参照

NetApp Console setup and administration

NetApp
March 03, 2026

目次

参照

エージェントメンテナンスコンソール

メンテナンスコンソールによるエージェントの検証

コンソール エージェント メンテナンス コンソールを使用して、コンソール エージェントのインストールと構成を検証できます。

エージェントメンテナンスコンソールにアクセスする

コンソール エージェント ホストからメンテナンス コンソールにアクセスできます。次のディレクトリに移動します。

```
/opt/application/netapp/service-manager-2/agent-maint-console
```

構成チェッカーの検証

その `config-checker validate`コマンドを使用すると、コンソール エージェントの構成を検証できます。

パラメータ

`--services <comma-separated list of services to validate>` - 必須 -

検証するサービスを 1 つ以上選択します。有効なサービス名は次のとおりです。*`PLATFORM`必要なコンソール エンドポイントへのネットワーク接続を検証します。

`--validationTypes <comma-separated list validation types to run>`--必須-- 実行する検証タイプを 1 つ以上選択します。有効な検証タイプは次のとおりです: * `NETWORK`必要なコンソール エンドポイントへのネットワーク接続を検証します。

`--proxy <url>`--オプション--

検証に使用するプロキシ サーバーの URL を指定します。エージェントがプロキシ サーバーを使用するように構成されている場合に必要です。

`--certs <paths>`--オプション--

検証に使用する 1 つ以上の証明書ファイルへのパスを指定します。証明書ファイルは PEM 形式である必要があります。複数のパスはコンマで区切ります。エージェントがカスタム証明書を使用する場合、このパラメータは必須です。

構成チェッカーの検証例

基本的な検証:

```
./agent-maint-console config-checker validate --services PLATFORM
--validationTypes NETWORK
```

エージェントにプロキシ サーバーが使用される場合の検証:

```
./agent-maint-console config-checker validate --services PLATFORM
--validationTypes NETWORK --proxy http://proxy.company.com:8080
```

エージェントに証明書が使用される場合の検証:

```
./agent-maint-console config-checker validate --services PLATFORM
--validationTypes NETWORK --certs /path/to/cert1.pem,/path/to/cert2.pem
```

任意のコマンドのヘルプを表示する

コマンドのヘルプを表示するには、 `--help`コマンドに。たとえば、 `proxy add`コマンドを実行するには、次のコマンドを使用します。

```
./agent-maint-console proxy add --help
```

透過プロキシコマンド

コンソール エージェント メンテナンス コンソールを使用して、透過プロキシ サーバーを使用するようにコンソール エージェントを構成できます。

エージェントメンテナンスコンソールにアクセスする

コンソール エージェント ホストからメンテナンス コンソールにアクセスできます。次のディレクトリに移動します。

```
/opt/application/netapp/service-manager-2/agent-maint-console
```

任意のコマンドのヘルプを表示する

コマンドのヘルプを表示するには、 `--help`コマンドに。たとえば、 `proxy add`コマンドを実行するには、次のコマンドを使用します。

```
./agent-maint-console proxy add --help
```

プロキシ取得

その `proxy get`コマンドは、現在の透過プロキシ サーバーの構成に関する情報を表示します。現在の透過プロキシ サーバーの構成を表示するには、次のコマンドを使用します。

プロキシ取得の例

現在の透過プロキシ サーバーの構成を表示するには、次のコマンドを使用します。

```
./agent-maint-console proxy get
```

プロキシ追加

その `proxy add`コマンドは、エージェントが透過プロキシ サーバーを使用するように構成します。

パラメータ

`-c <certificate file>`

プロキシ サーバーの証明書ファイルへのパスを指定します。証明書ファイルは PEM 形式である必要があります。証明書ファイルがコマンドと同じディレクトリにあることを確認するか、証明書ファイルへの完全パスを指定します。

プロキシ追加の例

透過プロキシサーバーを追加するには、次のコマンドを使用します。 `/home/ubuntu/myCA1.pem`プロキシ サーバーの証明書ファイルへのパスです。証明書ファイルは PEM 形式である必要があります。

```
./agent-maint-console proxy add -c /home/ubuntu/myCA1.pem
```

プロキシの更新

その `proxy update`コマンドを使用すると、透過プロキシの証明書を更新できます。

パラメータ

`-c <certificate file>`プロキシ サーバーの証明書ファイルへのパスを指定します。証明書ファイルは PEM 形式である必要があります。

証明書ファイルがコマンドと同じディレクトリにあることを確認するか、証明書ファイルへの完全パスを指定します。

プロキシ更新の例

透過プロキシサーバーの証明書を更新するには、次のコマンドを使用します。 `/home/ubuntu/myCA1.pem`プロキシ サーバーの新しい証明書ファイルへのパスです。証明書ファイルは PEM 形式である必要があります。

```
./agent-maint-console proxy update -c /home/ubuntu/myCA1.pem
```

プロキシ削除

その `proxy remove`コマンドは、エージェントから透過プロキシ サーバーの構成を削除します。

プロキシ削除の例

透過プロキシ サーバーを削除するには、次のコマンドを使用します。

```
./agent-maint-console proxy remove
```

クラウドプロバイダーエージェントの権限とネットワーク要件

NetApp Consoleの権限の概要

クラウド環境で操作を実行できるように、コンソール エージェントに適切な権限を付与する必要があります。このページのリンクを使用して、目標に応じて必要な権限にすばやくアクセスします。

AWS 権限

NetApp Consoleには、コンソールエージェントと個々のサービスに対する AWS 権限が必要です。

コンソールエージェント

目標	説明	リンク
コンソールからコンソールエージェントをデプロイする AWS にコンソールエージェントをデプロイするには、ユーザーに特定の権限が必要です。	"AWS権限を設定する"	コンソールエージェントに権限を付与する

NetApp Backup and Recovery

目標	説明	リンク
NetApp Backup and Recoveryを使用してオンプレミスのONTAPクラスターを Amazon S3 にバックアップする	ONTAPボリュームでバックアップをアクティブ化するときに、NetApp Backup and Recovery、特定の権限を持つ IAM ユーザーのアクセス キーとシークレットを入力するように求められます。	"バックアップ用のS3権限を設定する"

Cloud Volumes ONTAP

目標	説明	リンク
Cloud Volumes ONTAPノードに権限を付与する	AWS の各Cloud Volumes ONTAPノードに IAM ロールを添付する必要があります。 HA メディエーターについても同様です。デフォルトのオプションでは、コンソールで IAM ロールが自動的に作成されますが、コンソールでシステムを作成するときに独自のロールを使用することもできます。	"IAMロールを自分で設定する方法を学ぶ"

NetApp Copy and Sync

目標	説明	リンク
AWSにデータブローカーをデプロイする	データブローカーをデプロイするために使用する AWS ユーザー アカウントには、必要な権限が必要です。	"AWS にデータブローカーをデプロイするために必要な権限"
データブローカーに権限を付与する	NetApp Copy and Sync がデータ ブローカーを展開すると、データ ブローカー インスタンスの IAM ロールが作成されます。必要に応じて、独自の IAM ロールを使用してデータ ブローカーをデプロイすることもできます。	"AWS データブローカーで独自の IAM ロールを使用するための要件"
手動でインストールされたデータブローカーの AWS アクセスを有効にする	S3 バケットを含む同期関係でデータ ブローカーを使用する場合は、AWS アクセス用に Linux ホストを準備する必要があります。データブローカーをインストールするときは、プログラムによるアクセスと特定の権限を持つ IAM ユーザーに AWS キーを提供する必要があります。	"AWSへのアクセスを有効にする"

ONTAP向け FSx

目標	説明	リンク
FSx for ONTAP の作成と管理	Amazon FSx for NetApp ONTAPシステムを作成または管理するには、コンソールに必要な権限を付与する IAM ロールの ARN を指定して、AWS 認証情報をコンソールに追加する必要があります。	"FSx 用の AWS 認証情報を設定する方法を学ぶ"

NetApp Cloud Tiering

目標	説明	リンク
オンプレミスのONTAPクラスターを Amazon S3 に階層化する	NetApp Cloud Tiering to AWS を有効にするときは、アクセス キーとシークレット キーを入力します。これらの認証情報はONTAPクラスターに渡され、 ONTAP はデータを S3 バケットに階層化できるようになります。	"階層化のためのS3権限を設定する"

Azure のアクセス許可

コンソールには、コンソール エージェントと個々のサービスに対する Azure アクセス許可が必要です。

コンソールエージェント

目標	説明	リンク
コンソールからコンソールエージェントを展開する	コンソールからコンソール エージェントを展開する場合は、Azure にコンソール エージェント VM を展開する権限を持つ Azure アカウントまたはサービス プリンシパルを使用する必要があります。	"Azure の権限を設定する"
コンソールエージェントに権限を付与する	コンソールが Azure にコンソール エージェント VM を展開すると、その Azure サブスクリプション内のリソースとプロセスを管理するために必要なアクセス許可を提供するカスタム ロールが作成されます。 マーケットプレイスからコンソールエージェントを起動する場合、コンソールエージェントを手動でインストールする場合、または"コンソールエージェントにAzure資格情報を追加する"。 今後のリリースで新しい権限が追加されるので、ポリシーを最新の状態に保ってください。	"コンソールエージェントの Azure 権限"

NetApp Backup and Recovery

目標	説明	リンク
Cloud Volumes ONTAP をAzure BLOB ストレージにバックアップする	NetApp Backup and Recoveryを使用してCloud Volumes ONTAPをバックアップする場合、次のシナリオでコンソール エージェントに権限を追加する必要があります。 • 「検索と復元」機能を使用したい • 顧客管理暗号鍵（CMEK）を使用したい	• "バックアップとリカバリを使用して、 Cloud Volumes ONTAP データを Azure Blob ストレージにバックアップします。"
オンプレミスのONTAPクラスターを Azure BLOB ストレージにバックアップする	NetApp Backup and Recoveryを使用してオンプレミスのONTAPクラスターをバックアップする場合は、「検索と復元」機能を使用するために、コンソール エージェントに権限を追加する必要があります。	"バックアップとリカバリを使用してオンプレミスのONTAPデータをAzure Blob ストレージにバックアップする"

NetAppコピーと同期

目標	説明	リンク
Azureにデータブローカーをデプロイする	データ ブローカーをデプロイするために使用する Azure ユーザー アカウントには、必要なアクセス許可が必要です。	"Azure にデータ ブローカーをデプロイするために必要な権限"

Google Cloud の権限

コンソールでは、コンソール エージェントと個々のサービスに対する Google Cloud 権限が必要です。

コンソールエージェント

目標	説明	リンク
コンソールからコンソールエージェントを展開する	コンソールからコンソール エージェントをデプロイする Google Cloud ユーザーには、Google Cloud にコンソール エージェントをデプロイするための特定の権限が必要です。	"コンソールエージェントを作成するための権限を設定する"
コンソールエージェントに権限を付与する	コンソール エージェントのサービス アカウントには、日常的な操作のための特定の権限が必要です。展開中に、サービス アカウントをコンソール エージェントに関連付ける必要があります。今後のリリースで新しい権限が追加されるので、ポリシーを最新の状態に保ってください。	"コンソールエージェントの権限を設定する"

NetApp Backup and Recovery

目標	説明	リンク
Cloud Volumes ONTAPをGoogle Cloudにバックアップする	NetApp Backup and Recoveryを使用してCloud Volumes ONTAPをバックアップする場合、次のシナリオでコンソール エージェントに権限を追加する必要があります。 • 「検索と復元」機能を使用したい • 顧客管理暗号鍵（CMEK）を使用したい	• "バックアップとリカバリを使用して、 Cloud Volumes ONTAP データを Google Cloud Storage にバックアップします。" • "CMEK の権限"
オンプレミスのONTAPクラスタを Google Cloud にバックアップする	NetApp Backup and Recoveryを使用してオンプレミスのONTAPクラスターをバックアップする場合は、「検索と復元」機能を使用するために、コンソール エージェントに権限を追加する必要があります。	"バックアップとリカバリを使用してオンプレミスのONTAPデータを Google Cloud Storage にバックアップする"

NetApp Copy and Sync

目標	説明	リンク
Google Cloud にデータブローカーをデプロイする	データ ブローカーをデプロイする Google Cloud ユーザーに必要な権限があることを確認します。	"Google Cloud にデータブローカーをデプロイするために必要な権限"
手動でインストールされたデータブローカーの Google Cloud アクセスを有効にする	Google Cloud Storage バケットを含む同期関係でデータ ブローカーを使用する予定の場合は、Google Cloud アクセス用に Linux ホストを準備する必要があります。データ ブローカーをインストールするときは、特定の権限を持つサービス アカウントのキーを指定する必要があります。	"Google Cloudへのアクセスを有効にする"

StorageGRID権限

コンソールには、2 つのサービスに対するStorageGRID権限が必要です。

NetApp Backup and Recovery

目標	説明	リンク
オンプレミスのONTAPクラスターをStorageGRIDにバックアップする	StorageGRID をONTAPクラスターのバックアップ ターゲットとして準備する場合、 NetApp Backup and Recovery、特定の権限を持つ IAM ユーザーのアクセス キーとシークレットを入力するように求められます。	"StorageGRIDをバックアップターゲットとして準備する"

NetApp Cloud Tiering

目標	説明	リンク
オンプレミスのONTAPクラスターをStorageGRIDに階層化	NetApp Cloud Tiering をStorageGRIDに設定する場合は、Cloud Tiering に S3 アクセス キーと秘密キーを提供する必要があります。クラウド階層化では、キーを使用してバケットにアクセスします。	"StorageGRIDへの階層化を準備する"

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
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

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?
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

Azure のアクセス許可と必要なセキュリティ ルール

コンソールエージェントの**Azure**権限

NetApp ConsoleがAzure でコンソール エージェントを起動すると、その Azure サブスクリプション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提供するカスタム ロールが VM にアタッチされます。エージェントは、アクセス許可を使用して、複数の Azure サービスへの API 呼び出しを実行します。

エージェントに対してこのカスタム ロールを作成する必要があるかどうかは、エージェントをどのように展開したかによって異なります。

NetApp Consoleからの導入

コンソールを使用してAzureにエージェント仮想マシンを展開すると、 "システム割り当てマネージドID"仮想マシン上でカスタム ロールを作成し、それを仮想マシンに割り当てます。このロールは、その Azure サブスクリプション内のリソースとプロセスを管理するために必要な権限をコンソールに提供します。エージェント

がアップグレードされると、ロールの権限は最新の状態に保たれます。エージェントに対してこのロールを作成したり、更新を管理したりする必要はありません。

手動でのデプロイまたは**Azure Marketplace**からのデプロイ

Azure Marketplace からエージェントをデプロイする場合、または 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は、カスタム ロールを自分で設定し、変更を加えてそのアクセス許可を維持する必要があります。

以降のリリースで新しい権限が追加されるので、ロール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。

- 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。
  - "Azure Marketplace のデプロイの権限を設定する"
  - "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"

```
{
  "Name": "Console Operator",
  "Actions": [
    "Microsoft.Compute/disks/delete",
    "Microsoft.Compute/disks/read",
    "Microsoft.Compute/disks/write",
    "Microsoft.Compute/locations/operations/read",
    "Microsoft.Compute/locations/vmSizes/read",
    "Microsoft.Resources/subscriptions/locations/read",
    "Microsoft.Compute/operations/read",
    "Microsoft.Compute/virtualMachines/instanceView/read",
    "Microsoft.Compute/virtualMachines/powerOff/action",
    "Microsoft.Compute/virtualMachines/read",
    "Microsoft.Compute/virtualMachines/restart/action",
    "Microsoft.Compute/virtualMachines/deallocate/action",
    "Microsoft.Compute/virtualMachines/start/action",
    "Microsoft.Compute/virtualMachines/vmSizes/read",
    "Microsoft.Compute/virtualMachines/write",
    "Microsoft.Compute/images/read",
    "Microsoft.Network/locations/operationResults/read",
    "Microsoft.Network/locations/operations/read",
    "Microsoft.Network/networkInterfaces/read",
    "Microsoft.Network/networkInterfaces/write",
    "Microsoft.Network/networkInterfaces/join/action",
    "Microsoft.Network/networkSecurityGroups/read",
    "Microsoft.Network/networkSecurityGroups/write",
    "Microsoft.Network/networkSecurityGroups/join/action",
    "Microsoft.Network/virtualNetworks/read",
    "Microsoft.Network/virtualNetworks/checkIpAddressAvailability/read",
```

```
    "Microsoft.Network/virtualNetworks/subnets/read",
    "Microsoft.Network/virtualNetworks/subnets/write",
    "Microsoft.Network/virtualNetworks/subnets/virtualMachines/read",
    "Microsoft.Network/virtualNetworks/virtualMachines/read",
    "Microsoft.Network/virtualNetworks/subnets/join/action",
    "Microsoft.Resources/deployments/operations/read",
    "Microsoft.Resources/deployments/read",
    "Microsoft.Resources/deployments/write",
    "Microsoft.Resources/resources/read",
    "Microsoft.Resources/subscriptions/operationresults/read",
    "Microsoft.Resources/subscriptions/resourceGroups/delete",
    "Microsoft.Resources/subscriptions/resourceGroups/read",
    "Microsoft.Resources/subscriptions/resourcegroups/resources/read",
    "Microsoft.Resources/subscriptions/resourceGroups/write",
    "Microsoft.Storage/checknameavailability/read",
    "Microsoft.Storage/operations/read",
    "Microsoft.Storage/storageAccounts/listkeys/action",
    "Microsoft.Storage/storageAccounts/read",
    "Microsoft.Storage/storageAccounts/delete",
    "Microsoft.Storage/storageAccounts/write",
    "Microsoft.Storage/storageAccounts/blobServices/containers/read",
    "Microsoft.Storage/storageAccounts/listAccountSas/action",
    "Microsoft.Storage/usages/read",
    "Microsoft.Compute/snapshots/write",
    "Microsoft.Compute/snapshots/read",
    "Microsoft.Compute/availabilitySets/write",
    "Microsoft.Compute/availabilitySets/read",
    "Microsoft.Compute/disks/beginGetAccess/action",

"Microsoft.MarketplaceOrdering/offertypes/publishers/offers/plans/agreemen
ts/read",

"Microsoft.MarketplaceOrdering/offertypes/publishers/offers/plans/agreemen
ts/write",
    "Microsoft.Network/loadBalancers/read",
    "Microsoft.Network/loadBalancers/write",
    "Microsoft.Network/loadBalancers/delete",
    "Microsoft.Network/loadBalancers/backendAddressPools/read",
    "Microsoft.Network/loadBalancers/backendAddressPools/join/action",
    "Microsoft.Network/loadBalancers/loadBalancingRules/read",
    "Microsoft.Network/loadBalancers/probes/read",
    "Microsoft.Network/loadBalancers/probes/join/action",
    "Microsoft.Authorization/locks/*",
    "Microsoft.Network/routeTables/join/action",
    "Microsoft.NetApp/netAppAccounts/read",
    "Microsoft.NetApp/netAppAccounts/capacityPools/read",
```

```
    "Microsoft.NetApp/netAppAccounts/capacityPools/volumes/write",
    "Microsoft.NetApp/netAppAccounts/capacityPools/volumes/read",
    "Microsoft.NetApp/netAppAccounts/capacityPools/volumes/delete",
    "Microsoft.Network/privateEndpoints/write",

"Microsoft.Storage/storageAccounts/PrivateEndpointConnectionsApproval/acti
on",
    "Microsoft.Storage/storageAccounts/privateEndpointConnections/read",
    "Microsoft.Storage/storageAccounts/managementPolicies/read",
    "Microsoft.Storage/storageAccounts/managementPolicies/write",
    "Microsoft.Network/privateEndpoints/read",
    "Microsoft.Network/privateDnsZones/write",
    "Microsoft.Network/privateDnsZones/virtualNetworkLinks/write",
    "Microsoft.Network/virtualNetworks/join/action",
    "Microsoft.Network/privateDnsZones/A/write",
    "Microsoft.Network/privateDnsZones/read",
    "Microsoft.Network/privateDnsZones/virtualNetworkLinks/read",
    "Microsoft.Resources/deployments/operationStatuses/read",
    "Microsoft.Insights/Metrics/Read",
    "Microsoft.Compute/virtualMachines/extensions/write",
    "Microsoft.Compute/virtualMachines/extensions/delete",
    "Microsoft.Compute/virtualMachines/extensions/read",
    "Microsoft.Compute/virtualMachines/delete",
    "Microsoft.Network/networkInterfaces/delete",
    "Microsoft.Network/networkSecurityGroups/delete",
    "Microsoft.Resources/deployments/delete",
    "Microsoft.Compute/diskEncryptionSets/read",
    "Microsoft.Compute/snapshots/delete",
    "Microsoft.Network/privateEndpoints/delete",
    "Microsoft.Compute/availabilitySets/delete",
    "Microsoft.KeyVault/vaults/read",
    "Microsoft.KeyVault/vaults/accessPolicies/write",
    "Microsoft.Compute/diskEncryptionSets/write",
    "Microsoft.KeyVault/vaults/deploy/action",
    "Microsoft.Compute/diskEncryptionSets/delete",
    "Microsoft.Resources/tags/read",
    "Microsoft.Resources/tags/write",
    "Microsoft.Resources/tags/delete",
    "Microsoft.Network/applicationSecurityGroups/write",
    "Microsoft.Network/applicationSecurityGroups/read",

"Microsoft.Network/applicationSecurityGroups/joinIpConfiguration/action",
    "Microsoft.Network/networkSecurityGroups/securityRules/write",
    "Microsoft.Network/applicationSecurityGroups/delete",
    "Microsoft.Network/networkSecurityGroups/securityRules/delete",
    "Microsoft.Synapse/workspaces/write",
```

```
        "Microsoft.Synapse/workspaces/read",
        "Microsoft.Synapse/workspaces/delete",
        "Microsoft.Synapse/register/action",
        "Microsoft.Synapse/checkNameAvailability/action",
        "Microsoft.Synapse/workspaces/operationStatuses/read",
        "Microsoft.Synapse/workspaces/firewallRules/read",
        "Microsoft.Synapse/workspaces/replaceAllIpFirewallRules/action",
        "Microsoft.Synapse/workspaces/operationResults/read",

    "Microsoft.Synapse/workspaces/privateEndpointConnectionsApproval/action",
        "Microsoft.ManagedIdentity/userAssignedIdentities/assign/action",
        "Microsoft.Compute/images/write",
        "Microsoft.Network/loadBalancers/frontendIPConfigurations/read",
        "Microsoft.Compute/virtualMachineScaleSets/write",
        "Microsoft.Compute/virtualMachineScaleSets/read",
        "Microsoft.Compute/virtualMachineScaleSets/delete"
      ],
      "NotActions": [],
      "AssignableScopes": [],
      "Description": "Console Permissions",
      "IsCustom": "true"
    }
```

Azure の権限の使用方法

次のセクションでは、各NetAppストレージ システムおよびデータ サービスに対する権限の使用方法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。

Azure NetApp Files

NetApp Data Classification を使用してAzure NetApp Filesデータをスキャンすると、エージェントは次の API 要求を行います。

- Microsoft. NetApp/netAppAccounts/read
- Microsoft. NetApp/netAppAccounts/capacityPools/read
- Microsoft. NetApp/netAppAccounts/capacityPools/volumes/write
- Microsoft. NetApp/netAppAccounts/capacityPools/volumes/read
- Microsoft. NetApp/netAppAccounts/capacityPools/volumes/delete

NetApp Backup and Recovery

次のセクションでは、NetApp Backup and Recoveryで権限がどのように使用されるかについて説明します。

最小限の**NetApp Backup and Recovery**権限

コンソール エージェントは、基本的なNetApp Backup and Recovery機能に対して次の API 要求を行います。

- Microsoft.Storage/storageAccounts/listkeys/アクション
- Microsoft.Storage/storageAccounts/読み取り
- Microsoft.Storage/ストレージアカウント/書き込み
- Microsoft.Storage/storageAccounts/blobServices/containers/読み取り
- Microsoft.Storage/storageAccounts/listAccountSas/アクション
- Microsoft.Resources/サブスクリプション/場所/読み取り
- Microsoft.Resources/サブスクリプション/リソースグループ/読み取り
- Microsoft.Resources/サブスクリプション/リソースグループ/リソース/読み取り
- Microsoft.Resources/サブスクリプション/リソースグループ/書き込み
- Microsoft.Storage/storageAccounts/managementPolicies/読み取り
- Microsoft.Storage/storageAccounts/managementPolicies/書き込み
- Microsoft.Authorization/ロック/書き込み
- Microsoft.Authorization/ロック/読み取り

以下は、可能な限り少ない権限と可能な限り狭い範囲を使用するバックアップとリカバリのカスタム ポリシーです。

```
{
  "id":
"/subscriptions/{subscriptionId}/providers/Microsoft.Authorization/roleDef
initions/{roleDefinitionGuid}",
  "properties": {
    "roleName": "Custom Role",
    "description": "Minimal permissions required for Backup and
Recovery.",
    "assignableScopes": [
      "/subscriptions/{subscriptionId}",

"/subscriptions/{subscriptionId}/resourceGroups/{resourceGroupNameContaini
ngConnectorAndStorageAccount}",

"/subscriptions/{subscriptionId}/resourceGroups/{resourceGroupNameContaini
ngConnectorAndStorageAccount}/providers/Microsoft.Storage/storageAccounts/
{storageAccountNameWithObjectLockPreprovisioned}"
    ],
    "permissions": [
      {
        "actions": [
          "Microsoft.Storage/storageAccounts/listkeys/action",
          "Microsoft.Storage/storageAccounts/read",
          "Microsoft.Storage/storageAccounts/write",

"Microsoft.Storage/storageAccounts/blobServices/containers/read",
          "Microsoft.Storage/storageAccounts/listAccountSas/action",
          "Microsoft.Resources/subscriptions/locations/read",

"Microsoft.Resources/subscriptions/resourcegroups/resources/read",
          "Microsoft.Resources/subscriptions/resourceGroups/write",
          "Microsoft.Resources/subscriptions/resourceGroups/read",
          "Microsoft.Storage/storageAccounts/managementPolicies/read",
          "Microsoft.Storage/storageAccounts/managementPolicies/write",
          "Microsoft.Authorization/locks/write",
          "Microsoft.Authorization/locks/read"
        ],
        "notActions": [],
        "dataActions": [],
        "notDataActions": []
      }
    ]
  }
}
```

高度なバックアップとリカバリの権限

コンソール エージェントは、高度なバックアップとリカバリ操作および検索と復元機能に対して次の API 要求を行います。これらのアクセス許可により、ネットワーク、キー コンテナー、マネージド ID の管理が可能になります。

- Microsoft.KeyVault/vaults/accessPolicies/書き込み
- Microsoft.KeyVault/vaults/読み取り
- Microsoft.ManagedIdentity/userAssignedIdentities/割り当て/アクション
- Microsoft.Network/ネットワークインターフェイス/削除
- Microsoft.Network/ネットワークインターフェイス/読み取り
- Microsoft.Network/ネットワークセキュリティグループ/削除
- Microsoft.Network/privateDnsZones/読み取り
- Microsoft.Network/privateDnsZones/書き込み
- Microsoft.Network/privateEndpoints/読み取り
- Microsoft.Network/privateEndpoints/書き込み
- Microsoft.Network/仮想ネットワーク/参加/アクション
- Microsoft.Resources/デプロイメント/削除

バックアップとリカバリの従来の権限

検索と復元機能を使用するとき、エージェントは次の API 要求を行います。これらの権限は、2025 年 2 月のインデックス 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必要です。

- Microsoft.Synapse/ワークスペース/書き込み
- Microsoft.Synapse/ワークスペース/読み取り
- Microsoft.Synapse/ワークスペース/削除
- Microsoft.Synapse/登録/アクション
- Microsoft.Synapse/checkNameAvailability/アクション
- Microsoft.Synapse/ワークスペース/操作ステータス/読み取り
- Microsoft.Synapse/ワークスペース/ファイアウォールルール/読み取り
- Microsoft.Synapse/ワークスペース/replaceAllIpFirewallRules/アクション
- Microsoft.Synapse/ワークスペース/操作結果/読み取り
- Microsoft.Synapse/ワークスペース/プライベートエンドポイント接続承認/アクション

NetApp Data Classification

データ分類を使用する場合、エージェントは次の API リクエストを行います。

アクション	セットアップに使用しますか?	日常業務に使用されますか?
Microsoft.Compute/場所/操作/読み取り	はい	はい
Microsoft.Compute/場所/vmSizes/読み取り	はい	はい
Microsoft.Compute/操作/読み取り	はい	はい
Microsoft.Compute/virtualMachines/instanceView/読み取り	はい	はい
Microsoft.Compute/virtualMachines/powerOff/アクション	はい	いいえ
Microsoft.Compute/仮想マシン/読み取り	はい	はい
Microsoft.Compute/virtualMachines/再起動/アクション	はい	いいえ
Microsoft.Compute/virtualMachines/start/action	はい	いいえ
Microsoft.Compute/virtualMachines/vmSizes/読み取り	いいえ	はい
Microsoft.Compute/仮想マシン/書き込み	はい	いいえ
Microsoft.Compute/images/読み取り	はい	はい
Microsoft.Compute/ディスク/削除	はい	いいえ
Microsoft.Compute/ディスク/読み取り	はい	はい
Microsoft.Compute/ディスク/書き込み	はい	いいえ
Microsoft.Storage/checknameavailability/読み取り	はい	はい
Microsoft.Storage/操作/読み取り	はい	はい
Microsoft.Storage/storageAccounts/listkeys/アクション	はい	いいえ
Microsoft.Storage/storageAccounts/読み取り	はい	はい
Microsoft.Storage/ストレージアカウント/書き込み	はい	いいえ
Microsoft.Storage/storageAccounts/blobServices/containers/読み取り	はい	はい
Microsoft.Network/ネットワークインターフェイス/読み取り	はい	はい
Microsoft.Network/ネットワークインターフェイス/書き込み	はい	いいえ

アクション	セットアップに使用しますか?	日常業務に使用されますか?
Microsoft.Network/ネットワークインターフェイス/参加/アクション	はい	いいえ
Microsoft.Network/ネットワークセキュリティグループ/読み取り	はい	はい
Microsoft.Network/ネットワークセキュリティグループ/書き込み	はい	いいえ
Microsoft.Resources/サブスクリプション/場所/読み取り	はい	はい
Microsoft.Network/場所/操作結果/読み取り	はい	はい
Microsoft.Network/場所/操作/読み取り	はい	はい
Microsoft.Network/仮想ネットワーク/読み取り	はい	はい
Microsoft.Network/virtualNetworks/checkIpAddressAvailability/読み取り	はい	はい
Microsoft.Network/virtualNetworks/サブネット/読み取り	はい	はい
Microsoft.Network/virtualNetworks/サブネット/virtualMachines/読み取り	はい	はい
Microsoft.Network/virtualNetworks/virtualMachines/読み取り	はい	はい
Microsoft.Network/virtualNetworks/サブネット/参加/アクション	はい	いいえ
Microsoft.Network/virtualNetworks/サブネット/書き込み	はい	いいえ
Microsoft.Network/routeTables/join/アクション	はい	いいえ
Microsoft.Resources/デプロイメント/運用/読み取り	はい	はい
Microsoft.Resources/デプロイメント/読み取り	はい	はい
Microsoft.Resources/デプロイメント/書き込み	はい	いいえ
Microsoft.Resources/リソース/読み取り	はい	はい
Microsoft.Resources/サブスクリプション/操作結果/読み取り	はい	はい
Microsoft.Resources/サブスクリプション/リソースグループ/削除	はい	いいえ

アクション	セットアップに使用しますか?	日常業務に使用されますか?
Microsoft.Resources/サブスクリプション/リソースグループ/読み取り	はい	はい
Microsoft.Resources/サブスクリプション/リソースグループ/リソース/読み取り	はい	はい
Microsoft.Resources/サブスクリプション/リソースグループ/書き込み	はい	いいえ

Cloud Volumes ONTAP

エージェントは、Azure でCloud Volumes ONTAP をデプロイおよび管理するために、次の API 要求を行います。

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?
VMの作成と管理	Microsoft.Compute/場所/操作/読み取り	はい	はい	いいえ
	Microsoft.Compute/場所/vmSizes/読み取り	はい	はい	いいえ
	Microsoft.Resources/サブスクリプション/場所/読み取り	はい	いいえ	いいえ
	Microsoft.Compute/操作/読み取り	はい	はい	いいえ
	Microsoft.Compute/virtualMachines/instanceView/読み取り	はい	はい	いいえ
	Microsoft.Compute/virtualMachines/powerOff/アクション	はい	はい	いいえ
	Microsoft.Compute/仮想マシン/読み取り	はい	はい	いいえ
	Microsoft.Compute/virtualMachines/再起動/アクション	はい	はい	いいえ
	Microsoft.Compute/virtualMachines/start/action	はい	はい	いいえ
	Microsoft.Compute/virtualMachines/割り当て解除/アクション	いいえ	はい	はい
	Microsoft.Compute/virtualMachines/vmSizes/読み取り	いいえ	はい	いいえ
	Microsoft.Compute/仮想マシン/書き込み	はい	はい	いいえ
	Microsoft.Compute/仮想マシン/削除	はい	はい	はい
	Microsoft.Resources/デプロイメント/削除	はい	いいえ	いいえ
VHDからの展開を有効にする	Microsoft.Compute/images/読み取り	はい	いいえ	いいえ
	Microsoft.Compute/images/書き込み	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?
ターゲットサブネット内のネットワークインターフェースの作成と管理	Microsoft.Network/ネットワークインターフェイス/読み取り	はい	はい	いいえ
	Microsoft.Network/ネットワークインターフェイス/書き込み	はい	はい	いいえ
	Microsoft.Network/ネットワークインターフェイス/参加/アクション	はい	はい	いいえ
	Microsoft.Network/ネットワークインターフェイス/削除	はい	はい	いいえ
ネットワーク セキュリティ グループの作成と管理	Microsoft.Network/ネットワークセキュリティグループ/読み取り	はい	はい	いいえ
	Microsoft.Network/ネットワークセキュリティグループ/書き込み	はい	はい	いいえ
	Microsoft.Network/ネットワークセキュリティグループ/参加/アクション	はい	いいえ	いいえ
	Microsoft.Network/ネットワークセキュリティグループ/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?
リージョン、ターゲット VNet、サブネットに関するネットワーク情報を取得し、VM を VNet に追加します。	Microsoft.Network/場所/操作結果/読み取り	はい	はい	いいえ
	Microsoft.Network/場所/操作/読み取り	はい	はい	いいえ
	Microsoft.Network/仮想ネットワーク/読み取り	はい	いいえ	いいえ
	Microsoft.Network/virtualNetworks/checkIpAddressAvailability/読み取り	はい	いいえ	いいえ
	Microsoft.Network/virtualNetworks/サブネット/読み取り	はい	はい	いいえ
	Microsoft.Network/virtualNetworks/サブネット/virtualMachines/読み取り	はい	はい	いいえ
	Microsoft.Network/virtualNetworks/virtualMachines/読み取り	はい	はい	いいえ
	Microsoft.Network/virtualNetworks/サブネット/参加/アクション	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?
リソース グループの作成と管理	Microsoft.Resources/デプロイメント/運用/読み取り	はい	はい	いいえ
	Microsoft.Resources/デプロイメント/読み取り	はい	はい	いいえ
	Microsoft.Resources/デプロイメント/書き込み	はい	はい	いいえ
	Microsoft.Resources/リソース/読み取り	はい	はい	いいえ
	Microsoft.Resources/サブスクリプション/操作結果/読み取り	はい	はい	いいえ
	Microsoft.Resources/サブスクリプション/リソースグループ/削除	はい	はい	はい
	Microsoft.Resources/サブスクリプション/リソースグループ/読み取り	いいえ	はい	いいえ
	Microsoft.Resources/サブスクリプション/リソースグループ/リソース/読み取り	はい	はい	いいえ
	Microsoft.Resources/サブスクリプション/リソースグループ/書き込み	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?
Azure ストレージ アカウントとディスクを管理する	Microsoft.Compute/ディスク/読み取り	はい	はい	はい
	Microsoft.Compute/ディスク/書き込み	はい	はい	いいえ
	Microsoft.Compute/ディスク/削除	はい	はい	はい
	Microsoft.Storage/checknameavailability/読み取り	はい	はい	いいえ
	Microsoft.Storage/操作/読み取り	はい	はい	いいえ
	Microsoft.Storage/storageAccounts/listkeys/アクション	はい	はい	いいえ
	Microsoft.Storage/storageAccounts/読み取り	はい	はい	いいえ
	Microsoft.Storage/storageAccounts/削除	いいえ	はい	はい
	Microsoft.Storage/ストレージアカウント/書き込み	はい	はい	いいえ
	Microsoft.Storage/使用状況/読み取り	いいえ	はい	いいえ
BLOB ストレージへのバックアップとストレージ アカウントの暗号化を有効にする	Microsoft.Storage/storageAccounts/blobServices/containers/読み取り	はい	はい	いいえ
	Microsoft.KeyVault/vaults/読み取り	はい	はい	いいえ
	Microsoft.KeyVault/vaults/accessPolicies/書き込み	はい	はい	いいえ
データ階層化のために VNet サービス エンドポイントを有効にする	Microsoft.Network/virtualNetworks/サブネット/書き込み	はい	はい	いいえ
	Microsoft.Network/routeTables/join/アクション	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?
Azure 管理スナップショットの作成と管理	Microsoft.Compute/スナップショット/書き込み	はい	はい	いいえ
	Microsoft.Compute/スナップショット/読み取り	はい	はい	いいえ
	Microsoft.Compute/スナップショット/削除	いいえ	はい	はい
	Microsoft.Compute/ディスク/beginGetAccess/アクション	いいえ	はい	いいえ
可用性セットの作成と管理	Microsoft.Compute/availabilitySets/書き込み	はい	いいえ	いいえ
	Microsoft.Compute/availabilitySets/読み取り	はい	いいえ	いいえ
マーケットプレイスからのプログラムによる展開を可能にする	Microsoft.MarketplaceOrdering/オファータイプ/発行者/オファー/プラン/契約/読み取り	はい	いいえ	いいえ
	Microsoft.MarketplaceOrdering/オファータイプ/パブリッシャー/オファー/プラン/契約/書き込み	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?
HAペアのロードバランサを管理する	Microsoft.Network/ロードバランサー/読み取り	はい	はい	いいえ
	Microsoft.Network/ロードバランサー/書き込み	はい	いいえ	いいえ
	Microsoft.Network/loadBalancers/削除	いいえ	はい	はい
	Microsoft.Network/loadBalancers/backendAddressPools/読み取り	はい	いいえ	いいえ
	Microsoft.Network/loadBalancers/backendAddressPools/参加/アクション	はい	いいえ	いいえ
	Microsoft.Network/loadBalancers/frontendIPConfigurations/読み取り	はい	はい	いいえ
	Microsoft.Network/loadBalancers/loadBalancingRules/読み取り	はい	いいえ	いいえ
	Microsoft.Network/loadBalancers/プローブ/読み取り	はい	いいえ	いいえ
	Microsoft.Network/loadBalancers/プローブ/参加/アクション	はい	いいえ	いいえ
Azure ディスクのロックの管理を有効にする	Microsoft.Authorization/locks/*	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?
サブネット外に接続できない場合にHAペアのプライベートエンドポイントを有効にする	Microsoft.Network/privateEndpoints/書き込み	はい	はい	いいえ
	Microsoft.Storage/storageAccounts/PrivateEndpointConnectionsApproval/アクション	はい	いいえ	いいえ
	Microsoft.Storage/storageAccounts/privateEndpointConnections/読み取り	はい	はい	はい
	Microsoft.Network/privateEndpoints/読み取り	はい	はい	はい
	Microsoft.Network/privateDnsZones/書き込み	はい	はい	いいえ
	Microsoft.Network/privateDnsZones/virtualNetworkLinks/書き込み	はい	はい	いいえ
	Microsoft.Network/仮想ネットワーク/参加/アクション	はい	はい	いいえ
	Microsoft.Network/privateDnsZones/A/書き込み	はい	はい	いいえ
	Microsoft.Network/privateDnsZones/読み取り	はい	はい	いいえ
	Microsoft.Network/privateDnsZones/virtualNetworkLinks/読み取り	はい	はい	いいえ
基盤となる物理ハードウェアに応じて、一部の VM 展開に必要	Microsoft.Resources/デプロイメント/操作ステータス/読み取り	はい	はい	いいえ
デプロイメントの失敗または削除の場合にリソース グループからリソースを削除する	Microsoft.Network/privateEndpoints/削除	はい	はい	いいえ
	Microsoft.Compute/availabilitySets/削除	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?
API を使用する際に顧客管理の暗号化キーの使用を有効にする	Microsoft.Compute/diskEncryptionSets/読み取り	はい	はい	はい
	Microsoft.Compute/diskEncryptionSets/書き込み	はい	はい	いいえ
	Microsoft.KeyVault/vaults/deploy/action	はい	いいえ	いいえ
	Microsoft.Compute/diskEncryptionSets/削除	はい	はい	はい
HA ペアのアプリケーション セキュリティ グループを構成して、HA インターコネクトとクラスタ ネットワーク NIC を分離します。	Microsoft.Network/アプリケーションセキュリティグループ/書き込み	いいえ	はい	いいえ
	Microsoft.Network/applicationSecurityGroups/読み取り	いいえ	はい	いいえ
	Microsoft.Network/applicationSecurityGroups/joinIpConfiguration/アクション	いいえ	はい	いいえ
	Microsoft.Network/ネットワークセキュリティグループ/セキュリティルール/書き込み	はい	はい	いいえ
	Microsoft.Network/applicationSecurityGroups/削除	いいえ	はい	はい
	Microsoft.Network/ネットワークセキュリティグループ/セキュリティルール/削除	いいえ	はい	はい
Cloud Volumes ONTAPリソースに関連付けられたタグの読み取り、書き込み、削除	Microsoft.Resources/タグ/読み取り	いいえ	はい	いいえ
	Microsoft.Resources/タグ/書き込み	はい	はい	いいえ
	Microsoft.Resources/タグ/削除	はい	いいえ	いいえ
作成時にストレージアカウントを暗号化する	Microsoft.ManagedIdentity/userAssignedIdentities/割り当て/アクション	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の特定のゾーンを指定するには、柔軟なオーケストレーション モードで仮想マシン スケール セットを使用します。	Microsoft.Compute/仮想マシンスケールセット/書き込み	はい	いいえ	いいえ
	Microsoft.Compute/仮想マシンスケールセット/読み取り	はい	いいえ	いいえ
	Microsoft.Compute/virtualMachineScaleSets/削除	いいえ	いいえ	はい

階層化

NetApp Cloud Tieringをセットアップすると、エージェントは次の API 要求を行います。

- Microsoft.Storage/storageAccounts/listkeys/アクション
- Microsoft.Resources/サブスクリプション/リソースグループ/読み取り
- Microsoft.Resources/サブスクリプション/場所/読み取り

コンソール エージェントは、日常の操作のために次の API 要求を行います。

- Microsoft.Storage/storageAccounts/blobServices/containers/読み取り
- Microsoft.Storage/storageAccounts/managementPolicies/読み取り
- Microsoft.Storage/storageAccounts/managementPolicies/書き込み
- Microsoft.Storage/storageAccounts/読み取り

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。

2025年11月11日

可能な限り少ない権限と可能な限り狭い範囲を反映するカスタム JSON ポリシーが追加されました。

最小限のバックアップおよびリカバリ権限リストに次の権限が追加されました。

- Microsoft.Authorization/ロック/書き込み
- Microsoft.Authorization/ロック/読み取り

従来のインデックスを使用していない限り、バックアップとリカバリには次の権限は不要になりました。

- Microsoft.Synapse/ワークスペース/書き込み
- Microsoft.Synapse/ワークスペース/読み取り
- Microsoft.Synapse/ワークスペース/削除
- Microsoft.Synapse/登録/アクション

- Microsoft.Synapse/checkNameAvailability/アクション
- Microsoft.Synapse/ワークスペース/操作ステータス/読み取り
- Microsoft.Synapse/ワークスペース/ファイアウォールルール/読み取り
- Microsoft.Synapse/ワークスペース/replaceAllIpFirewallRules/アクション
- Microsoft.Synapse/ワークスペース/操作結果/読み取り
- Microsoft.Synapse/ワークスペース/プライベートエンドポイント接続承認/アクション

次の権限は、最小限の構成では必要ないため、「追加のバックアップおよび回復権限」セクションに移動されました。

- Microsoft.Storage/storageAccounts/listkeys/アクション
- Microsoft.Storage/storageAccounts/読み取り
- Microsoft.Storage/ストレージアカウント/書き込み
- Microsoft.Storage/storageAccounts/blobServices/containers/読み取り
- Microsoft.Storage/storageAccounts/listAccountSas/アクション
- Microsoft.Resources/サブスクリプション/場所/読み取り
- Microsoft.Resources/サブスクリプション/リソースグループ/読み取り
- Microsoft.Resources/サブスクリプション/リソースグループ/リソース/読み取り
- Microsoft.Resources/サブスクリプション/リソースグループ/書き込み
- Microsoft.Storage/storageAccounts/managementPolicies/読み取り
- Microsoft.Storage/storageAccounts/managementPolicies/書き込み

2024年9月9日

コンソールでは Kubernetes クラスターの検出と管理がサポートされなくなったため、次の権限が JSON ポリシーから削除されました。

- Microsoft.ContainerService/managedClusters/listClusterUserCredential/アクション
- Microsoft.ContainerService/managedClusters/読み取り

2024年8月22日

仮想マシン スケール セットのCloud Volumes ONTAPサポートに必要なため、次の権限が JSON ポリシーに追加されました。

- Microsoft.Compute/仮想マシンスケールセット/書き込み
- Microsoft.Compute/仮想マシンスケールセット/読み取り
- Microsoft.Compute/virtualMachineScaleSets/削除

2023年12月5日

ボリューム データを Azure Blob ストレージにバックアップする場合、 NetApp Backup and Recoveryでは次の権限は不要になりました。

- Microsoft.Compute/仮想マシン/読み取り
- Microsoft.Compute/virtualMachines/start/action
- Microsoft.Compute/virtualMachines/割り当て解除/アクション
- Microsoft.Compute/virtualMachines/拡張機能/削除
- Microsoft.Compute/仮想マシン/削除

これらの権限は他のコンソール ストレージ サービスに必要なので、他のストレージ サービスを使用している場合は、エージェントのカスタム ロールに引き続き残ります。

2023年**5**月**12**日

Cloud Volumes ONTAP管理に必要なため、次の権限が JSON ポリシーに追加されました。

- Microsoft.Compute/images/書き込み
- Microsoft.Network/loadBalancers/frontendIPConfigurations/読み取り

次の権限は不要になったため、JSON ポリシーから削除されました。

- Microsoft.Storage/storageAccounts/blobServices/コンテナー/書き込み
- Microsoft.Network/publicIPAddresses/削除

2023年**3**月**23**日

データ分類には「Microsoft.Storage/storageAccounts/delete」アクセス許可は不要になりました。

この権限は、Cloud Volumes ONTAPでも必要です。

2023年**1**月**5**日

次の権限が JSON ポリシーに追加されました。

- Microsoft.Storage/storageAccounts/listAccountSas/アクション
- Microsoft.Synapse/ワークスペース/プライベートエンドポイント接続承認/アクション

  これらの権限は、NetApp Backup and Recoveryに必要です。

- Microsoft.Network/loadBalancers/backendAddressPools/参加/アクション

  この権限は、Cloud Volumes ONTAP のデプロイメントに必要です。

Azure のコンソール エージェント セキュリティ グループ ルール

エージェントの Azure セキュリティ グループには、受信規則と送信規則の両方が必要です。 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。その他のインストール オプションについては、このセキュリティ グループを手動で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	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、AutoSupportメッセージをNetAppサポートに送信します。デプロイ後にこのポートを手動で開く必要があります。 "エージェントがAutoSupportメッセージのプロキシとしてどのように使用されるかを学びます"

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	Azure、 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	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

Google Cloud の権限と必要なファイアウォール ルール

コンソール エージェントの **Google Cloud** 権限

コンソール エージェントには、Google Cloud でアクションを実行するための権限が必要です。これらの権限は、 NetAppが提供するカスタム ロールに含まれています。エージェントがこれらの権限を使用して何を行うかを理解する必要があります。

Google Cloud ユーザー アカウントの権限

以下のカスタムロールは、Google Cloud ユーザーにエージェントのデプロイに必要な権限を付与します。このカスタム ロールを、エージェントを展開するユーザーに適用します。

Google Cloud ユーザー アカウントの権限を表示する

```
title: Console agent deployment policy
description: Permissions for the user who deploys the Console agent
stage: GA
includedPermissions:

- cloudbuild.builds.get
- compute.disks.create
- compute.disks.get
- compute.disks.list
- compute.disks.setLabels
- compute.disks.use
- compute.firewalls.create
- compute.firewalls.delete
- compute.firewalls.get
- compute.firewalls.list
- compute.globalOperations.get
- compute.images.get
- compute.images.getFromFamily
- compute.images.list
- compute.images.useReadOnly
- compute.instances.attachDisk
- compute.instances.create
- compute.instances.get
- compute.instances.list
- compute.instances.setDeletionProtection
- compute.instances.setLabels
- compute.instances.setMachineType
- compute.instances.setMetadata
- compute.instances.setTags
- compute.instances.start
- compute.instances.updateDisplayDevice
- compute.machineTypes.get
- compute.networks.get
- compute.networks.list
- compute.networks.updatePolicy
- compute.projects.get
- compute.regions.get
- compute.regions.list
- compute.subnetworks.get
- compute.subnetworks.list
- compute.zoneOperations.get
- compute.zones.get
- compute.zones.list
```

```
- config.deployments.create
- config.operations.get
- config.deployments.delete
- config.deployments.deleteState
- config.deployments.get
- config.deployments.getState
- config.deployments.list
- config.deployments.update
- config.deployments.updateState
- config.previews.get
- config.previews.list
- config.revisions.get
- config.resources.list
- deploymentmanager.compositeTypes.get
- deploymentmanager.compositeTypes.list
- deploymentmanager.deployments.create
- deploymentmanager.deployments.delete
- deploymentmanager.deployments.get
- deploymentmanager.deployments.list
- deploymentmanager.manifests.get
- deploymentmanager.manifests.list
- deploymentmanager.operations.get
- deploymentmanager.operations.list
- deploymentmanager.resources.get
- deploymentmanager.resources.list
- deploymentmanager.typeProviders.get
- deploymentmanager.typeProviders.list
- deploymentmanager.types.get
- deploymentmanager.types.list
- resourcemanager.projects.get
- compute.instances.setServiceAccount
- iam.serviceAccounts.actAs
- iam.serviceAccounts.create
- iam.serviceAccounts.list
- iam.serviceAccountKeys.create
- storage.buckets.create
- storage.buckets.get
- storage.objects.create
- storage.folders.create
- storage.objects.list
```

サービスアカウントの権限

以下のカスタムロールは、コンソール エージェントに接続された Google Cloud サービス アカウントに、Google Cloud ネットワーク内のリソースとプロセスを管理するために必要な権限を付与します。

このカスタム ロールを、コンソール エージェント VM に接続されたサービス アカウントに適用します。

- "標準モードの Google Cloud 権限を設定する"
- "制限モードの権限を設定する"

Google サービス アカウントの権限を表示する

後続のリリースで新しい権限が追加または削除されるので、ロールが最新であることを確認します。変更ログには、必要な新しい権限がすべてリストされます。"Google の権限変更ログを確認する" "Google Cloud サービス アカウントを追加する方法を確認する"

```
title: NetApp Console agent
description: Permissions for the service account associated with the
Console agent.
stage: GA
includedPermissions:
- cloudbuild.builds.get
- cloudbuild.connections.list
- cloudbuild.repositories.accessReadToken
- cloudbuild.repositories.list
- cloudbuild.workerpools.list
- cloudbuild.workerpools.get
- cloudquotas.quotas.get
- cloudkms.cryptoKeys.getIamPolicy
- cloudkms.cryptoKeys.setIamPolicy
- cloudkms.keyRings.get
- cloudkms.keyRings.getIamPolicy
- cloudkms.keyRings.setIamPolicy
- config.artifacts.import
- config.deployments.create
- config.deployments.delete
- config.deployments.deleteState
- config.deployments.get
- config.deployments.getLock
- config.deployments.getState
- config.deployments.list
- config.deployments.lock
- config.deployments.update
- config.deployments.updateState
- config.previews.upload
- config.revisions.get
- config.revisions.getState
- config.operations.get
- config.previews.get
- config.previews.list
- config.resources.list
- compute.regionBackendServices.create
- compute.regionBackendServices.get
- compute.regionBackendServices.list
- compute.regionBackendServices.update
- compute.networks.updatePolicy
```

```
- compute.addresses.createInternal
- compute.addresses.deleteInternal
- compute.addresses.list
- compute.addresses.setLabels
- compute.addresses.useInternal
- compute.backendServices.create
- compute.disks.create
- compute.disks.createSnapshot
- compute.disks.delete
- compute.disks.get
- compute.disks.list
- compute.disks.setLabels
- compute.disks.use
- compute.firewalls.create
- compute.firewalls.delete
- compute.firewalls.get
- compute.firewalls.list
- compute.forwardingRules.create
- compute.forwardingRules.delete
- compute.forwardingRules.get
- compute.forwardingRules.setLabels
- compute.forwardingRules.update
- compute.globalOperations.get
- compute.healthChecks.create
- compute.healthChecks.delete
- compute.healthChecks.get
- compute.healthChecks.useReadOnly
- compute.images.get
- compute.images.getFromFamily
- compute.images.list
- compute.images.useReadOnly
- compute.instances.addAccessConfig
- compute.instances.attachDisk
- compute.instances.create
- compute.instances.delete
- compute.instances.detachDisk
- compute.instances.get
- compute.instances.getSerialPortOutput
- compute.instances.list
- compute.instances.setDeletionProtection
- compute.instances.setLabels
- compute.instances.setMachineType
- compute.instances.setMetadata
- compute.instances.setTags
- compute.instances.start
- compute.instances.stop
```

```
- compute.instances.updateDisplayDevice
- compute.instances.use
- compute.instanceGroups.create
- compute.instanceGroups.delete
- compute.instanceGroups.get
- compute.instanceGroups.update
- compute.instanceGroups.use
- compute.addresses.get
- compute.instances.updateNetworkInterface
- compute.instances.setMinCpuPlatform
- compute.machineTypes.get
- compute.networks.get
- compute.networks.list
- compute.projects.get
- compute.regions.get
- compute.regions.list
- compute.regionBackendServices.delete
- compute.regionBackendServices.use
- compute.resourcePolicies.create
- compute.resourcePolicies.delete
- compute.resourcePolicies.get
- compute.snapshots.create
- compute.snapshots.delete
- compute.snapshots.get
- compute.snapshots.list
- compute.snapshots.setLabels
- compute.subnetworks.get
- compute.subnetworks.list
- compute.subnetworks.use
- compute.subnetworks.useExternalIp
- compute.zoneOperations.get
- compute.zones.get
- compute.zones.list
- compute.instances.setServiceAccount
- deploymentmanager.compositeTypes.get
- deploymentmanager.compositeTypes.list
- deploymentmanager.deployments.create
- deploymentmanager.deployments.delete
- deploymentmanager.deployments.get
- deploymentmanager.deployments.list
- deploymentmanager.manifests.get
- deploymentmanager.manifests.list
- deploymentmanager.operations.get
- deploymentmanager.operations.list
- deploymentmanager.resources.get
- deploymentmanager.resources.list
```

```
- deploymentmanager.typeProviders.get
- deploymentmanager.typeProviders.list
- deploymentmanager.types.get
- deploymentmanager.types.list
- logging.logEntries.list
- logging.privateLogEntries.list
- logging.logEntries.create
- logging.logEntries.route
- monitoring.timeSeries.list
- resourcemanager.projects.get
- storage.buckets.create
- storage.buckets.delete
- storage.buckets.get
- storage.buckets.list
- storage.objects.create
- storage.objects.delete
- storage.objects.get
- storage.objects.list
- storage.objects.update
- cloudkms.cryptoKeyVersions.useToEncrypt
- cloudkms.cryptoKeys.get
- cloudkms.cryptoKeys.list
- cloudkms.keyRings.list
- storage.buckets.update
- iam.serviceAccounts.actAs
- iam.serviceAccounts.create
- iam.serviceAccounts.get
- iam.serviceAccounts.getIamPolicy
- iam.serviceAccounts.list
- iam.serviceAccountKeys.create
- storage.buckets.getIamPolicy
```

Google Cloud の権限の使用方法

コンソール エージェントは、カスタムロールの権限を使用して、Google Cloud ネットワーク内のCloud Volumes ONTAPリソースとNetAppデータサービス プロセスを管理します。次のセクションでは、エージェントがこれらの権限をどのように使用するかについて説明します。

Cloud Volumes ONTAPで使用される権限

コンソール エージェントは、カスタム ロールの権限を使用して、Google Cloud ネットワーク内のCloud Volumes ONTAP のリソースとプロセスを管理します。次のセクションでは、エージェントがこれらの権限をどのように使用するかについて説明します。

Cloud Volumes ONTAPの権限

アクション	目的	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?
config.deployments.create	Google Cloud Infrastructure Manager を使用してCloud Volumes ONTAP仮想マシンインスタンスをデプロイします。	はい	いいえ	いいえ
config.deployments.delete		いいえ	いいえ	はい
config.deployments.deleteState		いいえ	いいえ	はい
config.deployments.get		いいえ	はい	はい
config.deployments.getLock		いいえ	はい	いいえ
config.deployments.getState		いいえ	はい	いいえ
config.deployments.list		いいえ	はい	いいえ
config.deployments.lock		いいえ	はい	いいえ
config.deployments.update		いいえ	はい	いいえ
config.deployments.updateState		いいえ	はい	いいえ
config.operations.get		いいえ	はい	いいえ
config.previews.get		いいえ	はい	いいえ
config.previews.list		いいえ	はい	いいえ
config.resources.list		いいえ	はい	いいえ
config.revisions.get		いいえ	はい	いいえ
コンピューティングディスクの作成	Cloud Volumes ONTAPのディスクを作成および管理します。	はい	はい	いいえ
compute.disks.createSnapshot		いいえ	はい	いいえ
計算ディスク削除		いいえ	はい	はい
compute.disks.get		いいえ	はい	いいえ
計算ディスクリスト		はい	はい	いいえ
compute.disks.setLabels		はい	はい	いいえ
計算ディスク使用		いいえ	はい	いいえ

アクション	目的	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?
compute.firewalls.create	Cloud Volumes ONTAPのファイアウォール ルールを作成します。	はい	いいえ	いいえ
compute.firewalls.delete		いいえ	はい	はい
compute.firewalls.get		はい	はい	いいえ
compute.firewalls.list		はい	はい	いいえ
compute.forwardingRules.create	バックエンド サービスへのトラフィック ルーティング用の転送ルールを作成します。	いいえ	はい	いいえ
compute.forwardingRules.delete	既存の転送ルールを削除します。	いいえ	はい	いいえ
compute.forwardingRules.get	既存の転送ルールの詳細を取得します。	いいえ	はい	いいえ
compute.forwardingRules.setLabels	組織の転送ルールのラベルを設定または更新します。	いいえ	はい	いいえ
compute.forwardingRules.update	トラフィック管理のために既存の転送ルールを更新します。	いいえ	はい	いいえ
compute.globalOperations.get	操作のステータスを取得します。	はい	はい	いいえ
compute.healthChecks.create	バックエンド サービスの健全性を監視するためにヘルス チェックを作成および管理します。	いいえ	はい	いいえ
compute.healthChecks.delete		いいえ	はい	いいえ
compute.healthChecks.get		いいえ	はい	いいえ
compute.healthChecks.useReadOnly		いいえ	はい	いいえ
計算画像取得	VM インスタンスのイメージを取得します。	はい	いいえ	いいえ
compute.images.getFromFamily		はい	いいえ	いいえ
計算画像リスト		はい	いいえ	いいえ
compute.images.useReadOnly		はい	いいえ	いいえ

アクション	目的	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?
compute.instances.attachDisk	Cloud Volumes ONTAPにディスクを接続および切断します。	はい	はい	いいえ
compute.instances.detachDisk		いいえ	はい	はい
コンピューティングインスタンスの作成	Cloud Volumes ONTAP VMインスタンスを作成および削除します。	はい	いいえ	いいえ
コンピューティングインスタンスの削除		いいえ	いいえ	はい
コンピューティングインスタンスの取得	VM インスタンスを一覧表示します。	はい	はい	いいえ
compute.instances.getSerialPortOutput	コンソールログを取得します。	はい	はい	いいえ
計算インスタンスリスト	ゾーン内のインスタンスのリストを取得します。	はい	はい	いいえ
compute.instances.setDeletionProtection	インスタンスに削除保護を設定します。	はい	いいえ	いいえ
compute.instances.setLabels	ラベルを追加します。	はい	いいえ	いいえ
compute.instances.setMachineType	Cloud Volumes ONTAPのマシンタイプを変更します。	はい	はい	いいえ
compute.instances.setMinCpuPlatform		はい	はい	いいえ
compute.instances.setMetadata	メタデータを追加します。	はい	はい	いいえ
compute.instances.setTags	ファイアウォールルールのタグを追加します。	はい	はい	いいえ
コンピューティングインスタンスの開始	Cloud Volumes ONTAP を起動および停止します。	はい	はい	いいえ
コンピューティングインスタンスの停止		はい	はい	いいえ
compute.instances.updateDisplayDevice		はい	はい	いいえ

アクション	目的	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?
コンピューティングインスタンスの使用	仮想マシン インスタンス (開始、停止、接続操作) を使用します。	いいえ	はい	いいえ
compute.machineTypes.get	クォータを確認するためのコア数を取得します。	はい	いいえ	いいえ
compute.projects.get	複数のプロジェクトをサポートします。	はい	いいえ	いいえ
compute.resourcePolicies.create	自動リソース管理のためのリソースポリシーを作成および管理します。	いいえ	はい	いいえ
compute.resourcePolicies.delete		いいえ	はい	いいえ
compute.resourcePolicies.get		いいえ	はい	いいえ
計算スナップショット作成	永続ディスクのスナップショットを作成および管理します。	はい	はい	いいえ
計算スナップショットの削除		いいえ	はい	はい
compute.snapshots.get		いいえ	はい	いいえ
計算スナップショットリスト		いいえ	はい	いいえ
compute.snapshots.setLabels		はい	はい	いいえ

アクション	目的	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?
compute.networks.get	新しいCloud Volumes ONTAP仮想マシンインスタンスを作成するために必要なネットワーク情報を取得します。	はい	はい	いいえ
compute.networks.list		はい	はい	いいえ
compute.regions.get		はい	はい	いいえ
compute.regions.list		はい	はい	いいえ
compute.subnetworks.get		はい	はい	いいえ
compute.subnetworks.list		はい	はい	いいえ
compute.zoneOperations.get		はい	はい	いいえ
compute.zones.get		はい	はい	いいえ
compute.zones.list		はい	はい	いいえ

アクション	目的	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?
デプロイメントマネージャー.複合タイプ.get	Google Cloud Deployment Manager を使用してCloud Volumes ONTAP仮想マシンインスタンスをデプロイします。	はい	いいえ	いいえ
デプロイメントマネージャー.複合タイプ.リスト		はい	いいえ	いいえ
デプロイメントマネージャー.デプロイメント.作成		はい	いいえ	いいえ
デプロイメントマネージャー.デプロイメント.削除		はい	いいえ	いいえ
デプロイメントマネージャー.デプロイメント.取得		はい	いいえ	いいえ
デプロイメントマネージャー.デプロイメントリスト		はい	いいえ	いいえ
デプロイメントマネージャーマニフェストの取得		はい	いいえ	いいえ
デプロイメントマネージャーマニフェストリスト		はい	いいえ	いいえ
デプロイメントマネージャー.操作.取得		はい	いいえ	いいえ
デプロイメントマネージャー操作リスト		はい	いいえ	いいえ
デプロイメントマネージャー.リソース.取得		はい	いいえ	いいえ
デプロイメントマネージャー.リソース.リスト		はい	いいえ	いいえ
デプロイメントマネージャー.typeProviders.get		はい	いいえ	いいえ
デプロイメントマネージャー.typeProviders.リスト		はい	いいえ	いいえ

アクション	目的	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?
デプロイメントマネージャータイプ取得		はい	いいえ	いいえ
デプロイメントマネージャータイプリスト		はい	いいえ	いいえ
ログ記録.logEntries.リスト	スタック ログ ドライブを取得します。	はい	はい	いいえ
ログ記録.privateLogEntries.リスト		はい	はい	いいえ
ログ記録.logEntries.create	監視、デバッグ、監査のためにログエントリを作成してルーティングします。	はい	はい	いいえ
ログ記録.logEntries.ルート		はい	はい	いいえ
リソースマネージャー.プロジェクト.取得	複数のプロジェクトをサポートします。	はい	はい	いいえ
ストレージバケットの作成	データ階層化用の Google Cloud Storage バケットを作成および管理します。	はい	はい	いいえ
ストレージバケットの削除		いいえ	はい	はい
ストレージバケットの取得		いいえ	はい	いいえ
ストレージバケットリスト		いいえ	はい	いいえ
ストレージ.バケット.更新		いいえ	はい	いいえ
cloudkms.cryptoKeyVersions.useToEncrypt	Cloud Volumes ONTAPで Cloud Key Management Service の顧客管理暗号化キーを使用する。	はい	はい	いいえ
cloudkms.cryptoKeys.get		はい	はい	いいえ
cloudkms.cryptoKeys.リスト		はい	はい	いいえ
cloudkms.keyRings.リスト		はい	はい	いいえ
cloudbuild.builds.get		はい	いいえ	いいえ

アクション	目的	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?
cloudbuild.workerpools.get	Infrastructure Manager を使用したプライベートモードの導入時および Cloud Volumes ONTAP システムの変換時にワーカープール情報にアクセスするため。	はい	はい	はい
cloudbuild.workerpools.list	Infrastructure Manager を使用した Cloud Volumes ONTAP システムのプライベートモード展開中にワーカープール情報を一覧表示するには。	はい	いいえ	いいえ
compute.instances.setServiceAccount	Cloud Volumes ONTAPインスタンスにサービス アカウントを設定します。このサービスアカウントは、Google Cloud Storage バケットへのデータ階層化の権限を付与します。	はい	はい	いいえ
iam.serviceAccounts.actAs		はい	いいえ	いいえ
iam.serviceAccounts.create		はい	いいえ	いいえ
iam.serviceAccounts.getIamPolicy		はい	はい	いいえ
iam.serviceAccounts.list		はい	はい	いいえ
iam.serviceAccountKeys.create		はい	いいえ	いいえ
ストレージオブジェクトの作成	Google Cloud Storage バケット内のオブジェクト (ファイル) を作成および管理します。	はい	はい	いいえ
ストレージオブジェクトの削除		いいえ	いいえ	はい
ストレージオブジェクト取得		はい	はい	いいえ
ストレージオブジェクトリスト		はい	はい	いいえ
計算アドレスリスト	HA ペアを展開するときにリージョン内のアドレスを取得します。	はい	いいえ	いいえ

アクション	目的	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?
compute.addresses.createInternal	リソース割り当てのために、VPC ネットワーク内に内部 IP アドレスを作成します。	いいえ	はい	いいえ
compute.addresses.deleteInternal	リソースのクリーンアップのために内部 IP アドレスを削除します。	いいえ	はい	いいえ
compute.addresses.setLabels	アドレス リソースのラベルを更新します。	いいえ	はい	いいえ
compute.addresses.useInternal	ネットワーク通信には内部 IP アドレスを使用します。	いいえ	はい	いいえ
compute.backendServices.create	HA ペアでトラフィックを分散するためのバックエンド サービスを設定します。	はい	いいえ	いいえ
compute.regionBackendServices.create	トラフィック ルーティング用のバックエンド サービスを作成および管理します。	はい	いいえ	いいえ
compute.regionBackendServices.delete		いいえ	はい	いいえ
compute.regionBackendServices.get		はい	いいえ	いいえ
compute.regionBackendServices.更新		はい	はい	いいえ
compute.regionBackendServices.リスト		はい	いいえ	いいえ
compute.regionBackendServices.use		いいえ	はい	いいえ
compute.networks.updatePolicy	HA ペアの VPC とサブネットにファイアウォール ルールを適用します。	はい	いいえ	いいえ

アクション	目的	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?
compute.instanceGroups.get	Cloud Volumes ONTAP HA ペアでストレージ VM を作成および管理します。	はい	はい	いいえ
計算アドレス取得		はい	はい	いいえ
compute.instances.updateNetworkInterface		はい	はい	いいえ
compute.instanceGroups.create		いいえ	はい	いいえ
compute.instanceGroups.delete		いいえ	はい	いいえ
compute.instanceGroups.update		いいえ	はい	いいえ
compute.instanceGroups.use		いいえ	はい	いいえ
監視.timeSeries.リスト	Google Cloud Storage バケットに関する情報を検出します。	はい	はい	いいえ
ストレージ.バケット.getIamPolicy		はい	はい	いいえ

NetApp Backup and Recoveryに使用される権限

コンソール エージェントは、カスタムロールの権限を使用して、Google Cloud ネットワーク内のNetApp Backup and Recovery のリソースとプロセスを管理します。次のセクションでは、エージェントがこれらの権限をどのように使用するかについて説明します。

NetApp Backup and Recoveryの権限の表示

アクション	目的	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?
• cloudkms.cryptoKeys.get • cloudkms.cryptoKeys.getIamPolicy • cloudkms.cryptoKeys.リスト • cloudkms.cryptoKeys.setIamPolicy • cloudkms.keyRings.get • cloudkms.keyRings.getIamPolicy • cloudkms.keyRings.リスト • cloudkms.keyRings.setIamPolicy	デフォルトの Google 管理暗号化キーを使用する代わりに、 NetApp Backup and Recoveryアクティベーション ウィザードで独自の顧客管理キーを選択します。	はい	はい	いいえ

NetApp Data Classificationに使用される権限

コンソール エージェントは、カスタムロールの権限を使用して、Google Cloud ネットワーク内のNetApp Data Classification のリソースとプロセスを管理します。次のセクションでは、エージェントがこれらの権限をどのように使用するかについて説明します。

NetApp Data Classificationの表示権限

アクション	目的	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?
• 計算サブネットワーク使用 • compute.subnetworks.useExternalIp • compute.instances.addAccessConfig	NetApp Data Classification を有効にします。	はい	いいえ	いいえ

変更ログ

追加された権限と削除された権限は以下に記載されています。

2026年**2**月**26**日

`cloudbuild.workerpools.get`および `cloudbuild.workerpools.list` の権限は、Google CloudでのCloud Volumes ONTAP のプライベートモード導入におけるInfrastructure Managerをサポートするために追加されました。

2026年**2**月**9**日

`compute.forwardingRules.update`権限は、Google Cloud での Cloud Volumes ONTAP 導入において Infrastructure Manager をサポートするために追加されました。

2025年**12**月**8**日

NetApp は、Google Cloud でコンソール エージェントをデプロイおよび実行するために、Google Cloud Deployment Manager から Google Cloud Infrastructure Manager（IM）に移行しています。この変更をサポートするために、次の権限が追加されました。

エージェントをデプロイする Google Cloud ユーザーには、次の追加権限が必要です。

- ストレージバケットの作成
- ストレージバケットの取得
- ストレージオブジェクトの作成
- ストレージフォルダの作成

- ストレージオブジェクトリスト
- iam.serviceAccount.actAs
- config.deployments.create
- config.operations.get

日常業務に使用する Google Cloud のサービス アカウントには、次の追加権限が必要です。

- cloudbuild.接続リスト
- cloudbuild.repositories.accessReadToken
- cloudbuild.リポジトリリスト
- cloudquotas.quotas.get
- config.artifacts.import
- config.deployments.deleteState
- config.deployments.getLock
- config.deployments.getState
- config.deployments.updateState
- config.previews.upload
- config.revisions.getState
- ログ記録.logEntries.create
- ストレージオブジェクトの作成
- ストレージオブジェクトの削除
- ストレージオブジェクトの更新
- iam.serviceAccounts.get

Cloud Volumes ONTAP をデプロイするには、次の追加の権限が必要です。

- cloudbuild.builds.get
- config.deployments.delete
- config.deployments.deleteState
- config.deployments.get
- config.deployments.getState
- config.deployments.list
- config.deployments.update
- config.deployments.updateState
- config.previews.get
- config.previews.list
- config.revisions.get
- config.resources.list
- iam.serviceAccountKeys.create

- iam.serviceAccounts.create

Cloud Volumes ONTAPの日常的な運用に使用するサービス アカウントには、次の追加の権限が必要です。

- compute.addresses.createInternal
- compute.addresses.deleteInternal
- compute.addresses.setLabels
- compute.addresses.useInternal
- compute.forwardingRules.create
- compute.forwardingRules.delete
- compute.forwardingRules.get
- compute.forwardingRules.setLabels
- compute.healthChecks.create
- compute.healthChecks.delete
- compute.healthChecks.get
- compute.healthChecks.useReadOnly
- compute.instanceGroups.create
- compute.instanceGroups.delete
- compute.instanceGroups.update
- compute.instanceGroups.use
- コンピューティングインスタンスの使用
- compute.regionBackendServices.delete
- compute.regionBackendServices.更新
- compute.regionBackendServices.use
- compute.resourcePolicies.create
- compute.resourcePolicies.delete
- compute.resourcePolicies.get
- ログ記録.logEntries.ルート
- config.deployments.create
- config.deployments.delete
- config.deployments.get
- config.deployments.update
- config.revisions.get
- config.deployments.lock
- config.operations.get

2025年11月26日

権限は使用法を明確にするために更新されていますが、権限の追加や削除は行われていません。各権限がデプロイメント、日常的な操作、または削除のいずれに使用されるかを示す 3 つの列が追加されます。これとは

別に、 NetApp Data ClassificationおよびNetApp Backup and Recoveryでの使用に基づいて、いくつかの権限が分離されています。

2023年2月6日

このポリシーに次の権限が追加されました:

- compute.instances.updateNetworkInterface

この権限はCloud Volumes ONTAPに必要です。

2023/01/27

このポリシーには次の権限が追加されました:

- cloudkms.cryptoKeys.getIamPolicy
- cloudkms.cryptoKeys.setIamPolicy
- cloudkms.keyRings.get
- cloudkms.keyRings.getIamPolicy
- cloudkms.keyRings.setIamPolicy

これらの権限は、NetApp Backup and Recoveryに必要です。

Google Cloud のエージェント ファイアウォール ルール

エージェントの Google Cloud ファイアウォール ルールには、受信ルールと送信ルールの両方が必要です。 NetApp Console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 グループが自動的に作成されます。その他のインストール オプションの場合は、このセキュリティ グループを手動で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	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HTTPSアクセスを提供します
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

エージェントの事前定義されたファイアウォール ルールにより、すべての送信トラフィックが開かれます。許容できる場合は基本的な送信ルールに従います。より厳しい要件の場合は、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ファイアウォール ルールには、次の送信ルールが含まれます。

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	Google Cloud、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	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	データ分類によるDNS解決に使用される

3.9.55 以前に必要なネットワーク アクセス

NetApp Console、 NetApp Consoleエージェント、およびNetAppデータ サービスでは、必要なエンドポイントに接続するために、アウトバウンド インターネット アクセスが必要です。

このトピックでは、 NetApp Console標準モード 3.9.55 以下のバージョンに必要なネットワーク アクセスについて説明します。 4.0.0以降に必要なエンドポイントについては、"4.0.0 以降に必要なエンドポイント" 。

次のネットワーク アクセスを設定する必要があります。

- NetApp Consoleに SaaS (Software as a Service) としてアクセスするコンピュータ
- オンプレミスまたはクラウドにインストールするコンソール エージェント。

エンドポイント リストを **4.0.0** 以降の改訂リストに更新します。

バージョン 4.0.0 以降、コンソール エージェントに必要なエンドポイントが少なくなります。 4.0.0 より前の既存のデプロイメントは引き続きサポートされます。 4.0.0 以降にアップグレードした後、都合の良いときに古いエンドポイントを許可リストから削除できます。

NetApp、ファイアウォール ルールを更新して、サイズが小さく、より安全で、管理が容易な改訂版エンドポイント リストを使用することをお勧めします。 NetAppワイルドカード エントリの必要性がなくなり、エージェント アップグレードのエンドポイントはすべてのデータ サービスをサポートします。

3.9.55 以下のエンドポイント	**4.0.0** 以降のエンドポイント	目的
• https://support.netapp.com • https://mysupport.netapp.com	• https://mysupport.netapp.com • https://signin.b2c.netapp.com • https://support.netapp.com	ライセンスおよびNetAppサポートへの連絡について。
• https://*.api.bluexp.netapp.com • https://api.bluexp.netapp.com • https://*.cloudmanager.cloud.netapp.com • https://cloudmanager.cloud.netapp.com • https://netapp-cloud-account.auth0.com • https://netapp-cloud-account.us.auth0.com • https://console.netapp.com • https://*.console.netapp.com	• https://api.bluexp.netapp.com • https://netapp-cloud-account.auth0.com • https://netapp-cloud-account.us.auth0.com • https://console.netapp.com • https://components.console.netapp.com • https://cdn.auth0.com	日常業務用。
• https://*.blob.core.windows.net • https://cloudmanagerinfraprod.azurecr.io	• https://bluexpinfraprod.eastus2.data.azurecr.io • https://bluexpinfraprod.azurecr.io	コンソール エージェントのアップグレード用のイメージを取得します。

手順

1. エージェントのバージョンが 4.0.0 以上であることを確認します。"エージェントのバージョンを表示します。"
2. エンドポイントをホワイトリストに登録する"4.0.0 以降でサポートされているエンドポイント"。
3. 次のコマンドを実行して、各エージェントのサービス マネージャー 2 サービスを再起動します。

```
systemctl restart netapp-service-manager.service
```

4. 次のコマンドを実行し、エージェントのステータスが *active(running)* と表示されていることを確認します: _

```
systemctl status netapp-service-manager.service
```

5. ファイアウォールの許可リストから古いエンドポイントを削除します。

NetApp Consoleおよびコンソール エージェント 3.9.55 以前のエンドポイント

これらのエンドポイントは、コンソール エージェント 3.9.55 以下に使用されます。

エンドポイント	目的
https://support.netapp.com https://mysupport.netapp.com	ライセンス情報を取得し、 AutoSupportメッセージをNetAppサポートに送信します。
https://*.api.bluexp.netapp.com https://api.bluexp.netapp.com https://*.cloudmanager.cloud.netapp.com https://cloudmanager.cloud.netapp.com https://netapp-cloud-account.auth0.com https://netapp-cloud-account.us.auth0.com	NetApp Console内で機能とサービスを提供します。

エンドポイント	目的
次の 2 つのエンドポイント セットから選択します。 • オプション1（推奨） https://bluexpinfraprod.eastus2.data.azurecr.io https://bluexpinfraprod.azurecr.io • オプション2 https://*.blob.core.windows.net https://cloudmanagerinfraprod.azurecr.io	コンソール エージェントのアップグレード用のイメージを取得します。 NetApp、ランサムウェア耐性またはバックアップとリカバリを使用していない限り、より安全なオプション 1 のエンドポイントをファイアウォールで許可し、オプション 2 のエンドポイントを禁止することを推奨しています。これらのエンドポイントについては、次の点に注意してください。 • オプション 1 エンドポイントは 3.9.47 以降でサポートされます。 3.9.47 より前のリリースでは下位互換性がサポートされていません。 • コンソール エージェントは、まずオプション 2 のエンドポイントとの接続を開始します。これらのエンドポイントにアクセスできない場合は、オプション 1 のエンドポイントに自動的に接続します。 • コンソール エージェントをNetApp Backup and Recoveryまたは Ransomware Resilience と併用する場合、システムはオプション 1 のエンドポイントをサポートしません。オプション 2 のエンドポイントを許可し、オプション 1 を禁止します。

コンソールエージェントが接続するクラウドプロバイダーエンドポイント

コンソール エージェントがクラウド プロバイダーに展開されている場合、追加のエンドポイントにアクセスできる必要があります。

コンソール エージェントをインストールする前に、クラウド プロバイダーのエンドポイントへのアクセスを有効にします。

- "コンソールエージェントの AWS ネットワークアクセスを設定する"
- "コンソール エージェントの Azure ネットワーク アクセスを設定する"
- "コンソール エージェントの Google Cloud ネットワーク アクセスを設定する"

クラウド プロバイダーのエンドポイントはすべてのバージョンで同じです。

コンソールエージェントが接続するデータサービスエンドポイント

コンソール エージェントでは、一部のNetAppデータ サービスとCloud Volumes ONTAP をサポートするために、追加の送信インターネット アクセスが必要です。

Cloud Volumes ONTAPのエンドポイント

- "AWS のCloud Volumes ONTAPのエンドポイント"
- "Azure のCloud Volumes ONTAPのエンドポイント"

- "Google Cloud のCloud Volumes ONTAPのエンドポイント"

Amazon EC2 インスタンスで IMDSv2 の使用を必須にする

NetApp Consoleは、コンソール エージェントとCloud Volumes ONTAP (HA 展開のメディエーターを含む) を使用して、Amazon EC2 インスタンス メタデータ サービス バージョン 2 (IMDSv2) をサポートします。ほとんどの場合、IMDSv2 は新しい EC2 インスタンスで自動的に構成されます。 IMDSv1 は 2024 年 3 月より前に有効化されました。セキュリティ ポリシーで必要な場合は、EC2 インスタンスで IMDSv2 を手動で設定する必要がある場合があります。

開始する前に

- コンソール エージェントのバージョンは 3.9.38 以降である必要があります。
- Cloud Volumes ONTAP は次のいずれかのバージョンを実行している必要があります。
  - 9.12.1 P2（またはそれ以降のパッチ）
  - 9.13.0 P4（またはそれ以降のパッチ）
  - 9.13.1 またはこのリリース以降のバージョン
- この変更を行うには、Cloud Volumes ONTAPインスタンスを再起動する必要があります。
- これらの手順では、応答ホップ制限を 3 に変更する必要があるため、AWS CLI を使用する必要があります。

タスク概要

IMDSv2 は脆弱性に対する保護を強化します。 "IMDSv2 の詳細については、AWS セキュリティブログをご覧ください。"

インスタンス メタデータ サービス (IMDS) は、EC2 インスタンスで次のように有効化されます。

- コンソールから、またはコンソールを使用して新しいコンソールエージェントを展開する場合 "Terraform スクリプト"、IMDSv2 は EC2 インスタンスでデフォルトで有効になっています。
- AWS で新しい EC2 インスタンスを起動し、コンソールエージェントソフトウェアを手動でインストールすると、IMDSv2 もデフォルトで有効になります。
- AWS Marketplace からコンソールエージェントを起動すると、IMDSv1 がデフォルトで有効になります。EC2 インスタンスで IMDSv2 を手動で設定できます。
- 既存のコンソールエージェントの場合、IMDSv1 は引き続きサポートされますが、必要に応じて EC2 インスタンスで IMDSv2 を手動で設定することもできます。
- Cloud Volumes ONTAPの場合、新規インスタンスと既存インスタンスで IMDSv1 がデフォルトで有効になっています。必要に応じて、EC2 インスタンスで IMDSv2 を手動で設定することもできます。

手順

1. コンソール エージェント インスタンスで IMDSv2 の使用を必須にします。

   a. コンソール エージェントの Linux VM に接続します。

      AWS でコンソール エージェント インスタンスを作成したときに、AWS アクセス キーとシークレット キーを指定しました。このキー ペアを使用してインスタンスに SSH 接続できます。 EC2 Linux イ

ンスタンスのユーザー名は ubuntu です (2023 年 5 月より前に作成されたコンソールエージェントの場合、ユーザー名は ec2-user でした)。

"AWS ドキュメント: Linux インスタンスに接続する"

b. AWS CLI をインストールします。

"AWS ドキュメント: AWS CLI の最新バージョンをインストールまたは更新する"

c. 使用 `aws ec2 modify-instance-metadata-options`IMDSv2 の使用を必須にし、PUT 応答のホップ制限を 3 に変更するコマンド。

例

```
aws ec2 modify-instance-metadata-options \
    --instance-id <instance-id> \
    --http-put-response-hop-limit 3 \
    --http-tokens required \
    --http-endpoint enabled
```

+

その `http-tokens`パラメータは IMDSv2 を必須に設定します。いつ `http-tokens`必須の場合は、 `http-endpoint`有効にします。

2. Cloud Volumes ONTAPインスタンスで IMDSv2 の使用を必須にします。
   a. に行く "Amazon EC2 コンソール"
   b. ナビゲーション ペインから、[インスタンス] を選択します。
   c. Cloud Volumes ONTAPインスタンスを選択します。
   d. *アクション > インスタンス設定 > インスタンスメタデータオプションの変更*を選択します。
   e. インスタンス メタデータ オプションの変更 ダイアログ ボックスで、以下を選択します。
      - インスタンス メタデータ サービス の場合は、有効 を選択します。
      - *IMDSv2*の場合は*必須*を選択します。
      - *保存*を選択します。
   f. HA メディエーターを含む他のCloud Volumes ONTAPインスタンスに対しても、これらの手順を繰り返します。
   g. "Cloud Volumes ONTAPインスタンスを停止して起動する"

結果

コンソール エージェント インスタンスとCloud Volumes ONTAPインスタンスが IMDSv2 を使用するように構成されました。

コンソールエージェントのデフォルト構成

AWS、Azure、Google Cloud 全体の標準展開（インターネット アクセスあり）とオンプレミス環境の制限付き展開（インターネット アクセスなし）のコンソール エージェントのデフォルト構成について説明します。

インターネットアクセスを備えたデフォルト構成

次の構成の詳細は、 NetApp Consoleから、クラウド プロバイダーのマーケットプレイスからコンソール エージェントを展開した場合、またはインターネットにアクセスできるオンプレミスの Linux ホストにコンソール エージェントを手動でインストールした場合に適用されます。

AWS のコンソールエージェント **VM** の詳細

コンソールまたはクラウド プロバイダーのマーケットプレイスからコンソール エージェントを展開した場合は、次の点に注意してください。

- EC2 インスタンスタイプは t3.2xlarge です。
- イメージのオペレーティング システムは Ubuntu 22.04 LTS です。

  オペレーティング システムには GUI が含まれていません。システムにアクセスするには端末を使用する必要があります。

- インストールには、必要なコンテナ オーケストレーション ツールである Docker Engine が含まれます。
- EC2 Linux インスタンスのユーザー名は ubuntu です (2023 年 5 月より前に作成されたエージェントの場合、ユーザー名は ec2-user です)。
- デフォルトのシステム ディスクは 100 GiB gp2 ディスクです。

Azure のコンソール エージェント **VM** の詳細

コンソールまたはクラウド プロバイダーのマーケットプレイスからコンソール エージェントを展開した場合は、次の点に注意してください。

- VM タイプは Standard_D8s_v3 です。
- イメージのオペレーティング システムは Ubuntu 22.04 LTS です。

  オペレーティング システムには GUI が含まれていません。システムにアクセスするには端末を使用する必要があります。

- インストールには、必要なコンテナ オーケストレーション ツールである Docker Engine が含まれます。
- デフォルトのシステム ディスクは 100 GiB のプレミアム SSD ディスクです。

Google Cloud のコンソール エージェント **VM** の詳細

コンソールからコンソール エージェントを展開した場合は、次の点に注意してください。

- VM インスタンスは n2-standard-8 です。
- イメージのオペレーティング システムは Ubuntu 22.04 LTS です。

オペレーティング システムには GUI が含まれていません。システムにアクセスするには端末を使用する必要があります。

- インストールには、必要なコンテナ オーケストレーション ツールである Docker Engine が含まれます。
- デフォルトのシステム ディスクは 100 GiB の SSD 永続ディスクです。

インストールフォルダ

エージェントのインストール フォルダーは次の場所にあります。

`/opt/application/netapp/cloudmanager`

ログ ファイル

ログ ファイルは次のフォルダーに保存されます。

- `/opt/application/netapp/cloudmanager/log` または
- `/opt/application/netapp/service-manager-2/logs` (3.9.23 の新規インストールから開始)

  これらのフォルダー内のログには、コンソール エージェントに関する詳細が記録されます。

- `/opt/application/netapp/cloudmanager/docker_occm/data/log`

  このフォルダー内のログには、クラウド サービスと、コンソール エージェントで実行されるコンソール サービスに関する詳細が記録されます。

コンソールエージェントサービス

- コンソール エージェント サービスの名前は occm です。
- occm サービスは MySQL サービスに依存します。

  MySQL サービスがダウンしている場合は、occm サービスもダウンします。

ポート

エージェントは Linux ホスト上で次のポートを使用します。

- HTTPアクセスの場合は80
- HTTPSアクセスの場合は443

インターネットアクセスなしのデフォルト設定

インターネットにアクセスできないオンプレミスの Linux ホストにコンソール エージェントを手動でインストールした場合は、次の構成が適用されます。"このインストールオプションの詳細" 。

- エージェントのインストール フォルダーは次の場所にあります。

  `/opt/application/netapp/ds`

- ログ ファイルは次のフォルダーに保存されます。

  `/var/lib/docker/volumes/ds_occmdata/_data/log`

  このフォルダー内のログには、コンソール エージェントと Docker イメージに関する詳細が記録されます。

- すべてのサービスはDockerコンテナ内で実行されています

  サービスはdockerランタイムサービスの実行に依存しています

- エージェントは Linux ホスト上で次のポートを使用します。
  - HTTPアクセスの場合は80
  - HTTPSアクセスの場合は443