Référence

NetApp Console setup and administration

NetApp
February 11, 2026

Sommaire

Référence

Console de maintenance des agents

Validation de l'agent avec la console de maintenance

Vous pouvez utiliser la console de maintenance de l'agent Console pour valider l'installation et la configuration d'un agent Console.

Accéder à la console de maintenance de l'agent

Vous pouvez accéder à la console de maintenance à partir de l'hôte de l'agent de console. Accédez au répertoire suivant :

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

config-checker valider

Le `config-checker validate` Cette commande permet de valider la configuration d'un agent de console.

Paramètres

`--services <comma-separated list of services to validate>`**--REQUIS--**

Choisissez un ou plusieurs services à valider. Les noms de service valides sont :*`PLATFORM` qui valide la connectivité réseau aux points de terminaison de la console requis.

`--validationTypes <comma-separated list validation types to run>`**--OBLIGATOIRE--** Choisissez un ou plusieurs types de validation à exécuter. Les types de validation valides sont : * `NETWORK` qui valide la connectivité réseau aux points de terminaison de la console requis.

`--proxy <url>`**--FACULTATIF--**

Spécifie l'URL du serveur proxy à utiliser pour la validation. Requis si votre agent est configuré pour utiliser un serveur proxy.

`--certs <paths>`**--FACULTATIF--**

Spécifie le chemin d'accès à un ou plusieurs fichiers de certificat à utiliser pour la validation. Les fichiers de certificat doivent être au format PEM. Séparez les chemins multiples par des virgules. Ce paramètre est requis si votre agent utilise un certificat personnalisé.

Exemples de validation du vérificateur de configuration

Validation de base :

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

Validation lorsqu'un serveur proxy est utilisé pour l'agent :

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

Validation lorsqu'un certificat est utilisé pour l'agent :

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

Afficher l'aide pour n'importe quelle commande

Pour afficher l'aide d'une commande, ajoutez `--help` à la commande. Par exemple, pour afficher l'aide relative à la `proxy add` commande, utilisez la commande suivante :

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

Commandes proxy transparentes

Vous pouvez utiliser la console de maintenance de l'agent de console pour configurer un agent de console afin d'utiliser un serveur proxy transparent.

Accéder à la console de maintenance de l'agent

Vous pouvez accéder à la console de maintenance à partir de l'hôte de l'agent de console. Accédez au répertoire suivant :

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

Afficher l'aide pour n'importe quelle commande

Pour afficher l'aide d'une commande, ajoutez `--help` à la commande. Par exemple, pour afficher l'aide relative à la `proxy add` commande, utilisez la commande suivante :

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

proxy obtenir

Le `proxy get` Cette commande affiche des informations sur la configuration actuelle du serveur proxy transparent. Pour afficher la configuration actuelle du serveur proxy transparent, utilisez la commande suivante :

Exemple de proxy get

Pour afficher la configuration actuelle du serveur proxy transparent, utilisez la commande suivante :

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

ajouter un proxy

Le `proxy add` Cette commande configure l'agent pour utiliser un serveur proxy transparent.

Paramètres

`-c <certificate file>`

Spécifie le chemin d'accès au fichier de certificat du serveur proxy. Le fichier de certificat doit être au format PEM. Assurez-vous que le fichier de certificat se trouve dans le même répertoire que la commande ou spécifiez le chemin d'accès complet au fichier de certificat.

Exemple d'ajout de proxy

Pour ajouter un serveur proxy transparent, utilisez la commande suivante, où `/home/ubuntu/myCA1.pem` est le chemin d'accès au fichier de certificat pour le serveur proxy. Le fichier de certificat doit être au format PEM :

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

mise à jour du proxy

Le `proxy update` Cette commande permet de mettre à jour le certificat d'un proxy transparent.

Paramètres

`-c <certificate file>`spécifie le chemin d'accès au fichier de certificat du serveur proxy. Le fichier de certificat doit être au format PEM.

Assurez-vous que le fichier de certificat se trouve dans le même répertoire que la commande ou spécifiez le chemin d'accès complet au fichier de certificat.

Exemple de mise à jour de proxy

Pour mettre à jour le certificat d'un serveur proxy transparent, utilisez la commande suivante, où `/home/ubuntu/myCA1.pem` est le chemin vers le nouveau fichier de certificat pour le serveur proxy. Le fichier de certificat doit être au format PEM :

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

suppression du proxy

Le `proxy remove` Cette commande supprime la configuration du serveur proxy transparent de l'agent.

Exemple de suppression de proxy

Pour supprimer le serveur proxy transparent, utilisez la commande suivante :

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

exigences relatives aux autorisations et au réseau de l'agent du fournisseur de cloud

Résumé des autorisations pour la NetApp Console

Vous devrez accorder à l'agent de la console les autorisations appropriées pour qu'il puisse effectuer des opérations dans votre environnement cloud. Utilisez les liens de cette page pour accéder rapidement aux autorisations dont vous avez besoin en fonction de votre objectif.

Autorisations AWS

La NetApp Console nécessite des autorisations AWS pour un agent de console et pour des services individuels.

Agents de console

But	Description	Lien
Déployer un agent de console depuis la console Pour déployer un agent de console dans AWS, l'utilisateur a besoin d'autorisations spécifiques.	"Configurer les autorisations AWS"	Fournir des autorisations pour un agent de console

NetApp Backup and Recovery

But	Description	Lien
Sauvegardez les clusters ONTAP sur site sur Amazon S3 avec NetApp Backup and Recovery	Lors de l'activation des sauvegardes sur vos volumes ONTAP , NetApp Backup and Recovery vous invite à saisir une clé d'accès et un secret pour un utilisateur IAM disposant d'autorisations spécifiques.	"Configurer les autorisations S3 pour les sauvegardes"

Cloud Volumes ONTAP

But	Description	Lien
Fournir des autorisations pour les nœuds Cloud Volumes ONTAP	Un rôle IAM doit être attaché à chaque nœud Cloud Volumes ONTAP dans AWS. Il en va de même pour le médiateur HA. L'option par défaut consiste à laisser la console créer les rôles IAM pour vous, mais vous pouvez utiliser les vôtres lors de la création du système dans la console.	"Apprenez à configurer vous-même les rôles IAM"

NetApp Copy and Sync

But	Description	Lien
Déployer le courtier de données dans AWS	Le compte utilisateur AWS que vous utilisez pour déployer le courtier de données doit disposer des autorisations nécessaires.	"Autorisations requises pour déployer le courtier de données dans AWS"
Fournir des autorisations au courtier de données	Lorsque NetApp Copy and Sync déploie le courtier de données, il crée un rôle IAM pour l'instance du courtier de données. Vous pouvez déployer le courtier de données à l'aide de votre propre rôle IAM, si vous préférez.	"Conditions requises pour utiliser votre propre rôle IAM avec le courtier de données AWS"
Activer l'accès AWS pour un courtier de données installé manuellement	Si vous utilisez le courtier de données avec une relation de synchronisation qui inclut un bucket S3, vous devez préparer l'hôte Linux pour l'accès AWS. Lorsque vous installez le courtier de données, vous devez fournir des clés AWS pour un utilisateur IAM disposant d'un accès programmatique et d'autorisations spécifiques.	"Activation de l'accès à AWS"

FSx pour ONTAP

But	Description	Lien
Créer et gérer FSx pour ONTAP	Pour créer ou gérer un système Amazon FSx for NetApp ONTAP , vous devez ajouter des informations d'identification AWS à la console en fournissant l'ARN d'un rôle IAM qui donne à la console les autorisations nécessaires.	"Découvrez comment configurer les informations d'identification AWS pour FSx"

NetApp Cloud Tiering

But	Description	Lien
Hiérarchiser les clusters ONTAP sur site vers Amazon S3	Lorsque vous activez NetApp Cloud Tiering pour AWS, vous devez saisir une clé d'accès et une clé secrète. Ces informations d'identification sont transmises au cluster ONTAP afin ONTAP puisse hiérarchiser les données vers le compartiment S3.	"Configurer les autorisations S3 pour la hiérarchisation"

Autorisations Azure

La console nécessite des autorisations Azure pour un agent de console et pour des services individuels.

Agent de console

But	Description	Lien
Déployer un agent de console à partir de la console	Lorsque vous déployez un agent de console à partir de la console, vous devez utiliser un compte Azure ou un principal de service disposant des autorisations nécessaires pour déployer une machine virtuelle d'agent de console dans Azure.	"Configurer les autorisations Azure"
Fournir des autorisations pour un agent de console	Lorsque la console déploie une machine virtuelle d'agent de console dans Azure, elle crée un rôle personnalisé qui fournit les autorisations requises pour gérer les ressources et les processus au sein de cet abonnement Azure. Vous devez configurer vous-même le rôle personnalisé si vous lancez un agent de console à partir de la place de marché, si vous installez manuellement un agent de console ou si vous"ajouter plus d'informations d'identification Azure à un agent de console" . Maintenez cette politique à jour à mesure que de nouvelles autorisations sont ajoutées dans les versions ultérieures.	"Autorisations Azure pour un agent de console"

NetApp Backup and Recovery

But	Description	Lien
Sauvegarder Cloud Volumes ONTAP sur le stockage blob Azure	Lorsque vous utilisez NetApp Backup and Recovery pour sauvegarder Cloud Volumes ONTAP, vous devez ajouter des autorisations à un agent de console dans les scénarios suivants : • Vous souhaitez utiliser la fonctionnalité « Rechercher et restaurer » • Vous souhaitez utiliser des clés de chiffrement gérées par le client (CMEK)	• "Sauvegardez les données Cloud Volumes ONTAP sur le stockage Azure Blob avec Backup and Recovery"
Sauvegarder les clusters ONTAP locaux sur le stockage blob Azure	Lorsque vous utilisez NetApp Backup and Recovery pour sauvegarder des clusters ONTAP sur site, vous devez ajouter des autorisations à un agent de console pour utiliser la fonctionnalité « Recherche et restauration ».	"Sauvegardez les données ONTAP locales sur le stockage Azure Blob avec Backup and Recovery"

Copie et synchronisation NetApp

But	Description	Lien
Déployer le courtier de données dans Azure	Le compte d'utilisateur Azure que vous utilisez pour déployer le courtier de données doit disposer des autorisations requises.	"Autorisations requises pour déployer le courtier de données dans Azure"

Autorisations Google Cloud

La console nécessite des autorisations Google Cloud pour un agent de console et pour des services individuels.

Agents de console

But	Description	Lien
Déployer un agent de console à partir de la console	L'utilisateur Google Cloud qui déploie un agent de console à partir de la console a besoin d'autorisations spécifiques pour déployer un agent de console dans Google Cloud.	"Configurer les autorisations pour créer un agent de console"
Fournir des autorisations pour un agent de console	Le compte de service d'un agent Console doit disposer d'autorisations spécifiques pour les opérations quotidiennes. Vous devez associer le compte de service à un agent de console lors du déploiement. Maintenez cette politique à jour à mesure que de nouvelles autorisations sont ajoutées dans les versions ultérieures.	"Configurer les autorisations pour un agent de console"

NetApp Backup and Recovery

But	Description	Lien
Sauvegarder Cloud Volumes ONTAP sur Google Cloud	Lorsque vous utilisez NetApp Backup and Recovery pour sauvegarder Cloud Volumes ONTAP, vous devez ajouter des autorisations à un agent de console dans les scénarios suivants : • Vous souhaitez utiliser la fonctionnalité « Rechercher et restaurer » • Vous souhaitez utiliser des clés de chiffrement gérées par le client (CMEK)	• "Sauvegardez les données Cloud Volumes ONTAP sur Google Cloud Storage avec Backup and Recovery" • "Autorisations pour les CMEK"
Sauvegarder les clusters ONTAP sur site sur Google Cloud	Lorsque vous utilisez NetApp Backup and Recovery pour sauvegarder des clusters ONTAP sur site, vous devez ajouter des autorisations à un agent de console pour utiliser la fonctionnalité « Recherche et restauration ».	"Sauvegardez les données ONTAP sur site sur Google Cloud Storage avec Backup and Recovery"

NetApp Copy and Sync

But	Description	Lien
Déployer le courtier de données dans Google Cloud	Assurez-vous que l'utilisateur Google Cloud qui déploie le courtier de données dispose des autorisations requises.	"Autorisations requises pour déployer le courtier de données dans Google Cloud"

But	Description	Lien
Activer l'accès à Google Cloud pour un courtier de données installé manuellement	Si vous prévoyez d'utiliser le courtier de données avec une relation de synchronisation qui inclut un bucket Google Cloud Storage, vous devez préparer l'hôte Linux pour l'accès à Google Cloud. Lorsque vous installez le courtier de données, vous devez fournir une clé pour un compte de service disposant d'autorisations spécifiques.	"Activation de l'accès à Google Cloud"

Autorisations StorageGRID

La console nécessite des autorisations StorageGRID pour deux services.

NetApp Backup and Recovery

But	Description	Lien
Sauvegarder les clusters ONTAP sur site sur StorageGRID	Lorsque vous préparez StorageGRID comme cible de sauvegarde pour les clusters ONTAP , NetApp Backup and Recovery vous invite à saisir une clé d'accès et un secret pour un utilisateur IAM disposant d'autorisations spécifiques.	"Préparez StorageGRID comme cible de sauvegarde"

NetApp Cloud Tiering

But	Description	Lien
Hiérarchiser les clusters ONTAP sur site vers StorageGRID	Lorsque vous configurez NetApp Cloud Tiering sur StorageGRID, vous devez fournir à Cloud Tiering une clé d'accès S3 et une clé secrète. La hiérarchisation du cloud utilise les clés pour accéder à vos buckets.	"Préparer la hiérarchisation vers StorageGRID"

Autorisations et règles de sécurité de l'agent AWS

Autorisations AWS pour l'agent de la console

Lorsque la NetApp Console lance un agent de console dans AWS, elle attache une stratégie à l'agent qui fournit à l'agent des autorisations pour gérer les ressources et les processus au sein de ce compte AWS. L'agent utilise les autorisations pour effectuer des appels d'API vers plusieurs services AWS, notamment EC2, S3, CloudFormation, IAM, le service de gestion de clés (KMS), etc.

Politiques IAM

Les stratégies IAM disponibles ci-dessous fournissent les autorisations dont un agent de console a besoin pour gérer les ressources et les processus au sein de votre environnement de cloud public en fonction de votre région AWS.

Notez ce qui suit :

- Si vous créez un agent Console dans une région AWS standard directement depuis la Console, celle-ci applique automatiquement les politiques à l'agent.
- Vous devez configurer les stratégies vous-même si vous déployez l'agent à partir d'AWS Marketplace, si

vous installez manuellement l'agent sur un hôte Linux ou si vous souhaitez ajouter des informations d'identification AWS supplémentaires à la console.

- Dans les deux cas, vous devez vous assurer que les politiques sont à jour à mesure que de nouvelles autorisations sont ajoutées dans les versions ultérieures. Si de nouvelles autorisations sont requises, elles seront répertoriées dans les notes de version.
- Si nécessaire, vous pouvez restreindre les politiques IAM en utilisant l'IAM `Condition` élément. "Documentation AWS : élément de condition"
- Pour consulter les instructions étape par étape pour utiliser ces politiques, reportez-vous aux pages suivantes :
  - "Configurer les autorisations pour un déploiement AWS Marketplace"
  - "Configurer les autorisations pour les déploiements sur site"
  - "Configurer les autorisations pour le mode restreint"

Sélectionnez votre région pour afficher les politiques requises :

Régions standard

Pour les régions standard, les autorisations sont réparties sur deux politiques. Deux politiques sont requises en raison d'une limite de taille maximale de caractères pour les politiques gérées dans AWS.

Politique n°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: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"
    }
  ]
}
```

Politique n° 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"
    }
  ]
}
```

Régions GovCloud (États-Unis)

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

Régions secrètes

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

Régions top secrètes

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

Comment les autorisations AWS sont utilisées

Les sections suivantes décrivent comment les autorisations sont utilisées pour chaque service de gestion ou de données de la NetApp Console . Ces informations peuvent être utiles si les politiques de votre entreprise stipulent que les autorisations ne sont accordées qu'en cas de besoin.

Amazon FSx pour ONTAP

L'agent de console effectue les requêtes API suivantes pour gérer un système de fichiers Amazon FSx for ONTAP :

- ec2 : Décrire les instances
- ec2 : Décrire l'état de l'instance
- ec2 : Décrire l'attribut d'instance
- ec2 : Décrire les tables d'itinéraires
- ec2:Décrire les images
- ec2:Créer des balises
- ec2 : Décrire les volumes
- ec2 : Décrire les groupes de sécurité
- ec2 : Décrire les interfaces réseau
- ec2 : Décrire les sous-réseaux

- ec2 : Décrire les Vpcs
- ec2 : Décrire les options DHCP
- ec2 : Décrire les instantanés
- ec2 : Décrire les paires de clés
- ec2 : Décrire les régions
- ec2:Décrire les balises
- ec2 : Décrire les associations de profils d'instance Iam
- ec2 : Décrire les offres d'instances réservées
- ec2 : Décrire les points de terminaison Vpc
- ec2 : Décrire les Vpcs
- ec2 : Décrire les modifications des volumes
- ec2 : Décrire les groupes de placement
- kms:Créer une subvention
- kms:ListeAliases
- fsx:Décrire*
- fsx:Liste*

Découverte de compartiment Amazon S3

L'agent de la console effectue la demande d'API suivante pour découvrir les compartiments Amazon S3 :

s3 : Obtenir la configuration du chiffrement

NetApp Backup and Recovery

L'agent effectue les requêtes API suivantes pour gérer les sauvegardes dans Amazon S3 :

- s3 : Obtenir l'emplacement du bucket
- s3 : ListeTousMesSeaux
- s3:ListBucket
- s3:Créer un bucket
- s3 : Obtenir la configuration du cycle de vie
- s3 : PutLifecycleConfiguration
- s3 : Mettre en place le balisage du bucket
- s3 : ListBucketVersions
- s3 : Obtenir l'Acl du bucket
- s3 : PutBucketPublicAccessBlock
- s3:Obtenir l'objet
- ec2 : Décrire les points de terminaison Vpc
- kms:ListeAliases
- s3 : PutEncryptionConfiguration

L’agent effectue les requêtes API suivantes lorsque vous utilisez la méthode Rechercher et restaurer pour restaurer des volumes et des fichiers :

- s3:Créer un bucket
- s3:Supprimer l’objet
- s3 : Supprimer la version de l’objet
- s3 : Obtenir l’Acl du bucket
- s3:ListBucket
- s3 : ListBucketVersions
- s3 : ListBucketMultipartUploads
- s3:PutObject
- s3:PutBucketAcl
- s3 : PutLifecycleConfiguration
- s3 : PutBucketPublicAccessBlock
- s3 : Abandonner le téléchargement en plusieurs parties
- s3 : ListeMultipartUploadParts

L’agent effectue les requêtes API suivantes lorsque vous utilisez DataLock et NetApp Ransomware Resilience pour vos sauvegardes de volume :

- s3 : Obtenir le balisage de la version de l’objet
- s3 : GetBucketObjectLockConfiguration
- s3 : ObtenirObjectVersionAcl
- s3 : Mettre en place un balisage d’objet
- s3:Supprimer l’objet
- s3 : Supprimer le balisage d’objet
- s3 : Obtenir la rétention d’objet
- s3 : Supprimer le balisage de version d’objet
- s3:PutObject
- s3:Obtenir l’objet
- s3 : PutBucketObjectLockConfiguration
- s3 : Obtenir la configuration du cycle de vie
- s3 : ListBucketByTags
- s3 : Obtenir le balisage du bucket
- s3 : Supprimer la version de l’objet
- s3 : ListBucketVersions
- s3:ListBucket
- s3 : Mettre en place le balisage du bucket
- s3 : Obtenir le balisage des objets
- s3 : PutBucketVersioning

- s3 : Mettre en place la version de l'objet
- s3 : Obtenir la gestion des versions du bucket
- s3 : Obtenir l'Acl du bucket
- s3 : Contournement de la gouvernance et de la rétention
- s3 : PutObjectRetention
- s3 : Obtenir l'emplacement du bucket
- s3 : Obtenir la version de l'objet

L'agent effectue les requêtes API suivantes si vous utilisez un compte AWS différent pour vos sauvegardes Cloud Volumes ONTAP de celui que vous utilisez pour les volumes sources :

- s3 : PutBucketPolicy
- s3 : PutBucketOwnershipControls

Autorisations héritées pour la sauvegarde et la récupération

Vous n'avez besoin des autorisations suivantes que si vous avez activé les fonctionnalités d'indexation héritées avant la sortie de l'indexation v2 :

- kms:Liste*
- kms:Décrire*
- athena:Démarrer l'exécution de la requête
- athéna:Obtenir les résultats de la requête
- athéna:GetQueryExecution
- athena:StopQueryExecution
- colle:Créer une base de données
- colle:Créer une table
- colle:Suppression par lots de partitions

Classification

L'agent effectue les requêtes API suivantes pour déployer la NetApp Data Classification:

- ec2 : Décrire les instances
- ec2 : Décrire l'état de l'instance
- ec2 : Exécuter les instances
- ec2 : Terminer les instances
- ec2:Créer des balises
- ec2:Créer un volume
- ec2:AttachVolume
- ec2 : Créer un groupe de sécurité
- ec2 : Supprimer le groupe de sécurité
- ec2 : Décrire les groupes de sécurité

- ec2 : Créer une interface réseau
- ec2 : Décrire les interfaces réseau
- ec2 : Supprimer l'interface réseau
- ec2 : Décrire les sous-réseaux
- ec2 : Décrire les Vpcs
- ec2:Créer un instantané
- ec2 : Décrire les régions
- cloudformation:Créer une pile
- cloudformation:Supprimer la pile
- cloudformation:DescribeStacks
- cloudformation:Décrire les événements de pile
- iam:Ajouter un rôle au profil d'instance
- ec2 : AssociateIamInstanceProfile
- ec2 : Décrire les associations de profils d'instance Iam

L'agent effectue les requêtes API suivantes pour analyser les compartiments S3 lorsque vous utilisez la NetApp Data Classification:

- iam:Ajouter un rôle au profil d'instance
- ec2 : AssociateIamInstanceProfile
- ec2 : Décrire les associations de profils d'instance Iam
- s3 : Obtenir le balisage du bucket
- s3 : Obtenir l'emplacement du bucket
- s3 : ListeTousMesSeaux
- s3:ListBucket
- s3 : Obtenir l'état de la politique du bucket
- s3 : Obtenir la politique du bucket
- s3 : Obtenir l'Acl du bucket
- s3:Obtenir l'objet
- je suis:GetRole
- s3:Supprimer l'objet
- s3 : Supprimer la version de l'objet
- s3:PutObject
- sts:Assumer le rôle

Cloud Volumes ONTAP

L'agent effectue les requêtes API suivantes pour déployer et gérer Cloud Volumes ONTAP dans AWS.

But	Action	Utilisé pour le déploiement ?	Utilisé pour les opérations quotidiennes ?	Utilisé pour la suppression ?
Créer et gérer des rôles IAM et des profils d'instance pour les instances Cloud Volumes ONTAP	iam:ListInstanceProfiles	Oui	Oui	Non
	je suis:Créer un rôle	Oui	Non	Non
	iam:Supprimer le rôle	Non	Oui	Oui
	je suis:PutRolePolicy	Oui	Non	Non
	iam:Créer un profil d'instance	Oui	Non	Non
	iam:Supprimer la politique de rôle	Non	Oui	Oui
	iam:Ajouter un rôle au profil d'instance	Oui	Non	Non
	iam:Supprimer le rôle du profil d'instance	Non	Oui	Oui
	iam:Supprimer le profil d'instance	Non	Oui	Oui
	je suis:PassRole	Oui	Non	Non
	ec2 : AssociateIamInstanceProfile	Oui	Oui	Non
	ec2 : Décrire les associations de profils d'instance Iam	Oui	Oui	Non
	ec2 : Dissocier le profil d'instance Iam	Non	Oui	Non
Décoder les messages d'état d'autorisation	sts:Décoder le message d'autorisation	Oui	Oui	Non
Décrivez les images spécifiées (AMI) disponibles pour le compte	ec2:Décrire les images	Oui	Oui	Non
Décrire les tables de routage dans un VPC (requis pour les paires HA uniquement)	ec2 : Décrire les tables d'itinéraires	Oui	Non	Non

But	Action	Utilisé pour le déploiement ?	Utilisé pour les opérations quotidiennes ?	Utilisé pour la suppression ?
Arrêter, démarrer et surveiller les instances	ec2 : StartInstances	Oui	Oui	Non
	ec2 : StopInstances	Oui	Oui	Non
	ec2 : Décrire les instances	Oui	Oui	Non
	ec2 : Décrire l'état de l'instance	Oui	Oui	Non
	ec2 : Exécuter les instances	Oui	Non	Non
	ec2 : Terminer les instances	Non	Non	Oui
	ec2 : Modifier l'attribut d'instance	Non	Oui	Non
Vérifiez que la mise en réseau améliorée est activée pour les types d'instances pris en charge	ec2 : Décrire l'attribut d'instance	Non	Oui	Non
Étiquetez les ressources avec les balises « WorkingEnvironment » et « WorkingEnvironmentId » qui sont utilisées pour la maintenance et l'allocation des coûts	ec2:Créer des balises	Oui	Oui	Non
Gérer les volumes EBS que Cloud Volumes ONTAP utilise comme stockage backend	ec2:Créer un volume	Oui	Oui	Non
	ec2 : Décrire les volumes	Oui	Oui	Oui
	ec2 : Modifier l'attribut de volume	Non	Oui	Oui
	ec2:AttachVolume	Oui	Oui	Non
	ec2:SupprimerVolume	Non	Oui	Oui
	ec2 : DétacherVolume	Non	Oui	Oui

But	Action	Utilisé pour le déploiement ?	Utilisé pour les opérations quotidiennes ?	Utilisé pour la suppression ?
Créer et gérer des groupes de sécurité pour Cloud Volumes ONTAP	ec2 : Créer un groupe de sécurité	Oui	Non	Non
	ec2 : Supprimer le groupe de sécurité	Non	Oui	Oui
	ec2 : Décrire les groupes de sécurité	Oui	Oui	Oui
	ec2 : RévoquerSecurityGroupEgress	Oui	Non	Non
	ec2 : Autoriser la sortie du groupe de sécurité	Oui	Non	Non
	ec2 : Autoriser l'entrée du groupe de sécurité	Oui	Non	Non
	ec2 : Révoquer l'entrée du groupe de sécurité	Oui	Oui	Non
Créer et gérer des interfaces réseau pour Cloud Volumes ONTAP dans le sous-réseau cible	ec2 : Créer une interface réseau	Oui	Non	Non
	ec2 : Décrire les interfaces réseau	Oui	Oui	Non
	ec2 : Supprimer l'interface réseau	Non	Oui	Oui
	ec2 : Modifier l'attribut d'interface réseau	Non	Oui	Non
Obtenir la liste des sous-réseaux de destination et des groupes de sécurité	ec2 : Décrire les sous-réseaux	Oui	Oui	Non
	ec2 : Décrire les Vpcs	Oui	Oui	Non
Obtenir les serveurs DNS et le nom de domaine par défaut pour les instances Cloud Volumes ONTAP	ec2 : Décrire les options DHCP	Oui	Non	Non

But	Action	Utilisé pour le déploiement ?	Utilisé pour les opérations quotidiennes ?	Utilisé pour la suppression ?
Prendre des instantanés des volumes EBS pour Cloud Volumes ONTAP	ec2:Créer un instantané	Oui	Oui	Non
	ec2 : Supprimer l'instantané	Non	Oui	Oui
	ec2 : Décrire les instantanés	Non	Oui	Non
Capturez la console Cloud Volumes ONTAP , qui est attachée aux messages AutoSupport	ec2 : Obtenir la sortie de la console	Oui	Oui	Non
Obtenir la liste des paires de clés disponibles	ec2 : Décrire les paires de clés	Oui	Non	Non
Obtenez la liste des régions AWS disponibles	ec2 : Décrire les régions	Oui	Oui	Non
Gérer les balises des ressources associées aux instances Cloud Volumes ONTAP	ec2:Supprimer les balises	Non	Oui	Oui
	ec2:Décrire les balises	Non	Oui	Non
Créer et gérer des piles pour les modèles AWS CloudFormation	cloudformation:Créer une pile	Oui	Non	Non
	cloudformation:Supprimer la pile	Oui	Non	Non
	cloudformation:DescribeStacks	Oui	Oui	Non
	cloudformation:Décrire les événements de pile	Oui	Non	Non
	cloudformation:Valider le modèle	Oui	Non	Non

But	Action	Utilisé pour le déploiement ?	Utilisé pour les opérations quotidiennes ?	Utilisé pour la suppression ?
Créer et gérer un compartiment S3 qu'un système Cloud Volumes ONTAP utilise comme niveau de capacité pour la hiérarchisation des données	s3:Créer un bucket	Oui	Oui	Non
	s3 : Supprimer le bucket	Non	Oui	Oui
	s3 : Obtenir la configuration du cycle de vie	Non	Oui	Non
	s3 : PutLifecycleConfiguration	Non	Oui	Non
	s3 : Mettre en place le balisage du bucket	Non	Oui	Non
	s3 : ListBucketVersions	Non	Oui	Non
	s3 : Obtenir l'état de la politique du bucket	Non	Oui	Non
	s3 : GetBucketPublicAccessBlock	Non	Oui	Non
	s3 : Obtenir l'Acl du bucket	Non	Oui	Non
	s3 : Obtenir la politique du bucket	Non	Oui	Non
	s3 : PutBucketPublicAccessBlock	Non	Oui	Non
	s3 : Obtenir le balisage du bucket	Non	Oui	Non
	s3 : Obtenir l'emplacement du bucket	Non	Oui	Non
	s3 : ListeTousMesSeaux	Non	Non	Non
	s3:ListBucket	Non	Oui	Non
Activer le chiffrement des données de Cloud Volumes ONTAP à l'aide d'AWS Key Management Service (KMS)	kms:ReEncrypt*	Oui	Non	Non
	kms:Créer une subvention	Oui	Oui	Non
	kms : générer une clé de données sans texte brut	Oui	Oui	Non

But	Action	Utilisé pour le déploiement ?	Utilisé pour les opérations quotidiennes ?	Utilisé pour la suppression ?
Créer et gérer un groupe de placement réparti AWS pour deux nœuds HA et le médiateur dans une seule zone de disponibilité AWS	ec2 : Créer un groupe de placement	Oui	Non	Non
	ec2 : Supprimer le groupe de placement	Non	Oui	Oui
Créer des rapports	fsx:Décrire*	Non	Oui	Non
	fsx:Liste*	Non	Oui	Non
Créer et gérer des agrégats prenant en charge la fonctionnalité Amazon EBS Elastic Volumes	ec2 : Décrire les modifications des volumes	Non	Oui	Non
	ec2:ModifierVolume	Non	Oui	Non
Vérifiez si la zone de disponibilité est une zone locale AWS et validez que tous les paramètres de déploiement sont compatibles	ec2 : Décrire les zones de disponibilité	Oui	Non	Oui

Journal des modifications

Au fur et à mesure que des autorisations sont ajoutées et supprimées, nous les noterons dans les sections ci-dessous.

11 novembre 2025

Les autorisations suivantes ne sont plus requises pour NetApp Backup and Recovery, sauf si vous utilisez l'indexation héritée. Ces autorisations ont été supprimées des politiques figurant sur cette page :

- kms:Liste*
- kms:Décrire*
- athena:Démarrer l'exécution de la requête
- athéna:Obtenir les résultats de la requête
- athéna:GetQueryExecution
- athena:StopQueryExecution
- colle:Créer une base de données
- colle:Créer une table
- colle:Suppression par lots de partitions

9 septembre 2024

Les autorisations ont été supprimées de la politique n° 2 pour les régions standard, car la NetApp Console ne prend plus en charge la mise en cache de périphérie NetApp , la découverte et la gestion des clusters Kubernetes.

Afficher les autorisations qui ont été supprimées de la politique

```
{
    "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"
}
```

9 mai 2024

L'autorisation suivante est désormais requise pour Cloud Volumes ONTAP:

ec2 : Décrire les zones de disponibilité

6 juin 2023

L'autorisation suivante est désormais requise pour Cloud Volumes ONTAP:

kms : générer une clé de données sans texte brut

14 février 2023

L'autorisation suivante est désormais requise pour NetApp Cloud Tiering:

ec2 : Décrire les points de terminaison Vpc

Règles du groupe de sécurité de l'agent de console dans AWS

Le groupe de sécurité AWS pour l'agent nécessite des règles entrantes et sortantes. La NetApp Console crée automatiquement ce groupe de sécurité lorsque vous créez un agent de console à partir de la console. Vous devez configurer ce groupe de sécurité pour toutes les autres options d'installation.

Règles entrantes

Protocole	Port	But
SSH	22	Fournit un accès SSH à l'hôte de l'agent
HTTP	80	• Fournit un accès HTTP depuis les navigateurs Web clients vers l'interface utilisateur locale • Utilisé pendant le processus de mise à niveau de Cloud Volumes ONTAP
HTTPS	443	Fournit un accès HTTPS à l'interface utilisateur locale et aux connexions à partir de l'instance de NetApp Data Classification
TCP	3128	Fournit à Cloud Volumes ONTAP un accès Internet. Vous devez ouvrir manuellement ce port après le déploiement.

Règles de sortie

Le groupe de sécurité prédéfini pour l'agent ouvre tout le trafic sortant. Si cela est acceptable, suivez les règles de sortie de base. Si vous avez besoin de règles plus rigides, utilisez les règles sortantes avancées.

Règles de base pour les voyages sortants

Le groupe de sécurité prédéfini pour l'agent inclut les règles sortantes suivantes.

Protocole	Port	But
Tous les TCP	Tous	Tout le trafic sortant
Tout UDP	Tous	Tout le trafic sortant

Règles sortantes avancées

Si vous avez besoin de règles rigides pour le trafic sortant, vous pouvez utiliser les informations suivantes pour ouvrir uniquement les ports requis pour la communication sortante par l'agent

L'adresse IP source est l'hôte de l'agent.

Service	Protocole	Port	Destination	But
Appels API et AutoSupport	HTTPS	443	Gestion de cluster Internet sortant et ONTAP LIF	Appels d'API vers AWS, ONTAP, NetApp Data Classification et envoi de messages AutoSupport à NetApp
Appels d'API	TCP	3000	Médiateur ONTAP HA	Communication avec le médiateur ONTAP HA
	TCP	8080	Classification des données	Sonder l'instance de classification des données pendant le déploiement
DNS	UDP	53	DNS	Utilisé pour la résolution DNS par la console

Autorisations Azure et règles de sécurité requises

Autorisations Azure pour l'agent de console

Lorsque la NetApp Console lance un agent de console dans Azure, elle attache un rôle personnalisé à la machine virtuelle qui fournit à l'agent des autorisations pour gérer les ressources et les processus au sein de cet abonnement Azure. L'agent utilise les autorisations pour effectuer des appels d'API vers plusieurs services Azure.

La nécessité ou non de créer ce rôle personnalisé pour l'agent dépend de la manière dont vous l'avez déployé.

Déploiement à partir de la NetApp Console

Lorsque vous utilisez la console pour déployer la machine virtuelle de l'agent dans Azure, cela active une "identité gérée attribuée par le système" sur la machine virtuelle, crée un rôle personnalisé et l'attribue à la machine virtuelle. Le rôle fournit à la console les autorisations requises pour gérer les ressources et les processus au sein de cet abonnement Azure. Les autorisations du rôle sont maintenues à jour lorsque l'agent est mis à niveau. Vous n'avez pas besoin de créer ce rôle pour l'agent ni de gérer les mises à jour.

Déploiement manuel ou à partir de la place de marché Azure

Lorsque vous déployez l'agent à partir d'Azure Marketplace ou si vous installez manuellement l'agent sur un hôte Linux, vous devez configurer vous-même le rôle personnalisé et conserver ses autorisations avec toutes les modifications.

Vous devrez vous assurer que le rôle est à jour à mesure que de nouvelles autorisations sont ajoutées dans

les versions ultérieures. Si de nouvelles autorisations sont requises, elles seront répertoriées dans les notes de version.

- Pour consulter les instructions étape par étape pour utiliser ces politiques, reportez-vous aux pages suivantes :
  - "Configurer les autorisations pour un déploiement Azure Marketplace"
  - "Configurer les autorisations pour les déploiements sur site"
  - "Configurer les autorisations pour le mode restreint"

```
{
  "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"
}
```

Comment les autorisations Azure sont utilisées

Les sections suivantes décrivent comment les autorisations sont utilisées pour chaque système de stockage et service de données NetApp . Ces informations peuvent être utiles si les politiques de votre entreprise stipulent que les autorisations ne sont accordées qu'en cas de besoin.

Azure NetApp Files

L'agent effectue les requêtes API suivantes lorsque vous utilisez NetApp Data Classification pour analyser les données Azure NetApp Files :

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

NetApp Backup and Recovery

Les sections suivantes décrivent comment les autorisations sont utilisées pour NetApp Backup and Recovery.

Autorisations minimales de NetApp Backup and Recovery

L'agent de la console effectue les requêtes API suivantes pour les fonctionnalités de base de NetApp Backup and Recovery :

- Microsoft.Storage/storageAccounts/listkeys/action
- Microsoft.Storage/storageAccounts/lecture
- Microsoft.Storage/storageAccounts/write
- Microsoft.Storage/storageAccounts/blobServices/containers/read
- Microsoft.Storage/storageAccounts/listAccountSas/action
- Microsoft.Ressources/abonnements/emplacements/lecture

- Microsoft.Resources/abonnements/resourceGroups/read
- Microsoft.Resources/abonnements/groupes de ressources/ressources/lecture
- Microsoft.Resources/abonnements/resourceGroups/write
- Microsoft.Storage/storageAccounts/managementPolicies/lecture
- Microsoft.Storage/storageAccounts/managementPolicies/write
- Microsoft.Authorization/locks/write
- Microsoft.Authorization/locks/read

Voici une stratégie personnalisée pour la sauvegarde et la restauration qui utilise le minimum d'autorisations et la portée la plus restreinte possible :

```
{
  "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": []
      }
    ]
  }
}
```

Autorisations avancées de sauvegarde et de restauration

L'agent de la console effectue les requêtes API suivantes pour les opérations avancées de sauvegarde et de récupération, ainsi que pour les fonctionnalités de recherche et de restauration. Ces autorisations permettent la gestion du réseau, des coffres-forts de clés et des identités gérées :

- Microsoft.KeyVault/vaults/accessPolicies/write
- Microsoft.KeyVault/vaults/lecture
- Microsoft.ManagedIdentity/userAssignedIdentities/assign/action
- Microsoft.Network/networkInterfaces/supprimer
- Microsoft.Network/networkInterfaces/lecture
- Microsoft.Network/networkSecurityGroups/supprimer
- Microsoft.Network/privateDnsZones/lecture
- Microsoft.Network/privateDnsZones/écriture
- Microsoft.Network/privateEndpoints/lecture
- Microsoft.Network/privateEndpoints/écriture
- Microsoft.Network/virtualNetworks/join/action
- Microsoft.Resources/deployments/delete

Autorisations héritées pour la sauvegarde et la récupération

L'agent effectue les requêtes API suivantes lorsque vous utilisez la fonctionnalité Rechercher et restaurer. Vous n'avez besoin de ces autorisations que si vous avez activé les fonctionnalités d'indexation héritées avant la sortie de l'indexation v2 en février 2025 :

- Microsoft.Synapse/espaces de travail/écriture
- Microsoft.Synapse/espaces de travail/lecture
- Microsoft.Synapse/espaces de travail/supprimer
- Microsoft.Synapse/register/action
- Microsoft.Synapse/checkNameAvailability/action
- Microsoft.Synapse/workspaces/operationStatuses/lecture
- Microsoft.Synapse/workspaces/firewallRules/lecture
- Microsoft.Synapse/workspaces/replaceAllIpFirewallRules/action
- Microsoft.Synapse/workspaces/operationResults/lecture
- Microsoft.Synapse/workspaces/privateEndpointConnectionsApproval/action

NetApp Data Classification

L'agent effectue les requêtes API suivantes lorsque vous utilisez la classification des données.

Action	Utilisé pour l'installation ?	Utilisé pour les opérations quotidiennes ?
Microsoft.Compute/locations/operations/read	Oui	Oui

Action	Utilisé pour l'installation ?	Utilisé pour les opérations quotidiennes ?
Microsoft.Compute/locations/vmSizes/lecture	Oui	Oui
Microsoft.Compute/opérations/lecture	Oui	Oui
Microsoft.Compute/virtualMachines/instanceView/read	Oui	Oui
Microsoft.Compute/virtualMachines/powerOff/action	Oui	Non
Microsoft.Compute/virtualMachines/read	Oui	Oui
Microsoft.Compute/virtualMachines/restart/action	Oui	Non
Microsoft.Compute/virtualMachines/start/action	Oui	Non
Microsoft.Compute/virtualMachines/vmSizes/lecture	Non	Oui
Microsoft.Compute/virtualMachines/write	Oui	Non
Microsoft.Compute/images/read	Oui	Oui
Microsoft.Compute/disks/delete	Oui	Non
Microsoft.Compute/disques/lecture	Oui	Oui
Microsoft.Compute/disques/écriture	Oui	Non
Microsoft.Storage/checknameavailability/lecture	Oui	Oui
Microsoft.Storage/opérations/lecture	Oui	Oui
Microsoft.Storage/storageAccounts/listkeys/action	Oui	Non
Microsoft.Storage/storageAccounts/lecture	Oui	Oui
Microsoft.Storage/storageAccounts/write	Oui	Non
Microsoft.Storage/storageAccounts/blobServices/containers/read	Oui	Oui
Microsoft.Network/networkInterfaces/lecture	Oui	Oui
Microsoft.Network/networkInterfaces/write	Oui	Non

Action	Utilisé pour l'installation ?	Utilisé pour les opérations quotidiennes ?
Microsoft.Network/networkInterfaces/join/action	Oui	Non
Microsoft.Network/networkSecurityGroups/lecture	Oui	Oui
Microsoft.Network/networkSecurityGroups/écriture	Oui	Non
Microsoft.Ressources/abonnements/emplacements/lecture	Oui	Oui
Microsoft.Network/locations/operationResults/lecture	Oui	Oui
Microsoft.Network/locations/operations/read	Oui	Oui
Microsoft.Network/virtualNetworks/lecture	Oui	Oui
Microsoft.Network/virtualNetworks/checkIpAddressAvailability/lecture	Oui	Oui
Microsoft.Network/virtualNetworks/sous-réseaux/lecture	Oui	Oui
Microsoft.Network/virtualNetworks/subnets/virtualMachines/read	Oui	Oui
Microsoft.Network/virtualNetworks/virtualMachines/lecture	Oui	Oui
Microsoft.Network/virtualNetworks/sous-réseaux/join/action	Oui	Non
Microsoft.Network/virtualNetworks/sous-réseaux/écriture	Oui	Non
Microsoft.Network/routeTables/join/action	Oui	Non
Microsoft.Ressources/déploiements/opérations/lecture	Oui	Oui
Microsoft.Ressources/déploiements/lecture	Oui	Oui
Microsoft.Ressources/déploiements/écriture	Oui	Non
Microsoft.Resources/ressources/lire	Oui	Oui
Microsoft.Resources/subscriptions/operationresults/read	Oui	Oui
Microsoft.Resources/subscriptions/resourceGroups/delete	Oui	Non

Action	Utilisé pour l'installation ?	Utilisé pour les opérations quotidiennes ?
Microsoft.Resources/abonnements/resourceGroups/read	Oui	Oui
Microsoft.Resources/abonnements/groupes de ressources/ressources/lecture	Oui	Oui
Microsoft.Resources/abonnements/resourceGroups/write	Oui	Non

Cloud Volumes ONTAP

L'agent effectue les requêtes API suivantes pour déployer et gérer Cloud Volumes ONTAP dans Azure.

But	Action	Utilisé pour le déploiement ?	Utilisé pour les opérations quotidiennes ?	Utilisé pour la suppression ?
Créer et gérer des machines virtuelles	Microsoft.Compute/locations/operations/read	Oui	Oui	Non
	Microsoft.Compute/locations/vmSizes/lecture	Oui	Oui	Non
	Microsoft.Ressources/abonnements/emplacements/lecture	Oui	Non	Non
	Microsoft.Compute/opérations/lecture	Oui	Oui	Non
	Microsoft.Compute/virtualMachines/instanceView/read	Oui	Oui	Non
	Microsoft.Compute/virtualMachines/powerOff/action	Oui	Oui	Non
	Microsoft.Compute/virtualMachines/read	Oui	Oui	Non
	Microsoft.Compute/virtualMachines/restart/action	Oui	Oui	Non
	Microsoft.Compute/virtualMachines/start/action	Oui	Oui	Non
	Microsoft.Compute/virtualMachines/deallocate/action	Non	Oui	Oui
	Microsoft.Compute/virtualMachines/vmSizes/lecture	Non	Oui	Non
	Microsoft.Compute/virtualMachines/write	Oui	Oui	Non
	Microsoft.Compute/virtualMachines/delete	Oui	Oui	Oui
	Microsoft.Resources/deployments/delete	Oui	Non	Non

But	Action	Utilisé pour le déploiement ?	Utilisé pour les opérations quotidiennes ?	Utilisé pour la suppression ?
Activer le déploiement à partir d'un disque dur virtuel	Microsoft.Compute/images/read	Oui	Non	Non
	Microsoft.Compute/images/write	Oui	Non	Non
Créer et gérer les interfaces réseau dans le sous-réseau cible	Microsoft.Network/networkInterfaces/lecture	Oui	Oui	Non
	Microsoft.Network/networkInterfaces/write	Oui	Oui	Non
	Microsoft.Network/networkInterfaces/join/action	Oui	Oui	Non
	Microsoft.Network/networkInterfaces/supprimer	Oui	Oui	Non
Créer et gérer des groupes de sécurité réseau	Microsoft.Network/networkSecurityGroups/lecture	Oui	Oui	Non
	Microsoft.Network/networkSecurityGroups/écriture	Oui	Oui	Non
	Microsoft.Network/networkSecurityGroups/join/action	Oui	Non	Non
	Microsoft.Network/networkSecurityGroups/supprimer	Non	Oui	Oui

But	Action	Utilisé pour le déploiement ?	Utilisé pour les opérations quotidiennes ?	Utilisé pour la suppression ?
Obtenez des informations réseau sur les régions, le VNet cible et le sous-réseau, et ajoutez les machines virtuelles aux VNets	Microsoft.Network/locations/operationResults/lecture	Oui	Oui	Non
	Microsoft.Network/locations/operations/read	Oui	Oui	Non
	Microsoft.Network/virtualNetworks/lecture	Oui	Non	Non
	Microsoft.Network/virtualNetworks/checkIpAddressAvailability/lecture	Oui	Non	Non
	Microsoft.Network/virtualNetworks/sous-réseaux/lecture	Oui	Oui	Non
	Microsoft.Network/virtualNetworks/subnets/virtualMachines/read	Oui	Oui	Non
	Microsoft.Network/virtualNetworks/virtualMachines/lecture	Oui	Oui	Non
	Microsoft.Network/virtualNetworks/sous-réseaux/join/action	Oui	Oui	Non

But	Action	Utilisé pour le déploiement ?	Utilisé pour les opérations quotidiennes ?	Utilisé pour la suppression ?
Créer et gérer des groupes de ressources	Microsoft.Ressources/déploiements/opérations/lecture	Oui	Oui	Non
	Microsoft.Ressources/déploiements/lecture	Oui	Oui	Non
	Microsoft.Ressources/déploiements/écriture	Oui	Oui	Non
	Microsoft.Resources/ressources/lire	Oui	Oui	Non
	Microsoft.Resources/subscriptions/operationresults/read	Oui	Oui	Non
	Microsoft.Resources/subscriptions/resourceGroups/delete	Oui	Oui	Oui
	Microsoft.Resources/abonnements/resourceGroups/read	Non	Oui	Non
	Microsoft.Resources/abonnements/groupes de ressources/ressources/lecture	Oui	Oui	Non
	Microsoft.Resources/abonnements/resourceGroups/write	Oui	Oui	Non

But	Action	Utilisé pour le déploiement ?	Utilisé pour les opérations quotidiennes ?	Utilisé pour la suppression ?
Gérer les comptes et les disques de stockage Azure	Microsoft.Compute/disques/lecture	Oui	Oui	Oui
	Microsoft.Compute/disques/écriture	Oui	Oui	Non
	Microsoft.Compute/disks/delete	Oui	Oui	Oui
	Microsoft.Storage/checknameavailability/lecture	Oui	Oui	Non
	Microsoft.Storage/opérations/lecture	Oui	Oui	Non
	Microsoft.Storage/storageAccounts/listkeys/action	Oui	Oui	Non
	Microsoft.Storage/storageAccounts/lecture	Oui	Oui	Non
	Microsoft.Storage/storageAccounts/supprimer	Non	Oui	Oui
	Microsoft.Storage/storageAccounts/write	Oui	Oui	Non
	Microsoft.Storage/usages/lecture	Non	Oui	Non
Activer les sauvegardes sur le stockage Blob et le chiffrement des comptes de stockage	Microsoft.Storage/storageAccounts/blobServices/containers/read	Oui	Oui	Non
	Microsoft.KeyVault/vaults/lecture	Oui	Oui	Non
	Microsoft.KeyVault/vaults/accessPolicies/write	Oui	Oui	Non
Activer les points de terminaison du service VNet pour la hiérarchisation des données	Microsoft.Network/virtualNetworks/sous-réseaux/écriture	Oui	Oui	Non
	Microsoft.Network/routeTables/join/action	Oui	Oui	Non

But	Action	Utilisé pour le déploiement ?	Utilisé pour les opérations quotidiennes ?	Utilisé pour la suppression ?
Créer et gérer des instantanés gérés par Azure	Microsoft.Compute/snapshots/write	Oui	Oui	Non
	Microsoft.Compute/snapshots/read	Oui	Oui	Non
	Microsoft.Compute/snapshots/delete	Non	Oui	Oui
	Microsoft.Compute/disques/beginGetAccess/action	Non	Oui	Non
Créer et gérer des ensembles de disponibilité	Microsoft.Compute/availabilitySets/write	Oui	Non	Non
	Microsoft.Compute/availabilitySets/lecture	Oui	Non	Non
Activer les déploiements programmatiques à partir du marché	Microsoft.MarketplaceOrdering/offertypes/publishers/offers/plans/agreements/read	Oui	Non	Non
	Microsoft.MarketplaceOrdering/offertypes/publishers/offers/plans/agreements/write	Oui	Oui	Non

But	Action	Utilisé pour le déploiement ?	Utilisé pour les opérations quotidiennes ?	Utilisé pour la suppression ?
Gérer un équilibreur de charge pour les paires HA	Microsoft.Network/loadBalancers/lecture	Oui	Oui	Non
	Microsoft.Network/loadBalancers/write	Oui	Non	Non
	Microsoft.Network/loadBalancers/supprimer	Non	Oui	Oui
	Microsoft.Network/loadBalancers/backendAddressPools/lecture	Oui	Non	Non
	Microsoft.Network/loadBalancers/backendAddressPools/join/action	Oui	Non	Non
	Microsoft.Network/loadBalancers/frontendIPConfigurations/lecture	Oui	Oui	Non
	Microsoft.Network/loadBalancers/loadBalancingRules/lecture	Oui	Non	Non
	Microsoft.Network/loadBalancers/sondes/lecture	Oui	Non	Non
	Microsoft.Network/loadBalancers/probes/join/action	Oui	Non	Non
Activer la gestion des verrous sur les disques Azure	Microsoft.Autorisation/locks/*	Oui	Oui	Non

But	Action	Utilisé pour le déploiement ?	Utilisé pour les opérations quotidiennes ?	Utilisé pour la suppression ?
Activer les points de terminaison privés pour les paires HA lorsqu'il n'y a pas de connectivité en dehors du sous-réseau	Microsoft.Network/privateEndpoints/écriture	Oui	Oui	Non
	Microsoft.Storage/storageAccounts/PrivateEndpointConnectionsApproval/action	Oui	Non	Non
	Microsoft.Storage/storageAccounts/privateEndpointConnections/lecture	Oui	Oui	Oui
	Microsoft.Network/privateEndpoints/lecture	Oui	Oui	Oui
	Microsoft.Network/privateDnsZones/écriture	Oui	Oui	Non
	Microsoft.Network/privateDnsZones/virtualNetworkLinks/écriture	Oui	Oui	Non
	Microsoft.Network/virtualNetworks/join/action	Oui	Oui	Non
	Microsoft.Network/privateDnsZones/A/écriture	Oui	Oui	Non
	Microsoft.Network/privateDnsZones/lecture	Oui	Oui	Non
	Microsoft.Network/privateDnsZones/virtualNetworkLinks/lecture	Oui	Oui	Non
Requis pour certains déploiements de machines virtuelles, en fonction du matériel physique sous-jacent	Microsoft.Resources/deployments/operationStatuses/lecture	Oui	Oui	Non

But	Action	Utilisé pour le déploiement ?	Utilisé pour les opérations quotidiennes ?	Utilisé pour la suppression ?
Supprimer des ressources d'un groupe de ressources en cas d'échec de déploiement ou de suppression	Microsoft.Network/privateEndpoints/supprimer	Oui	Oui	Non
	Microsoft.Compute/availabilitySets/delete	Oui	Oui	Non
Activer l'utilisation de clés de chiffrement gérées par le client lors de l'utilisation de l'API	Microsoft.Compute/diskEncryptionSets/lecture	Oui	Oui	Oui
	Microsoft.Compute/diskEncryptionSets/écriture	Oui	Oui	Non
	Microsoft.KeyVault/vaults/deploy/action	Oui	Non	Non
	Microsoft.Compute/diskEncryptionSets/delete	Oui	Oui	Oui
Configurer un groupe de sécurité d'application pour une paire HA afin d'isoler l'interconnexion HA et les cartes réseau du réseau de cluster	Microsoft.Network/applicationSecurityGroups/écriture	Non	Oui	Non
	Microsoft.Network/applicationSecurityGroups/lecture	Non	Oui	Non
	Microsoft.Network/applicationSecurityGroups/joinIpConfiguration/action	Non	Oui	Non
	Microsoft.Network/networkSecurityGroups/securityRules/écriture	Oui	Oui	Non
	Microsoft.Network/applicationSecurityGroups/supprimer	Non	Oui	Oui
	Microsoft.Network/networkSecurityGroups/securityRules/supprimer	Non	Oui	Oui

But	Action	Utilisé pour le déploiement ?	Utilisé pour les opérations quotidiennes ?	Utilisé pour la suppression ?
Lire, écrire et supprimer les balises associées aux ressources Cloud Volumes ONTAP	Microsoft.Ressources/tags/lecture	Non	Oui	Non
	Microsoft.Ressources/tags/write	Oui	Oui	Non
	Microsoft.Ressources/tags/supprimer	Oui	Non	Non
Crypter les comptes de stockage lors de la création	Microsoft.ManagedIdentity/userAssignedIdentities/assign/action	Oui	Oui	Non
Utilisez des ensembles de machines virtuelles évolutives en mode d'orchestration flexible afin de spécifier des zones spécifiques pour Cloud Volumes ONTAP	Microsoft.Compute/virtualMachineScaleSets/write	Oui	Non	Non
	Microsoft.Compute/virtualMachineScaleSets/lecture	Oui	Non	Non
	Microsoft.Compute/virtualMachineScaleSets/supprimer	Non	Non	Oui

hiérarchisation

L'agent effectue les requêtes API suivantes lorsque vous configurez NetApp Cloud Tiering.

- Microsoft.Storage/storageAccounts/listkeys/action
- Microsoft.Resources/abonnements/resourceGroups/read
- Microsoft.Ressources/abonnements/emplacements/lecture

L'agent de la console effectue les demandes d'API suivantes pour les opérations quotidiennes.

- Microsoft.Storage/storageAccounts/blobServices/containers/read
- Microsoft.Storage/storageAccounts/managementPolicies/lecture
- Microsoft.Storage/storageAccounts/managementPolicies/write
- Microsoft.Storage/storageAccounts/lecture

Journal des modifications

Au fur et à mesure que des autorisations sont ajoutées et supprimées, nous les noterons dans les sections ci-dessous.

11 novembre 2025

Une politique JSON personnalisée a été ajoutée, reflétant le minimum d'autorisations et la portée la plus restreinte possibles.

Les autorisations suivantes ont été ajoutées à la liste minimale des autorisations de sauvegarde et de restauration :

- Microsoft.Authorization/locks/write
- Microsoft.Authorization/locks/read

Les autorisations suivantes ne sont plus nécessaires pour la sauvegarde et la restauration, sauf si vous utilisez l'indexation héritée :

- Microsoft.Synapse/espaces de travail/écriture
- Microsoft.Synapse/espaces de travail/lecture
- Microsoft.Synapse/espaces de travail/supprimer
- Microsoft.Synapse/register/action
- Microsoft.Synapse/checkNameAvailability/action
- Microsoft.Synapse/workspaces/operationStatuses/lecture
- Microsoft.Synapse/workspaces/firewallRules/lecture
- Microsoft.Synapse/workspaces/replaceAllIpFirewallRules/action
- Microsoft.Synapse/workspaces/operationResults/lecture
- Microsoft.Synapse/workspaces/privateEndpointConnectionsApproval/action

Les autorisations suivantes ont été déplacées vers la section « Autorisations supplémentaires de sauvegarde et de restauration » car elles ne sont pas nécessaires pour une configuration minimale :

- Microsoft.Storage/storageAccounts/listkeys/action
- Microsoft.Storage/storageAccounts/lecture
- Microsoft.Storage/storageAccounts/write
- Microsoft.Storage/storageAccounts/blobServices/containers/read
- Microsoft.Storage/storageAccounts/listAccountSas/action
- Microsoft.Ressources/abonnements/emplacements/lecture
- Microsoft.Resources/abonnements/resourceGroups/read
- Microsoft.Resources/abonnements/groupes de ressources/ressources/lecture
- Microsoft.Resources/abonnements/resourceGroups/write
- Microsoft.Storage/storageAccounts/managementPolicies/lecture
- Microsoft.Storage/storageAccounts/managementPolicies/write

9 septembre 2024

Les autorisations suivantes ont été supprimées de la politique JSON car la console ne prend plus en charge la découverte et la gestion des clusters Kubernetes :

- Microsoft.ContainerService/managedClusters/listClusterUserCredential/action
- Microsoft.ContainerService/managedClusters/lecture

22 août 2024

Les autorisations suivantes ont été ajoutées à la stratégie JSON, car elles sont requises pour la prise en charge des ensembles de machines virtuelles identiques par Cloud Volumes ONTAP :

- Microsoft.Compute/virtualMachineScaleSets/write
- Microsoft.Compute/virtualMachineScaleSets/lecture
- Microsoft.Compute/virtualMachineScaleSets/supprimer

5 décembre 2023

Les autorisations suivantes ne sont plus nécessaires pour NetApp Backup and Recovery lors de la sauvegarde de données de volume sur le stockage Azure Blob :

- Microsoft.Compute/virtualMachines/read
- Microsoft.Compute/virtualMachines/start/action
- Microsoft.Compute/virtualMachines/deallocate/action
- Microsoft.Compute/virtualMachines/extensions/delete
- Microsoft.Compute/virtualMachines/delete

Ces autorisations sont requises pour d'autres services de stockage de la console. Elles resteront donc dans le rôle personnalisé de l'agent si vous utilisez ces autres services de stockage.

12 mai 2023

Les autorisations suivantes ont été ajoutées à la stratégie JSON car elles sont requises pour la gestion de Cloud Volumes ONTAP :

- Microsoft.Compute/images/write
- Microsoft.Network/loadBalancers/frontendIPConfigurations/lecture

Les autorisations suivantes ont été supprimées de la politique JSON car elles ne sont plus nécessaires :

- Microsoft.Storage/storageAccounts/blobServices/containers/write
- Microsoft.Network/publicIPAddresses/supprimer

23 mars 2023

L'autorisation « Microsoft.Storage/storageAccounts/delete » n'est plus nécessaire pour la classification des données.

Cette autorisation est toujours requise pour Cloud Volumes ONTAP.

5 janvier 2023

Les autorisations suivantes ont été ajoutées à la politique JSON :

- Microsoft.Storage/storageAccounts/listAccountSas/action
- Microsoft.Synapse/workspaces/privateEndpointConnectionsApproval/action

  Ces autorisations sont requises pour NetApp Backup and Recovery.

- Microsoft.Network/loadBalancers/backendAddressPools/join/action

  Cette autorisation est requise pour le déploiement de Cloud Volumes ONTAP .

Règles du groupe de sécurité de l'agent de console dans Azure

Le groupe de sécurité Azure pour l'agent nécessite des règles entrantes et sortantes. La NetApp Console crée automatiquement ce groupe de sécurité lorsque vous créez un agent de console à partir de la console. Pour les autres options d'installation, vous devez configurer ce groupe de sécurité manuellement.

Règles entrantes

Protocole	Port	But
SSH	22	Fournit un accès SSH à l'hôte de l'agent
HTTP	80	• Fournit un accès HTTP depuis les navigateurs Web clients vers l'interface utilisateur locale • Utilisé pendant le processus de mise à niveau de Cloud Volumes ONTAP
HTTPS	443	Fournit un accès HTTPS depuis les navigateurs Web clients à l'interface utilisateur locale et des connexions depuis l'instance de NetApp Data Classification
TCP	3128	Fournit à Cloud Volumes ONTAP un accès Internet pour envoyer des messages AutoSupport au support NetApp . Vous devez ouvrir manuellement ce port après le déploiement. "Découvrez comment l'agent est utilisé comme proxy pour les messages AutoSupport"

Règles de sortie

Le groupe de sécurité prédéfini pour l'agent ouvre tout le trafic sortant. Si cela est acceptable, suivez les règles de sortie de base. Si vous avez besoin de règles plus rigides, utilisez les règles sortantes avancées.

Règles de base pour les voyages sortants

Le groupe de sécurité prédéfini pour l'agent inclut les règles sortantes suivantes.

Protocole	Port	But
Tous les TCP	Tous	Tout le trafic sortant

Protocole	Port	But
Tout UDP	Tous	Tout le trafic sortant

Règles sortantes avancées

Si vous avez besoin de règles strictes pour le trafic sortant, vous pouvez utiliser les informations suivantes pour ouvrir uniquement les ports requis pour la communication sortante par l'agent.

L'adresse IP source est l'hôte de l'agent.

Service	Protocole	Port	Destination	But
Appels API et AutoSupport	HTTPS	443	Gestion de cluster Internet sortant et ONTAP LIF	Appels d'API vers Azure, vers ONTAP, vers NetApp Data Classification et envoi de messages AutoSupport à NetApp
Appels d'API	TCP	8080	Classification des données	Sonder l'instance de classification des données pendant le déploiement
DNS	UDP	53	DNS	Utilisé pour la résolution DNS par la console

Autorisations Google Cloud et règles de pare-feu requises

Autorisations Google Cloud pour l'agent de la console

L'agent de la console nécessite des autorisations pour effectuer des actions dans Google Cloud. Ces autorisations sont incluses dans un rôle personnalisé fourni par NetApp. Vous devez comprendre ce que l'agent fait avec ces autorisations.

Autorisations du compte utilisateur Google Cloud

Le rôle personnalisé ci-dessous confère à un utilisateur Google Cloud les autorisations nécessaires pour déployer un agent. Attribuez ce rôle personnalisé à l'utilisateur qui déploiera l'agent.

Afficher les autorisations du compte utilisateur Google Cloud

```
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
```

Autorisations du compte de service

Le rôle personnalisé ci-dessous confère au compte de service Google Cloud associé à l'agent Console les autorisations nécessaires pour gérer les ressources et les processus de votre réseau Google Cloud.

Appliquez ce rôle personnalisé à un compte de service associé à la machine virtuelle de l'agent de console.

- "Configurer les autorisations Google Cloud pour le mode standard"
- "Configurer les autorisations pour le mode restreint"

Afficher les autorisations du compte de service Google

Veillez à ce que le rôle soit à jour, car de nouvelles autorisations sont ajoutées ou supprimées dans les versions ultérieures. Le journal des modifications répertorie toutes les nouvelles autorisations requises."Consultez le journal des modifications des autorisations Google" "Consultez la procédure pour ajouter des comptes de service Google Cloud."

```
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
- 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.update
- config.deployments.updateState
- config.previews.upload
- config.revisions.get
- config.revisions.getState
- config.deployments.getLock
- config.deployments.list
- config.deployments.lock
- 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.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.objects.get
- storage.objects.list
- storage.buckets.getIamPolicy
```

Comment les autorisations Google Cloud sont utilisées

L'agent Console utilise les autorisations du rôle personnalisé pour gérer les ressources Cloud Volumes ONTAP et les processus de services de données NetApp sur votre réseau Google Cloud. Les sections suivantes décrivent comment l'agent utilise ces autorisations.

Autorisations utilisées pour Cloud Volumes ONTAP

L'agent Console utilise les autorisations du rôle personnalisé pour gérer les ressources et les processus Cloud Volumes ONTAP de votre réseau Google Cloud. Les sections suivantes décrivent comment l'agent utilise ces autorisations.

Autorisations pour Cloud Volumes ONTAP

Actions	But	Utilisé pour le déploiement ?	Utilisé pour les opérations quotidiennes ?	Utilisé pour la suppression ?
config.déploiements.créer	Pour déployer l'instance de machine virtuelle Cloud Volumes ONTAP à l'aide de Google Cloud Infrastructure Manager.	Oui	Non	Non
config.deployments.delete		Non	Non	Oui
config.deployments.deleteState		Non	Non	Oui
config.deployments.get		Non	Oui	Non
config.deployments.getLock		Non	Oui	Non
config.deployments.getState		Non	Oui	Non
config.déploiements.liste		Non	Oui	Non
config.déploiements.lock		Non	Oui	Non
config.déploiements.mise à jour		Non	Oui	Non
config.deployments.updateState		Non	Oui	Non
config.operations.get		Non	Oui	Non
config.previews.get		Non	Oui	Non
config.previews.list		Non	Oui	Non
config.resources.list		Non	Oui	Non
config.revisions.get		Non	Oui	Non

Actions	But	Utilisé pour le déploiement ?	Utilisé pour les opérations quotidiennes ?	Utilisé pour la suppression ?
calculer.disques.créer	Pour créer et gérer des disques pour Cloud Volumes ONTAP.	Oui	Oui	Non
calculer.disques.créerSnapshot		Non	Oui	Non
supprimer.disques.calculer		Non	Oui	Oui
calculer.disques.obtenir		Non	Oui	Non
liste des disques de calcul		Oui	Oui	Non
calculer.disques.setLabels		Oui	Oui	Non
calculer.disques.utiliser		Non	Oui	Non
calculer.firewalls.create	Pour créer des règles de pare-feu pour Cloud Volumes ONTAP.	Oui	Non	Non
calculer.firewalls.delete		Non	Oui	Oui
calculer.firewalls.get		Oui	Oui	Non
liste des pare-feu		Oui	Oui	Non
calculer.forwardingRules.créer	Créez des règles de transfert pour le routage du trafic vers les services backend.	Non	Oui	Non
calculer.forwardingRules.delete	Supprimer les règles de transfert existantes.	Non	Oui	Non
calculer.forwardingRules.get	Récupérer les détails des règles de redirection existantes.	Non	Oui	Non
calculer.forwardingRules.setLabels	Définir ou mettre à jour les étiquettes des règles de transfert pour l'organisation.	Non	Oui	Non

Actions	But	Utilisé pour le déploiement ?	Utilisé pour les opérations quotidiennes ?	Utilisé pour la suppression ?
compute.forwardingRules.update	Mettre à jour les règles de transfert existantes pour la gestion du trafic.	Non	Oui	Non
calculer.globalOperations.get	Pour obtenir l'état des opérations.	Oui	Oui	Non
calculer.healthChecks.créer	Créer et gérer des contrôles d'intégrité pour surveiller l'état des services backend.	Non	Oui	Non
calculer.healthChecks.supprimer		Non	Oui	Non
calculer.healthChecks.get		Non	Oui	Non
calculer.healthChecks.useReadOnly		Non	Oui	Non
calculer.images.obtenir	Pour obtenir des images pour les instances de VM.	Oui	Non	Non
calculer.images.getFromFamily		Oui	Non	Non
calculer.images.liste		Oui	Non	Non
calculer.images.utiliserLectureSeule		Oui	Non	Non
calculer.instances.attacherDisque	Pour attacher et détacher des disques à Cloud Volumes ONTAP.	Oui	Oui	Non
calculer.instances.détacherDisque		Non	Oui	Oui
calculer.instances.créer	Pour créer et supprimer des instances de machine virtuelle Cloud Volumes ONTAP .	Oui	Non	Non
calculer.instances.supprimer		Non	Non	Oui
calculer.instances.get	Pour répertorier les instances de VM.	Oui	Oui	Non
compute.instances.getSerialPortOutput	Pour obtenir les journaux de la console.	Oui	Oui	Non
liste des instances de calcul	Pour récupérer la liste des instances dans une zone.	Oui	Oui	Non

Actions	But	Utilisé pour le déploiement ?	Utilisé pour les opérations quotidiennes ?	Utilisé pour la suppression ?
calculer.instances.setDeletionProtection	Pour définir la protection contre la suppression sur l'instance.	Oui	Non	Non
calculer.instances.setLabels	Pour ajouter des étiquettes.	Oui	Non	Non
compute.instances.setMachineType	Pour modifier le type de machine pour Cloud Volumes ONTAP.	Oui	Oui	Non
compute.instances.setMinCpuPlatform		Oui	Oui	Non
compute.instances.setMetadata	Pour ajouter des métadonnées.	Oui	Oui	Non
calculer.instances.setTags	Pour ajouter des balises pour les règles de pare-feu.	Oui	Oui	Non
calculer.instances.démarrer	Pour démarrer et arrêter Cloud Volumes ONTAP.	Oui	Oui	Non
calculer.instances.stop		Oui	Oui	Non
calculer.instances.updateDisplayDevice		Oui	Oui	Non
calculer.instances.utiliser	Utiliser des instances de machines virtuelles (opérations de démarrage, d'arrêt et de connexion).	Non	Oui	Non
calculer.machineTypes.get	Pour obtenir le nombre de cœurs afin de vérifier les quotas.	Oui	Non	Non
calculer.projets.obtenir	Pour soutenir des projets multiples.	Oui	Non	Non
calculer.resourcePolicies.créer	Créer et gérer des politiques de ressources pour la gestion automatisée des ressources.	Non	Oui	Non
calculer.resourcePolicies.supprimer		Non	Oui	Non
calculer.resourcePolicies.get		Non	Oui	Non

Actions	But	Utilisé pour le déploiement ?	Utilisé pour les opérations quotidiennes ?	Utilisé pour la suppression ?
calculer.instantanés.créer	Pour créer et gérer des instantanés de disque persistants.	Oui	Oui	Non
calculer.instantanés.supprimer		Non	Oui	Oui
calculer.instantanés.obtenir		Non	Oui	Non
liste des instantanés de calcul		Non	Oui	Non
calculer.instantanés.setLabels		Oui	Oui	Non
calculer.réseaux.obtenir	Pour obtenir les informations réseau nécessaires à la création d'une nouvelle instance de machine virtuelle Cloud Volumes ONTAP .	Oui	Oui	Non
liste des réseaux de calcul		Oui	Oui	Non
calculer.régions.obtenir		Oui	Oui	Non
calculer.régions.liste		Oui	Oui	Non
calculer.sous-réseaux.obtenir		Oui	Oui	Non
liste des sous-réseaux		Oui	Oui	Non
calculer.zoneOperations.get		Oui	Oui	Non
calculer.zones.obtenir		Oui	Oui	Non
liste des zones de calcul		Oui	Oui	Non

Actions	But	Utilisé pour le déploiement ?	Utilisé pour les opérations quotidiennes ?	Utilisé pour la suppression ?
deploymentmanager.compositeTypes.get	Pour déployer l'instance de machine virtuelle Cloud Volumes ONTAP à l'aide de Google Cloud Deployment Manager.	Oui	Non	Non
deploymentmanager.compositeTypes.list		Oui	Non	Non
deploymentmanager.deployments.create		Oui	Non	Non
deploymentmanager.deployments.delete		Oui	Non	Non
deploymentmanager.deployments.get		Oui	Non	Non
gestionnaire de déploiement.déploiements.liste		Oui	Non	Non
deploymentmanager.manifests.get		Oui	Non	Non
deploymentmanager.manifests.list		Oui	Non	Non
deploymentmanager.operations.get		Oui	Non	Non
deploymentmanager.operations.list		Oui	Non	Non
deploymentmanager.resources.get		Oui	Non	Non
deploymentmanager.resources.list		Oui	Non	Non
deploymentmanager.typeProviders.get		Oui	Non	Non
deploymentmanager.typeFournisseurs.liste		Oui	Non	Non
deploymentmanager.types.get		Oui	Non	Non
deploymentmanager.types.list		Oui	Non	Non

Actions	But	Utilisé pour le déploiement ?	Utilisé pour les opérations quotidiennes ?	Utilisé pour la suppression ?
logging.logEntries.list	Pour obtenir les lecteurs de journaux de pile.	Oui	Oui	Non
logging.privateLogEntries.list		Oui	Oui	Non
logging.logEntries.create	Créer et acheminer les entrées de journal à des fins de surveillance, de débogage et d'audit.	Oui	Oui	Non
logging.logEntries.route		Oui	Oui	Non
resourcemanager.projects.get	Pour soutenir des projets multiples.	Oui	Oui	Non
storage.buckets.create	Pour créer et gérer un bucket Google Cloud Storage pour la hiérarchisation des données.	Oui	Oui	Non
suppression des buckets de stockage		Non	Oui	Oui
storage.buckets.get		Non	Oui	Non
liste des compartiments de stockage		Non	Oui	Non
mise à jour des buckets de stockage		Non	Oui	Non
cloudkms.cryptoKeyVersions.useToEncrypt	Pour utiliser les clés de chiffrement gérées par le client à partir du service Cloud Key Management avec Cloud Volumes ONTAP.	Oui	Oui	Non
cloudkms.cryptoKeys.get		Oui	Oui	Non
cloudkms.cryptoKeys.list		Oui	Oui	Non
cloudkms.keyRings.list		Oui	Oui	Non
cloudbuild.builds.get		Oui	Non	Non

Actions	But	Utilisé pour le déploiement ?	Utilisé pour les opérations quotidiennes ?	Utilisé pour la suppression ?
compute.instances.setServiceAccount	Pour définir un compte de service sur l'instance Cloud Volumes ONTAP . Ce compte de service fournit des autorisations pour la hiérarchisation des données vers un bucket Google Cloud Storage.	Oui	Oui	Non
je suis.comptesdeservice.agirEnTantQue		Oui	Non	Non
je suis.comptesdeservice.créer		Oui	Non	Non
iam.serviceAccounts.getIamPolicy		Oui	Oui	Non
liste des comptes de service iam		Oui	Oui	Non
iam.serviceAccountKeys.create		Oui	Non	Non
création d'objets de stockage	Créez et gérez des objets (fichiers) dans un bucket Google Cloud Storage.	Oui	Oui	Non
suppression des objets de stockage		Non	Non	Oui
storage.objects.get		Oui	Oui	Non
liste des objets de stockage		Oui	Oui	Non
liste des adresses calculées	Pour récupérer les adresses dans une région lors du déploiement d'une paire HA.	Oui	Non	Non
calculer.adresses.créerInterne	Créer des adresses IP internes au sein du réseau VPC pour l'allocation des ressources.	Non	Oui	Non
calculer.adresses.supprimerInterne	Suppression des adresses IP internes pour le nettoyage des ressources.	Non	Oui	Non
calculer.adresses.setLabels	Mettre à jour les étiquettes de la ressource Adresse.	Non	Oui	Non

Actions	But	Utilisé pour le déploiement ?	Utilisé pour les opérations quotidiennes ?	Utilisé pour la suppression ?
calculer.adresses.utiliserInterne	Utilisez les adresses IP internes pour les communications réseau.	Non	Oui	Non
calculer.backendServices.créer	Pour configurer un service backend pour distribuer le trafic dans une paire HA.	Oui	Non	Non
calculer.regionBackendServices.créer	Créer et gérer les services backend pour le routage du trafic.	Oui	Non	Non
compute.regionBackendServices.delete		Non	Oui	Non
compute.regionBackendServices.get		Oui	Non	Non
calculer.regionBackendServices.update		Oui	Oui	Non
compute.regionBackendServices.list		Oui	Non	Non
compute.regionBackendServices.use		Non	Oui	Non
compute.networks.updatePolicy	Pour appliquer des règles de pare-feu sur les VPC et les sous-réseaux pour une paire HA.	Oui	Non	Non

Actions	But	Utilisé pour le déploiement ?	Utilisé pour les opérations quotidiennes ?	Utilisé pour la suppression ?
calculer.instanceGroups.get	Pour créer et gérer des machines virtuelles de stockage sur des paires Cloud Volumes ONTAP HA.	Oui	Oui	Non
calculer.adresses.obtenir		Oui	Oui	Non
compute.instances.updateNetworkInterface		Oui	Oui	Non
calculer.instanceGroups.créer		Non	Oui	Non
calculer.instanceGroups.supprimer		Non	Oui	Non
calculer.instanceGroups.update		Non	Oui	Non
calculer.instanceGroups.utiliser		Non	Oui	Non
monitoring.timeSeries.list	Pour découvrir des informations sur les buckets Google Cloud Storage.	Oui	Oui	Non
storage.buckets.getIamPolicy		Oui	Oui	Non

Autorisations utilisées pour NetApp Backup and Recovery

L’agent de la console utilise les autorisations du rôle personnalisé pour gérer les ressources et les processus NetApp Backup and Recovery sur votre réseau Google Cloud. Les sections suivantes décrivent comment l’agent utilise ces autorisations.

Afficher les autorisations pour NetApp Backup and Recovery

Actions	But	Utilisé pour le déploiement ?	Utilisé pour les opérations quotidiennes ?	Utilisé pour la suppression ?
• cloudkms.cryptoKeys.get • cloudkms.cryptoKeys.getIamPolicy • cloudkms.cryptoKeys.list • cloudkms.cryptoKeys.setIamPolicy • cloudkms.porte-clés.get • cloudkms.keyRings.getIamPolicy • cloudkms.keyRings.list • cloudkms.keyRings.setIamPolicy	Pour sélectionner vos propres clés gérées par le client dans l'assistant d'activation de NetApp Backup and Recovery au lieu d'utiliser les clés de chiffrement par défaut gérées par Google.	Oui	Oui	Non

Autorisations utilisées pour la NetApp Data Classification

L'agent de la console utilise les autorisations du rôle personnalisé pour gérer les ressources et les processus de NetApp Data Classification sur votre réseau Google Cloud. Les sections suivantes décrivent comment l'agent utilise ces autorisations.

Autorisations d’affichage pour la NetApp Data Classification

Actions	But	Utilisé pour le déploiement ?	Utilisé pour les opérations quotidiennes ?	Utilisé pour la suppression ?
• calculer.sous-réseaux.utiliser • calculer.subnetworks.useExternalIp • compute.instances.addAccessConfig	Pour activer la NetApp Data Classification.	Oui	Non	Non

Journal des modifications

Les autorisations ajoutées et supprimées sont indiquées ci-dessous.

09 février 2026

L' `compute.forwardingRules.update`autorisation est ajoutée pour prendre en charge Infrastructure Manager dans les déploiements Cloud Volumes ONTAP sur Google Cloud.

8 décembre 2025

NetApp passe de Google Cloud Deployment Manager à Google Cloud Infrastructure Manager (IM) pour déployer et exécuter l’agent Console dans Google Cloud. Les autorisations suivantes ont été ajoutées pour prendre en charge cette modification.

Les autorisations supplémentaires suivantes sont requises pour l’utilisateur Google Cloud qui déploie l’agent :

- storage.buckets.create
- storage.buckets.get
- création d’objets de stockage
- storage.folders.create
- liste des objets de stockage
- je suis.compte_de_service.agir_en
- config.déploiements.créer
- config.operations.get

Les autorisations supplémentaires suivantes sont requises pour le compte de service Google Cloud utilisé pour les opérations quotidiennes :

- cloudbuild.connections.list
- cloudbuild.repositories.accessReadToken

- cloudbuild.repositories.list
- cloudquotas.quotas.get
- config.artifacts.import
- config.deployments.deleteState
- config.deployments.getLock
- config.deployments.getState
- config.deployments.updateState
- config.previews.upload
- config.revisions.getState
- logging.logEntries.create
- création d’objets de stockage
- suppression des objets de stockage
- mise à jour des objets de stockage
- iam.serviceAccounts.get

Les autorisations supplémentaires suivantes sont requises pour déployer Cloud Volumes ONTAP:

- cloudbuild.builds.get
- config.deployments.delete
- config.deployments.deleteState
- config.deployments.get
- config.deployments.getState
- config.déploiements.liste
- config.déploiements.mise à jour
- config.deployments.updateState
- config.previews.get
- config.previews.list
- config.revisions.get
- config.resources.list
- iam.serviceAccountKeys.create
- je suis.comptesdeservice.créer

Les autorisations supplémentaires suivantes sont requises pour le compte de service utilisé pour les opérations quotidiennes de Cloud Volumes ONTAP.

- calculer.adresses.créerInterne
- calculer.adresses.supprimerInterne
- calculer.adresses.setLabels
- calculer.adresses.utiliserInterne
- calculer.forwardingRules.créer

- calculer.forwardingRules.delete
- calculer.forwardingRules.get
- calculer.forwardingRules.setLabels
- calculer.healthChecks.créer
- calculer.healthChecks.supprimer
- calculer.healthChecks.get
- calculer.healthChecks.useReadOnly
- calculer.instanceGroups.créer
- calculer.instanceGroups.supprimer
- calculer.instanceGroups.update
- calculer.instanceGroups.utiliser
- calculer.instances.utiliser
- compute.regionBackendServices.delete
- calculer.regionBackendServices.update
- compute.regionBackendServices.use
- calculer.resourcePolicies.créer
- calculer.resourcePolicies.supprimer
- calculer.resourcePolicies.get
- logging.logEntries.route
- config.déploiements.créer
- config.deployments.delete
- config.deployments.get
- config.déploiements.mise à jour
- config.revisions.get
- config.déploiements.lock
- config.operations.get

26 novembre 2025

Les autorisations ont été mises à jour afin de clarifier leur utilisation, mais aucune autorisation n'a été ajoutée ni supprimée. Trois colonnes ont été ajoutées pour indiquer si chaque autorisation est utilisée pour le déploiement, les opérations quotidiennes ou la suppression. En outre, certaines autorisations sont segmentées en fonction de leur utilisation pour la NetApp Data Classification et la NetApp Backup and Recovery.

06 février 2023

L'autorisation suivante a été ajoutée à cette politique :

- compute.instances.updateNetworkInterface

Cette autorisation est requise pour Cloud Volumes ONTAP.

27/01/2023

Les autorisations suivantes ont été ajoutées à cette politique :

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

Ces autorisations sont requises pour NetApp Backup and Recovery.

Règles de pare-feu d'agent dans Google Cloud

Les règles de pare-feu Google Cloud pour l'agent nécessitent des règles entrantes et sortantes. La NetApp Console crée automatiquement ce groupe de sécurité lorsque vous créez un agent de console à partir de la console. Pour les autres options d'installation, vous devez configurer ce groupe de sécurité manuellement.

Règles entrantes

Protocole	Port	But
SSH	22	Fournit un accès SSH à l'hôte de l'agent
HTTP	80	• Fournit un accès HTTP depuis les navigateurs Web clients vers l'interface utilisateur locale • Utilisé pendant le processus de mise à niveau de Cloud Volumes ONTAP
HTTPS	443	Fournit un accès HTTPS depuis les navigateurs Web clients vers l'interface utilisateur locale
TCP	3128	Fournit à Cloud Volumes ONTAP un accès Internet. Vous devez ouvrir manuellement ce port après le déploiement.

Règles de sortie

Les règles de pare-feu prédéfinies de l'agent ouvrent tout le trafic sortant. Suivez les règles sortantes de base si elles sont acceptables, ou utilisez des règles sortantes avancées pour des exigences plus strictes.

Règles de base pour les voyages sortants

Les règles de pare-feu prédéfinies pour l'agent incluent les règles sortantes suivantes.

Protocole	Port	But
Tous les TCP	Tous	Tout le trafic sortant
Tout UDP	Tous	Tout le trafic sortant

Règles sortantes avancées

Si vous avez besoin de règles strictes pour le trafic sortant, vous pouvez utiliser les informations suivantes pour ouvrir uniquement les ports requis pour la communication sortante par l'agent.

L'adresse IP source est l'hôte de l'agent.

Service	Protocole	Port	Destination	But
Appels API et AutoSupport	HTTPS	443	Gestion de cluster Internet sortant et ONTAP LIF	Appels d'API vers Google Cloud, vers ONTAP, vers NetApp Data Classification et envoi de messages AutoSupport à NetApp
Appels d'API	TCP	8080	Classification des données	Sonder l'instance de classification des données pendant le déploiement
DNS	UDP	53	DNS	Utilisé pour la résolution DNS par classification des données

Accès réseau requis pour la version 3.9.55 et les versions antérieures

La NetApp Console, l'agent de la NetApp Console et les services de données NetApp nécessitent un accès Internet sortant pour contacter les points de terminaison nécessaires.

Cette rubrique documente l'accès réseau requis pour les versions du mode standard de la NetApp Console 3.9.55 et inférieures. Pour les points de terminaison requis pour la version 4.0.0 et supérieure, consultez"les points de terminaison requis pour la version 4.0.0 et supérieure" .

Vous devez configurer l'accès au réseau pour les éléments suivants :

- Ordinateurs qui accèdent à la NetApp Console en tant que logiciel en tant que service (SaaS)
- Agents de console que vous installez sur site ou dans le cloud.

Mettez à jour votre liste de points de terminaison vers la liste révisée pour la version 4.0.0 et supérieure

À partir de la version 4.0.0, les agents de console nécessitent moins de points de terminaison. Les déploiements existants avant la version 4.0.0 restent pris en charge. Après la mise à niveau vers la version 4.0.0 ou une version ultérieure, vous pouvez supprimer les anciens points de terminaison de votre liste d'autorisation lorsque cela vous convient.

NetApp recommande de mettre à jour les règles de pare-feu pour utiliser la liste de points de terminaison révisée, qui est plus petite, plus sécurisée et plus facile à gérer. NetApp supprime le besoin d'entrées génériques et les points de terminaison pour les mises à niveau des agents prennent en charge tous les services de données.

Points de terminaison pour la version 3.9.55 et les versions antérieures	Points de terminaison pour 4.0.0 et versions ultérieures	But
• \ https://support.netapp.com • \ https://mysupport.netapp.com	• \ https://mysupport.netapp.com • \ https://signin.b2c.netapp.com • \ https://support.netapp.com	Pour obtenir une licence et contacter le support NetApp .
• 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.bluexp.netapp.com • https://*.console.bluexp.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.bluexp.netapp.com • \ https://cdn.auth0.com	Pour les opérations quotidiennes.
• https://*.blob.core.windows.net • \ https://cloudmanagerinfraprod.azurecr.io	• \ https://bluexpinfraprod.eastus2.data.azurecr.io • \ https://bluexpinfraprod.azurecr.io	Pour obtenir des images pour les mises à niveau de l'agent de console.

Étapes

1. Vérifiez que votre agent est en version 4.0.0 ou supérieure."Afficher la version de l'agent."
2. Mettre sur liste blanche les points de terminaison dans"Points de terminaison pris en charge pour la version 4.0.0 et supérieure" .
3. Redémarrez le service Service Manager 2 sur chaque agent en exécutant la commande suivante :

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

4. Exécutez la commande suivante et vérifiez que l'état de l'agent indique *actif (en cours d'exécution)* : _

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

5. Supprimez les anciens points de terminaison de votre liste d'autorisation de pare-feu.

Points de terminaison pour la NetApp Console et les agents de console pour la version 3.9.55 et les versions antérieures

Ces points de terminaison sont utilisés pour les agents de console 3.9.55 et versions antérieures.

Points de terminaison	But
\ https://support.netapp.com \ https://mysupport.netapp.com	Pour obtenir des informations de licence et envoyer des messages AutoSupport au support NetApp .
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	Pour fournir des fonctionnalités et des services au sein de la NetApp Console.

Points de terminaison	But
Choisissez entre deux ensembles de points de terminaison : • Option 1 (recommandée) \ https://bluexpinfraprod.eastus2.data.azurecr.io \ https://bluexpinfraprod.azurecr.io • Option 2 https://*.blob.core.windows.net \ https://cloudmanagerinfraprod.azurecr.io	Pour obtenir des images pour les mises à niveau de l'agent de console. NetApp recommande d'autoriser les points de terminaison de l'option 1 dans votre pare-feu, car ils sont plus sécurisés, et d'interdire les points de terminaison de l'option 2, sauf si vous utilisez Ransomware Resilience ou Backup and Recovery. Notez les points suivants à propos de ces points de terminaison : • Les points de terminaison de l'option 1 sont pris en charge dans la version 3.9.47 et supérieure. Les versions antérieures à la version 3.9.47 ne prennent pas en charge la compatibilité descendante. • L'agent de console initie d'abord le contact avec les points de terminaison de l'option 2. Si ces points de terminaison ne sont pas accessibles, il contacte automatiquement les points de terminaison de l'option 1. • Si vous utilisez l'agent de console avec NetApp Backup and Recovery ou Ransomware Resilience, le système ne prend pas en charge les points de terminaison Option 1. Autoriser les points de terminaison de l'option 2 et interdire l'option 1.

Points de terminaison du fournisseur de cloud contactés par l'agent de la console

Les agents de console doivent avoir accès à des points de terminaison supplémentaires s'ils sont déployés chez votre fournisseur de cloud.

Activez l'accès aux points de terminaison du fournisseur cloud avant d'installer l'agent de la console.

- "Configurer l'accès au réseau AWS pour un agent de console"
- "Configurer l'accès au réseau Azure pour un agent de console"
- "Configurer l'accès au réseau Google Cloud pour un agent de console"

Les points de terminaison du fournisseur de cloud sont les mêmes pour toutes les versions.

Points de terminaison des services de données contactés par l'agent de la console

L'agent de console nécessite un accès Internet sortant supplémentaire pour prendre en charge certains services de données NetApp et Cloud Volumes ONTAP.

Points de terminaison pour Cloud Volumes ONTAP

- "Points de terminaison pour Cloud Volumes ONTAP dans AWS"

- "Points de terminaison pour Cloud Volumes ONTAP dans Azure"
- "Points de terminaison pour Cloud Volumes ONTAP dans Google Cloud"

Exiger l'utilisation d'IMDSv2 sur les instances Amazon EC2

La NetApp Console prend en charge le service de métadonnées d'instance Amazon EC2 version 2 (IMDSv2) avec l'agent de console et avec Cloud Volumes ONTAP (y compris le médiateur pour les déploiements HA). Dans la plupart des cas, IMDSv2 est automatiquement configuré sur les nouvelles instances EC2. IMDSv1 a été activé avant mars 2024. Si vos politiques de sécurité l'exigent, vous devrez peut-être configurer manuellement IMDSv2 sur vos instances EC2.

Avant de commencer

- La version de l'agent de console doit être 3.9.38 ou ultérieure.
- Cloud Volumes ONTAP doit exécuter l'une des versions suivantes :
  - 9.12.1 P2 (ou tout correctif ultérieur)
  - 9.13.0 P4 (ou tout correctif ultérieur)
  - 9.13.1 ou toute version ultérieure à cette version
- Cette modification nécessite le redémarrage des instances Cloud Volumes ONTAP .
- Ces étapes nécessitent l'utilisation de l'AWS CLI car vous devez modifier la limite de saut de réponse à 3.

À propos de cette tâche

IMDSv2 offre une protection renforcée contre les vulnérabilités. "En savoir plus sur IMDSv2 sur le blog de sécurité AWS"

Le service de métadonnées d'instance (IMDS) est activé comme suit sur les instances EC2 :

- Pour les nouveaux déploiements d'agents de console à partir de la console ou à l'aide "Scripts Terraform" IMDSv2 est activé par défaut sur l'instance EC2.
- Si vous lancez une nouvelle instance EC2 dans AWS, puis installez manuellement le logiciel de l'agent de la console, IMDSv2 est également activé par défaut.
- Si vous lancez l'agent de console depuis AWS Marketplace, IMDSv1 est activé par défaut. Vous pouvez configurer manuellement IMDSv2 sur l'instance EC2.
- Pour les agents de console existants, IMDSv1 est toujours pris en charge, mais vous pouvez configurer manuellement IMDSv2 sur l'instance EC2 si vous préférez.
- Pour Cloud Volumes ONTAP, IMDSv1 est activé par défaut sur les instances nouvelles et existantes. Vous pouvez configurer manuellement IMDSv2 sur les instances EC2 si vous préférez.

Étapes

1. Exiger l'utilisation d'IMDSv2 sur l'instance de l'agent de console :

   a. Connectez-vous à la machine virtuelle Linux pour l'agent de console.

      Lorsque vous avez créé l'instance de l'agent de console dans AWS, vous avez fourni une clé d'accès AWS et une clé secrète. Vous pouvez utiliser cette paire de clés pour vous connecter en SSH à l'instance. Le nom d'utilisateur de l'instance EC2 Linux est ubuntu (pour les agents de console créés avant mai 2023, le nom d'utilisateur était ec2-user).

"Documentation AWS : connectez-vous à votre instance Linux"

b. Installez l'AWS CLI.

"Documentation AWS : Installer ou mettre à jour vers la dernière version de l'AWS CLI"

c. Utilisez le `aws ec2 modify-instance-metadata-options` commande pour exiger l'utilisation d'IMDSv2 et pour modifier la limite de saut de réponse PUT à 3.

Exemple

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

+

Le `http-tokens` les paramètres définissent IMDSv2 comme requis. Quand `http-tokens` est requis, vous devez également définir `http-endpoint` à activé.

2. Exiger l'utilisation d'IMDSv2 sur les instances Cloud Volumes ONTAP :
   a. Aller à la "Console Amazon EC2"
   b. Dans le volet de navigation, sélectionnez **Instances**.
   c. Sélectionnez une instance Cloud Volumes ONTAP .
   d. Sélectionnez **Actions > Paramètres de l'instance > Modifier les options de métadonnées de l'instance**.
   e. Dans la boîte de dialogue **Modifier les options des métadonnées d'instance**, sélectionnez les éléments suivants :
      - Pour **Service de métadonnées d'instance**, sélectionnez **Activer**.
      - Pour **IMDSv2**, sélectionnez **Obligatoire**.
      - Sélectionnez **Enregistrer**.
   f. Répétez ces étapes pour les autres instances Cloud Volumes ONTAP , y compris le médiateur HA.
   g. "Arrêter et démarrer les instances Cloud Volumes ONTAP"

Résultat

L'instance de l'agent de console et les instances Cloud Volumes ONTAP sont désormais configurées pour utiliser IMDSv2.

Configuration par défaut de l'agent de console

Découvrez les configurations par défaut de l'agent Console pour les déploiements standard (avec accès Internet) sur AWS, Azure et Google Cloud, ainsi que pour les déploiements restreints (sans accès Internet) dans les environnements sur site.

Configuration par défaut avec accès Internet

Les détails de configuration suivants s'appliquent si vous avez déployé un agent de console à partir de la NetApp Console, à partir de la place de marché de votre fournisseur de cloud ou si vous avez installé manuellement un agent de console sur un hôte Linux local disposant d'un accès Internet.

Détails de la machine virtuelle de l'agent de console pour AWS

Si vous avez déployé un agent de console à partir de la console ou de la place de marché du fournisseur de cloud, notez les points suivants :

- Le type d'instance EC2 est t3.2xlarge.
- Le système d'exploitation de l'image est Ubuntu 22.04 LTS.

  Le système d'exploitation n'inclut pas d'interface graphique. Vous devez utiliser un terminal pour accéder au système.

- L'installation inclut Docker Engine, qui est l'outil d'orchestration de conteneurs requis.
- Le nom d'utilisateur de l'instance EC2 Linux est ubuntu (pour les agents créés avant mai 2023, le nom d'utilisateur est ec2-user).
- Le disque système par défaut est un disque gp2 de 100 Gio.

Détails de la machine virtuelle de l'agent de console pour Azure

Si vous avez déployé un agent de console à partir de la console ou de la place de marché du fournisseur de cloud, notez les points suivants :

- Le type de machine virtuelle est Standard_D8s_v3.
- Le système d'exploitation de l'image est Ubuntu 22.04 LTS.

  Le système d'exploitation n'inclut pas d'interface graphique. Vous devez utiliser un terminal pour accéder au système.

- L'installation inclut Docker Engine, qui est l'outil d'orchestration de conteneurs requis.
- Le disque système par défaut est un disque SSD premium de 100 Gio.

Détails de la machine virtuelle de l'agent de console pour Google Cloud

Si vous avez déployé un agent de console à partir de la console, notez les points suivants :

- L'instance de VM est n2-standard-8.
- Le système d'exploitation de l'image est Ubuntu 22.04 LTS.

  Le système d'exploitation n'inclut pas d'interface graphique. Vous devez utiliser un terminal pour accéder au système.

- L'installation inclut Docker Engine, qui est l'outil d'orchestration de conteneurs requis.
- Le disque système par défaut est un disque persistant SSD de 100 Gio.

Dossier d'installation

Le dossier d'installation de l'agent se trouve à l'emplacement suivant :

`/opt/application/netapp/cloudmanager`

Fichiers journaux

Les fichiers journaux sont contenus dans les dossiers suivants :

- `/opt/application/netapp/cloudmanager/log` ou
- `/opt/application/netapp/service-manager-2/logs` (à partir des nouvelles installations 3.9.23)

  Les journaux de ces dossiers fournissent des détails sur l'agent de la console.

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

  Les journaux de ce dossier fournissent des détails sur les services cloud et le service de console qui s'exécute sur l'agent de console.

Service d'agent de console

- Le service d'agent de console est nommé occm.
- Le service occm dépend du service MySQL.

  Si le service MySQL est en panne, le service occm l'est également.

Ports

L'agent utilise les ports suivants sur l'hôte Linux :

- 80 pour l'accès HTTP
- 443 pour l'accès HTTPS

Configuration par défaut sans accès Internet

La configuration suivante s'applique si vous avez installé manuellement l'agent de console sur un hôte Linux local qui n'a pas accès à Internet. "En savoir plus sur cette option d'installation" .

- Le dossier d'installation de l'agent se trouve à l'emplacement suivant :

  `/opt/application/netapp/ds`

- Les fichiers journaux sont contenus dans les dossiers suivants :

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

  Les journaux de ce dossier fournissent des détails sur l'agent de console et les images Docker.

- Tous les services s'exécutent dans des conteneurs Docker

  Les services dépendent du service d'exécution Docker en cours d'exécution

- L’agent utilise les ports suivants sur l’hôte Linux :
  - 80 pour l’accès HTTP
  - 443 pour l’accès HTTPS