AWSエージェントの権限とセキュリティルール

NetApp Console setup and administration

NetApp
March 02, 2026

目次

AWSエージェントの権限とセキュリティルール

コンソールエージェントのAWS権限

NetApp ConsoleがAWS でコンソールエージェントを起動すると、その AWS アカウント内のリソースとプロセスを管理するための権限をエージェントに付与するポリシーがエージェントにアタッチされます。エージェントは、権限を使用して、EC2、S3 、CloudFormation、IAM、キー管理サービス (KMS) などの複数の AWS サービスへの API 呼び出しを実行します。

IAMポリシー

以下の IAM ポリシーは、AWS リージョンに基づいてパブリッククラウド環境内のリソースとプロセスを管理するためにコンソールエージェントに必要な権限を提供します。

次の点に注意してください。

- コンソールから直接標準 AWS リージョンにコンソールエージェントを作成すると、コンソールはエージェントにポリシーを自動的に適用します。
- AWS Marketplace からエージェントをデプロイする場合、Linux ホストにエージェントを手動でインストールする場合、またはコンソールに追加の AWS 認証情報を追加する場合は、ポリシーを自分で設定する必要があります。
- いずれの場合も、後続のリリースで新しい権限が追加されるため、ポリシーが最新であることを確認する必要があります。新しい権限が必要な場合は、リリース ノートに記載されます。
- 必要に応じて、IAMを使用してIAMポリシーを制限することができます。 `Condition`要素。 "AWS ドキュメント: 条件要素"
- これらのポリシーの使用方法の詳細な手順については、次のページを参照してください。
  - "AWS Marketplace デプロイメントの権限を設定する"
  - "オンプレミス展開の権限を設定する"
  - "制限モードの権限を設定する"
  - "プライベートモードの権限を設定する"

必要なポリシーを表示するには、地域を選択してください。

標準地域

標準リージョンの場合、権限は 2 つのポリシーに分散されます。 AWS の管理ポリシーの最大文字サイズ制限により、2 つのポリシーが必要になります。

ポリシー**1**

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": [
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeInstances",
        "ec2:DescribeInstanceStatus",
        "ec2:RunInstances",
        "ec2:ModifyInstanceAttribute",
        "ec2:DescribeInstanceAttribute",
        "ec2:DescribeRouteTables",
        "ec2:DescribeImages",
        "ec2:CreateTags",
        "ec2:CreateVolume",
        "ec2:DescribeVolumes",
        "ec2:ModifyVolumeAttribute",
        "ec2:CreateSecurityGroup",
        "ec2:DescribeSecurityGroups",
        "ec2:RevokeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:RevokeSecurityGroupIngress",
        "ec2:CreateNetworkInterface",
        "ec2:DescribeNetworkInterfaces",
        "ec2:ModifyNetworkInterfaceAttribute",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:DescribeDhcpOptions",
        "ec2:CreateSnapshot",
        "ec2:DescribeSnapshots",
        "ec2:GetConsoleOutput",
        "ec2:DescribeKeyPairs",
        "ec2:DescribeRegions",
        "ec2:DescribeTags",
        "ec2:AssociateIamInstanceProfile",
        "ec2:DescribeIamInstanceProfileAssociations",
        "ec2:DisassociateIamInstanceProfile",
        "ec2:CreatePlacementGroup",
        "ec2:DescribeReservedInstancesOfferings",
        "ec2:AssignPrivateIpAddresses",
        "ec2:CreateRoute",
        "ec2:DescribeVpcs",
```

```
        "ec2:ReplaceRoute",
        "ec2:UnassignPrivateIpAddresses",
        "ec2:DeleteSecurityGroup",
        "ec2:DeleteNetworkInterface",
        "ec2:DeleteSnapshot",
        "ec2:DeleteTags",
        "ec2:DeleteRoute",
        "ec2:DeletePlacementGroup",
        "ec2:DescribePlacementGroups",
        "ec2:DescribeVolumesModifications",
        "ec2:ModifyVolume",
        "cloudformation:CreateStack",
        "cloudformation:DescribeStacks",
        "cloudformation:DescribeStackEvents",
        "cloudformation:ListStacks",
        "cloudformation:ValidateTemplate",
        "cloudformation:DeleteStack",
        "iam:PassRole",
        "iam:CreateRole",
        "iam:PutRolePolicy",
        "iam:CreateInstanceProfile",
        "iam:AddRoleToInstanceProfile",
        "iam:RemoveRoleFromInstanceProfile",
        "iam:ListInstanceProfiles",
        "iam:DeleteRole",
        "iam:DeleteRolePolicy",
        "iam:DeleteInstanceProfile",
        "iam:GetRolePolicy",
        "iam:GetRole",
        "sts:DecodeAuthorizationMessage",
        "sts:AssumeRole",
        "s3:GetBucketTagging",
        "s3:GetBucketLocation",
        "s3:ListBucket",
        "s3:CreateBucket",
        "s3:GetLifecycleConfiguration",
        "s3:ListBucketVersions",
        "s3:GetBucketPolicyStatus",
        "s3:GetBucketPublicAccessBlock",
        "s3:GetBucketPolicy",
        "s3:GetBucketAcl",
        "s3:PutObjectTagging",
        "s3:GetObjectTagging",
        "s3:DeleteObject",
        "s3:DeleteObjectVersion",
        "s3:PutObject",
```

```
            "s3:ListAllMyBuckets",
            "s3:GetObject",
            "s3:GetEncryptionConfiguration",
            "kms:ReEncrypt*",
            "kms:CreateGrant",
            "fsx:Describe*",
            "fsx:List*",
            "kms:GenerateDataKeyWithoutPlaintext"
        ],
        "Resource": "*",
        "Effect": "Allow",
        "Sid": "cvoServicePolicy"
    },
    {
        "Action": [
            "ec2:StartInstances",
            "ec2:StopInstances",
            "ec2:DescribeInstances",
            "ec2:DescribeInstanceStatus",
            "ec2:RunInstances",
            "ec2:TerminateInstances",
            "ec2:DescribeInstanceAttribute",
            "ec2:DescribeImages",
            "ec2:CreateTags",
            "ec2:CreateVolume",
            "ec2:CreateSecurityGroup",
            "ec2:DescribeSubnets",
            "ec2:DescribeVpcs",
            "ec2:DescribeRegions",
            "cloudformation:CreateStack",
            "cloudformation:DeleteStack",
            "cloudformation:DescribeStacks",
            "ec2:DescribeVpcEndpoints",
            "kms:ListAliases",
            "glue:GetDatabase",
            "glue:GetTable",
            "glue:GetPartitions"
        ],
        "Resource": "*",
        "Effect": "Allow",
        "Sid": "backupPolicy"
    },
    {
        "Action": [
            "s3:GetBucketLocation",
            "s3:ListAllMyBuckets",
```

```
            "s3:ListBucket",
            "s3:CreateBucket",
            "s3:GetLifecycleConfiguration",
            "s3:PutLifecycleConfiguration",
            "s3:PutBucketTagging",
            "s3:ListBucketVersions",
            "s3:GetBucketAcl",
            "s3:PutBucketPublicAccessBlock",
            "s3:GetObject",
            "s3:PutEncryptionConfiguration",
            "s3:DeleteObject",
            "s3:DeleteObjectVersion",
            "s3:ListBucketMultipartUploads",
            "s3:PutObject",
            "s3:PutBucketAcl",
            "s3:AbortMultipartUpload",
            "s3:ListMultipartUploadParts",
            "s3:DeleteBucket",
            "s3:GetObjectVersionTagging",
            "s3:GetObjectVersionAcl",
            "s3:GetObjectRetention",
            "s3:GetObjectTagging",
            "s3:GetObjectVersion",
            "s3:PutObjectVersionTagging",
            "s3:PutObjectRetention",
            "s3:DeleteObjectTagging",
            "s3:DeleteObjectVersionTagging",
            "s3:GetBucketObjectLockConfiguration",
            "s3:GetBucketVersioning",
            "s3:PutBucketObjectLockConfiguration",
            "s3:PutBucketVersioning",
            "s3:BypassGovernanceRetention",
            "s3:PutBucketPolicy",
            "s3:PutBucketOwnershipControls"
        ],
        "Resource": [
            "arn:aws:s3:::netapp-backup-*"
        ],
        "Effect": "Allow",
        "Sid": "backupS3Policy"
    },
    {
        "Action": [
            "s3:CreateBucket",
            "s3:GetLifecycleConfiguration",
            "s3:PutLifecycleConfiguration",
```

```
            "s3:PutBucketTagging",
            "s3:ListBucketVersions",
            "s3:GetBucketPolicyStatus",
            "s3:GetBucketPublicAccessBlock",
            "s3:GetBucketAcl",
            "s3:GetBucketPolicy",
            "s3:PutBucketPublicAccessBlock",
            "s3:DeleteBucket"
        ],
        "Resource": [
            "arn:aws:s3:::fabric-pool*"
        ],
        "Effect": "Allow",
        "Sid": "fabricPoolS3Policy"
    },
    {
        "Action": [
            "ec2:DescribeRegions"
        ],
        "Resource": "*",
        "Effect": "Allow",
        "Sid": "fabricPoolPolicy"
    },
    {
        "Condition": {
            "StringLike": {
                "ec2:ResourceTag/netapp-adc-manager": "*"
            }
        },
        "Action": [
            "ec2:StartInstances",
            "ec2:StopInstances",
            "ec2:TerminateInstances"
        ],
        "Resource": [
            "arn:aws:ec2:*:*:instance/*"
        ],
        "Effect": "Allow"
    },
    {
        "Condition": {
            "StringLike": {
                "ec2:ResourceTag/WorkingEnvironment": "*"
            }
        },
        "Action": [
```

```
            "ec2:StartInstances",
            "ec2:TerminateInstances",
            "ec2:AttachVolume",
            "ec2:DetachVolume",
            "ec2:StopInstances",
            "ec2:DeleteVolume"
        ],
        "Resource": [
            "arn:aws:ec2:*:*:instance/*"
        ],
        "Effect": "Allow"
    },
    {
        "Action": [
            "ec2:AttachVolume",
            "ec2:DetachVolume"
        ],
        "Resource": [
            "arn:aws:ec2:*:*:volume/*"
        ],
        "Effect": "Allow"
    },
    {
        "Condition": {
            "StringLike": {
                "ec2:ResourceTag/WorkingEnvironment": "*"
            }
        },
        "Action": [
            "ec2:DeleteVolume"
        ],
        "Resource": [
            "arn:aws:ec2:*:*:volume/*"
        ],
        "Effect": "Allow"
    }
  ]
}
```

ポリシー**2**

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": [
        "ec2:CreateTags",
        "ec2:DeleteTags",
        "ec2:DescribeTags",
        "tag:getResources",
        "tag:getTagKeys",
        "tag:getTagValues",
        "tag:TagResources",
        "tag:UntagResources"
      ],
      "Resource": "*",
      "Effect": "Allow",
      "Sid": "tagServicePolicy"
    }
  ]
}
```

GovCloud（米国）リージョン

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "iam:ListInstanceProfiles",
        "iam:CreateRole",
        "iam:DeleteRole",
        "iam:PutRolePolicy",
        "iam:CreateInstanceProfile",
        "iam:DeleteRolePolicy",
        "iam:AddRoleToInstanceProfile",
        "iam:RemoveRoleFromInstanceProfile",
        "iam:DeleteInstanceProfile",
        "ec2:ModifyVolumeAttribute",
        "sts:DecodeAuthorizationMessage",
        "ec2:DescribeImages",
        "ec2:DescribeRouteTables",
        "ec2:DescribeInstances",
        "iam:PassRole",
        "ec2:DescribeInstanceStatus",
        "ec2:RunInstances",
        "ec2:ModifyInstanceAttribute",
        "ec2:CreateTags",
        "ec2:CreateVolume",
        "ec2:DescribeVolumes",
        "ec2:DeleteVolume",
        "ec2:CreateSecurityGroup",
        "ec2:DeleteSecurityGroup",
        "ec2:DescribeSecurityGroups",
        "ec2:RevokeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:RevokeSecurityGroupIngress",
        "ec2:CreateNetworkInterface",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DeleteNetworkInterface",
        "ec2:ModifyNetworkInterfaceAttribute",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:DescribeDhcpOptions",
        "ec2:CreateSnapshot",
```

```
        "ec2:DeleteSnapshot",
        "ec2:DescribeSnapshots",
        "ec2:StopInstances",
        "ec2:GetConsoleOutput",
        "ec2:DescribeKeyPairs",
        "ec2:DescribeRegions",
        "ec2:DeleteTags",
        "ec2:DescribeTags",
        "cloudformation:CreateStack",
        "cloudformation:DeleteStack",
        "cloudformation:DescribeStacks",
        "cloudformation:DescribeStackEvents",
        "cloudformation:ListStacks",
        "cloudformation:ValidateTemplate",
        "s3:GetObject",
        "s3:ListBucket",
        "s3:ListAllMyBuckets",
        "s3:GetBucketTagging",
        "s3:GetBucketLocation",
        "s3:CreateBucket",
        "s3:GetBucketPolicyStatus",
        "s3:GetBucketPublicAccessBlock",
        "s3:GetBucketAcl",
        "s3:GetBucketPolicy",
        "kms:ReEncrypt*",
        "kms:CreateGrant",
        "ec2:AssociateIamInstanceProfile",
        "ec2:DescribeIamInstanceProfileAssociations",
        "ec2:DisassociateIamInstanceProfile",
        "ec2:DescribeInstanceAttribute",
        "ec2:CreatePlacementGroup",
        "ec2:DeletePlacementGroup"
      ],
      "Resource": "*"
    },
    {
      "Sid": "fabricPoolPolicy",
      "Effect": "Allow",
      "Action": [
        "s3:DeleteBucket",
        "s3:GetLifecycleConfiguration",
        "s3:PutLifecycleConfiguration",
        "s3:PutBucketTagging",
        "s3:ListBucketVersions",
        "s3:GetBucketPolicyStatus",
        "s3:GetBucketPublicAccessBlock",
```

```
        "s3:GetBucketAcl",
        "s3:GetBucketPolicy",
        "s3:PutBucketPublicAccessBlock"
      ],
      "Resource": [
        "arn:aws-us-gov:s3:::fabric-pool*"
      ]
    },
    {
      "Sid": "backupPolicy",
      "Effect": "Allow",
      "Action": [
        "s3:DeleteBucket",
        "s3:GetLifecycleConfiguration",
        "s3:PutLifecycleConfiguration",
        "s3:PutBucketTagging",
        "s3:ListBucketVersions",
        "s3:GetObject",
        "s3:ListBucket",
        "s3:ListAllMyBuckets",
        "s3:GetBucketTagging",
        "s3:GetBucketLocation",
        "s3:GetBucketPolicyStatus",
        "s3:GetBucketPublicAccessBlock",
        "s3:GetBucketAcl",
        "s3:GetBucketPolicy",
        "s3:PutBucketPublicAccessBlock"
      ],
      "Resource": [
        "arn:aws-us-gov:s3:::netapp-backup-*"
      ]
    },
    {
      "Effect": "Allow",
      "Action": [
        "ec2:StartInstances",
        "ec2:TerminateInstances",
        "ec2:AttachVolume",
        "ec2:DetachVolume"
      ],
      "Condition": {
        "StringLike": {
          "ec2:ResourceTag/WorkingEnvironment": "*"
        }
      },
      "Resource": [
```

```
        "arn:aws-us-gov:ec2:*:*:instance/*"
      ]
    },
    {
      "Effect": "Allow",
      "Action": [
        "ec2:AttachVolume",
        "ec2:DetachVolume"
      ],
      "Resource": [
        "arn:aws-us-gov:ec2:*:*:volume/*"
      ]
    }
  ]
}
```

秘密の地域

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "ec2:DescribeInstances",
        "ec2:DescribeInstanceStatus",
        "ec2:RunInstances",
        "ec2:ModifyInstanceAttribute",
        "ec2:DescribeRouteTables",
        "ec2:DescribeImages",
        "ec2:CreateTags",
        "ec2:CreateVolume",
        "ec2:DescribeVolumes",
        "ec2:ModifyVolumeAttribute",
        "ec2:DeleteVolume",
        "ec2:CreateSecurityGroup",
        "ec2:DeleteSecurityGroup",
        "ec2:DescribeSecurityGroups",
        "ec2:RevokeSecurityGroupEgress",
        "ec2:RevokeSecurityGroupIngress",
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:CreateNetworkInterface",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DeleteNetworkInterface",
        "ec2:ModifyNetworkInterfaceAttribute",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:DescribeDhcpOptions",
        "ec2:CreateSnapshot",
        "ec2:DeleteSnapshot",
        "ec2:DescribeSnapshots",
        "ec2:GetConsoleOutput",
        "ec2:DescribeKeyPairs",
        "ec2:DescribeRegions",
        "ec2:DeleteTags",
        "ec2:DescribeTags",
        "cloudformation:CreateStack",
        "cloudformation:DeleteStack",
        "cloudformation:DescribeStacks",
        "cloudformation:DescribeStackEvents",
```

```
        "cloudformation:ListStacks",
        "cloudformation:ValidateTemplate",
        "iam:PassRole",
        "iam:CreateRole",
        "iam:DeleteRole",
        "iam:PutRolePolicy",
        "iam:CreateInstanceProfile",
        "iam:DeleteRolePolicy",
        "iam:AddRoleToInstanceProfile",
        "iam:RemoveRoleFromInstanceProfile",
        "iam:DeleteInstanceProfile",
        "s3:GetObject",
        "s3:ListBucket",
        "s3:GetBucketTagging",
        "s3:GetBucketLocation",
        "s3:ListAllMyBuckets",
        "ec2:AssociateIamInstanceProfile",
        "ec2:DescribeIamInstanceProfileAssociations",
        "ec2:DisassociateIamInstanceProfile",
        "ec2:DescribeInstanceAttribute",
        "ec2:CreatePlacementGroup",
        "ec2:DeletePlacementGroup",
        "iam:ListinstanceProfiles"
      ],
      "Resource": "*"
    },
    {
      "Sid": "fabricPoolPolicy",
      "Effect": "Allow",
      "Action": [
        "s3:DeleteBucket",
        "s3:GetLifecycleConfiguration",
        "s3:PutLifecycleConfiguration",
        "s3:PutBucketTagging",
        "s3:ListBucketVersions"
      ],
      "Resource": [
        "arn:aws-iso-b:s3:::fabric-pool*"
      ]
    },
    {
      "Effect": "Allow",
      "Action": [
        "ec2:StartInstances",
        "ec2:StopInstances",
        "ec2:TerminateInstances",
```

```
            "ec2:AttachVolume",
            "ec2:DetachVolume"
        ],
        "Condition": {
            "StringLike": {
                "ec2:ResourceTag/WorkingEnvironment": "*"
            }
        },
        "Resource": [
            "arn:aws-iso-b:ec2:*:*:instance/*"
        ]
    },
    {
        "Effect": "Allow",
        "Action": [
            "ec2:AttachVolume",
            "ec2:DetachVolume"
        ],
        "Resource": [
            "arn:aws-iso-b:ec2:*:*:volume/*"
        ]
    }
  ]
}
```

极秘地域

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "ec2:DescribeInstances",
        "ec2:DescribeInstanceStatus",
        "ec2:RunInstances",
        "ec2:ModifyInstanceAttribute",
        "ec2:DescribeRouteTables",
        "ec2:DescribeImages",
        "ec2:CreateTags",
        "ec2:CreateVolume",
        "ec2:DescribeVolumes",
        "ec2:ModifyVolumeAttribute",
        "ec2:DeleteVolume",
        "ec2:CreateSecurityGroup",
        "ec2:DeleteSecurityGroup",
        "ec2:DescribeSecurityGroups",
        "ec2:RevokeSecurityGroupEgress",
        "ec2:RevokeSecurityGroupIngress",
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:CreateNetworkInterface",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DeleteNetworkInterface",
        "ec2:ModifyNetworkInterfaceAttribute",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:DescribeDhcpOptions",
        "ec2:CreateSnapshot",
        "ec2:DeleteSnapshot",
        "ec2:DescribeSnapshots",
        "ec2:GetConsoleOutput",
        "ec2:DescribeKeyPairs",
        "ec2:DescribeRegions",
        "ec2:DeleteTags",
        "ec2:DescribeTags",
        "cloudformation:CreateStack",
        "cloudformation:DeleteStack",
        "cloudformation:DescribeStacks",
        "cloudformation:DescribeStackEvents",
```

```
        "cloudformation:ListStacks",
        "cloudformation:ValidateTemplate",
        "iam:PassRole",
        "iam:CreateRole",
        "iam:DeleteRole",
        "iam:PutRolePolicy",
        "iam:CreateInstanceProfile",
        "iam:DeleteRolePolicy",
        "iam:AddRoleToInstanceProfile",
        "iam:RemoveRoleFromInstanceProfile",
        "iam:DeleteInstanceProfile",
        "s3:GetObject",
        "s3:ListBucket",
        "s3:GetBucketTagging",
        "s3:GetBucketLocation",
        "s3:ListAllMyBuckets",
        "ec2:AssociateIamInstanceProfile",
        "ec2:DescribeIamInstanceProfileAssociations",
        "ec2:DisassociateIamInstanceProfile",
        "ec2:DescribeInstanceAttribute",
        "ec2:CreatePlacementGroup",
        "ec2:DeletePlacementGroup",
        "iam:ListinstanceProfiles"
      ],
      "Resource": "*"
    },
    {
      "Sid": "fabricPoolPolicy",
      "Effect": "Allow",
      "Action": [
        "s3:DeleteBucket",
        "s3:GetLifecycleConfiguration",
        "s3:PutLifecycleConfiguration",
        "s3:PutBucketTagging",
        "s3:ListBucketVersions"
      ],
      "Resource": [
        "arn:aws-iso:s3:::fabric-pool*"
      ]
    },
    {
      "Effect": "Allow",
      "Action": [
        "ec2:StartInstances",
        "ec2:StopInstances",
        "ec2:TerminateInstances",
```

```
            "ec2:AttachVolume",
            "ec2:DetachVolume"
        ],
        "Condition": {
            "StringLike": {
                "ec2:ResourceTag/WorkingEnvironment": "*"
            }
        },
        "Resource": [
            "arn:aws-iso:ec2:*:*:instance/*"
        ]
    },
    {
        "Effect": "Allow",
        "Action": [
            "ec2:AttachVolume",
            "ec2:DetachVolume"
        ],
        "Resource": [
            "arn:aws-iso:ec2:*:*:volume/*"
        ]
    }
  ]
}
```

AWS権限の使用方法

次のセクションでは、各NetApp Console管理サービスまたはデータ サービスに対して権限がどのように使用されるかについて説明します。この情報は、必要な場合にのみ権限を付与するように企業ポリシーで定められている場合に役立ちます。

Amazon FSx for ONTAP

コンソールエージェントは、 Amazon FSx for ONTAPファイルシステムを管理するために次の API リクエストを行います。

- ec2:インスタンスの説明
- ec2:インスタンスステータスの説明
- ec2:インスタンス属性の説明
- ec2:ルートテーブルの説明
- ec2:画像の説明
- ec2:タグの作成
- ec2:ボリュームの説明

- ec2:セキュリティグループの説明
- ec2:ネットワークインターフェースの説明
- ec2:サブネットの説明
- ec2:Vpcs の説明
- ec2:Dhcpオプションの説明
- ec2:スナップショットの説明
- ec2:キーペアの説明
- ec2:リージョンの説明
- ec2:タグの説明
- ec2:IamInstanceProfileAssociations の説明
- ec2:予約済みインスタンスの提供内容の説明
- ec2:Vpcエンドポイントの説明
- ec2:Vpcs の説明
- ec2:ボリュームの変更の説明
- ec2:配置グループの説明
- kms:許可の作成
- kms:エイリアスのリスト
- fsx:説明*
- fsx:リスト*

Amazon S3 バケット検出

コンソールエージェントは、Amazon S3 バケットを検出するために次の API リクエストを行います。

s3:暗号化設定の取得

NetApp Backup and Recovery

エージェントは、Amazon S3 内のバックアップを管理するために次の API リクエストを行います。

- s3:GetBucketLocation
- s3:すべてのバケットをリスト
- s3:リストバケット
- s3:バケットの作成
- s3:GetLifecycleConfiguration
- s3:PutLifecycleConfiguration
- s3:PutBucketTagging
- s3:バケットバージョンのリスト
- s3:GetBucketAcl

- s3:PutBucketパブリックアクセスブロック
- s3:GetObject
- ec2:Vpcエンドポイントの説明
- kms:エイリアスのリスト
- s3:PutEncryptionConfiguration

検索と復元方法を使用してボリュームとファイルを復元する場合、エージェントは次の API 要求を行います。

- s3:バケットの作成
- s3:オブジェクトの削除
- s3:オブジェクトバージョンの削除
- s3:GetBucketAcl
- s3:リストバケット
- s3:バケットバージョンのリスト
- s3:リストバケットマルチパートアップロード
- s3:PutObject
- s3:PutBucketAcl
- s3:PutLifecycleConfiguration
- s3:PutBucketパブリックアクセスブロック
- s3:マルチパートアップロードの中止
- s3:ListMultipartUploadParts

ボリュームのバックアップに DataLock とNetApp Ransomware Resilienceを使用する場合、エージェントは次の API 要求を行います。

- s3:GetObjectVersionTagging
- s3:GetBucketObjectLockConfiguration
- s3:GetObjectVersionAcl
- s3:オブジェクトのタグ付け
- s3:オブジェクトの削除
- s3:オブジェクトのタグ付けを削除
- s3:GetObjectRetention
- s3:オブジェクトバージョンタグ付けの削除
- s3:PutObject
- s3:GetObject
- s3:PutBucketObjectLockConfiguration
- s3:GetLifecycleConfiguration
- s3:タグによるバケットのリスト

- s3:GetBucketTagging
- s3:オブジェクトバージョンの削除
- s3:バケットバージョンのリスト
- s3:リストバケット
- s3:PutBucketTagging
- s3:GetObjectTagging
- s3:PutBucketバージョン管理
- s3:PutObjectVersionTagging
- s3:GetBucketVersioning
- s3:GetBucketAcl
- s3:バイパスガバナンス保持
- s3:PutObjectRetention
- s3:GetBucketLocation
- s3:GetObjectVersion

Cloud Volumes ONTAPバックアップにソースボリュームに使用しているものとは異なる AWS アカウントを使用する場合、エージェントは次の API リクエストを実行します。

- s3:PutBucketポリシー
- s3:PutBucketOwnershipControls

バックアップとリカバリの従来の権限

インデックス v2 のリリース前に従来のインデックス機能を有効にした場合にのみ、次の権限が必要です。

- kms:リスト*
- kms:説明*
- athena:クエリ実行の開始
- athena:GetQueryResults
- athena:GetQueryExecution
- athena:StopQueryExecution
- グルー:データベースの作成
- グルー:CreateTable
- グルー:バッチ削除パーティション

NetApp Data Classification

エージェントは、NetApp Data Classificationを展開するために次の API 要求を行います。

- ec2:インスタンスの説明
- ec2:インスタンスステータスの説明

- ec2:インスタンスの実行
- ec2:インスタンスの終了
- ec2:タグの作成
- ec2:ボリュームの作成
- ec2:ボリュームのアタッチ
- ec2:セキュリティグループの作成
- ec2:セキュリティグループの削除
- ec2:セキュリティグループの説明
- ec2:ネットワークインターフェースの作成
- ec2:ネットワークインターフェースの説明
- ec2:ネットワークインターフェースの削除
- ec2:サブネットの説明
- ec2:Vpcs の説明
- ec2:スナップショットの作成
- ec2:リージョンの説明
- cloudformation:スタックの作成
- cloudformation:スタックの削除
- cloudformation:スタックの説明
- cloudformation:スタックイベントの説明
- cloudformation：ListStacks
- iam:インスタンスプロファイルにロールを追加
- ec2:Iamインスタンスプロファイルの関連付け
- ec2:IamInstanceProfileAssociations の説明

NetApp Data Classificationを使用する場合、エージェントは次の API 要求を行って S3 バケットをスキャンします。

- iam:インスタンスプロファイルにロールを追加
- ec2:Iamインスタンスプロファイルの関連付け
- ec2:IamInstanceProfileAssociations の説明
- s3:GetBucketTagging
- s3:GetBucketLocation
- s3:すべてのバケットをリスト
- s3:リストバケット
- s3:GetBucketPolicyStatus
- s3:GetBucketPolicy

- s3:GetBucketAcl
- s3:GetObject
- iam:GetRole
- s3:オブジェクトの削除
- s3:オブジェクトバージョンの削除
- s3:PutObject
- sts:役割を担う

Cloud Volumes ONTAP

エージェントは、AWS でCloud Volumes ONTAP をデプロイおよび管理するために、次の API リクエストを行います。

目的	アクション	展開に使用されますか?	日常業務に使用されますか?	削除に使用されますか?
Cloud Volumes ONTAPインスタンスのIAMロールとインスタンスプロファイルを作成および管理します	iam:ListInstanceProfiles	はい	はい	いいえ
	iam:CreateRole	はい	いいえ	いいえ
	iam:DeleteRole	いいえ	はい	はい
	iam:PutRolePolicy	はい	いいえ	いいえ
	iam:インスタンスプロファイルの作成	はい	いいえ	いいえ
	iam:DeleteRolePolicy	いいえ	はい	はい
	iam:インスタンスプロファイルにロールを追加	はい	いいえ	いいえ
	iam:インスタンスプロファイルからロールを削除	いいえ	はい	はい
	iam:インスタンスプロファイルの削除	いいえ	はい	はい
	iam:PassRole	はい	いいえ	いいえ
	ec2:Iamインスタンスプロファイルの関連付け	はい	はい	いいえ
	ec2:IamInstanceProfileAssociations の説明	はい	はい	いいえ
	ec2:IamInstanceProfileの関連付けを解除	いいえ	はい	いいえ

目的	アクション	展開に使用されますか?	日常業務に使用されますか?	削除に使用されますか?
認証ステータスメッセージをデコードする	sts:DecodeAuthorizationMessage	はい	はい	いいえ
アカウントで利用可能な指定されたイメージ（AMI）について説明します	ec2:画像の説明	はい	はい	いいえ
VPC 内のルートテーブルについて説明します（HA ペアの場合のみ必要）	ec2:ルートテーブルの説明	はい	いいえ	いいえ
インスタンスの停止、起動、監視	ec2:インスタンスの開始	はい	はい	いいえ
	ec2:インスタンスの停止	はい	はい	いいえ
	ec2:インスタンスの説明	はい	はい	いいえ
	ec2:インスタンスステータスの説明	はい	はい	いいえ
	ec2:インスタンスの実行	はい	いいえ	いいえ
	ec2:インスタンスの終了	いいえ	いいえ	はい
	ec2:インスタンス属性の変更	いいえ	はい	いいえ
サポートされているインスタンスタイプで拡張ネットワークが有効になっていることを確認します	ec2:インスタンス属性の説明	いいえ	はい	いいえ
メンテナンスとコスト配分に使用される「WorkingEnvironment」および「WorkingEnvironmentId」タグでリソースにタグを付ける	ec2:タグの作成	はい	はい	いいえ

目的	アクション	展開に使用されますか?	日常業務に使用されますか?	削除に使用されますか?
Cloud Volumes ONTAP がバックエンド ストレージとして使用する EBS ボリュームを管理する	ec2:ボリュームの作成	はい	はい	いいえ
	ec2:ボリュームの説明	はい	はい	はい
	ec2:ボリューム属性の変更	いいえ	はい	はい
	ec2:ボリュームのアタッチ	はい	はい	いいえ
	ec2:ボリュームの削除	いいえ	はい	はい
	ec2:ボリュームのデタッチ	いいえ	はい	はい
Cloud Volumes ONTAPのセキュリティ グループの作成と管理	ec2:セキュリティグループの作成	はい	いいえ	いいえ
	ec2:セキュリティグループの削除	いいえ	はい	はい
	ec2:セキュリティグループの説明	はい	はい	はい
	ec2:セキュリティグループの出力を取り消す	はい	いいえ	いいえ
	ec2:セキュリティグループ出力の承認	はい	いいえ	いいえ
	ec2:セキュリティグループイングレスの承認	はい	いいえ	いいえ
	ec2:セキュリティグループの入力を取り消す	はい	はい	いいえ
ターゲットサブネットでCloud Volumes ONTAPのネットワークインターフェースを作成および管理する	ec2:ネットワークインターフェースの作成	はい	いいえ	いいえ
	ec2:ネットワークインターフェースの説明	はい	はい	いいえ
	ec2:ネットワークインターフェースの削除	いいえ	はい	はい
	ec2:ネットワークインターフェース属性の変更	いいえ	はい	いいえ

目的	アクション	展開に使用されますか?	日常業務に使用されますか?	削除に使用されますか?
宛先サブネットとセキュリティグループのリストを取得する	ec2:サブネットの説明	はい	はい	いいえ
	ec2:Vpcs の説明	はい	はい	いいえ
Cloud Volumes ONTAPインスタンスのDNSサーバーとデフォルトのドメイン名を取得します	ec2:Dhcpオプションの説明	はい	いいえ	いいえ
Cloud Volumes ONTAPの EBS ボリュームのスナップショットを作成します	ec2:スナップショットの作成	はい	はい	いいえ
	ec2:スナップショットの削除	いいえ	はい	はい
	ec2:スナップショットの説明	いいえ	はい	いいえ
AutoSupportメッセージに添付されているCloud Volumes ONTAPコンソールをキャプチャします。	ec2:GetConsoleOutput	はい	はい	いいえ
利用可能なキーペアのリストを取得する	ec2:キーペアの説明	はい	いいえ	いいえ
利用可能なAWSリージョンのリストを取得する	ec2:リージョンの説明	はい	はい	いいえ
Cloud Volumes ONTAPインスタンスに関連付けられたリソースのタグを管理する	ec2:タグを削除	いいえ	はい	はい
	ec2:タグの説明	いいえ	はい	いいえ
AWS CloudFormation テンプレートのスタックを作成および管理する	cloudformation:スタックの作成	はい	いいえ	いいえ
	cloudformation:スタックの削除	はい	いいえ	いいえ
	cloudformation:スタックの説明	はい	はい	いいえ
	cloudformation:スタックイベントの説明	はい	いいえ	いいえ
	cloudformation:テンプレートの検証	はい	いいえ	いいえ

目的	アクション	展開に使用されますか?	日常業務に使用されますか?	削除に使用されますか?
Cloud Volumes ONTAPシステムがデータ階層化の容量層として使用するS3 バケットを作成および管理します	s3:バケットの作成	はい	はい	いいえ
	s3:バケットの削除	いいえ	はい	はい
	s3:GetLifecycleConfiguration	いいえ	はい	いいえ
	s3:PutLifecycleConfiguration	いいえ	はい	いいえ
	s3:PutBucketTagging	いいえ	はい	いいえ
	s3:バケットバージョンのリスト	いいえ	はい	いいえ
	s3:GetBucketPolicyStatus	いいえ	はい	いいえ
	s3:GetBucketPublicAccessBlock	いいえ	はい	いいえ
	s3:GetBucketAcl	いいえ	はい	いいえ
	s3:GetBucketPolicy	いいえ	はい	いいえ
	s3:PutBucketパブリックアクセスブロック	いいえ	はい	いいえ
	s3:GetBucketTagging	いいえ	はい	いいえ
	s3:GetBucketLocation	いいえ	はい	いいえ
	s3:すべてのバケットをリスト	いいえ	いいえ	いいえ
	s3:リストバケット	いいえ	はい	いいえ
AWS Key Management Service (KMS) を使用してCloud Volumes ONTAPのデータ暗号化を有効にする	kms:再暗号化*	はい	いいえ	いいえ
	kms:許可の作成	はい	はい	いいえ
	kms:プレーンテキストなしでデータキーを生成する	はい	はい	いいえ
単一の AWS アベイラビリティゾーン内の 2 つの HA ノードとメディエーターの AWS スプレッド配置グループを作成および管理します。	ec2:配置グループの作成	はい	いいえ	いいえ
	ec2:配置グループの削除	いいえ	はい	はい

目的	アクション	展開に使用されますか?	日常業務に使用されますか?	削除に使用されますか?
レポートを作成する	fsx:説明*	いいえ	はい	いいえ
	fsx:リスト*	いいえ	はい	いいえ
Amazon EBS エラスティックボリューム機能をサポートするアグリゲートを作成および管理します	ec2:ボリュームの変更の説明	いいえ	はい	いいえ
	ec2:ボリュームの変更	いいえ	はい	いいえ
アベイラビリティゾーンがAWSローカルゾーンであるかどうかを確認し、すべてのデプロイメントパラメータが互換性があるかどうかを検証します。	ec2:アベイラビリティゾーンの説明	はい	いいえ	はい

変更ログ

権限が追加または削除されると、以下のセクションでその旨を記録します。

2026年2月24日

データ分類には次の権限が必要になりました：

cloudformation：ListStacks

2025年11月11日

従来のインデックスを使用しない限り、 NetApp Backup and Recoveryには次の権限は不要になりました。このページのポリシーから次の権限が削除されました:

- kms:リスト*
- kms:説明*
- athena:クエリ実行の開始
- athena:GetQueryResults
- athena:GetQueryExecution
- athena:StopQueryExecution
- グルー:データベースの作成
- グルー:CreateTable
- グルー:バッチ削除パーティション

2024年9月9日

NetApp ConsoleはNetAppエッジ キャッシングと Kubernetes クラスターの検出および管理をサポートしなくなったため、標準リージョンのポリシー #2 から権限が削除されました。

ポリシーから削除された権限を表示する

```
{
    "Action": [
        "ec2:DescribeRegions",
        "eks:ListClusters",
        "eks:DescribeCluster",
        "iam:GetInstanceProfile"
    ],
    "Resource": "*",
    "Effect": "Allow",
    "Sid": "K8sServicePolicy"
},
{
    "Action": [
        "cloudformation:DescribeStacks",
        "cloudwatch:GetMetricStatistics",
        "cloudformation:ListStacks"
    ],
    "Resource": "*",
    "Effect": "Allow",
    "Sid": "GFCservicePolicy"
},
{
    "Condition": {
        "StringLike": {
            "ec2:ResourceTag/GFCInstance": "*"
        }
    },
    "Action": [
        "ec2:StartInstances",
        "ec2:TerminateInstances",
        "ec2:AttachVolume",
        "ec2:DetachVolume"
    ],
    "Resource": [
        "arn:aws:ec2:*:*:instance/*"
    ],
    "Effect": "Allow"
}
```

2024年5月9日

Cloud Volumes ONTAPには次の権限が必要になりました。

ec2:アベイラビリティゾーンの説明

2023年6月6日

Cloud Volumes ONTAPには次の権限が必要になりました。

kms:プレーンテキストなしでデータキーを生成する

2023年2月14日

NetApp Cloud Tieringには次の権限が必要になりました。

ec2:Vpcエンドポイントの説明

AWS のコンソールエージェントのセキュリティグループルール

エージェントの AWS セキュリティグループには、インバウンドルールとアウトバウンドルールの両方が必要です。 NetApp Consoleは、コンソールからコンソール エージェントを作成すると、このセキュリティ グループを自動的に作成します。他のすべてのインストール オプションに対して、このセキュリティ グループを設定する必要があります。

インバウンドルール

プロトコル	ポート	目的
SSH	22	エージェントホストへのSSHアクセスを提供します
HTTP	80	• クライアントのWebブラウザからローカルユーザーインターフェースへのHTTPアクセスを提供します • Cloud Volumes ONTAPのアップグレードプロセス中に使用されます
HTTPS	443	ローカル ユーザー インターフェイスへの HTTPS アクセスとNetApp Data Classificationインスタンスからの接続を提供します。
TCP	3128	Cloud Volumes ONTAPにインターネット アクセスを提供します。デプロイ後にこのポートを手動で開く必要があります。

アウトバウンドルール

エージェントの定義済みセキュリティ グループは、すべての送信トラフィックを開きます。それが許容できる場合は、基本的な送信ルールに従ってください。より厳格なルールが必要な場合は、高度な送信ルールを使用します。

基本的なアウトバウンドルール

エージェントの定義済みセキュリティ グループには、次の送信ルールが含まれています。

プロトコル	ポート	目的
すべてのTCP	全て	すべての送信トラフィック
すべてUDP	全て	すべての送信トラフィック

高度なアウトバウンドルール

送信トラフィックに厳格なルールが必要な場合は、次の情報を使用して、エージェントによる送信通信に必要なポートのみを開くことができます。

送信元 IP アドレスはエージェント ホストです。

サービス	プロトコル	ポート	デスティネーション	目的
API呼び出しとAutoSupport	HTTPS	443	アウトバウンドインターネットとONTAPクラスタ管理 LIF	AWS、 ONTAP、NetApp Data ClassificationへのAPI呼び出し、およびNetAppへのAutoSupportメッセージの送信
API呼び出し	TCP	3000	ONTAP HAメディエーター	ONTAP HAメディエーターとの通信
	TCP	8080	データ分類	デプロイメント中にデータ分類インスタンスにプローブする
DNS	UDP	53	DNS	コンソールによるDNS解決に使用

著作権に関する情報

商標に関する情報