetObject
- s3:GetObjectAcl
- s3:GetObjectTagging
- s3:GetReplicationConfiguration
- s3:ListBucket

- s3:PutAccountPublicAccessBlock
- s3:PutBucketACL
- s3:PutBucketOwnershipControls
- s3:PutBucketPolicy
- s3:PutBucketPublicAccessBlock
- s3:PutBucketTagging
- s3:PutBucketVersioning
- s3:PutObject
- s3:PutObjectAcl
- s3express:CreateSession
- s3express:DeleteBucketPolicy
- s3express:GetBucketPolicy
- s3express:PutBucketPolicy
- ssm:DescribeAutomationExecutions

다음은에 필요한 권한을 부여하는 IAM 정책의 예입니다. AutomationAssumeRole

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "S3Permissions",
      "Effect": "Allow",
      "Action": [
        "s3:CreateBucket",
        "s3:DeleteBucketPolicy",
        "s3:DeleteObjectTagging",
        "s3:GetAccountPublicAccessBlock",
        "s3:GetBucketAcl",
        "s3:GetBucketLocation",
        "s3:GetBucketOwnershipControls",
        "s3:GetBucketPolicy",
        "s3:GetBucketPolicyStatus",
        "s3:GetBucketTagging",
```

```

        "s3:GetEncryptionConfiguration",
        "s3:GetObject",
        "s3:GetObjectAcl",
        "s3:GetObjectTagging",
        "s3:GetReplicationConfiguration",
        "s3:ListBucket",
        "s3:PutAccountPublicAccessBlock",
        "s3:PutBucketACL",
        "s3:PutBucketOwnershipControls",
        "s3:PutBucketPolicy",
        "s3:PutBucketPublicAccessBlock",
        "s3:PutBucketTagging",
        "s3:PutBucketVersioning",
        "s3:PutObject",
        "s3:PutObjectAcl"
    ],
    "Resource": "*"
},
{
    "Sid": "S3ExpressPermissions",
    "Effect": "Allow",
    "Action": [
        "s3express:CreateSession",
        "s3express:DeleteBucketPolicy",
        "s3express:GetBucketPolicy",
        "s3express:PutBucketPolicy"
    ],
    "Resource": "*"
},
{
    "Sid": "SSMPermissions",
    "Effect": "Allow",
    "Action": [
        "ssm:DescribeAutomationExecutions"
    ],
    "Resource": "*"
}
]
}

```

지침

다음 단계에 따라 자동화를 구성합니다.

1. Systems Manager [AWSSupport-ContainS3Resource](#)의 문서로 이동합니다.
2. Execute automation(자동화 실행)을 선택합니다.
3. 입력 파라미터에 다음을 입력합니다.
 - BucketName(필수):
 - 설명: (필수) Amazon S3 버킷의 이름입니다.
 - 유형: AWS::S3::Bucket::Name
 - 작업(필수):
 - 설명: (필수) Amazon S3 리소스를 Contain 격리Restore하거나 이전 백업에서 리소스 구성을 원래 상태로 복원하려고 합니다.
 - 유형: String
 - 허용된 값: Contain|Restore
 - DryRun(선택 사항):
 - 설명: (선택 사항) true로 설정하면 자동화는 대상 Amazon S3 리소스를 변경하지 않고 변경하려고 시도한 내용을 출력합니다. 기본값: true.
 - 유형: Boolean
 - 허용되는 값: true|false
 - BucketKeyName(선택 사항):
 - 설명: (선택 사항) 포함하거나 복원하려는 Amazon S3 객체의 키입니다. 객체 수준 억제 중에 사용됩니다.
 - 유형: 문자열
 - 허용된 패턴: `^[a-zA-Z0-9\\.\_-\\\\\\!*'()/]{0,1024}$`
 - BucketRestrictAccess(조건부):
 - 설명: (조건부) 억제 작업을 실행한 후 대상 Amazon S3 리소스에 대한 액세스가 허용되는 IAM 사용자 또는 역할의 ARN입니다. Action이 Contain로 설정되는 경우 이 파라미터가 필요합니다.
 - 유형: StringList
 - 허용된 패턴: `^$|^arn:(aws|aws-cn|aws-us-gov|aws-iso(-[a-z]))?:iam::[0-9]{12}:(role|user)\\/[\\w+\\V/=, .@-]+$`
 - TagIdentifier(선택 사항):
 - 설명: (선택 사항) 억제 워크플로 중에이 실행서에 의해 생성되거나 수정된 리소스에 추가될 Key=BatchId,Value=78925 형식의 태그입니다.
 - 유형: 문자열

- 허용된 패턴: `^$|^([Kk][Ee][Yy]=[\\+\\-\\=\\.\\_\\\\:\\/@a-zA-Z0-9]{1,128},[Vv][Aa][Ll][Uu][Ee]=[\\+\\-\\=\\.\\_\\\\:\\/@a-zA-Z0-9]{0,128})$`
 - BackupS3BucketName(조건부):
 - 설명: (조건부)가 로 설정된 경우 대상 리소스 구성을 백업Contain하거나 Action가 로 설정된 경우 구성을 복원하는 Amazon S3 버킷Action입니다Restore.
 - 유형: `AWS::S3::Bucket::Name`
 - BackupS3KeyName(조건부):
 - 설명: (조건부) Action이 로 설정된 경우 Restore자동화가 대상 리소스 구성을 복원하는 데 사용할 Amazon S3 키를 지정합니다.
 - 유형: 문자열
 - 허용된 패턴: `^[a-zA-Z0-9\\.\\-\\_\\\\\\!*'()]/]{0,1024}$`
 - BackupS3BucketAccess(조건부):
 - 설명: (조건부) 억제 작업을 실행한 후 백업 Amazon S3 버킷에 대한 액세스가 허용되는 IAM 사용자 또는 역할의 ARN입니다. 이 파라미터는 이 Action 일 때 필요합니다Contain.
 - 유형: `StringList`
 - 허용된 패턴: `^$|^arn:(aws|aws-cn|aws-us-gov|aws-iso(-[a-z]))?:iam::[0-9]{12}:(role|user)\\/[\\w+\\/=,\\.@-]+$`
 - AutomationAssumeRole(선택 사항):
 - 설명: (선택 사항) Systems Manager Automation이 사용자를 대신하여 작업을 수행할 수 있도록 허용하는 IAM 역할의 Amazon 리소스 이름(ARN)입니다.
 - 유형: `AWS::IAM::Role::Arn`
4. 실행을 선택합니다.
 5. 자동화가 시작됩니다.
 6. 문서는 다음 단계를 수행합니다.
 - `validateRequiredInputs`

지정된 작업을 기반으로 필요한 자동화 입력 파라미터를 검증합니다.
 - `assertBucketExists`

대상 Amazon S3 버킷이 존재하고 액세스할 수 있는지 확인합니다.
 - `backupBucketPreChecks`

백업 Amazon S3 버킷이 객체에 대한 퍼블릭 읽기 또는 쓰기 액세스 권한을 부여할 가능성이 있는지 확인합니다.

- backupTargetBucketMetadata

대상 Amazon S3 버킷의 현재 구성을 설명하고 백업을 지정된 백업 Amazon S3 버킷에 업로드합니다.

- containBucket

대상 Amazon S3 버킷을 포함하는 버킷 수준 작업을 수행합니다.

- BranchOnActionAndMode

입력 파라미터 Action 및 DryRun을 기반으로 자동화를 분기합니다.

- RestoreInstanceConfiguration

백업에서 Amazon S3 버킷 구성을 복원합니다.

- containFinalOutput

격납 활동을 읽기 가능한 형식으로 통합합니다.

- ReportContain

억제 작업에 대한 모의 실행 세부 정보를 출력합니다.

- ReportRestore

복원 작업에 대한 모의 실행 세부 정보를 출력합니다.

- ReportRestoreFailure

복원 워크플로 실패 시나리오 중에 Amazon S3 버킷 원래 구성을 복원하는 지침을 제공합니다.

- ReportContainmentFailure

억제 워크플로 실패 시나리오 중에 Amazon S3 버킷 원래 구성을 복원하는 지침을 제공합니다.

- FinalOutput

억제 작업의 세부 정보를 출력합니다.

7. 실행이 완료되면 출력 섹션에서 실행의 자세한 결과를 검토합니다.

- ContainFinalOutput.Output

- `RestoreFinalOutput.Output`

DryRun이 False로 설정된 경우 이 실행서에서 수행하는 복원 작업의 세부 정보를 출력합니다.

- `ContainS3ResourceDryRun.Output`

DryRun이 True로 설정된 경우 이 실행서에서 수행하는 억제 작업의 세부 정보를 출력합니다.

- `RestoreS3ResourceDryRun.Output`

이 True로 DryRun 설정된 경우 이 실행서에서 수행하는 복원 작업의 세부 정보를 출력합니다.

- `ReportContainmentFailure.Output`

억제 워크플로 실패 시나리오 중에 대상 Amazon S3 리소스 원래 구성을 복원하는 지침을 제공합니다.

- `ReportRestoreFailure.Output`

복원 워크플로 실패 시나리오 중에 대상 Amazon S3 리소스 원래 구성을 복원하는 지침을 제공합니다.

참조

Systems Manager Automation

- [이 자동화 실행\(콘솔\)](#)
- [자동화 실행](#)
- [Automation 설정](#)
- [자동화 워크플로 지원](#)

Amazon SES

AWS Systems Manager Automation은 Amazon Simple Email Service에 사전 정의된 실행서를 제공합니다. 실행서에 대한 자세한 내용은 [실행서 작업](#)을 참조하세요. 실행서 콘텐츠를 보는 방법에 대한 자세한 내용은 [실행서 콘텐츠 보기](#)(을)를 참조하세요.

주제

- [AWSsupport-AnalyzeSESMessagesSendingStatus](#)
- [AWSsupport-DeploySESSendingLogsToCloudWatchLogs](#)

AWSSupport-AnalyzeSESMessagesSendingStatus

설명

AWSSupport-AnalyzeSESMessagesSendingStatus 자동화 실행서는 전송되지 않은 이메일 메시지의 이메일 전송 상태를 요약하고 전송되지 않은 이유를 해결하기 위한 조언을 제공합니다. 실행서는 Amazon SES에서 게시한 Amazon CloudWatch Logs 그룹에 저장된 Amazon Simple Email Service(Amazon SES) 이메일 전송 이벤트를 검색합니다. Amazon CloudWatch 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. 이러한 메시지는 각 실행의 출력 섹션에서 찾을 수 있습니다. 이 실행서는 이벤트 스토어 배포 후에만 이벤트 문제를 해결할 수 있습니다.

어떻게 작동하나요?

실행서는 다음 단계를 수행합니다.

- 동일한 CloudWatch Logs 그룹에 대한 동시 자동화 실행을 확인합니다.
- 자동화 파라미터에서 제공하는 메시지 IDs에 해당하는 Amazon SES 이벤트를 분석합니다.
- 자동화 실행의 출력 섹션에 대한 출력 전송 요약입니다.

Important

- 이 실행서를 실행하기 전에 게시된 Amazon SES 이벤트를 자동화 파라미터로 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

파라미터

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-AnalyzeSESMessagesSendingStatus](#)의 문서로 이동합니다.
2. Execute automation(자동화 실행)을 선택합니다.
3. 입력 파라미터에 다음을 입력합니다.

- AutomationAssumeRole(선택 사항):

Systems Manager Automation이 사용자를 대신하여 작업을 수행하도록 허용하는 (IAM) 역할의 Amazon 리소스 이름 AWS AWS Identity and Access Management (ARN)입니다. 역할이 지정되지 않은 경우 Systems Manager Automation은 이 실행서를 시작하는 사용자의 권한을 사용합니다.

- MessageIds(필수)

분석하려는 Amazon Simple Email Service 이벤트의 Amazon Simple Email Service 메시지 IDs를 쉼표로 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 사용하려면이 필드에 로그 그룹 이름을 입력하십시오.",

- **QueryStartTime(선택 사항)**

이벤트 분석을 위한 시간 범위의 시작 시간입니다. 유효한 시간 형식은 ISO8601(예: ``yyyy-MM-ddTHH: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-ddTHH:mm:ss``, ``1970-01-01T00:00:00``)입니다. 기본 날짜 시간은 현재 시간입니다.

Input parameters

AutomationAssumeRole
(Optional) The Amazon Resource Name (ARN) of the AWS Identity and Access Management (IAM) role that allows Systems Manager Automation to perform the actions on your behalf. If no role is specified, Systems Manager Automation uses the permissions of the user that starts this runbook.

▼

↺

CloudWatchLogsGroup
(Optional) The Amazon CloudWatch Logs group which stores Amazon SES events. The default log group name is `/ses/sending_event_logs`. If you would like to utilize another log group than the default log group, please enter your log group name in this field.

QueryEndTime
(Optional) The end time of the time range for the event analysis. The valid time format is ISO8601 (e.g. ``yyyy-MM-ddTHH:mm:ss``, ``1970-01-01T00:00:00``). The default date time is the current time.

MessageIds
(Required) Comma separated Amazon SES message IDs of the Amazon SES events that you would like to analyze.

QueryStartTime
(Optional) The start time of the time range for the event analysis. The valid time format is ISO8601 (e.g. ``yyyy-MM-ddTHH:mm:ss``, ``1970-01-01T00:00:00``). The default date time is 30 days ago.

4. 실행을 선택합니다.

5. 자동화가 시작됩니다.

6. 문서는 다음 단계를 수행합니다.

- **CheckConcurrency:**

Amazon CloudWatch Logs 그룹을 대상으로 하는이 실행서의 실행이 하나만 있는지 확인합니다. 실행서가 동일한 로그 그룹을 대상으로 하는 다른 실행을 찾으면 오류가 반환되고 종료됩니다.

- **AnalyzeSesEvents:**

자동화 파라미터로 지정된 Amazon CloudWatch Logs 그룹에 저장된 Amazon Simple Email Service 이벤트를 분석합니다.

- **OutputFailureReason:**

단계가 실패할 때 실행 AnalyzeSESMessagesSendingStatus 단계 실패 메시지를 출력합니다.

7. 완료되면 출력 섹션에서 실행의 자세한 결과를 검토합니다.

- 반송 메일로 인해 전송되지 않은 이메일 메시지에 대한 분석 출력

반송 메일로 인해 대상 사서함에 도달하지 못한 이메일 메시지에 대한 자동화 실행의 출력입니다.

▼ Outputs

OutputFailureReason.FailureReason

No output available yet because the step is not successfully executed

AnalyzeSesEvents.ResultMessage

```

==== Delivery summary of the message ID [REDACTED] ====
SES received bounces or complaints.

==== Timeline of [REDACTED] =====
[2024-08-21 06:22:58.193000+00:00] Your email message was sent from SES.
[2024-08-21 06:22:58.193000+00:00] SES received a bounce from [REDACTED].
Bounce type: Permanent(General)
Bounce sources:
- email address: [REDACTED] diagnostic code: "smtp; 550 5.1.1 user unknown"

==== Next Action ====
Please fix the issues described in the delivery error messages returned from the destination email servers in the Timeline section. In the case you received s

===== Recommendations for arn:aws:ses:[REDACTED] =====
- The SES account in this region seems to be in the sandbox environment. If you haven't requested the production access, please consider to move out of the san

```

참조

Systems Manager Automation

- [이 자동화 실행\(콘솔\)](#)
- [자동화 실행](#)
- [Automation 설정](#)
- [Support Automation Workflows 랜딩 페이지](#)

AWSSupport-DeploySESSendingLogsToCloudWatchLogs

설명

AWSSupport-DeploySESSendingLogsToCloudWatchLogs 자동화 실행서는 Amazon Simple Email Service(Amazon SES) 이벤트를 Amazon CloudWatch Logs(CloudWatch Logs)에 게시하는 데 필요한 인프라를 구성하는 데 도움이 됩니다. 이 실행서는 이메일 전송 이벤트를 캡처하고 모니터링 및 분석을

위해 CloudWatch Logs에 저장하는 데 필요한 구성 요소를 설정합니다. Amazon SES 이벤트 게시에 대한 자세한 내용은 [Amazon SES 이벤트 게시를 사용하여 이메일 전송 모니터링을 참조하세요](#).

ApproveDeployAnalyticEnvironment 파라미터가 로 설정되면 approve이 실행서는 AWS 계정에 새 AWS 리소스를 생성합니다. 로 설정하지 않으면 SleepTime 파라미터에 지정된 시간이 지나면 CloudFormation 스택이 자동으로 삭제됩니다.

어떻게 작동하나요?

이 실행서는 다음 작업을 수행합니다.

- Amazon Simple Notification Service(Amazon SNS) 주제 또는 전송 스트림에 대해 이벤트 대상이 구성된 기존 구성 세트를 나열합니다.
- ApproveDeployAnalyticEnvironment 파라미터가 로 설정된 경우 Amazon SES 이벤트가 CloudWatch Logs에 게시하는 데 필요한 인프라를 생성합니다 approve.

ApproveDeployAnalyticEnvironment 파라미터가 로 설정되면 approve 실행서는 다음 리소스를 생성합니다.

- 다음을 AWSSupport-SESSendingLogsToCloudWatchLogs 포함하는 라는 CloudFormation 스택:
 - AWS Key Management Service (AWS KMS) 암호화가 포함된 Amazon SNS 주제
 - Amazon Simple Queue Service(Amazon SQS) 대기열
 - AWS Lambda 이메일 전송 이벤트 처리를 위한 함수
 - AWS Identity and Access Management Amazon SQS 및 CloudWatch Logs에 대한 권한이 있는 (IAM) 실행 역할
 - CloudWatch Logs 로그 그룹
 - AWS KMS 암호화를 위한 키
 - 이벤트 대상이 있는 Amazon SES 구성 세트
- 인프라는 Amazon SES 이메일 전송 이벤트 → Amazon SES 구성 세트 → Amazon SNS 주제 → Amazon SQS 대기열 → Lambda 함수 → CloudWatch Logs 흐름에서 이메일 전송 이벤트를 처리합니다.
- SesIdentity 파라미터가 제공될 때 생성된 구성 세트를 지정된 Amazon SES 자격 증명의 기본 구성 세트로 연결합니다.

[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`
- `cloudformation:DescribeStackEvents`
- `cloudformation:DescribeStacks`
- `iam:CreateRole`
- `iam:AttachRolePolicy`
- `iam:PassRole`
- `kms:CreateKey`
- `kms:CreateAlias`
- `lambda:CreateFunction`
- `lambda:AddPermission`
- `logs:CreateLogGroup`
- `logs:PutRetentionPolicy`
- `ses:CreateConfigurationSet`
- `ses:CreateConfigurationSetEventDestination`
- `ses:ListConfigurationSets`
- `ses:PutEmailIdentityConfigurationSetAttributes`
- `sns:CreateTopic`
- `sns:Subscribe`
- `sqs:CreateQueue`

- sqs:SetQueueAttributes
- ssm:DescribeAutomationExecutions

정책 예제:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "cloudformation:CreateStack",
        "cloudformation>DeleteStack",
        "cloudformation:DescribeStackEvents",
        "cloudformation:DescribeStacks",
        "iam:CreateRole",
        "iam:AttachRolePolicy",
        "iam:PassRole",
        "kms:CreateKey",
        "kms:CreateAlias",
        "lambda:CreateFunction",
        "lambda:AddPermission",
        "logs:CreateLogGroup",
        "logs:PutRetentionPolicy",
        "ses:CreateConfigurationSet",
        "ses:CreateConfigurationSetEventDestination",
        "ses:ListConfigurationSets",
        "ses:PutEmailIdentityConfigurationSetAttributes",
        "sns:CreateTopic",
        "sns:Subscribe",
        "sqs:CreateQueue",
        "sqs:SetQueueAttributes",
        "ssm:DescribeAutomationExecutions"
      ],
      "Resource": "*"
    }
  ]
}
```

지침

다음 단계에 따라 자동화를 구성합니다.

1. Systems Manager [AWSSupport-DeploySESSendingLogsToCloudWatchLogs](#)의 문서로 이동합니다.
2. Execute automation(자동화 실행)을 선택합니다.
3. 입력 파라미터에 다음을 입력합니다.
 - AutomationAssumeRole(선택 사항):
 - 설명: (선택 사항) Systems Manager Automation이 사용자를 대신하여 작업을 수행할 수 있도록 허용하는 IAM 역할의 Amazon 리소스 이름(ARN)입니다. 역할을 지정하지 않은 경우, Systems Manager Automation에서는 이 실행서를 시작하는 사용자의 권한을 사용합니다.
 - 유형: `AWS::IAM::Role::Arn`
 - ApproveDeployAnalyticEnvironment(선택 사항):
 - 설명: (선택 사항) Amazon SES 이벤트 게시 인프라를 배포하기 위한 승인입니다. approve를 입력하여 CloudFormation 스택 및 관련 리소스를 생성합니다. 비워 두면 실행서는 현재 리전에 또는 Amazon SNS 이벤트 대상이 있는 기존 구성 세트만 표시합니다.
 - 유형: `String`
 - 패턴 허용: `^$|^approve$`
 - 기본값: `""`
 - SesIdentity(선택 사항):
 - 설명: (선택 사항) 새로 생성된 구성 세트와 연결할 Amazon SES 자격 증명(이메일 주소 또는 도메인)을 기본 구성 세트로 설정합니다. 이렇게 하면 지정된 자격 증명에 대한 기존 기본 구성 세트를 덮어씁니다.
 - 유형: `String`
 - 기본값: `""`
 - CloudWatchLogGroupName(선택 사항):
 - 설명: (선택 사항) Amazon SES 이메일 전송 이벤트를 저장하기 위해 생성할 CloudWatch Logs 로그 그룹의 이름입니다.
 - 유형: `String`
 - 패턴 허용: `^[0-9a-zA-Z_.#/\-]{1,512}$`
 - 기본값: `/ses/sending_event_logs`
 - MaskPIIData(선택 사항):
 - 설명: (선택 사항) CloudWatch Logs에서 대상 이메일 주소 및 이메일 제목과 같은 개인 식별 정보(PII) 데이터를 마스킹할지 여부를 지정합니다. 로그에 이 정보를 포함 `False`하려면 `로 설정합`

- 유형: String
 - 허용된 값: [True, False]
 - 기본값: True
 - SleepTime(선택 사항):
 - 설명: (선택 사항) CloudFormation 스택을 자동으로 삭제하기 전에 기다려야 하는 분 수입니다. 기본값은 24시간(1,440분), 최대 7일(10,080분)입니다. 자동 삭제0를 방지하려면 로 설정합니다.
 - 유형: String
 - 패턴 허용: `^(?:[0-9]|[1-9]\\d{1,3}|100[0-7][0-9])$`
 - 기본값: 1440
 - RetainCloudWatchLogsOnDeletion(선택 사항):
 - 설명: (선택 사항) CloudFormation 스택이 삭제될 때 CloudWatch Logs 로그 그룹을 유지할지 여부를 지정합니다. 스택과 함께 로그 그룹을 삭제False하려면 로 설정합니다.
 - 유형: String
 - 허용된 값: [True, False]
 - 기본값: True
 - UniqueId(선택 사항):
 - 설명: (선택 사항) 워크플로의 고유한 식별자입니다.
 - 유형: String
 - 패턴 허용: `\\{\\{ automation:EXECUTION_ID \\}\\}\\{[a-zA-Z0-9-]+`
 - 기본값: `{{ automation:EXECUTION_ID }}`
 - ax 문자: 64
4. 실행을 선택합니다.
 5. 자동화가 시작됩니다.
 6. 문서는 다음 단계를 수행합니다.
 - BranchOnValueOfParameterApproveDeployAnalyticEnvironment

ApproveDeployAnalyticEnvironment 파라미터 값을 기반으로 Amazon SES 이벤트 게시 인프라를 배포할지 여부를 결정합니다.

 - GetEligibleConfigurationSets

기존 Amazon SES 구성 세트를 검색하고 전송 스트림 또는 Amazon SNS 주제에 대해 구성된 이벤트 대상이 있는 세트를 식별합니다.

- CheckConcurrency

기존 스택이 없고 이 실행서의 다른 동시 실행이 동일한 스택을 생성하고 있지 않은지 확인합니다.

- DeploySesEventDestinations

Amazon SNS 주제, Amazon SQS 대기열, Lambda 함수 및 CloudWatch Logs 로그 그룹을 포함한 Amazon SES 이벤트 게시 인프라가 포함된 CloudFormation 스택을 생성합니다. Amazon SNS Amazon SQS CloudWatch

- RelateConfigurationSetAsDefaultConfigurationSet

새로 생성된 Amazon SES 구성 세트를 지정된 Amazon SES 자격 증명의 기본 구성 세트로 연결합니다(제공된 경우).

- SleepBeforeDeleteCloudFormationStack

CloudFormation 스택 삭제를 진행하기 전에 SleepTime 파라미터에서 지정된 기간 동안 기다립니다.

- DeleteCloudFormationStack

지정된 기간 이후에 CloudFormation 스택을 삭제합니다.

7. 완료 후 출력 섹션에서 실행의 자세한 결과를 검토합니다.

참조

Systems Manager Automation

- [이 자동화 실행\(콘솔\)](#)
- [자동화 실행](#)
- [Automation 설정](#)
- [Support Automation Workflows 랜딩 페이지](#)

SageMaker AI

AWS Systems Manager 자동화는 Amazon SageMaker AI를 위한 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-DisableSageMakerNotebookRootAccess](#)
- [AWSSupport-RequestSageMakerLimitIncrease](#)

AWS-DisableSageMakerNotebookRootAccess

설명

AWS-DisableSageMakerNotebookRootAccess 실행서는 Amazon SageMaker AI 노트북 인스턴스에서 루트 액세스를 비활성화합니다. 자동화 중에 필요한 변경을 수행하기 위해 노트북 인스턴스가 중지됩니다. SageMaker AI Studio 노트북 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.

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

- NotebookInstanceName

유형: 문자열

설명: (필수) 루트 액세스를 비활성화할 SageMaker AI 노트북 인스턴스의 이름입니다.

- StartInstanceAfterUpdate

유형: Boolean

기본값: true

설명: (선택 사항) 루트 액세스를 비활성화한 후 노트북 인스턴스가 시작되는지 여부를 결정합니다. 이 파라미터의 기본 설정은 `true`입니다. `true`로 설정하면 루트 액세스가 비활성화된 후 인스턴스가 시작됩니다. `false`로 설정하면 루트 액세스가 비활성화된 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 `in`인 경우 인스턴스를 시작합니다 `stopped`.
- `WaitForInstanceToStop(aws:waitForAwsResourceProperty)`: 인스턴스가 `in`인지 확인합니다 `stopped`.

- UpdateNotebookInstance(aws:executeAwsApi): 노트북 인스턴스에서 루트 액세스를 비활성화합니다.
- WaitForNotebookUpdate(aws:waitForAwsResourceProperty): 루트 액세스가 비활성화되었고 인스턴스가 stopped 상태인지 확인합니다.
- ChooseInstanceStart(aws:branch): 인스턴스를 시작해야 하는지 여부에 따라 분기합니다.
- StartNotebookInstance(aws:executeAwsApi): 노트북 인스턴스를 시작합니다.
- VerifyNotebookInstanceStatus(aws:waitForAwsResourceProperty): 루트 액세스를 비활성화available하기 전에 인스턴스가 인지 확인합니다.
- VerifyNotebookInstanceRootAccess(aws:assertAwsResourceProperty): 노트북 인스턴스 루트 액세스 설정이 성공적으로 비활성화되었는지 확인합니다.

AWSsupport-RequestSageMakerLimitIncrease

설명

AWSsupport-RequestSageMakerLimitIncrease 실행서를 사용하면 단일 작업으로 여러 Amazon SageMaker AI(SageMaker AI) 할당량 증가 요청을 대량으로 제출할 수 있으므로 대규모 기계 학습 워크로드에 대한 할당량 관리를 간소화할 수 있습니다. 실행서는 조정 가능한 SageMaker AI 서비스 할당량에 대해 각 요청을 검증하고, 즉각적인 처리를 위해 자동 승인 임계값 내에서 요청을 라우팅하고, 수동 검토가 필요한 요청에 대한 AWS 지원 사례를 생성합니다. 할당량 증가는 실행서가 실행되는 리전과 동일한 AWS 리전에 적용됩니다.

Important

이 실행서는 P4, P5, Trainium 인스턴스 유형을 포함한 특수 컴퓨팅 인스턴스에 대한 할당량 증가 요청을 지원하지 않습니다. 이러한 인스턴스 유형의 경우 AWS Service Quotas 콘솔 또는 AWS 지원을 통해 개별 할당량 증가 요청을 제출합니다.

실행서는 Amazon Simple Notification Service(Amazon SNS) 알림을 통해 지정된 보안 주체의 승인을 기다리는 동안 최대 1시간 동안 일시 중지됩니다. 승인된 할당량 증가는 되돌릴 수 없으므로 승인하기 전에 ApproveQuotaCodeLimitMapping 단계 출력을 주의 깊게 검토하세요.

[이 자동화 실행\(콘솔\)](#)

문서 유형

자동화

소유자

Amazon

플랫폼

Linux, macOS, Windows

파라미터

- AutomationAssumeRole

유형: AWS::IAM::Role::Arn

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

- ResourcesMapping

유형: StringList

설명: (필수) 콜론으로 구분된 값으로 지정된 늘릴 SageMaker AI 서비스 할당량입니다. 다음 세 가지 형식을 지원합니다.

- Category:Resource:NewValue - 범주 및 리소스 이름을 모두 사용할 수 있는 경우. 예시: spot-training-job:ml.c4.xlarge:25
- Resource:NewValue - 리소스 이름만 사용할 수 있는 경우. 예시: max_number_of_experiment_trial_associations:501
- QuotaCode:NewValue - 직접 할당량 코드를 사용하는 경우. 예시: L-9xAxx23x:25

동일한 요청에서 형식을 쉼표로 구분하여 혼합할 수 있습니다. 최대 50개 항목. 예시: studio:CodeEditor-ml.r6id.large:787,spot-training-job:ml.c4.xlarge:34,L-99AEC235:2

- SNSTopicArn

유형: 문자열

설명: (필수) 자동화 실행 중에 승인 알림을 보내는 데 사용되는 Amazon SNS 주제의 ARN입니다.

- ApproverIAM

유형: StringList

설명: (필수) 할당량 증가 요청을 승인하거나 거부할 수 있는 AWS 인증된 보안 주체 목록입니다. 최대 10명의 승인자. 허용되는 형식: IAM 사용자 이름, IAM 사용자 ARN, IAM 역할 ARN 또는 IAM 수임 역할 사용자 ARN.

- MinimumRequiredApprovals

유형: 정수

유효한 값: 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10

기본값: 1

설명: (선택 사항) 자동화를 재개하는 데 필요한 최소 승인 수입니다. 예 정의된 승인자 수를 초과할 수 없습니다ApproverIAM.

필수 IAM 권한

실행서를 성공적으로 사용하려면 AutomationAssumeRole 파라미터에 다음 작업이 필요합니다.

- servicequotas:ListServiceQuotas
- servicequotas:RequestServiceQuotaIncrease
- servicequotas:GetRequestedServiceQuotaChange
- sns:Publish
- ssm:SendAutomationSignal

문서 단계

1. VerifyCategoriesAndResources - AWS Service Quotas API를 사용하여 조정 가능한 SageMaker AI 서비스 할당량과 비교하여 지정된 모든 범주 및 리소스를 검증합니다. 각 범주 및 리소스 이름이 존재하고 수정 가능한지 확인하고 새 제한이 현재 값보다 낮은 요청을 식별합니다.
2. BranchOnValidCategoriesFound - 유효한 할당량 매핑이 발견되었는지 확인합니다. 유효한 매핑이 있는 경우는 로 진행합니다ApproveQuotaCodeLimitMapping. 그렇지 않으면가 로 직접 건너뛸니다GenerateSummaryReport.

3. **ApproveQuotaCodeLimitMapping** - 처리할 준비가 된 유효한 요청, 설명이 포함된 잘못된 요청 (예: 현재 값보다 낮은 제한 또는 지원되지 않는 할당량 코드), 승인 전 검토를 위한 모든 할당량 증가 요청의 전체 분석을 보여주는 자세한 승인 메시지를 준비합니다.
4. **WaitingForApproval** - 자동화를 일시 중지하고 지정된 Amazon SNS 주제에 승인 알림을 보냅니다. 지정된 승인자는 **ApproveQuotaCodeLimitMapping** 단계 출력을 검토하고 요청을 승인하거나 거부해야 합니다. 이 단계는 아무 조치도 취하지 않으면 3600초(1시간) 후에 시간 초과됩니다.
5. **RequestQuotaIncreases** - AWS Service Quotas API를 통해 유효한 각 리소스에 대한 개별 할당량 증가 요청을 제출합니다. API 제한을 방지하기 위해 초당 1회 요청의 속도가 조정됩니다. 지수 재시도로 API 예외를 처리합니다.
6. **WaitForRequestQuotaIncreaseResults** - PENDING 상태가 유지되지 않을 때까지 제출된 모든 할당량 증가 요청의 상태를 폴링합니다. 허용되는 터미널 상태는 CASE_OPENED, , APPROVED, DENIED, NOT_APPROVED 및 CASE_CLOSED입니다. INVALID_REQUEST.
7. **GetRequestQuotaIncreaseResults** - AWS Service Quotas API에서 제출된 모든 할당량 증가 요청의 최종 상태를 검색하고 보고를 위해 지원 사례 IDs 해당 리소스 및 요청 IDs에 매핑합니다.
8. **GenerateSummaryReport** - 총 요청 수, 요청별 세부 정보, 수동 검토가 필요한 요청에 대한 지원 사례 IDs 대한 포괄적인 요약은 컴파일합니다.

출력

GenerateSummaryReport.SummaryReport - 모든 할당량 증가 요청, 상태 및 수동 검토를 위해 생성된 지원 사례 IDs에 대한 포괄적인 요약입니다.

Secrets Manager

AWS Systems Manager 자동화에는 대한 사전 정의된 실행서를 제공합니다 AWS Secrets Manager. 실행서에 대한 자세한 내용은 [실행서 작업](#)을 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 암호와에 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

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.

- 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 실행서에는 저장된 보안 암호를 교체합니다 AWS Secrets Manager.

[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.

- RotationInterval

유형: 간격

유효한 값: 1-365

설명: (필수) 보안 암호의 교체 사이의 일수입니다.

- RotationLambdaArn

유형: 문자열

설명: (필수) 보안 암호를 교체할 수 있는 AWS Lambda 함수의 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 CSPM

AWS Systems Manager 자동화하는에 대한 사전 정의된 실행서를 제공합니다 AWS Security Hub CSPM. 실행서에 대한 자세한 내용은 [실행서 작업](#)을 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 CSPM)를 활성화합니다 AWS Security Hub CSPM . Security Hub CSPM에 대한 자세한 내용은 [란 무엇입니까 AWS Security Hub CSPM?](#)를 참조하세요. AWS Security Hub 사용 설명서의 .

[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.

- EnableDefaultStandards

유형: Boolean

기본값: true

설명: (필수) true 로 설정하면 Security Hub CSPM에서 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 Hub CSPM을 활성화합니다.
- aws:executeAwsApi - Security Hub CSPM이 활성화되었는지 확인합니다.

AWS Shield

AWS Systems Manager 자동화에는 대한 사전 정의된 실행서를 제공합니다 AWS Shield. 실행서에 대한 자세한 내용은 [실행서 작업](#)을 참조하세요. 실행서 콘텐츠를 보는 방법에 대한 자세한 내용은 [실행서 콘텐츠 보기](#)(을)를 참조하세요.

주제

- [AWSPremiumSupport-DDoSResiliencyAssessment](#)

AWSPremiumSupport-DDoSResiliencyAssessment

설명

AWSPremiumSupport-DDoSResiliencyAssessment, AWS Systems Manager automation 실행서에는 대한 AWS Shield Advanced 보호에 따라 리소스의 DDoS 취약성 및 구성을 확인하는 데 도움이 됩니다 AWS 계정. 분산 서비스 거부(DDoS) 공격에 취약한 리소스에 대한 구성 설정 보고서를 제

공합니다. 이는 AWS Shield Advanced 보호에 대한 권장 모범 사례에 따라 구성 설정에 대한 Amazon Route 53, Amazon Load Balancer, Amazon CloudFront 배포 및 AWS 탄력적 IPs 리소스를 수집, 분석 AWS Global Accelerator 및 평가하는 데 사용됩니다. 최종 구성 보고서는 선택한 Amazon S3 버킷에서 HTML 파일로 제공됩니다.

어떻게 작동하나요?

이 실행서에는 퍼블릭 액세스가 활성화된 다양한 유형의 리소스와 [AWS DDoS 모범 사례 백서](#)의 권장 사항에 따라 구성된 보호 기능이 있는지 여부에 대한 일련의 검사가 포함되어 있습니다. 실행서는 다음을 수행합니다.

- 에 대한 구독 AWS Shield Advanced 이 활성화되어 있는지 확인합니다.
- 활성화되어 있다면, Shield Advanced로 보호되는 리소스가 있는지 확인합니다.
- AWS 계정 에서 모든 글로벌 및 지역 리소스를 찾아 Shield로 보호되는지 확인합니다.
- 여기에는 평가를 위한 리소스 유형 파라미터, Amazon S3 버킷 이름 및 Amazon S3 버킷 AWS 계정 ID(S3BucketOwner)가 필요합니다.
- 제공된 Amazon S3 버킷에 저장된 HTML 보고서로 결과를 반환합니다.

입력 파라미터 AssessmentType은 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 Business + Support, Enterprise Support 또는 통합 운영 구독이 필요합니다. 자세한 내용은 [AWS Support 플랜 비교](#)를 참조하세요.
- 이 실행서에는 ACTIVE [AWS Shield Advanced 구독](#)이 필요합니다.

[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.

- AssessmentType

유형: 문자열

설명: (선택 사항) DDoS 탄력성 평가를 위해 평가할 리소스 유형을 결정합니다. 기본적으로, 실행서는 글로벌 및 지역 리소스를 모두 평가합니다. 지역 리소스의 경우, 실행서에는 AWS 계정/리전의 모든 애플리케이션(ALB) 및 네트워크(NLB) 로드 밸런서와 모든 Auto Scaling 그룹이 설명되어 있습니다.

유효한 값: ['Global Resources', 'Regional Resources', 'Global and Regional Resources']

기본값: Global and Regional Resources

- S3BucketName

유형: AWS::S3::Bucket::Name

설명: (필수) 보고서가 업로드될 Amazon S3 버킷 이름입니다.

허용된 패턴: `^[0-9a-z][a-z0-9\-\.\.]{3,63}$`

- S3BucketOwnerAccount

유형: 문자열

설명: (선택 사항) Amazon S3 버킷을 소유 AWS 계정 하는 입니다. Amazon S3 버킷이 다른에 속하는 경우가 파라미터를 지정하고 AWS 계정, 그렇지 않으면이 파라미터를 비워 둘 수 있습니다.

허용된 패턴: `^$|^[\0-9]{12,13}$`

- S3BucketOwnerRoleArn

유형: `AWS::IAM::Role::Arn`

설명: (선택 사항) Amazon S3 버킷을 설명하고 버킷이 다른에 있는 경우 퍼블릭 액세스 구성을 AWS 계정 차단할 수 있는 권한이 있는 IAM 역할의 ARN입니다 AWS 계정. 이 파라미터를 지정하지 않은 경우, 실행서는 이 실행서를 시작하는 AutomationAssumeRole 또는 IAM 사용자 (AutomationAssumeRole를 지정하지 않은 경우)를 사용합니다. 실행서 설명의 필수 권한 섹션을 참조하세요.

허용된 패턴: `^$|^arn:(aws|aws-cn|aws-us-gov|aws-iso|aws-iso-b):iam:[\0-9]{12,13}:role/.*$`

- S3BucketPrefix

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 수임 역할에 대한 IAM 정책 예시

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": [
        "s3:ListBucket",
        "s3:GetBucketAcl",
```

```

        "s3:GetAccountPublicAccessBlock"
    ],
    "Resource": "*",
    "Effect": "Allow"
},
{
    "Action": [
        "s3:ListBucket",
        "s3:GetBucketAcl",
        "s3:GetBucketLocation",
        "s3:GetBucketPublicAccessBlock",
        "s3:GetBucketPolicyStatus",
        "s3:GetEncryptionConfiguration"
    ],
    "Resource": "arn:aws:s3:::<bucket-name>",
    "Effect": "Allow"
},
{
    "Action": [
        "s3:PutObject"
    ],
    "Resource": "arn:aws:s3:::<bucket-name>/*",
    "Effect": "Allow"
},
{
    "Action": [
        "autoscaling:DescribeAutoScalingGroups",
        "cloudfront:ListDistributions",
        "ec2:DescribeInstances",
        "ec2:DescribeAddresses",
        "ec2:DescribeNetworkAcls",
        "elasticloadbalancing:DescribeLoadBalancers",
        "elasticloadbalancing:DescribeTargetGroups",
        "globalaccelerator:ListAccelerators",
        "iam:GetRole",
        "iam:ListAttachedRolePolicies",
        "route53:ListHostedZones",
        "route53:GetHealthCheck",
        "shield:ListProtections",
        "shield:GetSubscriptionState",
        "shield:DescribeSubscription",
        "shield:DescribeEmergencyContactSettings",
        "shield:DescribeDRTAccess",
        "waf:GetWebACL",

```



```

        "waf:GetRateBasedRule",
        "wafv2:GetWebACL",
        "wafv2:GetWebACLForResource",
        "waf-regional:GetWebACLForResource",
        "waf-regional:GetWebACL"
    ],
    "Resource": "*",
    "Effect": "Allow"
},
{
    "Action": "iam:PassRole",
    "Resource":
    "arn:aws:iam::111122223333:role/automation-assume-role-name",
    "Effect": "Allow"
}
]
}

```

지침

1. AWS Systems Manager 콘솔에서 [AWSPremiumSupport-DDoSResiliencyAssessment](#)로 이동합니다.
2. 자동화 실행을 선택합니다.
3. 입력 파라미터에 다음을 입력합니다.

- AutomationAssumeRole(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.

- AssessmentType(선택 사항):

DDoS 탄력성 평가를 위해 평가할 리소스 유형을 결정합니다. 기본적으로, 실행서는 글로벌 및 지역 리소스를 모두 평가합니다.

- S3BucketName(필수):

평가 보고서를 HTML 형식으로 저장하는 Amazon S3 버킷의 이름입니다.

- S3BucketOwner(선택 사항):

소유권 확인을 위한 Amazon S3 버킷의 AWS 계정 ID입니다. 보고서가 교차 계정 Amazon S3 버킷에 게시해야 하는 경우 AWS 계정 ID가 필요하고 Amazon S3 버킷이 자동화 시작 AWS 계정과 동일한에 있는 경우 선택 사항입니다.

- S3BucketPrefix(선택 사항):

결과를 저장하기 위한 Amazon S3 내 경로의 모든 접두사입니다.

Input parameters

AutomationAssumeRole
(Optional) The Amazon Resource Name (ARN) of the AWS Identity and Access Management (IAM) role that allows Systems Manager Automation to perform the actions on your behalf. If no role is specified, Systems Manager Automation uses the permissions of the user that starts this runbook.

Select an existing IAM Role

ssm-admin
arn:aws:iam::[redacted]:role/ssm-admin

S3BucketName
(Required) The name of the Amazon S3 bucket to save the assessment report in HTML format.

Select an existing S3 Bucket

[redacted]

S3BucketPrefix
(Optional) Any prefix for the path inside Amazon S3 for storing the results. Example path with prefix: S3://<BucketName>/<Prefix>

String

ResourceType
(Required) Determines the type of resources to be evaluated for DDoS resiliency assessment. By default, the runbook will evaluate both global and regional resources.

Global and Regional Resources

S3BucketOwner
(Required) The Account ID of the Amazon S3 bucket for ownership verification.

[redacted]

4. 실행을 선택합니다.

5. 자동화가 시작됩니다.

6. 문서는 다음 단계를 수행합니다.

- CheckShieldAdvancedState:

AWS 계정 가 구독 AWS Shield Advanced 되는지 여부와 실행서가 Amazon S3 버킷에 액세스할 수 있는지 확인합니다.

- S3BucketSecurityChecks:

“S3bucketName”에 지정된 Amazon S3 버킷이 익명 또는 공개 읽기 또는 쓰기 액세스 권한을 허용하는지, 버킷에 저장된 암호화가 활성화되어 있는지, “S3BucketOwner”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 대응 팀에 대한 IAM 액세스(SRT) 팀, 연락처 목록 세부 정보 및 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 Hosted Zones, CloudFront Distributions 및 Global Accelerator와 같은 Shield Advanced의 보호 대상 글로벌 리소스를 검토합니다.

- BranchOnResourceType:

리소스 유형 선택(글로벌, 지역 또는 둘 다)을 기반으로 문서 단계를 분기합니다.

- ReviewRegionalResources:

Application Load Balancer, Network Load Balancer, Classic Load Balancer, Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스(탄력적 IP)와 같은 Shield Advanced의 보호 대상 지역 리소스를 검토합니다.

- SendReportToS3:

Amazon S3 버킷에 DDoS 평가 보고서 세부 정보를 업로드합니다.

7. 작업이 완료되면 평가 보고서 HTML 파일의 URI가 Amazon S3 버킷에 제공됩니다.

실행서의 성공적인 실행에 대한 보고서의 S3 콘솔 링크 및 Amazon S3 URI

▼ Outputs

SendReportToS3.AssessmentReportS3ConsoleUrl

https://s3.console.aws.amazon.com/s3/object/ddos-readiness-review?region=us-east-1&prefix=ddos-resiliency-assessment-report-71278beb-f36f-4dff-a505-7faeafb373ce-2023-06-24_04.08.37.html

SendReportToS3.AssessmentReportS3Uri

S3://ddos-readiness-review/ddos-resiliency-assessment-report-71278beb-f36f-4dff-a505-7faeafb373ce-2023-06-24_04.08.37.html

Execution status

Overall status	All executed steps	# Succeeded
🟢 Success	9	9
# Failed	# Cancelled	# TimedOut
0	0	0

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 Automation은 Amazon Simple Notification Service에 사전 정의된 실행서를 제공합니다. 실행서에 대한 자세한 내용은 [실행서 작업](#)을 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(Amazon SQS) 엔드포인트에 대한 전송 상태 로깅을 구성합니다. 이를 통해 Amazon SNS는 실패한 알림과 성공한 알림의 샘플 비율을 Amazon CloudWatch에 로깅할 수 있습니다. 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

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.

- EndpointType

유형: 문자열

유효한 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 주제의 ARN입니다.

- SuccessFeedbackRoleArn

유형: 문자열

설명: (필수) Amazon SNS가 CloudWatch에 성공한 알림 메시지에 대한 로그를 보내는 데 사용하는 IAM 역할의 ARN입니다.

- SuccessFeedbackSampleRate

유형: 문자열

유효한 값: 0~100

설명: (필수) 지정된 Amazon SNS 주제에 대해 샘플링할 성공 메시지의 백분율입니다.

- FailureFeedbackRoleArn

유형: 문자열

설명: (필수) Amazon SNS가 실패 알림 메시지에 대한 로그를 CloudWatch로 전송하는 데 사용하는 IAM 역할의 ARN입니다.

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 주제에 전송 상태 로깅이 활성화되어 있는지 확인합니다.

출력

VerifyDeliveryStatusLoggingEnabled.GetTopicAttributesResponse - GetTopicAttributes API 작업의 응답입니다.

VerifyDeliveryStatusLoggingEnabled.VerifyDeliveryStatusLoggingEnabled - 전송 상태 로깅의 성공적인 확인을 나타내는 메시지입니다.

AWSConfigRemediation-EncryptSNSTopic

설명

AWSConfigRemediation-EncryptSNSTopic 실행서는 AWS Key Management Service () 고객 관리형 키를 사용하여 지정한 Amazon Simple Notification Service(Amazon SNS AWS KMS) 주제에서 암호화를 활성화합니다. 이 실행서는 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

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.

- KmsKeyArn

유형: 문자열

설명: (필수) Amazon SNS 주제를 암호화하는 데 사용하려는 AWS KMS 고객 관리형 키의 Amazon 리소스 이름(ARN)입니다.

- TopicArn

유형: 문자열

설명: (필수) 암호화하려는 Amazon SNS 주제의 ARN입니다.

필수 IAM 권한

실행서를 성공적으로 사용하려면 AutomationAssumeRole 파라미터에 다음 작업이 필요합니다.

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- sns:GetTopicAttributes
- sns:SetTopicAttributes

문서 단계

- aws:executeAwsApi - TopicArn 파라미터에서 지정하는 Amazon SNS 주제를 암호화합니다.
- aws:assertAwsResourceProperty - Amazon SNS 주제에서 암호화가 활성화되었는지 확인합니다.

AWS-PublishSNSNotification

설명

Amazon SNS에 알림을 게시합니다.

[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.

- 메시지

유형: 문자열

설명: (필수) SNS 알림에 포함할 메시지입니다.

- TopicArn

유형: 문자열

설명: (필수) 알림을 게시할 SNS 주제의 ARN입니다.

Amazon SQS

AWS Systems Manager 자동화는 Amazon Simple Queue Service(Amazon SQS)를 위한 사전 정의된 실행서를 제공합니다. 실행서에 대한 자세한 내용은 [실행서 작업](#)을 참조하세요. 실행서 콘텐츠를 보는 방법에 대한 자세한 내용은 [실행서 콘텐츠 보기](#)(을)를 참조하세요.

주제

- [AWS-EnableSQSEncryption](#)

AWS-EnableSQSEncryption

설명

AWS-EnableSQSEncryption 실행서는 Amazon Simple Queue Service(Amazon SQS) 대기열에 대해 유틸리티 암호화를 활성화합니다. Amazon SQS 대기열은 Amazon SQS 관리형 키(SSE-SQS) 또는 AWS Key Management Service (AWS KMS) 관리형 키(SSE-KMS)로 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

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.

- QueueUrl

유형: 문자열

설명: (필수) 암호화를 활성화하려는 Amazon SQS 대기열의 URL입니다.

- KmsKeyId

유형: 문자열

설명: (선택 사항) 암호화에 사용할 AWS KMS 키입니다. 이 값은 전역 고유 식별자, 별칭 또는 키에 대한 ARN 또는 "alias/" 접두사가 붙은 별칭 이름일 수 있습니다. 별칭 aws/sqs를 지정하여 AWS 관리형 키를 사용할 수도 있습니다.

- KmsDataKeyReusePeriodSeconds

유형: 문자열

유효한 값: 60~86400

기본값: 300

설명: (선택 사항) Amazon SQS 대기열이 데이터 키를 재사용하여 메시지를 암호화하거나 복호화한 후 AWS KMS 다시 호출할 수 있는 초 단위의 시간입니다.

필수 IAM 권한

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 대기열에서 암호화가 활성화되었는지 확인합니다.
- VerifySqsEncryptionDefault(aws:assertAwsResourceProperty) - Amazon SQS 대기열에서 암호화가 활성화되었는지 확인합니다.

단계 함수

AWS Systems Manager 자동화는 AWS Step Functions (Step Functions)에 대한 사전 정의된 실행서를 제공합니다. 실행서에 대한 자세한 내용은 [실행서 작업](#)을 참조하세요. 실행서 콘텐츠를 보는 방법에 대한 자세한 내용은 [실행서 콘텐츠 보기](#)(을)를 참조하세요.

주제

- [AWS-EnableStepFunctionsStateMachineLogging](#)

AWS-EnableStepFunctionsStateMachineLogging

설명

AWS-EnableStepFunctionsStateMachineLogging 실행서는 지정한 AWS Step Functions 상태 시스템에 대한 로깅을 활성화하거나 업데이트합니다. 최소 로깅 수준은 ALL, ERROR 또는 로 설정해야 합니다 FATAL.

[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.

- 수준

유형: 문자열

유효한 값: ALL | ERROR | FATAL

설명: (필수) 암호화를 활성화하려는 Amazon SQS 대기열의 URL입니다.

- LogGroupArn

유형: 문자열

설명: (필수) 상태 시스템 로그를 보내려는 Amazon CloudWatch Logs 로그 그룹의 ARN입니다.

- StateMachineArn

유형: 문자열

설명: (필수) 로깅을 활성화하려는 상태 시스템의 ARN입니다.

- IncludeExecutionData

유형: 부울

기본값: False

설명: (선택 사항) 실행 데이터가 로그에 포함되는지 여부를 결정합니다.

- TracingConfiguration

유형: 부울

기본값: False

설명: (선택 사항) AWS X-Ray 추적이 활성화되었는지 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 로깅 구성으로 지정된 상태 시스템을 업데이트합니다.
- `VerifyStepFunctionsStateMachineLoggingEnabled` (`aws:assertAwsResourceProperty`) - 지정된 상태 시스템에 대해 로깅이 활성화되었는지 확인합니다.

출력

- `EnableStepFunctionsStateMachineLogging.Response` - `UpdateStateMachine` API 호출의 응답입니다.

Systems Manager

AWS Systems Manager Automation은 Systems Manager용 사전 정의된 실행서를 제공합니다. 실행서에 대한 자세한 내용은 [실행서 작업](#)을 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

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.

- AssociationIds

유형: StringList

설명: (필수) 삭제하려는 연결의 ID를 쉼표로 구분한 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 AWS Systems Manager OpsItems의 상태, 심각도, 범주 또는 우선 순위를 편집하는 데 도움이 됩니다. 이 자동화는 한 번에 최대 50개의 OpsItems를 편집할 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.

- 카테고리

유형: 문자열

유효한 값:

- 가용성
- 비용
- No change
- 성능
- 복구
- 보안

기본값: 변경 없음

설명: (선택 사항) 편집한 OpsItems에 대해 지정하려는 새 범주입니다.

- OpsItemIds

유형: StringList

설명: (필수) 편집하려는 OpSiteMS ID의 심표로 구분된 목록입니다(예: oi-XXXXXXXXXXXXX,oi-XXXXXXXXXXXXX).

- 우선순위

유형: 문자열

유효한 값:

- No change
- 1
- 2
- 3
- 4
- 5

기본값: 변경 없음

설명: (선택 사항) 시스템에 있는 다른 OpsItem과 비교하여 편집된 OpsItem의 중요도입니다.

- 심각도

유형: 문자열

유효한 값:

- No change
- 1
- 2
- 3
- 4

기본값: 변경 없음

설명: (선택 사항) 편집한 OpsItems의 심각도입니다.

- WaitTimeBetweenEditsInSecs

유형: 문자열

유효한 값: 0.0-2.0

기본값: 0.8

설명: (선택 사항) UpdateOpsItems 작업 호출 사이에 자동화가 대기하는 시간입니다.

- Status

유형: 문자열

유효한 값:

- InProgress
- No change
- Open
- Resolved

기본값: 변경 없음

설명: (선택 사항) 편집한 OpsItems의 새로운 상태입니다.

필수 IAM 권한

실행서를 성공적으로 사용하려면 AutomationAssumeRole 파라미터에 다음 작업이 필요합니다.

- ssm:GetAutomationExecution
- ssm:StartAutomationExecution
- ssm:UpdateOpsItem

문서 단계

- aws:executeScript - Category , Priority , Severity 및 Status 파라미터에서 지정하는 값을 기준으로 OpsItemIds 파라미터에서 지정한 OpsItems를 편집합니다.

AWS-BulkResolveOpsItems

설명

AWS-BulkResolveOpsItems 실행서는 지정한 필터와 일치하는 AWS Systems Manager OpsItems를 확인합니다. OpsInsightsId 파라미터를 사용하여 확인된 OpsItems에 추가할 OpsItemId를 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 OpsItems를 해결합니다.

[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.

- 필터

유형: 문자열

설명: (필수) 확인하려는 OpsItems를 반환하는 키-값 필터 쌍입니다. 예: [{"Key": "Status", "Values": ["Open"], "Operator": "Equal"}]. OpsItems 응답을 필터링하는 데 사용할 수 있는 옵션에 대해 자세히 알아보려면, AWS Systems Manager API 참조의 [OpsItemFilters](#)를 참조하세요.

- OpsInsightId

유형: 문자열

설명: (선택 사항) 해결된 OpsItems에 추가하려는 관련 리소스 식별자입니다.

- 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)가 보내도록 하려는 알림입니다.

- SnsTopicArn

유형: 문자열

설명: (선택 사항) 결과 요약이 Amazon S3로 전송되었을 때 알리려는 Amazon SNS 주제의 ARN입니다.

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 - 지정하는 필터를 기반으로 OpsItems를 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, SnsMessage 파라미터 값(지정된 경우)을 포함하여 결과 요약이 Amazon S3에 전송된 후 Amazon SNS 주제에 알림이 전송됩니다.

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

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.

- MaintenanceWindows

유형: StringList

설명: (필수) 활성화하거나 비활성화할 유지 관리 기간의 심포로 구분된 ID 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 Linux용 EC2 인스턴스를 생성합니다.

[이 자동화 실행\(콘솔\)](#)

문서 유형

자동화

소유자

Amazon

플랫폼

Linux

파라미터

- Amild

유형: 문자열

설명: (필수) 인스턴스를 시작하는 데 사용할 AMI ID입니다.

- 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.

- GroupName

유형: 문자열

기본값: SSMSecurityGroupForLinuxInstances

설명: (필수) 생성할 보안 그룹 이름입니다.

- HttpTokens

유형: 문자열

유효한 값: optional | required

기본값: optional

설명: (선택 사항) IMDSv2는 토큰 지원 세션을 사용합니다. HTTP 토큰 사용을 optional 또는 required로 설정하여 IMDSv2가 선택 사항인지 필수인지를 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) CIDR에서 지정한 IP(기본값은 0.0.0.0/0)에 대해 열려 있는 SSH용 포트(포트 범위 22)를 사용하여 보안 그룹을 생성합니다. 보안 그룹이 이미 존재하는 경우, 해당 보안 그룹이 수정되지 않으며 규칙이 변경되지 않습니다.

- RoleName

유형: 문자열

기본값: SSMMManagedInstanceProfileRole

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 인스턴스가 이 Amazon Virtual Private Cloud(VPC) 또는 기본 Amazon VPC(지정하지 않은 경우)에 배포됩니다.

AWS-CreateManagedWindowsInstance

설명

Systems Manager에 대해 구성된 Windows Server용 EC2 인스턴스를 생성합니다.

[이 자동화 실행\(콘솔\)](#)

문서 유형

자동화

소유자

Amazon

플랫폼

Windows

파라미터

파라미터

- Amild

유형: 문자열

기본값: `{{ssm:/aws/service/ami-windows-latest/Windows_Server-2016-English-Full-Base}}`

설명: (필수) 인스턴스를 시작하는 데 사용할 AMI ID입니다.

- 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.

- GroupName

유형: 문자열

기본값: `SSMSecurityGroupForLinuxInstances`

설명: (필수) 생성할 보안 그룹 이름입니다.

- HttpTokens

유형: 문자열

유효한 값: `optional` | `required`

기본값: `optional`

설명: (선택 사항) IMDSv2는 토큰 지원 세션을 사용합니다. HTTP 토큰 사용을 `optional` 또는 `required`로 설정하여 IMDSv2가 선택 사항인지 필수인지를 결정합니다.

- InstanceType

유형: 문자열

기본값: `t2.medium`

설명: (필수) 시작할 인스턴스 유형을 선택합니다. 기본값은 `t2.medium`입니다.

- KeyPairName

유형: 문자열

설명: (필수) 인스턴스를 생성할 때 사용할 키 페어입니다.

- RemoteAccessCidr

유형: 문자열

기본값: 0.0.0.0/0

설명: (필수) CIDR에서 지정한 IP(기본값은 0.0.0.0/0)에 대해 열려 있는 RDP용 포트(포트 범위 3389)를 사용하여 보안 그룹을 생성합니다. 보안 그룹이 이미 존재하는 경우, 해당 보안 그룹이 수정되지 않으며 규칙이 변경되지 않습니다.

- RoleName

유형: 문자열

기본값: SSManagedInstanceProfileRole

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 인스턴스가 이 Amazon Virtual Private Cloud(VPC) 또는 기본 Amazon VPC(지정하지 않은 경우)에 배포됩니다.

AWSConfigRemediation-EnableCWLoggingForSessionManager

설명

AWSConfigRemediation-EnableCWLoggingForSessionManager 실행서를 통해 AWS Systems Manager Session Manager(Session Manager) 세션은 출력 로그를 Amazon CloudWatch(CloudWatch) 로그 그룹에 저장할 수 있습니다.

[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.

- DestinationLogGroup

유형: 문자열

설명: (필수 사항) 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, 존재하지 않는 경우 새 문서를 생성합니다.

AWS-ExportOpsDataToS3

설명

이 실행서는 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

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.

- 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) getOpsSummary 요청에 대한 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 알림을 받을 Amazon Simple Notification Service(Amazon SNS) 주제 ARN입니다.

- syncName

유형: 문자열

설명: (선택 사항) 리소스 데이터 동기화의 이름입니다.

문서 단계

getOpsSummaryStep - CSV 파일로 내보내기 위해 최대 5,000개의 작업 요약을 검색합니다.

출력

OpsData 객체 - 실행서가 성공적으로 실행되면 내보낸 OpsData 객체를 대상 S3 버킷에서 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

파라미터

- assumeRole

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. 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) 다운로드 완료 시 알림을 전송할 Amazon Simple Notification Service(Amazon SNS) 주제의 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 요약を検査하고 데이터를 .csv 파일로 내보냅니다.

targets가 **instanceids=<instance-id>** 형식인 경우, 단계는 계정의 지정된 인스턴스에 대한 패치 요약과 모든 패치를 모두 검색하여 .csv 파일로 내보냅니다.

출력

PatchSummary/Patches 객체 - 실행서가 성공적으로 실행되면 내보낸 패치 보고서 객체가 대상 S3 버킷으로 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 인벤토리](#)를 참조하세요.

이 자동화 실행(콘솔)

문서 유형

자동화

소유자

Amazon

플랫폼

Linux, macOS, Windows

파라미터

- 애플리케이션

유형: 문자열

기본값: 활성화됨

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

기본 값: PT5M

설명: (선택 사항) 인벤토리 연결 시작 시간에 도달했을 때 인벤토리 수집을 일시 중지해야 하는 시간 길이입니다. 이 시간에는 ISO 8601 형식이 사용됩니다.

- 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.

- AwsComponents

유형: 문자열

기본값: 활성화됨

설명: (선택 사항) amazon-ssm-agent와 같은 AWS 구성 요소에 대한 메타데이터를 수집합니다.

- CustomInventory

유형: 문자열

기본값: 활성화됨

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 작업](#)을 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: 활성화됨

설명: (선택 사항) CPU 모델, 속도, 코어 수 등 인스턴스에 대한 추가 정보를 수집합니다.

- InstanceIds

유형: 문자열

기본값: *

설명: (필수) 인벤토리를 작성할 EC2 인스턴스입니다.

- 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.

- NetworkConfig

유형: 문자열

기본값: 활성화됨

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 있는의 이름입니다.

- 일정

유형: 문자열

기본값: cron(0 */30 * * * ? *)

설명: (선택 사항) 인벤토리 연결 일정의 Cron 표현식입니다. 기본값은 30분입니다.

- 서비스

유형: 문자열

기본값: 활성화됨

설명: (선택 사항, Windows OS에만 해당, SSMAgent 버전 2.2.64.0 이상 필요) 서비스 구성에 대한 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 작업](#)을 참조하세요. SSM Agent 버전 2.2.64.0 이상이 필요합니다. 예: [{"Path": "HKEY_CURRENT_CONFIG\System", "Recursive": true}, {"Path": "HKEY_LOCAL_MACHINE\SOFTWARE\Amazon\MachineImage", "ValueNames": ["AMIName"]}]]

- WindowsRoles

유형: 문자열

기본값: 활성화됨

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: 활성화됨

설명: (선택 사항) 인스턴스의 모든 Windows 업데이트에 대한 데이터를 수집합니다.

AWS-SetupManagedInstance

설명

Systems Manager 액세스를 위한 AWS Identity and Access Management (IAM) 역할로 인스턴스를 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.

- InstanceId

유형: 문자열

설명: (필수) 구성할 EC2 인스턴스의 ID입니다.

- 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.

- RoleName

유형: 문자열

기본값: SSMMRoleForManagedInstance

설명: (선택 사항) EC2 인스턴스의 IAM 역할 이름입니다. 이 역할이 없는 경우에는 생성됩니다. 이 값을 지정할 경우 역할에 AmazonSSMMManagedInstanceCore 관리형 정책이 포함되어 있는지 확인합니다.

AWS-SetupManagedRoleOnEC2Instance

설명

Systems Manager 액세스용 SSMMRoleForManagedInstance 관리형 IAM 역할을 사용하여 인스턴스를 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.

- InstanceId

유형: 문자열

설명: (필수) 구성할 EC2 인스턴스의 ID입니다.

- 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.

- RoleName

유형: 문자열

기본값: SSMRoleForManagedInstance

설명: (선택 사항) EC2 인스턴스의 IAM 역할 이름입니다. 이 역할이 없는 경우에는 생성됩니다. 이 값을 지정할 경우 역할에 AmazonSSMManagedInstanceCore 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 필요한 권한이 포함된 AWS Identity and Access Management (IAM) 인스턴스 프로파일이 인스턴스에 연결되어 있는지 확인합니다.

Important

이 자동화 실행서는 IPv6 규칙을 평가하지 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.

- 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` 셸 스크립트에 대한 참조를 제공합니다.
- `aws:executeScript` - `ssmagent-toolkit-windows` PowerShell 스크립트에 대한 참조를 제공합니다.

- `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 실행서는의 도구인 Patch Manager를 사용하여 Linux 기반 관리형 노드에서 패치 장애를 일으킬 수 있는 일반적인 문제를 해결합니다 AWS Systems Manager. 이 런북의 주요 목표는 패치 명령 실패의 근본 원인을 식별하고 문제 해결 계획을 제안하는 것입니다.

어떻게 작동하나요?

AWSSupport-TroubleshootPatchManagerLinux 실행서는 문제 해결을 위해 사용자가 제공한 두 인스턴스 ID/명령 ID를 고려합니다. 명령 ID가 제공되지 않은 경우 제공된 인스턴스에서 지난 30일 이내에 실패한 최신 패치 명령을 선택합니다. 명령 상태, 사전 조건 이행 및 OS 배포를 확인한 후 실행서는 로그 분석기 패키지를 다운로드하고 실행합니다. 출력에는 문제 근본 원인과 문제를 해결하는 데 필요한 작업이 포함됩니다.

문서 유형

자동화

소유자

Amazon

플랫폼

- Amazon Linux 2 및 AL2023
- Red Hat Enterprise Linux 8.X 및 9.X
- Centos 8.X 및 9.X
- SUSE 15.X

파라미터

필수 IAM 권한

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. AWS Systems Manager 콘솔 [AWSsupport-TroubleshootPatchManagerLinux](#)에서 로 이동합니다.
2. Execute automation(자동화 실행)을 선택합니다.
3. 입력 파라미터에 다음을 입력합니다.

- InstanceId(필수):

대화형 인스턴스 선택기를 사용하여 패치 명령이 실패한 Linux 기반 SSM 관리형 노드(Amazon Elastic Compute Cloud(Amazon EC2) 또는 하이브리드 활성화 서버)의 ID를 선택하거나 SSM 관리형 인스턴스의 ID를 수동으로 입력합니다.

- AutomationAssumeRole(선택 사항):

Automation이 사용자를 대신하여 작업을 수행할 수 있도록 허용하는 IAM 역할의 ARN을 입력합니다. 역할이 지정되지 않은 경우 Automation은 이 실행서를 시작하는 사용자의 권한을 사용합니다.

- RunCommandId(선택 사항):

AWS-RunPatchBaseline 문서의 실패 실행 명령 ID를 입력합니다. 명령 ID를 제공하지 않으면 실행서는 선택한 인스턴스에서 지난 30일 이내에 실패한 최신 패치 명령을 찾습니다.

Input parameters

InstanceId
 (Required) The ID of the Amazon EC2 instance you want to troubleshoot EC2 Instance Connect.
☒ Show interactive instance picker

AutomationAssumeRole
 (Optional) The Amazon Resource Name (ARN) of the AWS Identity and Access Management (IAM) role that allows Systems Manager Automation to perform the actions on your behalf. If no role is specified, Systems Manager Automation uses the permissions of the user that starts this runbook.

RunCommandId
 (Optional) Failed Run Command ID of AWS-RunPatchBaseline. If not provided, we look for the latest unsuccessful execution of AWS-RunPatchBaseline for the instance and evaluate it. To confirm the command ID, look under Command History tab in the Run Command Console under AWS Systems Manager.

4. 실행을 선택합니다.

5. 자동화가 시작됩니다.

6. 문서는 다음 단계를 수행합니다.

- CheckConcurrency:

동일한 인스턴스를 대상으로 하는 이 실행서의 실행이 하나만 있는지 확인합니다. 실행서가 동일한 인스턴스를 대상으로 진행 중인 다른 실행을 찾으면 오류가 반환되고 종료됩니다.

- ValidateCommandID:

제공된 명령 ID가 입력 파라미터로 AWS-RunPatchBaseline SSM 문서에 대해 실행되었는지 확인합니다. 명령 ID가 제공되지 않은 경우 실행서는 선택한 인스턴스에서 지난 30일 AWS-RunPatchBaseline 동안 실행에 실패한 최근 실행을 고려합니다.

- BranchOnCommandStatus:

제공된 명령의 상태가 실패했는지 확인합니다. 그렇지 않으면 실행서가 실행을 종료하고 제공된 명령이 성공적으로 실행되었다는 보고서를 생성합니다.

- VerifyPrerequisites:

위에서 언급한 사전 조건이 충족되었는지 확인합니다.

- GetPlatformDetails:

운영 체제(OS) 배포 및 버전을 검색합니다.

- GetDownloadURL:

PatchManager Log Analyzer 패키지의 다운로드 URL을 검색합니다.

- EvaluatePatchManagerLogs:

인스턴스에서 PatchManager Log Analyzer python 패키지를 다운로드하고 실행하여 로그 파일을 평가합니다.

- GenerateReport:

식별된 문제와 제안된 솔루션을 포함하는 실행서 실행에 대한 최종 보고서를 생성합니다.

7. 완료되면 출력 섹션에서 실행의 자세한 결과를 검토합니다.

```

▼ Outputs

GenerateReportOutput
Starting 'python3 main.py i-0[REDACTED] 3e016680-82f4-45f4-845c-aa4685b4fab Ubuntu 22.04'

=====
TROUBLESHOOTING RESULTS
=====

[PROBLEM] :
-----
The error found in the log file at /var/lib/amazon/ssm/i-0[REDACTED]/document/orchestration/3e016680-82f4-45f4-845c-aa4685b4fab/awsrunShellScript/PatchLinux/stdout is :

Unable to download payload: https://s3.dualstack.eu-west-1.amazonaws.com/aws-ssm-eu-west-1/patchbaselineoperations/linux/payloads/patch-baseline-operations-1.115.tar.gz.failed to run commands: exit status 156

-----
[SOLUTION] :
-----
Here are some suggestions to troubleshoot the issue:

Possible reasons for the above error are :

1. Network connectivity issue while accessing the s3 service endpoint from the instance to download the payload.
2. Instance doesn't have the required permissions to access the specified Amazon Simple Storage Service (Amazon S3) bucket.
3. No space left on the Instance.

To resolve this, ensure network connectivity to S3 endpoint from the instance. For more details, see information about required access to S3 buckets for Patch Manager in https://docs.aws.amazon.com/systems-manager/latest/userguide/ssm-agent-minimum-s3-permissions.

For testing purpose, try to manually access the above payload URL using curl or wget from within Instance. Command to run:

curl https://s3.dualstack.eu-west-1.amazonaws.com/aws-ssm-eu-west-1/patchbaselineoperations/linux/payloads/patch-baseline-operations-1.115.tar.gz --output payload.tar.gz

```

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(Amazon EC2) 인스턴스에 연결하지 못하게 하는 일반적인 문제를 해결하는 데 도움이 됩니다. Session Manager는의 도구입니다 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 Agent 버전을 확인합니다.
- Session Manager에 대한 권장 AWS Identity and Access Management (IAM) 정책이 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 엔드포인트 연결성을 분석합니다.

고려 사항

- 하이브리드 관리형 노드는 지원되지 않습니다.
- 이 실행서는 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 Analyzer](#)를 사용하여 소스와 서비스 엔드포인트 간의 네트워크 연결을 분석합니다. 소스와 대상 간의 분석 실행당 요금이 부과됩니다. 자세한 내용은 [Amazon VPC 요금](#)을 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.

- 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 프로파일의 ARN을 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`: Linux 또는 macOS 인스턴스의 `ssm-cli`에서 로그 출력을 수집합니다.
9. `aws:runCommand`: Windows 인스턴스의 `ssm-cli`에서 로그 출력을 수집합니다.
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`: `ssm-cli` 로그와 세션 기본 설정을 기반으로 CloudWatch Logs 엔드포인트 연결을 평가할지 여부를 결정합니다.
19. `aws:executeAutomation`: 인스턴스를 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 서비스를 위한 사전 정의된 실행서를 제공합니다. 실행서에 대한 자세한 내용은 [실행서 작업](#)을 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.

Note

제어 및 검증을 개선하려면 AWS-CreateJiraIssue 실행서를 [복제](#)하여 자체 프라이빗 버전을 생성하는 것이 좋습니다. 복제된 실행서에서 JiraURL 파라미터에 대한 [검증 로직](#)을 추가하여 실행 전에 승인된 Jira 인스턴스와 일치하는지 확인합니다. 그런 다음 AWS 관리형 실행서 대신 복제된 실행서를 사용하고 실행을 위한 IAM 권한을 제한합니다 AWS-CreateJiraIssue. 이 접근 방식은 유연성을 높이고 파라미터가 조직의 보안 및 규정 준수 요구 사항을 충족하도록 합니다.

[이 자동화 실행\(콘솔\)](#)

문서 유형

자동화

소유자

Amazon

플랫폼

Linux, macOS, Windows

파라미터

- AssigneeName

유형: 문자열

설명: (선택 사항) 문제가 할당되어야 할 사람의 사용자 이름입니다.

- DueDate

유형: 문자열

설명: (선택 사항) 문제의 기한입니다(yyyy-mm-dd 형식).

- 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.

- SSMPParameterName

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

Issueld: 새로 생성된 Jira 문제의 ID

AWS-CreateServiceNowIncident

설명

ServiceNow 인시던트 테이블에서 인시던트를 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.

- 카테고리

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 암호를 포함하는 암호화된 SSM 파라미터의 이름입니다.

- ServiceNowInstanceURL

유형: 문자열

설명: (필수) ServiceNow 인스턴스의 URL입니다.

- ShortDescription

유형: 문자열

설명: (필수) 인시던트에 대한 간략한 설명입니다.

- Subcategory

유형: 문자열

설명: (선택 사항) 인시던트의 하위 범주입니다.

유효한 값: None | Antivirus | Email | Internal Application | Operating System | CPU | Disk | Keyboard | Hardware | Memory | Monitor | Mouse | DHCP | DNS | IP Address | VPN | Wireless | DB2 | MS SQL Server | Oracle

기본값: None

문서 단계

Push_incident - ServiceNow에 인시던트 정보를 푸시합니다.

출력

Push_incident.incidentID - 생성된 인시던트 ID.

AWS-RunPacker

설명

이 실행서는 HashiCorp [Paacker](#) 도구를 사용하여 머신 이미지를 생성하는 데 사용되는 Packer 템플릿의 유효성을 검사하거나, 해당 템플릿을 수정 또는 빌드합니다. 이 실행서는 Packer v1.11.2를 사용합니다.

Note

vpc_id 값을 지정하는 경우 퍼블릭 서브넷의 subnet_id 값도 지정해야 합니다. 서브넷의 IPv4 퍼블릭 주소 지정 속성을 수정하지 않는 한 associate_public_ip_address(을)를 true로 설정해야 합니다.

⚠ Important

Packer 프로비저너는 임시 EC2 인스턴스에서 루트 수준 권한으로 실행됩니다. Packer 템플릿을 작성할 때 최소 권한 관행을 따릅니다. 프로비저닝자에게 민감한 인스턴스 메타데이터 또는 로컬 자격 증명 파일에 대한 액세스 권한을 부여하지 마세요. [기본 호스트 관리 구성](#)에서 사용하는 IAM 역할에 정책을 추가한 경우 인스턴스에서 루트로 실행되는 모든 프로세스가 확장된 권한에 액세스할 수 있습니다. Packer 템플릿을 검토하여 신뢰할 수 있는 명령만 포함되어 있는지 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.

- 강제

유형: Boolean

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 Fix이 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 도구에서 나온 stdout.

RunPackerProcessTemplate.fixed_template_key - “수정(Fix)” 모드를 실행할 때만 사용할 S3 버킷에 저장된 템플릿 이름입니다.

RunPackerProcessTemplate.s3_bucket - “수정(Fix)” 모드를 실행할 때만 사용할 고정된 템플릿을 포함하는 S3 버킷의 이름.

Amazon VPC

AWS Systems Manager 자동화는 Amazon Virtual Private Cloud에 사전 정의된 실행서를 제공합니다. 실행서에 대한 자세한 내용은 [실행서 작업](#)을 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

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.

- SecurityGroupId

유형: 문자열

설명: (필수) 닫으려는 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 Virtual Private Cloud(VPC) 또는 Amazon Route 53 호스팅 영역에서 시작되는 DNS 쿼리에 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

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.

- LogDestinationArn

유형: 문자열

설명: (선택 사항) 쿼리 로그를 전송할 CloudWatch Logs 그룹, Amazon S3 버킷 또는 Firehose 스트림의 ARN입니다. 단, Route 53 퍼블릭 DNS 쿼리 로깅은 CloudWatch 로그 그룹만 지원합니다. 이 파라미터의 값을 지정하지 않으면 자동화가 AWSSupport-ConfigureDNSQueryLogging-

{automation: *EXECUTION_ID* } 형식의 CloudWatch 로그 그룹과 쿼리 로그를 게시하기 위한 IAM 리소스 정책을 생성합니다. 자동화로 생성된 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 Public을 지정하는 경우 리소스는 Route 53 프라이빗 호스팅 영역의 ID여야 합니다. QueryLogType 파라미터에 대해 Resolver/Private를 지정하는 경우 리소스는 VPC의 ID여야 합니다.

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 로그를 CloudWatch Logs 로그 그룹에 게시하는 데 필요한 권한을 확인하고, 존재하지 않는 경우 필요한 IAM 리소스 정책을 생성합니다.
- `aws:executeScript` - 선택한 대상에서 DNS 쿼리 로깅을 활성화합니다.

AWSSupport-ConfigureTrafficMirroring

설명

AWSSupport-ConfigureTrafficMirroring 실행서는 로드 밸런서와 Amazon Elastic Compute Cloud(Amazon EC2) 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 DNS를 제외한 모든 프로토콜의 모든 인바운드 및 아웃바운드 트래픽에 대한 미러링을 구성합니다. 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

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.

- SourceENI

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 Balancer를 지정하는 경우 포트 4789에 UDP 리스너가 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(Amazon VPC) 내의 리소스
- AWS VPCs 피어링을 사용하여 연결된 동일한 내의 서로 다른 Amazon VPC에 AWS 리전 있는 리소스
- AWS Amazon VPC의 리소스 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

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.

- DestinationIP

유형: 문자열

설명: (필수) 연결을 테스트하려는 리소스의 IPv4 주소입니다.

- DestinationPort

유형: 문자열

기본값: true

설명: (필수) 대상 리소스에서 연결하려는 포트 번호입니다.

- DestinationVpc

유형: 문자열

기본값: All

설명: (선택 사항) 연결을 테스트하려는 Amazon VPC의 ID입니다.

- SourceIP

유형: 문자열

설명: (필수) 연결을 테스트하려는 Amazon VPC에 있는 AWS 리소스의 프라이빗 IPv4 주소입니다.

- SourcePortRange

유형: 문자열

설명: (선택 사항) 연결을 테스트하려는 Amazon VPC의 AWS 리소스에서 사용하는 포트 범위입니다.

- SourceVpc

유형: 문자열

기본값: All

설명: (선택 사항) 연결을 테스트할 Amazon VPC의 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 리소스의 네트워크 트래픽 대상을 결정합니다.
- aws:branch - 네트워크 트래픽의 대상을 기반으로 분기합니다.
- aws:executeAwsApi - 대상 리소스에 대한 세부 정보를 수집합니다.
- aws:executeScript - 대상 Amazon VPC에 대해 반환된 ID가 DestinationVpc 파라미터에서 지정된 값(있는 경우)과 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(NACL)을 수집합니다.
- `aws:executeScript` - NACL이 소스 및 대상 리소스 간에 필요한 트래픽을 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 연결된 NACL을 수집합니다.
- `aws:executeScript` - NACL이 소스 리소스로부터 필요한 트래픽을 허용하는지 확인합니다.
- `aws:executeAwsApi` - NAT 게이트웨이에 대한 세부 정보를 수집합니다.
- `aws:executeAwsApi` - NAT 게이트웨이의 서브넷과 연결된 NACL을 수집합니다.
- `aws:executeScript` - NACL이 NAT 게이트웨이의 서브넷에서 필요한 트래픽을 허용하는지 확인합니다.
- `aws:executeScript` - NAT 게이트웨이의 서브넷과 연결된 경로를 수집합니다.
- `aws:executeScript` - NAT 게이트웨이에 인터넷 게이트웨이로 이어지는 경로가 있는지 확인합니다.
- `aws:executeAwsApi` - VPC 피어링 연결에 대한 세부 정보를 수집합니다.
- `aws:executeScript` - 두 VPC가 동일한 리전에 있고 대상 VPC에 대해 반환된 ID가 `DestinationVpc` 파라미터에 지정된 값(있는 경우)과 일치하는지 확인합니다.
- `aws:executeAwsApi` - 대상 리소스의 서브넷을 반환합니다.
- `aws:executeScript` - 피어링된 VPC의 서브넷과 연결된 경로를 수집합니다.
- `aws:executeScript` - 피어링된 VPC에 피어링 연결에 대한 경로가 있는지 확인합니다.
- `aws:executeScript` - 자동화가 대상을 지원하지 않는 경우 소스 리소스로부터 트래픽이 허용되는지 확인합니다.

AWSSupport-TroubleshootVPN

설명

AWSSupport-TroubleshootVPN 실행서는 AWS Site-to-Site VPN 연결에서 오류를 추적하고 해결하는 데 도움이 됩니다. 자동화에는 AWS Site-to-Site VPN 연결 터널과 관련된 IKEv1 또는 IKEv2 오

류를 추적하도록 설계된 몇 가지 자동 검사가 포함되어 있습니다. 자동화는 특정 오류를 일치시키려고 시도하고 해당 해결 방법은 일반적인 문제 목록을 형성합니다.

참고: 이 자동화는 오류를 수정하지 않습니다. 언급된 시간 범위 동안 실행되며, [VPN CloudWatch 로그 그룹](#)의 오류가 있는지 로그 그룹을 스캔합니다.

어떻게 작동하나요?

실행서는 파라미터 검증을 실행하여 입력 파라미터에 포함된 Amazon CloudWatch 로그 그룹이 존재하는지, 로그 그룹에 VPN 터널 로깅에 해당하는 로그 스트림이 있는지, VPN 연결 ID가 존재하는지, 터널 IP 주소가 존재하는지 확인합니다. VPN 로깅을 위해 구성된 CloudWatch 로그 그룹에서 Logs Insights API 호출을 수행합니다.

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.

- LogGroupName

유형: 문자열

설명: (필수) AWS Site-to-Site VPN 연결 로깅을 위해 구성된 Amazon CloudWatch 로그 그룹 이름입니다.

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}\$

- TunnelAIPAddress

유형: 문자열

설명: (필수) AWS Site-to-Site VPN과 연결된 터널 번호 1 IPv4 주소입니다.

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}\$

- TunnelBIPAddress

유형: 문자열

설명: (선택 사항) AWS Site-to-Site VPN과 연결된 터널 번호 2 IPv4 주소입니다.

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

유효한 값: ['IKEv1', 'IKEv2']

- StartTimeinEpoch

유형: 문자열

설명: (선택 사항) 로그 분석 시작 시간입니다. StartTimeinEpoch/EndTimeinEpoch 또는 LookBackPeriod를 로그 분석에 사용할 수 있습니다.

허용된 패턴: ^\d{10}|^\$

- EndTimeinEpoch

유형: 문자열

설명: (선택 사항) 로그 분석 종료 시간입니다. StartTimeinEpoch/EndTimeinEpoch 또는 LookBackPeriod를 로그 분석에 사용할 수 있습니다. StartTimeinEpoch/EndTimeinEpoch 및 LookBackPeriod가 모두 지정될 경우, LookBackPeriod가 우선합니다.

허용된 패턴: `^\d{10}|^$`

- LookBackPeriod

유형: 문자열

설명: (선택 사항) 로그 분석을 위해 되돌아보는 두 자리 시간(시간)입니다. 유효 범위: 01~99. StartTimeinEpoch 및 EndTime도 제공할 경우, 이 값이 우선합니다.

허용된 패턴: `^(\d?[1-9]|[1-9]00)|^$`

필수 IAM 권한

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 JSON인 경우 VPN 터널 로깅용으로 구성된 CloudWatch 로그 그룹에서 작동합니다.

다음 단계에 따라 자동화를 구성합니다.

1. AWS Systems Manager 콘솔에서 [AWSSupport-TroubleshootVPN](#)으로 이동합니다.
2. 입력 파라미터의 경우, 다음 내용을 입력합니다.
 - AutomationAssumeRole(선택 사항):

Systems Manager Automation이 사용자를 대신하여 작업을 수행하도록 허용하는 (IAM) 역할의 Amazon 리소스 이름 AWS Identity and Access Management (ARN)입니다. 역할을 지정하지 않

은 경우, Systems Manager Automation에서는 이 실행서를 시작하는 사용자의 권한을 사용합니다.

- logGroupName(필수):

검증할 Amazon CloudWatch 로그 그룹 이름입니다. 이는 VPN이 로그를 보내도록 구성된 CloudWatch 로그 그룹이어야 합니다.

- VpnConnectionId(필수):

VPN 오류에 대해 로그 그룹이 추적되는 AWS Site-to-Site VPN 연결 ID입니다.

- TunnelAIPAddress(필수):

터널 AWS Site-to-Site VPN 연결과 연결된 IP 주소입니다.

- TunnelBIPAddress(선택 사항):

AWS Site-to-Site VPN 연결과 연결된 터널 B IP 주소입니다.

- IKEVersion(필수):

사용 중인 IKEVersion을 선택합니다. 허용된 값: IKEv1, IKEv2.

- StartTimeinEpoch(선택 사항):

오류를 쿼리할 시간 범위의 시작입니다. 범위가 포함되므로, 지정된 시작 시간이 쿼리에 포함됩니다. 1970년 1월 1일 00:00:00 UTC 이후의 초 수인 에포크 시간으로 지정됩니다.

- EndTimeinEpoch(선택 사항):

오류를 쿼리할 시간 범위의 끝입니다. 범위가 포함되므로, 지정된 종료 시간이 쿼리에 포함됩니다. 1970년 1월 1일 00:00:00 UTC 이후의 초 수인 에포크 시간으로 지정됩니다.

- LookBackPeriod(필수):

오류에 대한 쿼리를 다시 검토하는 데 걸리는 시간(시간)입니다.

참고: StartTimeinEpoch, EndTimeinEpoch 또는 LookBackPeriod를 구성하여 로그 분석을 위한 시간 범위를 수정합니다. 두 자리 숫자를 시간 단위로 부여하여 자동화 시작 시간부터 과거에 오류가 발생했는지 확인하세요. 또는 특정 시간 범위 내에서 과거에 오류가 발생한 경우, LookBackPeriod 대신 StartTimeinEpoch 및 EndTimeinEpoch를 포함하세요.

Input parameters	
AutomationAssumeRole (Optional) The ARN of the role that allows Automation to perform the actions on your behalf. Choose an option	LogGroupName (Required) The Amazon CloudWatch log group name to be validated. This must be the CloudWatch log group which is destined for VPN logs. vpnlog
VpnConnectionId (Required) The AWS Site-to-Site VPN connection id to be validated. vpn-123abc456xyz	TunnelAPIAddress (Required) The tunnel number 1 IP address associated with your AWS Site-to-Site VPN to be validated. 1.1.1.1
TunnelBIPAddress (Optional) The tunnel number 2 IP address associated with your AWS Site-to-Site VPN to be validated. String	IKEVersion (Required) Select what IKE Version you are using. Allowed values : IKEv1, IKEv2 or both. IKEv1
StartTimeEpoch (Optional) Start time for log analysis. You can either use StartTimeEpoch/EndTimeEpoch or LookBackPeriod for logs analysis. String	EndTimeEpoch (Optional) End time for log analysis. You can either use StartTimeEpoch/EndTimeEpoch or LookBackPeriod for logs analysis. String
LookBackPeriod (Required) Time in hours to look back for log analysis. 05	

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 CloudWatch 로그 그룹에 로그 스트림이 존재하는지 확인합니다. 유효하지 않은 경우, 자동화 단계의 추가 시작을 중단합니다.

- branchOnValidationOfVpnConnectionId:

파라미터에 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 CloudWatch 로그 그룹에서 로그 인사이트 API를 호출하고 관련된 제안 해결 방법과 함께 IKEv1/IKEv2 관련 오류를 검색합니다.

6. 완료 후에는 Outputs 섹션에서 실행의 세부 결과를 검토합니다.

▼ Outputs	
parameterValidation.LogGroupName LogGroupValid	parameterValidation.LogStream validLogStream
parameterValidation.VpnConnection validVpnConnection	parameterValidation.VpnIpAddress validVpnIP
traceErrorTunnel1IKEv2 ["IKEv2ErrorCount":0]	traceErrorTunnel2IKEv1 ["IKEv1ErrorCount":0]
traceErrorTunnel2IKEv2 ["IKEv2ErrorCount":0]	
traceErrorTunnel1IKEv1 ["Error related to : AWS tunnel received DELETE for Phase 2 SA"] Please treat below as Potential resolution of this error :	
AWS CloudWatch monitoring has identified that your VPN tunnel went down because CGW has sent Delete_SA message for Phase 2. When AWS receives Delete_SA for Phase 2 from CGW it deletes the Phase 2 of SPI mentioned in Delete_SA request. Possible reason of CGW sending Delete_SA message can be due to any configurational changes made in CGW side Next Steps: • Check IPsec Logs on the CGW Device to verify if you are able to see information pertaining to this issue. References: [1] Tunnel stability issues during a rekey: https://aws.amazon.com/premiumsupport/knowledge-center/vpn-fix-ikev2-tunnel-instability-rekey/ [2] Phase 2 Troubleshooting: https://aws.amazon.com/premiumsupport/knowledge-center/vpn-tunnel-phase-2-ipsec/	
","Error related to : AWS tunnel received DELETE for "IKE_SA from CGW":" Please treat below as Potential resolution of this error : AWS CloudWatch monitoring has identified that your VPN tunnel went down because CGW has sent the Delete_SA message for Parent/IKE_SA. When AWS receives Delete_SA from CGW, it honours the message and brings down the VPN tunnel. There can be various reasons for CGW sending Delete_SA message like : • A reset to clear active SAs has been performed on the CGW side • IKE SA has been timed out • Configurational changes have been made on CGW Next Steps: • Review your VPN device idle timeout settings using information from your device vendor. When there is no traffic through a VPN tunnel for the duration of your vendor-specific VPN idle time, the IPsec session terminates. For more information on tunnel inactivity and instability refer to this documentation [1] • Check logs on your CGW device to verify if you are able to see information pertaining to this issue. References: [1] Tunnel inactivity or instability: https://aws.amazon.com/premiumsupport/knowledge-center/vpn-tunnel-instability-inactivity/	
","Error related to : No proposal chosen":" Please treat below as Potential resolution of this error : AWS CloudWatch monitoring has detected that IKE Phase 2 parameters (such as encryption algorithm, hashing algorithm and DH group) configured on Customer Gateway (CGW) device and AWS VPN endpoint do not match or the CGW is using parameters that are not supported by the AWS VPN. Next Steps: • Verify that the Phase 2 parameters (Integrity algorithm, Encryption algorithm and DH group) being proposed by CGW are matching with those configured on AWS side. If you are using default settings on AWS side then verify that parameters being proposed are supported by AWS VPN. To Find list of parameters supported by • If you want to modify the parameters on the AWS VPN side you can follow below steps: Step 1: Open the Amazon VPC console at https://console.aws.amazon.com/vpc/ Step 2: In the navigation pane, choose Site-to-Site VPN Connections. Step 3: Select the Site-to-Site VPN connection, and choose Actions, Modify VPN Tunnel Options. Step 4: For VPN Tunnel Outside IP Address, choose the tunnel endpoint IP of the VPN tunnel that you are modifying options for. Step 5: Choose or enter new values for the tunnel options. Step 6: Choose Save.	

참조

Systems Manager Automation

- [이 자동화 실행\(콘솔\)](#)
- [자동화 실행](#)
- [Automation 설정](#)
- [Support Automation Workflows 랜딩 페이지](#)

AWS 서비스 설명서

- [Site-to-Site VPN 로그의 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

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.

- 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 detached인 탄력적 네트워크 인터페이스(ENI)를 삭제합니다.

[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.

- NetworkInterfaceId

유형: 문자열

설명: (필수) 삭제하려는 ENI의 ID입니다.

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 지정한 ENI를 삭제합니다.
- `aws:executeScript` - ENI가 삭제되었는지 확인합니다.

AWSConfigRemediation-DeleteUnusedSecurityGroup

설명

AWSConfigRemediation-DeleteUnusedSecurityGroup 실행서는 `GroupId` 파라미터에서 지정하는 보안 그룹을 삭제합니다. Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스와 연결된 보안 그룹이나 다른 보안 그룹에서 참조하는 보안 그룹의 삭제를 시도하는 경우 자동화 작업이 실패합니다. 이 자동화는 기본 보안 그룹을 삭제하지 않습니다.

[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.

- `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 연결되어 있지 않은 네트워크 액세스 제어 목록(ACL)을 삭제합니다.

[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.

- NetworkACLId

유형: 문자열

설명: (필수) 삭제하려는 네트워크 ACL의 ID입니다.

필수 IAM 권한

실행서를 성공적으로 사용하려면 AutomationAssumeRole 파라미터에 다음 작업이 필요합니다.

- ssm:StartAutomationExecution
- ssm:GetAutomationExecution
- ec2:DeleteNetworkACL
- ec2:DescribeNetworkACLs

문서 단계

- aws:executeAwsApi - NetworkACLId 파라미터에서 지정된 네트워크 ACL을 삭제합니다.
- aws:executeScript - NetworkACLId 파라미터에서 지정된 네트워크 ACL이 삭제되었는지 확인합니다.

AWSConfigRemediation-DeleteVPCFlowLog

설명

AWSConfigRemediation-DeleteVPCFlowLog 실행서는 지정하는 Virtual Private Cloud(VPC) 흐름 로그를 삭제합니다.

[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.

- 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. Virtual Private Cloud(VPC)의 Amazon EC2 인스턴스에 탄력적 IP 주소 또는 퍼블릭 IPv4 주소가 연결되어 있는 경우, 실행서가 작동하지 않습니다.

[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.

- 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`의 속성이 `attached`로 변경되거나 제한 시간이 초과될 때까지 기다립니다.
- `aws:executeAwsApi` - 가상 프라이빗 게이트웨이의 ID와 Amazon VPC의 ID를 입력으로 수락하고 Amazon VPC에서 가상 프라이빗 게이트웨이를 분리합니다.
- `aws:waitForAwsResourceProperty` - 가상 프라이빗 게이트웨이의 ID를 수락하고 가상 프라이빗 게이트웨이의 `VPCAttachments.state`의 속성이 `detached`로 변경되거나 제한 시간이 초과될 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 ID에서 VPC ID를 수집합니다.
- `aws:executeAwsApi` - VPC에서 인터넷 게이트웨이 ID를 분리합니다.
- `aws:executeAwsApi` - 인터넷 게이트웨이를 삭제합니다.

AWSConfigRemediation-DetachAndDeleteVirtualPrivateGateway

설명

AWSConfigRemediation-DetachAndDeleteVirtualPrivateGateway 실행서는 Amazon Virtual Private Cloud(Amazon VPC)에서 생성된 Virtual Private Cloud(VPC)에 연결된 특정 Amazon Elastic Compute Cloud(Amazon EC2) 가상 프라이빗 게이트웨이를 분리하고 삭제합니다.

[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.

- 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`의 속성이 `attached`로 변경되거나 제한 시간이 초과될 때까지 기다립니다.
- `aws:executeAwsApi` - 가상 프라이빗 게이트웨이의 ID와 Amazon VPC의 ID를 입력으로 수락하고 Amazon VPC에서 가상 프라이빗 게이트웨이를 분리합니다.
- `aws:waitForAwsResourceProperty` - 가상 프라이빗 게이트웨이의 ID를 수락하고 가상 프라이빗 게이트웨이의 `VPCAttachments.state`의 속성이 `detached`로 변경되거나 제한 시간이 초과될 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

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.

- SecurityGroupIds

유형: 문자열

설명: (필수) SSH 트래픽을 제한하려는 보안 그룹의 IDs를 쉼표로 구분한 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

DisableIncomingSSTemplate.RestrictedSecurityGroupIds - 인바운드 SSH 규칙이 제거된 보안 그룹의 IDs 목록입니다.

AWS-DisablePublicAccessForSecurityGroup

설명

이 실행서는 모든 IP 주소에 개방된 기본 SSH 및 RDP 포트를 비활성화합니다.

Important

이 실행서는 다음 두 가지 기준을 모두 충족하는 보안 그룹에 대해 "InvalidPermission.NotFound" 오류의 경우 실행되지 않습니다: 1) 보안 그룹이 기본이 아닌 VPC에 위치합니다. 2) 보안 그룹의 인바운드 규칙이 다음 4가지 패턴을 모두 사용하는 개방 포트를 지정하지 않습니다.

- 0.0.0.0/0
- ::/0
- SSH or RDP port + 0.0.0.0/0
- SSH or RDP port + ::/0

Note

중국 내에 AWS 리전 있는 에서는 이 실행서를 사용할 수 없습니다.

[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.

- GroupId

유형: 문자열

설명: (필수) 비활성화되어야 하는 포트의 보안 그룹 ID입니다.

- IpAddressToBlock

유형: 문자열

설명: (선택 사항) 액세스가 차단되어야 하는 추가 IPv4 주소(1.2.3.4/32 형식)입니다.

AWSConfigRemediation-DisableSubnetAutoAssignPublicIP

설명

AWSConfigRemediation-DisableSubnetAutoAssignPublicIP 실행서는 지정하는 서브넷의 IPv4 퍼블릭 주소 지정 속성을 비활성화합니다.

[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.

- SubnetId

유형: 문자열

설명: (필수) 퍼블릭 IPv4 주소 자동 할당 속성을 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 파라미터에서 지정된 서브넷의 퍼블릭 IPv4 주소 자동 할당 속성을 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 Amazon CloudWatch Logs 로그 그룹 또는 지정하는 Amazon Simple Storage Service(Amazon S3) 버킷에 게시됩니다. 흐름 로그에 대한 자세한 내용은 Amazon VPC 사용 설명서의 [VPC 흐름 로그](#)를 참조하세요.

⚠ Important

CloudWatch Logs 또는 Amazon S3에 흐름 로그를 게시할 때는 판매된 로그에 대한 데이터 수집 및 아카이브 요금이 부과됩니다. 자세한 내용은 [흐름 로그 요금](#)을 참조하세요.

이 자동화 실행(콘솔)**i Note**

로그 대상으로 s3를 선택할 때 버킷 정책이 버킷에 대한 로그 전송 서비스 액세스를 허용하는지 확인합니다. 자세한 내용은 [흐름 로그에 대한 Amazon S3 버킷 권한](#)을 참조하세요.

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.

- DeliverLogsPermissionArn

유형: 문자열

설명: (선택 사항) Amazon Elastic Compute Cloud(Amazon EC2)가 계정의 CloudWatch Logs 로그 그룹에 흐름 로그를 게시하도록 허용하는 IAM 역할의 ARN입니다. LogDestinationType 파라미터에 대해 s3을 지정하는 경우, 이 파라미터의 값을 제공하지 마십시오. 자세한 내용은 Amazon VPC 사용 설명서의 [CloudWatch 로그에 흐름 로그 게시](#)를 참조하세요.

- LogDestinationARN

유형: 문자열

설명: (선택 사항) 흐름 로그 데이터가 게시되는 리소스의 ARN입니다. LogDestinationType 파라미터에 대해 cloud-watch-logs가 지정되는 경우, 흐름 로그 데이터를 게시하려는 CloudWatch Logs 로그 그룹의 ARN을 제공하십시오. 또는 LogGroupName을 대신 사용합니다. s3이 LogDestinationType 파라미터에 대해 지정되는 경우, 이 파라미터에 대해 흐름 로그 데이터를 게시하려는 Amazon S3 버킷의 ARN을 지정해야 합니다. 버킷에 폴더를 지정할 수도 있습니다.

 Important

를 s3로 선택할 때는 선택한 버킷이 [Amazon S3 버킷 보안 모범 사례](#)를 따르고 조직 및 지리적 리전의 데이터 개인 정보 보호법을 준수하는지 LogDestinationType 확인해야 합니다.

- LogDestinationType

유형: 문자열

유효한 값: cloud-watch-logs | s3

설명: (필수) 흐름 로그 데이터가 게시되는 위치를 결정합니다. LogDestinationType을 s3로 지정한 경우 DeliverLogsPermissionArn 또는 LogGroupName을 지정하지 마십시오.

- LogFormat

유형: 문자열

설명: (선택 사항) 흐름 로그 레코드에 포함할 필드 및 레코드에 표시되는 순서입니다. 사용 가능한 필드 목록은 Amazon VPC 사용 설명서의 [흐름 로그 레코드](#)를 참조하세요. 이 파라미터에 대해 값을 제공하지 않으면 기본 형식을 사용하여 흐름 로그가 생성됩니다. 이 파라미터를 지정하는 경우 하나 이상의 필드를 지정해야 합니다.

- LogGroupName

유형: 문자열

설명: (선택 사항) 흐름 로그 데이터가 게시되는 CloudWatch Logs 로그 그룹의 이름입니다.

LogDestinationType 파라미터에 대해 s3을 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

유형: 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

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "SSMExecutionPermissions",
      "Effect": "Allow",
      "Action": [
        "ssm:StartAutomationExecution",
        "ssm:GetAutomationExecution"
      ],
      "Resource": "*"
    }
  ]
}
```

```

    },
    {
      "Sid": "EC2FlowLogsPermissions",
      "Effect": "Allow",
      "Action": [
        "ec2:CreateFlowLogs",
        "ec2>DeleteFlowLogs",
        "ec2:DescribeFlowLogs"
      ],
      "Resource": [
        "arn:aws:ec2:us-east-1:111122223333:instance/resource-id",
        "arn:aws:ec2:us-east-1:111122223333:subnet/resource-id",
        "arn:aws:ec2:us-east-1:111122223333:vpc/resource-id",
        "arn:aws:ec2:us-east-1:111122223333:transit-gateway/resource-id",
        "arn:aws:ec2:us-east-1:111122223333:transit-gateway-
attachment/resource-id"
      ]
    },
    {
      "Sid": "IAMCreateRolePermissions",
      "Effect": "Allow",
      "Action": [
        "iam:AttachRolePolicy",
        "iam:CreateRole",
        "iam:CreatePolicy",
        "iam>DeletePolicy",
        "iam>DeleteRole",
        "iam>DeleteRolePolicy",
        "iam:GetPolicy",
        "iam:GetRole",
        "iam:TagRole",
        "iam:PassRole",
        "iam:PutRolePolicy",
        "iam:UpdateRole"
      ],
      "Resource": [
        "arn:aws:iam::111122223333:role/role-name",
        "arn:aws:iam::111122223333:role/AWSSupportCreateFlowLogsRole"
      ]
    },
    {
      "Sid": "CloudWatchLogsPermissions",
      "Effect": "Allow",
      "Action": [

```

```

        "logs:CreateLogDelivery",
        "logs:CreateLogGroup",
        "logs>DeleteLogDelivery",
        "logs>DeleteLogGroup",
        "logs:DescribeLogGroups",
        "logs:DescribeLogStreams"
    ],
    "Resource": [
        "arn:aws:logs:us-east-1:111122223333:log-group:log-group-name",
        "arn:aws:logs:us-east-1:111122223333:log-group:log-group-name:"
    ]
},
{
    "Sid": "S3Permissions",
    "Effect": "Allow",
    "Action": [
        "s3:GetBucketLocation",
        "s3:GetBucketPublicAccessBlock",
        "s3:GetAccountPublicAccessBlock",
        "s3:GetBucketPolicyStatus",
        "s3:GetBucketAcl",
        "s3:ListBucket",
        "s3:PutObject"
    ],
    "Resource": [
        "arn:aws:s3:::amzn-s3-demo-bucket",
        "arn:aws:s3:::amzn-s3-demo-bucket/"
    ]
}
]
}

```

문서 단계

- `aws:branch - LogDestinationType` 파라미터에 대해 지정된 값을 기반으로 분기합니다.
- `aws:executeScript` - 대상 Amazon Simple Storage Service(Amazon S3)가 객체에 대한 읽기 또는 쓰기 `public` 액세스 권한을 부여할 가능성이 있는지 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 로그 데이터를 Amazon Simple Storage Service (Amazon S3)에 게시하는 기존 Amazon VPC 흐름 로그를 지정하는 Amazon CloudWatch Logs(CloudWatch Logs) 버킷에 흐름 로그 데이터를 게시하는 흐름 로그로 대체합니다.

[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.

- DestinationLogGroup

유형: 문자열

설명: (필수) 흐름 로그 데이터를 게시하려는 CloudWatch Logs 로그 그룹의 이름입니다.

- DeliverLogsPermissionArn

유형: 문자열

설명: (필수) CloudWatch Logs에 흐름 로그 데이터를 게시하는 데 필요한 권한을 Amazon Elastic Compute Cloud(Amazon EC2)에 제공하는 사용하려는 AWS Identity and Access Management (IAM) 역할의 ARN입니다.

- 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 파라미터에서 지정하는 값에서 VPC에 대한 세부 정보를 수집합니다.
- aws:executeAwsApi - 실행서 파라미터에 대해 지정하는 값을 기반으로 흐름 로그를 생성합니다.
- aws:assertAwsResourceProperty - 새로 생성된 흐름 로그가 CloudWatch Logs에 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 흐름 로그 데이터를 Amazon CloudWatch Logs(CloudWatch Logs)에 게시하는 기존 Amazon VPC 흐름 로그를 지정하는 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

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.

- DestinationS3BucketArn

유형: 문자열

설명: (필수) 흐름 로그 데이터를 게시하려는 Amazon S3 버킷의 ARN입니다.

- FlowLogId

유형: 문자열

설명: (필수) 교체하려는 CloudWatch Logs에 게시되는 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 파라미터에서 지정하는 값에서 VPC에 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 - CloudWatch Logs에 게시하는 흐름 로그를 삭제합니다.
- aws:executeScript - CloudWatch Logs에 게시된 흐름 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

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.

- AllocationId

유형: 문자열

설명: (필수) 탄력적 IP 주소의 할당 ID입니다.

AWS-RemoveNetworkACLUnrestrictedSSHRDP

설명

AWS-RemoveNetworkACLUnrestrictedSSHRDP 실행서는 지정된 네트워크 ACL에서 모든 소스 주소에서 기본 SSH 및 RDP 포트로의 수신 트래픽을 허용하는 모든 네트워크 액세스 제어 목록(ACL) 규

칙을 제거합니다. 기본 SSH 및 RDP 포트와 중첩되는 포트 범위를 포함하는 규칙은 제거되지 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.

- NetworkAcId

유형: 문자열

설명: (필수) 모든 소스 주소에서 기본 SSH 및 RDP 포트로의 수신 트래픽을 허용하는 무제한 규칙을 제거하려는 네트워크 ACL의 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 규칙 및 `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

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.

- 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 지정하는 Virtual Private Cloud(VPC)의 기본 보안 그룹에서 모든 규칙을 제거합니다.

[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.

- 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-SetupIPMonitoringFromVPC는 지정된 서브넷에서 Amazon Elastic Compute Cloud(Amazon EC2) 인스턴스를 생성하고 ping, MTR, traceroute 및 tracetcp 테스트 등을 지속적으로 실행하여 선택된 대상 IP(IPv4 또는 IPv6)를 모니터링합니다. 결과가 Amazon CloudWatch Logs 로그에 저장되며, 지표 필터가 적용되어 CloudWatch 대시보드의 지연 시간 및 패킷 손실 통계가 신속히 시각화됩니다.

추가 정보

CloudWatch Logs 데이터는 네트워크 문제 해결 및 패턴/트렌드 분석용으로 사용할 수 있습니다. 또는 패킷 손실 및/또는 지연 시간이 임계값에 도달할 때 Amazon SNS 알림을 사용하여 CloudWatch 경보를 구성할 수 있습니다. 또한에서 사례를 열 때 데이터를 사용하여 문제를 신속하게 AWS Support격리하고 네트워크 문제를 조사할 때 해결 시간을 단축할 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.

- 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.xlarge | t4g.micro | t4g.small | t4g.medium | t4g.large

기본값: t3.micro

설명: (선택 사항) EC2Rescue 인스턴스의 EC2 인스턴스 유형입니다. 권장 크기: t3.micro.

- SubnetId

유형: 문자열

설명: (필수) 모니터 인스턴스의 서브넷 ID입니다. 프라이빗 서브넷을 지정할 경우, 모니터 인스턴스에서 테스트를 설정하도록 허용하기 위한 인터넷 액세스 권한이 있는지 확인해야 합니다(즉, CloudWatch 로그 에이전트 설치, Systems Manager 및 CloudWatch와 상호 작용).

- TargetIPs

유형: 문자열

설명: (필수) 모니터링할 심표로 구분된 IPv4 및/또는 IPv6 목록입니다. 공백은 사용할 수 없습니다. 최대 크기는 255자입니다. 잘못된 IP를 지정하는 경우 자동화가 작동하지 않으며, 테스트 설정이 롤백됩니다.

- TestInstanceSecurityGroupId

유형: 문자열

설명: (선택 사항) 테스트 인스턴스의 보안 그룹 ID입니다. 지정하지 않으면 인스턴스 생성 중에 자동화가 하나를 생성합니다. 보안 그룹이 모니터링 IPs에 대한 아웃바운드 액세스를 허용하는지 확인합니다.

- `TestInstanceProfileName`

유형: 문자열

설명: (선택 사항) 테스트 인스턴스에 대한 기존 IAM 인스턴스 프로파일의 이름입니다. 지정하지 않으면 인스턴스 생성 중에 자동화가 하나를 생성합니다. 역할에는 `logs:CreateLogStream`, `logs:DescribeLogGroups`, `logs:DescribeLogStreams`, `logs:PutLogEvents` 및 AWS 관리형 정책과 같은 권한이 있어야 합니다 `AmazonSSMManagedInstanceCore`.

- `TestInterval`

유형: 문자열

설명: (선택 사항) 테스트 간격 사이의 분 수입니다. 기본값은 1 분이고 최대값은 10 분입니다.

- `RetainDashboardAndLogsOnDeletion`

유형: 문자열

설명: (선택 사항) AWS CloudFormation 스택을 삭제할 때 Amazon CloudWatch 대시보드 및 로그를 삭제하도록 지정합니다. 기본값은 `True`입니다. 기본적으로 대시보드와 로그는 유지되며 더 이상 필요하지 않은 경우 수동으로 삭제해야 합니다.

필수 IAM 권한

실행서를 성공적으로 사용하려면 `AutomationAssumeRole` 파라미터에 다음 작업이 필요합니다.

Warning

변경 가능한 IAM 권한의 오용을 방지하기 위해 `TestInstanceProfileName` 파라미터를 전달하거나 보안 가드레일을 마련하는 것이 좋습니다.

자동화를 실행하는 사용자에게 `AmazonSSMAutomationRole` IAM 관리형 정책이 연결되도록 하는 것이 좋습니다. 또한, 사용자의 사용자 계정, 그룹 또는 역할에 다음 정책이 연결되어 있어야 합니다.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": [
        "iam:CreateRole",
        "iam:CreateInstanceProfile",
        "iam:GetRole",
        "iam:GetInstanceProfile",
        "iam:DetachRolePolicy",
        "iam:AttachRolePolicy",
        "iam:PassRole",
        "iam:AddRoleToInstanceProfile",
        "iam:GetRolePolicy",
        "iam:RemoveRoleFromInstanceProfile",
        "iam>DeleteRole",
        "iam>DeleteRolePolicy",
        "iam>DeleteInstanceProfile",
        "iam:PutRolePolicy",
        "iam:TagRole"
      ],
      "Resource": [
        "arn:aws:iam::111122223333:role/SetupIPMonitoringFromVPC*",
        "arn:aws:iam::111122223333:instance-profile/SetupIPMonitoringFromVPC*"
      ],
      "Effect": "Allow"
    },
    {
      "Action": [
        "cloudformation:CreateStack",
        "cloudformation:CreateChangeSet",
        "cloudformation>DeleteStack",
        "cloudformation:DescribeStacks",
        "cloudformation:DescribeStackEvents",
        "cloudwatch:PutDashboard",
        "cloudwatch>DeleteDashboards",
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:CreateSecurityGroup",
        "ec2:CreateLaunchTemplate",
        "ec2>DeleteSecurityGroup",

```

```

        "ec2:DescribeImages",
        "ec2:DescribeSubnets",
        "ec2:DescribeInstanceTypes",
        "ec2:DescribeVpcs",
        "ec2:DeleteLaunchTemplate",
        "ec2:DeleteSecurityGroup",
        "ec2:RunInstances",
        "ec2:TerminateInstances",
        "ec2:DescribeInstanceStatus",
        "ec2:CreateTags",
        "ec2:AssignIpv6Addresses",
        "ec2:DescribeTags",
        "ec2:DescribeInstances",
        "ec2:DescribeSecurityGroups",
        "ec2:DescribeLaunchTemplates",
        "ec2:RevokeSecurityGroupEgress",
        "logs:CreateLogGroup",
        "logs:DeleteLogGroup",
        "logs:PutMetricFilter",
        "logs:PutRetentionPolicy",
        "logs:TagResource",
        "ssm:DescribeInstanceInformation",
        "ssm:GetParameter",
        "ssm:GetParameters",
        "ssm:SendCommand",
        "ssm:ListCommands",
        "ssm:ListCommandInvocations"
    ],
    "Resource": [
        "*"
    ],
    "Effect": "Allow"
}
]
}

```

TestInstanceProfileName 파라미터가 제공된 경우 실행서를 실행하는 데 다음 IAM 권한이 필요하지 않습니다.

- iam:CreateRole
- iam:CreateInstanceProfile

- iam:DetachRolePolicy
- iam:AttachRolePolicy
- iam:AddRoleToInstanceProfile
- iam:RemoveRoleFromInstanceProfile
- iam>DeleteRole
- iam>DeleteRolePolicy
- iam>DeleteInstanceProfile

문서 단계

1. **aws:executeAwsApi** - 제공된 서브넷을 설명하여 VPC ID 및 IPv6 CIDR 블록 연결 상태를 가져옵니다.
2. **aws:executeScript** - 제공된 대상 IPs가 구문상 올바른 IPv4 및/또는 IPv6 주소인지 확인하고, 선택한 인스턴스 유형의 아키텍처를 가져오고, 대상 IP가 IPv6인 경우 서브넷에 IPv6 풀 연결이 있는지 확인합니다.
3. **aws:createStack** - 테스트 Amazon EC2 인스턴스, IAM 인스턴스 프로파일(제공되지 않은 경우), 보안 그룹(제공되지 않은 경우), CloudWatch 로그 그룹 및 CloudWatch 대시보드를 프로비저닝하는 AWS CloudFormation 스택을 생성합니다.

(정리) 단계가 실패하는 경우:

aws:executeScript - CloudFormation 스택 이벤트를 설명하여 실패 이유를 식별합니다.

aws:deleteStack - CloudFormation 스택과 연결된 모든 리소스를 삭제합니다.

4. **aws:waitForAwsResourceProperty** - CloudFormation 스택 생성이 완료될 때까지 기다립니다.

(정리) 단계가 실패하는 경우:

aws:executeScript - CloudFormation 스택 이벤트를 설명하여 실패 이유를 식별합니다.

aws:deleteStack - CloudFormation 스택과 연결된 모든 리소스를 삭제합니다.

5. **aws:executeScript** - CloudFormation 스택 리소스를 설명하여 테스트 인스턴스 ID, 보안 그룹 ID, IAM 역할, 인스턴스 프로파일 및 대시보드 이름을 가져옵니다.

(정리) 단계가 실패하는 경우:

aws:executeScript - CloudFormation 스택 이벤트를 설명하여 실패 이유를 식별합니다.

aws:deleteStack - CloudFormation 스택과 모든 관련 리소스를 삭제합니다.

6. **aws:waitForAwsResourceProperty** - 테스트 인스턴스가 관리형 인스턴스가 될 때까지 기다립니다.

(정리) 단계가 실패하는 경우:

aws:deleteStack - CloudFormation 스택과 연결된 모든 리소스를 삭제합니다.

7. **aws:runCommand** - 테스트 인스턴스에 CloudWatch 에이전트를 설치합니다.

(정리) 단계가 실패하는 경우:

aws:deleteStack - CloudFormation 스택과 모든 관련 리소스를 삭제합니다.

8. **aws:runCommand** - 제공된 각 IPs에 대한 네트워크 테스트 스크립트(MTR, ping, tracepath 및 traceroute)를 정의합니다.

(정리) 단계가 실패하는 경우:

aws:deleteStack - CloudFormation 스택과 연결된 모든 리소스를 삭제합니다.

9. **aws:runCommand** - TestInterval 분마다 실행되는 cronjobs를 사용하여 네트워크 테스트를 시작하고 후속 실행을 예약합니다.

(정리) 단계가 실패하는 경우:

aws:deleteStack - CloudFormation 스택과 모든 관련 리소스를 삭제합니다.

- 10 **aws:runCommand** - 테스트 결과에서 CloudWatch Logs로 푸시하도록 CloudWatch 에이전트/home/ec2-user/logs/를 구성합니다.

(정리) 단계가 실패하는 경우:

aws:deleteStack - CloudFormation 스택과 연결된 모든 리소스를 삭제합니다.

- 11 **aws:runCommand** -에서 테스트 결과에 대한 로그 교체를 구성합니다/home/ec2-user/logs/.

- 12 **aws:executeScript** - CloudFormation 스택에서 생성된 모든 CloudWatch 로그 그룹에 대해 보존 정책을 설정합니다.

- 13 **aws:executeScript** - ping 지연 시간 및 ping 패킷 손실을 위한 CloudWatch 로그 그룹 지표 필터를 생성합니다.

(정리) 단계가 실패하는 경우:

aws:deleteStack - CloudFormation 스택과 모든 관련 리소스를 삭제합니다.

14 **aws:executeScript** - ping 지연 시간 및 ping 패킷 손실 통계를 위한 위젯을 포함하도록 CloudWatch 대시보드를 업데이트합니다.

(정리) 단계가 실패하는 경우:

aws:executeAwsApi - CloudWatch 대시보드가 있는 경우 해당 대시보드를 삭제합니다.

aws:deleteStack - CloudFormation 스택과 연결된 모든 리소스를 삭제합니다.

15 **aws:branch** - SleepTime 파라미터를 평가합니다. 로 설정하면 스택을 삭제하지 않고 자동화가 종료됩니다.

16 **aws:sleep** - CloudFormation 스택을 삭제하기 전에 지정된 SleepTime 기간을 기다립니다.

17 **aws:deleteStack** - CloudFormation 스택을 삭제합니다. RetainDashboardAndLogsOnDeletion 파라미터를 기반으로 CloudWatch 대시보드 및 로그 그룹은 유지되거나 삭제됩니다.

(정리) 스택 삭제에 실패하는 경우:

aws:executeScript - CloudFormation 스택 이벤트를 설명하여 삭제 실패 이유를 식별합니다.

출력

updateCloudWatchDashboard.StackUrl - CloudFormation 스택의 URL입니다.

updateCloudWatchDashboard.DashboardUrl - CloudWatch 대시보드의 URL입니다.

updateCloudWatchDashboard.DashboardName - CloudWatch 대시보드의 이름입니다.

updateCloudWatchDashboard.LogGroups - 생성된 CloudWatch 로그 그룹 목록입니다.

describeStackResources.HelperInstanceId - 테스트 인스턴스 ID입니다.

describeStackResources.StackName - CloudFormation 스택 이름입니다.

AWSSupport-TerminateIPMonitoringFromVPC

설명

AWSSupport-TerminateIPMonitoringFromVPCAWSSupport-SetupIPMonitoringFromVPC에서 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

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.

- 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 사용자에게 AmazonSSMAutomationRole IAM 관리형 정책이 연결되도록 하는 것이 좋습니다. 또한, 사용자, 그룹 또는 역할에 다음 정책이 연결되어 있어야 합니다.

JSON

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": [
        "iam:DetachRolePolicy",
        "iam:RemoveRoleFromInstanceProfile",
        "iam>DeleteRole",
        "iam>DeleteInstanceProfile",
        "iam>DeleteRolePolicy"
      ],
      "Resource": [
        "arn:aws:iam::111122223333:role/AWSSupport/SetupIPMonitoringFromVPC_*",
        "arn:aws:iam::111122223333:instance-profile/AWSSupport/SetupIPMonitoringFromVPC_*"
      ],
      "Effect": "Allow"
    },
    {
      "Action": [
        "iam:DetachRolePolicy"
      ],
      "Resource": [
        "arn:aws:iam::aws:policy/service-role/AmazonSSMManagedInstanceCore"
      ],
      "Effect": "Allow"
    }
  ]
}
```

```

    },
    {
      "Action": [
        "cloudwatch:DeleteDashboards"
      ],
      "Resource": [
        "*"
      ],
      "Effect": "Allow"
    },
    {
      "Action": [
        "ec2:DescribeTags",
        "ec2:DescribeInstances",
        "ec2:DescribeSecurityGroups",
        "ec2>DeleteSecurityGroup",
        "ec2:TerminateInstances",
        "ec2:DescribeInstanceStatus"
      ],
      "Resource": [
        "*"
      ],
      "Effect": "Allow"
    }
  ]
}

```

문서 단계

1. `aws:assertAwsResourceProperty` - AutomationExecutionId 및 InstanceId가 동일 테스트와 관련이 있는지 확인합니다.
2. `aws:assertAwsResourceProperty` - SubnetId 및 InstanceId가 동일 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` - 자동화를 통해 생성된 IAM 인스턴스 프로파일을 삭제합니다.
8. `aws:executeAwsApi` - 자동화를 통해 생성된 역할에서 CloudWatch 인라인 정책을 삭제합니다.

9. `aws:executeAwsApi` - 자동화를 통해 생성된 역할에서 AmazonSSMManagedInstanceCore 관리형 정책을 분리합니다.
10. `aws:executeAwsApi` - 자동화를 통해 생성된 IAM 역할을 삭제합니다.
11. `aws:executeAwsApi` - 자동화를 통해 생성된 보안 그룹을 삭제합니다(있는 경우).

출력

없음

AWS WAF

AWS Systems Manager 자동화에는 대한 사전 정의된 실행서를 제공합니다 AWS WAF. 실행서에 대한 자세한 내용은 [실행서 작업](#)을 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 리전 규칙 그룹에 기존 AWS WAF AWS WAF 리전 규칙을 추가합니다. AWS WAF Classic 리전 규칙 그룹만 지원됩니다. AWS WAF Classic 리전 규칙 그룹은 최대 10개의 규칙을 가질 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.

- RuleGroupId

유형: 문자열

설명: (필수) 업데이트하려는 규칙 그룹의 ID입니다.

- RulePriority

유형: 정수

설명: (필수) 새 규칙의 우선 순위입니다. 규칙 우선 순위에 따라 리전 그룹의 규칙이 평가되는 순서가 결정됩니다. 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 규칙의 조건과 일치할 때가 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

- `GetWAFChangeToken(aws:executeAwsApi)` - AWS WAF 변경 토큰을 검색하여 실행서가 서비스에 충돌하는 요청을 제출하지 않도록 합니다.
- `AddWAFRuleToWAFRegionalRuleGroup(aws:executeScript)` - 지정된 규칙을 AWS WAF 리전 규칙 그룹에 추가합니다.
- `VerifyChangeTokenPropagating(aws:waitForAwsResourceProperty)` - 변경 토큰의 상태가 PENDING 또는 인지 확인합니다INSYNC.
- `VerifyRuleAddedToRuleGroup(aws:executeScript)` - 지정된 AWS WAF 규칙이 대상 리전 규칙 그룹에 추가되었는지 확인합니다.

출력

- `VerifyRuleAddedToRuleGroup.VerifyRuleAddedToRuleGroupResponse` - 새 규칙이 리전 규칙 그룹에 추가되었는지 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(ACL)에 추가합니다. 이 실행서는에서 관리하는 기존 AWS WAF Classic 리전 웹 ACL을 업데이트하지 않습니다 AWS Firewall Manager.

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.

- WebACLIId

유형: 문자열

설명: (필수) 업데이트하려는 웹 ACL의 ID입니다.

- ActivatedRulePriority

유형: 정수

설명: (필수) 새 규칙의 우선 순위입니다. 규칙 우선 순위에 따라 웹 ACL의 규칙이 평가되는 순서가 결정됩니다. 값이 낮은 규칙은 값이 높은 규칙보다 우선 순위가 높습니다. 이 값은 고유한 정수여야 합니다. 리전 웹 ACL에 여러 규칙을 추가하는 경우 값이 연속적일 필요는 없습니다.

- ActivatedRuleRuleId

유형: 문자열

설명: (필수) 웹 ACL에 추가할 일반 규칙, 속도 기반 규칙 또는 그룹의 ID입니다.

- **ActivatedRuleAction**

유형: 문자열

유효한 값: ALLOW | BLOCK | COUNT

설명: (선택 사항) 웹 요청이 규칙의 조건과 일치할 때가 AWS WAF 수행하는 작업을 지정합니다.

- **ActivatedRuleType**

유형: 문자열

유효한 값: REGULAR | RATE_BASED | GROUP

기본값: REGULAR

설명: (선택 사항) 웹 ACL에 추가할 규칙 유형입니다. 이 필드는 선택 사항이지만 유형을 설정하지 않고 웹 ACL에 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 웹 ACL이 Firewall Manager 보안 정책에 있는지 확인하고 우선 순위 ID가 기존 ACL과 충돌하지 않는지 확인합니다.
- `AddRuleOrRuleGroupToWebACL(aws:executeScript)` - 지정된 규칙을 AWS WAF 웹 ACL에 추가합니다.
- `VerifyRuleOrRuleGroupAddedToWebAcl(aws:executeScript)` - 지정된 AWS WAF 규칙이 대상 웹 ACL에 추가되었는지 확인합니다.

출력

- `DetermineWebACLNotInFMSAndRulePriority.PrereqResponse`:
`DetermineWebACLNotInFMSAndRulePriority` 단계의 출력입니다.
- `VerifyRuleOrRuleGroupAddedToWebAcl.VerifyRuleOrRuleGroupAddedToWebACLResponse`:
`AddRuleOrRuleGroupToWebACL` 단계의 출력입니다.
- `VerifyRuleOrRuleGroupAddedToWebAcl.ListActivatedRulesOrRuleGroupsInWebACLResponse`:
`VerifyRuleOrRuleGroupAddedToWebAcl` 단계의 출력입니다.

AWSConfigRemediation-EnableWAFClassicLogging

설명

`AWSConfigRemediation-EnableWAFClassicLogging` 실행서를 사용하면 지정한 AWS WAF 웹 액세스 제어 목록(웹 ACL)에 대해 Amazon Data Firehose(Firehose)에 로깅할 수 있습니다.

[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.

- `DeliveryStreamName`

유형: 문자열

설명: (필수) 로그를 전송할 Firehose 전송 스트림의 이름입니다.

- WebACLId

유형: 문자열

설명: (필수) 로그인을 활성화하려는 AWS WAF 웹 ACL의 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 - DeliveryStreamName에서 지정하는 전송 스트림이 존재하는지 확인합니다.
- aws:executeAwsApi - WebACLId 파라미터에 지정된 AWS WAF 웹 ACL의 ARN을 수집합니다.
- aws:executeAwsApi - 웹 ACL에 대한 로깅을 활성화합니다.
- aws:assertAwsResourceProperty - AWS WAF 웹 ACL에서 로깅이 활성화되었는지 확인합니다.

AWSConfigRemediation-EnableWAFClassicRegionalLogging

설명

AWSConfigRemediation-EnableWAFClassicRegionalLogging 실행서를 사용하면 지정한 AWS WAF 웹 액세스 제어 목록(ACL)에 대해 Amazon Data Firehose(Firehose)에 로깅할 수 있습니다.

[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.

- LogDestinationConfigs

유형: 문자열

설명: (필수) 로그를 전송할 Firehose 전송 스트림의 Amazon 리소스 이름(ARN)입니다.

- WebACLIId

유형: 문자열

설명: (필수) 로그인을 활성화하려는 AWS WAF 웹 ACL의 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` - `WebACLIId` 파라미터에 지정된 AWS WAF 웹 ACL의 ARN을 수집합니다.
- `aws:executeAwsApi` - 웹 ACL에 대한 로깅을 활성화합니다.
- `aws:assertAwsResourceProperty` - AWS WAF 웹 ACL에서 로깅이 활성화되었는지 확인합니다.

AWSConfigRemediation-EnableWAFV2Logging

설명

AWSConfigRemediation-EnableWAFV2Logging 실행서는 지정된 Amazon Data Firehose(Firehose) 전송 스트림을 사용하여 AWS WAF (AWS WAF V2) 웹 액세스 제어 목록(웹 ACL)에 대한 로깅을 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.

- `LogDestinationConfigs`

유형: 문자열

설명: (필수) 웹 ACL과 연결할 Firehose 전송 스트림 ARN입니다.

 Note

Firehose 전송 스트림 ARN은 접두사 `aws-waf-logs-` 로 시작해야 합니다. 예: `aws-waf-logs-us-east-2-analytics`. 자세한 내용은 [Amazon Data Firehose](#) 섹션을 참조하세요.

- WebAclArn

유형: 문자열

설명: (필수) 로깅이 활성화될 웹 ACL의 ARN입니다.

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 웹 ACL에 대한 로깅을 활성화하고 로깅에 지정된 구성이 있는지 확인합니다.

Amazon WorkSpaces

AWS Systems Manager 자동화는 Amazon WorkSpaces에 사전 정의된 실행서를 제공합니다. 실행서에 대한 자세한 내용은 [실행서 작업](#)을 참조하세요. 실행서 콘텐츠를 보는 방법에 대한 자세한 내용은 [실행서 콘텐츠 보기\(을\)](#)를 참조하세요.

주제

- [AWS-CreateWorkspace](#)
- [AWSSupport-RecoverWorkspace](#)

AWS-CreateWorkspace

설명

AWS-CreateWorkspace 실행서는 입력 파라미터에 대해 지정하는 값을 기반으로 Workspace라고 하는 새로운 Amazon WorkSpaces 가상 데스크톱을 생성합니다. WorkSpaces에 대한 자세한 내용은 Amazon WorkSpaces 관리 안내서의 [Amazon WorkSpaces란 무엇입니까?](#)를 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.

- BundleId

유형: 문자열

설명: (필수) Workspace에 사용할 번들의 ID입니다.

- ComputeTypeName

유형: 문자열

유효한 값: VALUE | STANDARD | PERFORMANCE | POWER | GRAPHICS | POWERPRO | GRAPHICSPRO

설명: (선택 사항) Workspace의 컴퓨팅 유형입니다.

- DirectoryId

유형: 문자열

설명: (필수) Workspace를 추가할 디렉터리의 ID입니다.

- RootVolumeEncryptionEnabled

유형: Boolean

유효한 값: true | false

기본값: false

설명: (선택 사항) Workspace의 루트 볼륨이 암호화되는지 여부를 결정합니다.

- RootVolumeSizeGib

유형: 정수

설명: (필수) Workspace에 대한 루트 볼륨의 크기입니다.

- RunningMode

유형: 문자열

유효한 값: ALWAYS_ON | AUTO_STOP

설명: (필수) Workspace의 실행 모드입니다.

- RunningModeAutoStopTimeoutInMinutes

유형: 정수

설명: (선택 사항) WorkSpaces가 중지될 때 사용자가 로그오프한 후의 시간입니다. 60분 간격으로 값을 지정합니다.

- Tags

유형: 문자열

설명: (선택 사항) Workspace에 적용하려는 태그입니다.

- Username

유형: 문자열

설명: (필수) Workspace에 연결할 사용자 이름입니다.

- UserVolumeEncryptionEnabled

유형: Boolean

유효한 값: true | false

기본값: false

설명: (선택 사항) Workspace의 사용자 볼륨이 암호화되는지 여부를 결정합니다.

- UserVolumeSizeGib

유형: 정수

설명: (필수) Workspace의 사용자 볼륨 크기입니다.

- VolumeEncryptionKey

유형: 문자열

설명: (선택 사항) Workspace에 저장된 데이터를 암호화하는 데 사용할 대칭 AWS Key Management Service 키입니다.

필수 IAM 권한

실행서를 성공적으로 사용하려면 AutomationAssumeRole 파라미터에 다음 작업이 필요합니다.

- workspaces:CreateWorkspaces
- workspaces:DescribeWorkspaces

문서 단계

- aws:executeScript - 입력 파라미터에 대해 지정하는 값을 기반으로 Workspace를 생성합니다.

- `aws:waitForAwsResourceProperty` - `WorkSpace`의 상태가 `AVAILABLE`인지 확인합니다.

출력

`CreateWorkspace.WorkspaceId`

AWSSupport-RecoverWorkSpace

설명

`AWSSupport-RecoverWorkSpace` 실행서는 지정하는 `WorkSpace`라고 하는 Amazon WorkSpaces 가상 데스크톱에서 복구 단계를 수행합니다. 실행서는 `WorkSpace`를 재부팅하고, 상태가 여전히 `UNHEALTHY`이면 입력 파라미터에서 지정하는 값을 기반으로 `WorkSpace`를 복원하거나 재빌드합니다. 이 실행서를 사용하기 전에 Amazon WorkSpaces 관리 안내서의 [WorkSpaces 문제 해결](#)을 검토하는 것이 좋습니다.

Important

`WorkSpace`를 복원하거나 재빌드하는 작업은 데이터 손실을 초래할 수 있는 잠재적으로 파괴적인 작업입니다. 이는 `WorkSpace`가 사용 가능한 마지막 스냅샷에서 복원되고 스냅샷에서 복구되는 데이터가 12시간 가량 경과된 내용일 수 있기 때문입니다.

복원 옵션은 최신 스냅샷을 기반으로 루트 볼륨과 사용자 볼륨을 모두 재생성합니다. 재빌드 옵션은 가장 최근 스냅샷에서 사용자 볼륨을 재생성하고 `WorkSpace`가 생성된 번들과 연결된 이미지에서 `WorkSpace`를 다시 생성합니다. `WorkSpace`가 생성된 이후에 변경된 시스템 설정 또는 설치된 애플리케이션이 손실됩니다. 작업 영역 복원 및 재빌드에 대한 자세한 내용은 Amazon WorkSpaces 관리 안내서의 [WorkSpace 복원](#) 및 [WorkSpace 재빌드](#)를 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.

- 확인

유형: 문자열

유효한 값: Yes

설명: (필수) 'yes'를 입력하면 복원 및 재빌드 작업이 가장 최근 스냅샷에서 WorkSpace를 복구하려고 시도하고 이러한 스냅샷에서 복원되는 데이터가 12시간 가량 경과된 내용일 수 있음을 이해한다는 의미입니다.

- 재부팅

유형: 문자열

유효한 값: Yes | No

기본값: Yes

설명: (필수) WorkSpace를 재부팅할지 여부를 결정합니다.

- 재빌드

유형: 문자열

유효한 값: Yes | No

기본값: 아니요

설명: (필수) WorkSpace를 재빌드할지 여부를 결정합니다.

- 복원

유형: 문자열

유효한 값: Yes | No

기본값: 아니요

설명: (필수) Workspace의 복원 여부를 결정합니다.

- WorkspaceId

유형: 문자열

설명: (필수) 복구하려는 Workspace의 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 지정하는 Workspace의 상태를 수집합니다.
- aws:assertAwsResourceProperty - Workspace의 상태가 AVAILABLE , ERROR , IMPAIRED , STOPPED 또는 UNHEALTHY인지 확인합니다.
- aws:branch - Workspace의 상태를 기반으로 분기합니다.
- aws:executeAwsApi - Workspace를 시작합니다.
- aws:branch - Action 파라미터에 대해 지정하는 값을 기반으로 분기합니다.
- aws:waitForAwsResourceProperty - 시작 후 Workspace 상태가 표시될 때까지 기다립니다.

- `aws:waitForAwsResourceProperty` - 시작 후 WorkSpace 상태가 AVAILABLE, ERROR, IMPAIRED 또는 UNHEALTHY로 변경될 때까지 기다립니다.
- `aws:executeAwsApi` - WorkSpace가 시작된 후의 상태를 수집합니다.
- `aws:branch` - 시작 후 WorkSpace의 상태를 기반으로 분기합니다.
- `aws:executeAwsApi` - WorkSpace를 복원하거나 재빌드하는 데 사용할 수 있는 스냅샷을 수집합니다.
- `aws:branch` - Reboot 파라미터에 대해 지정하는 값을 기반으로 분기합니다.
- `aws:executeAwsApi` - WorkSpace를 재부팅합니다.
- `aws:executeAwsApi` - WorkSpace가 시작된 후의 상태를 수집합니다.
- `aws:waitForAwsResourceProperty` - WorkSpace의 상태가 REBOOTING(으)로 변경될 때까지 기다립니다.
- `aws:waitForAwsResourceProperty` - 재부팅 후 WorkSpace 상태가 AVAILABLE ERROR 또는 UNHEALTHY로 변경될 때까지 기다립니다.
- `aws:executeAwsApi` - WorkSpace가 재부팅된 후의 상태를 수집합니다.
- `aws:branch` - 재부팅 후 WorkSpace의 상태를 기반으로 분기합니다.
- `aws:branch` - Restore 파라미터에 대해 지정하는 값을 기반으로 분기합니다.
- `aws:executeAwsApi` - WorkSpace를 복원합니다. 복원이 실패하면 Runbook은 WorkSpace를 재빌드하려고 시도합니다.
- `aws:waitForAwsResourceProperty` - WorkSpace의 상태가 RESTORING(으)로 변경될 때까지 기다립니다.
- `aws:waitForAwsResourceProperty` - 복원 후 WorkSpace 상태가 AVAILABLE, ERROR 또는 UNHEALTHY로 변경될 때까지 기다립니다.
- `aws:executeAwsApi` - 복원 후 WorkSpace 상태를 수집합니다.
- `aws:branch` - 복원 후 WorkSpace의 상태를 기반으로 분기합니다.
- `aws:branch` - Rebuild 파라미터에 대해 지정하는 값을 기반으로 분기합니다.
- `aws:executeAwsApi` - WorkSpace를 재빌드합니다.
- `aws:waitForAwsResourceProperty` - WorkSpace의 상태가 REBUILDING(으)로 변경될 때까지 기다립니다.
- `aws:waitForAwsResourceProperty` - 다시 빌드된 후 WorkSpace 상태가 AVAILABLE , ERROR 또는 UNHEALTHY로 변경될 때까지 기다립니다.
- `aws:executeAwsApi` - WorkSpace가 재빌드된 후의 상태를 수집합니다.
- `aws:assertAwsResourceProperty` - WorkSpace의 상태가 AVAILABLE인지 확인합니다.

X-Ray

AWS Systems Manager 자동화하는에 대한 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 실행서는 최소 권장 보안 모범 사례에 따라 AWS X-Ray 데이터를 암호화하기 위한 기준으로만 사용해야 합니다. 서로 다른 KMS 키를 사용하여 여러 데이터 세트를 암호화하는 것이 좋습니다.

[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.

- KeyId

유형: 문자열

설명: (필수) 데이터를 암호화하는 데 AWS X-Ray 사용할 KMS 키의 Amazon 리소스 이름(ARN), 키 ID 또는 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 파라미터에서 지정하는 KMS 키를 사용하여 X-Ray 데이터에 대한 암호화를 활성화할 수 있습니다.
- aws:waitForAwsResourceProperty - X-Ray의 암호화 구성 상태가 ACTIVE가 될 때까지 기다립니다.
- aws:executeAwsApi - KeyId 파라미터에서 지정하는 키의 ARN을 수집합니다.
- aws:assertAwsResourceProperty - X-Ray에서 암호화가 활성화되었는지 확인합니다.

기계 번역으로 제공되는 번역입니다. 제공된 번역과 원본 영어의 내용이 상충하는 경우에는 영어 버전이 우선합니다.