Référence

Set up and administration

NetApp
December 01, 2022

Table des matières

Référence

Autorisations

Résumé des autorisations pour BlueXP

Pour utiliser les fonctionnalités et services de BlueXP, vous devez fournir des autorisations pour que BlueXP 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

Objectif	Description	Lien
Déploiement de connecteurs	L'utilisateur qui crée un connecteur depuis BlueXP a besoin d'autorisations spécifiques pour déployer l'instance dans AWS.	"Créez un connecteur dans AWS à partir de BlueXP"
Fonctionnement du connecteur	Lorsque BlueXP lance le connecteur, il attache une stratégie à l'instance qui fournit les autorisations nécessaires pour gérer les ressources et les processus de votre compte AWS. Vous devez définir vous-même la stratégie si vous "Lancez un connecteur sur le Marketplace" ou si vous "Ajoutez des identifiants AWS à un connecteur". Vous devez également vous assurer que la stratégie est à jour lorsque de nouvelles autorisations sont ajoutées dans les versions suivantes.	"Autorisations AWS pour le connecteur"
Fonctionnement du Cloud Volumes ONTAP	Un rôle IAM doit être associé à chaque nœud Cloud Volumes ONTAP dans AWS. Il en va de même pour le médiateur HA. L'option par défaut est de permettre à BlueXP de créer les rôles IAM pour vous, mais vous pouvez utiliser votre propre.	"Découvrez comment configurer vous-même les rôles IAM"

Autorisations Azure

Objectif	Description	Lien
Déploiement de connecteurs	Lorsque vous déployez un connecteur depuis BlueXP, vous devez utiliser un compte ou un service principal Azure disposant des autorisations pour déployer la machine virtuelle Connector dans Azure.	"Créez un connecteur dans Azure à partir de BlueXP"

Objectif	Description	Lien
Fonctionnement du connecteur	Lorsque BlueXP déploie la machine virtuelle Connector dans Azure, il crée un rôle personnalisé qui fournit les autorisations requises pour gérer les ressources et les processus au sein de cet abonnement Azure. Vous devez définir vous-même le rôle personnalisé si vous le souhaitez "Lancez un connecteur sur le Marketplace" ou si vous "Ajoutez des identifiants Azure à un connecteur". Vous devez également vous assurer que la stratégie est à jour lorsque de nouvelles autorisations sont ajoutées dans les versions suivantes.	"Autorisations Azure pour le connecteur"

Autorisations Google Cloud

Objectif	Description	Lien
Déploiement de connecteurs	L'utilisateur Google Cloud qui déploie un connecteur depuis BlueXP a besoin d'autorisations spécifiques pour déployer le connecteur dans Google Cloud.	"Configurez les autorisations de déploiement du connecteur"
Fonctionnement du connecteur	Le compte de service de l'instance de VM Connector doit disposer d'autorisations spécifiques pour les opérations quotidiennes. Vous devez associer le compte de service au connecteur lorsque vous le déployez depuis BlueXP. Vous devez également vous assurer que la stratégie est à jour lorsque de nouvelles autorisations sont ajoutées dans les versions suivantes.	"Configurez un compte de service pour le connecteur"

Autorisations AWS pour le connecteur

Lorsque BlueXP lance l'instance Connector dans AWS, il attache une règle à l'instance qui fournit au connecteur des autorisations pour gérer les ressources et les processus au sein de ce compte AWS. Le connecteur utilise les autorisations pour effectuer des appels d'API vers plusieurs services AWS, notamment EC2, S3, CloudFormation, IAM, Le service de gestion des clés (KMS), et plus encore.

Règles IAM

Les règles IAM disponibles ci-dessous fournissent les autorisations nécessaires à un connecteur pour gérer les ressources et les processus au sein de votre environnement de cloud public, en fonction de votre région AWS.

Si vous créez un connecteur dans une région AWS standard directement depuis BlueXP, BlueXP applique automatiquement des stratégies au connecteur. Vous n'avez rien à faire dans ce cas.

Si vous déployez le connecteur depuis AWS Marketplace ou si vous installez manuellement le connecteur sur un hôte Linux, vous devrez définir vous-même les règles.

Vous devez également vous assurer que les règles sont à jour lorsque de nouvelles autorisations sont ajoutées dans les versions suivantes.

Sélectionnez votre région pour afficher les stratégies requises :

Régions standard

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

La première politique fournit des autorisations pour les services suivants :

- La sauvegarde dans le cloud
- Sens des données cloud
- Tiering dans le cloud
- Cloud Volumes ONTAP
- FSX pour ONTAP
- Découverte des compartiments S3

La deuxième politique fournit des autorisations pour les services suivants :

- Balisage AppTemplate
- Cache global de fichiers
- Kubernetes

Politique no 1

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "cvoServicePolicy",
            "Effect": "Allow",
            "Action": [
                "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",
                "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:List*",
                "kms:ReEncrypt*",
                "kms:Describe*",
                "kms:CreateGrant",
                "ce:GetReservationUtilization",
                "ce:GetDimensionValues",
                "ce:GetCostAndUsage",
                "ce:GetTags",
                "fsx:Describe*",
                "fsx:List*"
            ],
            "Resource": "*"
        },
        {
            "Sid": "backupPolicy",
            "Effect": "Allow",
            "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",
                "kms:List*",
                "kms:Describe*",
                "ec2:describeVpcEndpoints",
                "kms:ListAliases",
                "athena:StartQueryExecution",
                "athena:GetQueryResults",
                "athena:GetQueryExecution",
                "glue:GetDatabase",
                "glue:GetTable",
                "glue:CreateTable",
                "glue:CreateDatabase",
                "glue:GetPartitions",
```

```
                "glue:BatchCreatePartition",
                "glue:BatchDeletePartition"
            ],
            "Resource": "*"
        },
        {
            "Sid": "backupS3Policy",
            "Effect": "Allow",
            "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-*"
            ]
        },
        {
            "Sid": "fabricPoolS3Policy",
            "Effect": "Allow",
            "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*"
            ]
        },
        {
            "Sid": "fabricPoolPolicy",
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeRegions"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:StartInstances",
                "ec2:StopInstances",
                "ec2:TerminateInstances"
            ],
            "Condition": {
                "StringLike": {
                    "ec2:ResourceTag/netapp-adc-manager": "*"
                }
            },
            "Resource": [
                "arn:aws:ec2:*:*:instance/*"
```

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

```
  }
```

Politique no 2

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Sid": "K8sServicePolicy",
      "Effect": "Allow",
      "Action": [
          "ec2:DescribeRegions",
          "eks:ListClusters",
          "eks:DescribeCluster",
          "iam:GetInstanceProfile"
      ],
      "Resource": "*"
    },
    {
        "Sid": "GFCservicePolicy",
        "Effect": "Allow",
        "Action": [
            "cloudformation:DescribeStacks",
            "cloudwatch:GetMetricStatistics",
            "cloudformation:ListStacks"
        ],
        "Resource": "*"
    },
    {
        "Effect": "Allow",
        "Action": [
            "ec2:StartInstances",
            "ec2:TerminateInstances",
            "ec2:AttachVolume",
            "ec2:DetachVolume"
        ],
        "Condition": {
            "StringLike": {
                "ec2:ResourceTag/GFCInstance": "*"
            }
        },
        "Resource": [
            "arn:aws:ec2:*:*:instance/*"
        ]
    },
    {
```

```
        "Sid": "tagServicePolicy",
        "Effect": "Allow",
        "Action": [
            "ec2:CreateTags",
            "ec2:DeleteTags",
            "ec2:DescribeTags",
            "tag:getResources",
            "tag:getTagKeys",
            "tag:getTagValues",
            "tag:TagResources",
            "tag:UntagResources"
        ],
        "Resource": "*"
    }
  ]
}
```

GovCloud (USA)

```
{
    "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:List*",
                "kms:ReEncrypt*",
                "kms:Describe*",
                "kms:CreateGrant",
                "ec2:AssociateIamInstanceProfile",
                "ec2:DescribeIamInstanceProfileAssociations",
                "ec2:DisassociateIamInstanceProfile",
                "ec2:DescribeInstanceAttribute",
                "ce:GetReservationUtilization",
                "ce:GetDimensionValues",
                "ce:GetCostAndUsage",
                "ce:GetTags",
                "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/*"
            ]
        }
    ]
}
```

Environnement C2S

```
{
    "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",
                "kms:List*",
                "kms:Describe*",
                "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/*"
            ]
        }
    ]
}
```

Utilisation des autorisations AWS

Les sections suivantes décrivent la manière dont les autorisations sont utilisées pour chaque service cloud NetApp. Ces informations peuvent être utiles si vos stratégies d'entreprise exigent que les autorisations ne sont fournies que si nécessaire.

Balises AppTemplate

Lorsque vous utilisez le service de balisage AppTemplate, le connecteur effectue les requêtes API suivantes pour gérer les balises sur les ressources AWS :

- ec2:CreateTags
- ec2:DeleteTags
- ec2:Etiquettes descriptives
- Tag:getResources
- Tag:getTagKeys
- Tag:getTagValues
- Tag:TagResources
- Tag:UntagResources

La sauvegarde dans le cloud

Il crée les demandes d'API suivantes pour déployer l'instance de restauration pour Cloud Backup :

- ec2:déclarations de début
- ec2:StopInances
- ec2:descriptifs
- ec2:DécriesInstanceStatus
- ec2:RunInstances
- ec2:désactivation des instructions
- ec2:DescribeInstanceAttribute
- ec2:descriptifs
- ec2:CreateTags
- ec2 : CreateVolume
- ec2:CreateSecurityGroup
- ec2:DescribeSubnets
- ec2 : descriptif
- ec2:régions descriptives
- Cloudformation:CreateStack
- Cloudformation:DeleteStack
- Cloudformation:DescribeSacks

Ce connecteur effectue les requêtes API suivantes pour gérer les sauvegardes dans Amazon S3 :

- s3:GetBucketLocation
- s3:ListAllMyseaux
- s3:ListBucket
- s3:CreateBucket
- s3:GetLifecyclConfiguration
- s3:PutLifecyclConfiguration
- s3:PutBuckeTagging
- s3:ListBuckeVersions
- s3:GetBucketAcl
- s3:PutBuckePublicAccessBlock
- Km:liste*
- Km:décrire*
- s3:GetObject
- ec2:descriptionVpcEndpoints
- Kms:Listalas
- s3:PutEncryptionConfiguration

Lorsque vous utilisez la méthode de recherche et de restauration pour restaurer des volumes et des fichiers, le connecteur effectue les demandes d'API suivantes :

- s3:CreateBucket
- s3:DeleteObject
- s3:DeleteObjectVersion
- s3:GetBucketAcl
- s3:ListBucket
- s3:ListBuckeVersions
- s3:ListBuckMultipartUploads
- s3:PutObject
- s3:PutBuckeAcl
- s3:PutLifecyclConfiguration
- s3:PutBuckePublicAccessBlock
- s3:AbortMultipartUpload
- s3:ListMultipartUploadParts
- athena:StartQueryExecutionc
- athena:GetQueryResults
- athena:GetQueryExecution
- athena:StopQueryExecution
- Colle:CreateDatabase
- Colle:CreateTable
- Colle:BatchDeletepartition

Lorsque vous utilisez DataLock et protection contre les attaques par ransomware pour vos sauvegardes de volumes, le connecteur effectue les requêtes API suivantes :

- s3:GetObjectVersionTagging
- s3:GetBuckeObjectLockConfiguration
- s3:GetObjectVersionAcl
- s3:PutObjectTagging
- s3:DeleteObject
- s3:DeleteObjectTagging
- s3:GetObjectRetention
- s3:DeleteObjectVersionTagging
- s3:PutObject
- s3:GetObject
- s3:PutBuckObjectLockConfiguration
- s3:GetLifecyclConfiguration
- s3:ListBuckeByTags

- s3:GetBucketTagging
- s3:DeleteObjectVersion
- s3:ListBuckeVersions
- s3:ListBucket
- s3:PutBuckeTagging
- s3:GetObjectTagging
- s3:PutBuckeVersioning
- s3:PutObjectVersionTagging
- s3:GetBucketVersioning
- s3:GetBucketAcl
- s3:BipassGovernanceRetention
- s3:PutObjectRetention
- s3:GetBucketLocation
- s3:GetObjectVersion

Si vous utilisez un autre compte AWS pour vos sauvegardes Cloud Volumes ONTAP que ce que vous utilisez pour les volumes source, ce connecteur effectue les requêtes d'API suivantes :

- s3:PutBuckePolicy
- s3 : commandes PutBuckeOwnerShipControls

Sens des données cloud

Il crée l'instance Cloud Data Sense suivante :

- ec2:descriptifs
- ec2:DécriesInstanceStatus
- ec2:RunInstances
- ec2:désactivation des instructions
- ec2:CreateTags
- ec2 : CreateVolume
- ec2 : AttachVolume
- ec2:CreateSecurityGroup
- ec2:DeleteSecurityGroup
- ec2:descriptifs des groupes de sécurité
- ec2:CreateNetworkinterface
- ec2:DescribeNetworkinterfaces
- ec2:DeleteNetworkinterface
- ec2:DescribeSubnets
- ec2 : descriptif
- ec2 : CreateSnapshot

- ec2:régions descriptives
- Cloudformation:CreateStack
- Cloudformation:DeleteStack
- Cloudformation:DescribeSacks
- Cloudformation:DescribeStackEvents
- iam:AddRoleToInstanceProfile
- ec2:AssociateIamInstanceProfile
- ec2:DécriesIamInstanceProfileassociations

Lors de l'utilisation de Cloud Data Sense, il effectue les demandes d'API suivantes pour analyser les compartiments S3 :

- iam:AddRoleToInstanceProfile
- ec2:AssociateIamInstanceProfile
- ec2:DécriesIamInstanceProfileassociations
- s3:GetBucketTagging
- s3:GetBucketLocation
- s3:ListAllMyseaux
- s3:ListBucket
- s3:GetBucketPolicyStatus
- s3:GetBucketPolicy
- s3:GetBucketAcl
- s3:GetObject
- iam:GetRole
- s3:DeleteObject
- s3:DeleteObjectVersion
- s3:PutObject
- sts : AssumeRole

Tiering dans le cloud

Ce connecteur effectue les demandes d'API suivantes pour transférer les données vers Amazon S3 lorsque vous utilisez NetApp Cloud Tiering.

Action	Utilisé pour la configuration ?	Utilisé pour les opérations quotidiennes ?
s3:CreateBucket	Oui.	Non
s3:PutLifecyclConfiguration	Oui.	Non
s3:GetLifecyclConfiguration	Oui.	Oui.
ec2:régions descriptives	Oui.	Oui.

Cloud Volumes ONTAP

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

Objectif	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:ListenceProfiles	Oui.	Oui.	Non
	iam:CreateRole	Oui.	Non	Non
	iam:DeleteRole	Non	Oui.	Oui.
	iam:PutRolePolicy	Oui.	Non	Non
	iam:CreateInstanceProfile	Oui.	Non	Non
	iam:DeleteRolePolicy	Non	Oui.	Oui.
	iam:AddRoleToInstanceProfile	Oui.	Non	Non
	iam:RemoveRoleFromInstanceProfile	Non	Oui.	Oui.
	iam:DeleteInstanceProfile	Non	Oui.	Oui.
	iam:PassRole	Oui.	Non	Non
	ec2:AssociateIamInstanceProfile	Oui.	Oui.	Non
	ec2:DécrieIamInstanceProfileassociations	Oui.	Oui.	Non
	ec2:DisassociateIamInstanceProfile	Non	Oui.	Non
Décoder les messages d'état d'autorisation	sts:DecodeAuthorationmessage	Oui.	Oui.	Non
Décrivez les images spécifiées (amis) disponibles pour le compte	ec2:descriptifs	Oui.	Oui.	Non
Décrire les tableaux de routage d'un VPC (requis pour les paires haute disponibilité uniquement)	ec2:DescribeRoutetables	Oui.	Non	Non

Objectif	Action	Utilisé pour le déploiement ?	Utilisé pour les opérations quotidiennes ?	Utilisé pour la suppression ?
Arrêtez, démarrez et surveillez les instances	ec2:déclarations de début	Oui.	Oui.	Non
	ec2:StopInances	Oui.	Oui.	Non
	ec2:descriptifs	Oui.	Oui.	Non
	ec2:DécriesInstance Status	Oui.	Oui.	Non
	ec2:RunInstances	Oui.	Non	Non
	ec2:désactivation des instructions	Non	Non	Oui.
	ec2:Modimodificace Attribute	Non	Oui.	Non
Vérifiez que la mise en réseau améliorée est activée pour les types d'instances pris en charge	ec2:DescribeInstanceAttribute	Non	Oui.	Non
Marquez les ressources avec les balises « WorkingEnvironment » et « WorkingEnvironment » qui sont utilisées pour la maintenance et l'allocation des coûts	ec2:CreateTags	Oui.	Oui.	Non
Gérez des volumes EBS que Cloud Volumes ONTAP utilise comme stockage interne	ec2 : CreateVolume	Oui.	Oui.	Non
	ec2:Describvolumes	Oui.	Oui.	Oui.
	ec2:ModimodityVolumeAttribute	Non	Oui.	Oui.
	ec2 : AttachVolume	Oui.	Oui.	Non
	ec2:DeleteVolume	Non	Oui.	Oui.
	ec2 : DetachVolume	Non	Oui.	Oui.

Objectif	Action	Utilisé pour le déploiement ?	Utilisé pour les opérations quotidiennes ?	Utilisé pour la suppression ?
Création et gestion des groupes de sécurité pour Cloud Volumes ONTAP	ec2:CreateSecurityGroup	Oui.	Non	Non
	ec2:DeleteSecurityGroup	Non	Oui.	Oui.
	ec2:descriptifs des groupes de sécurité	Oui.	Oui.	Oui.
	ec2 : RevokeSecurityGroupEgress	Oui.	Non	Non
	ec2:AuthoreSecurityGroupEgress	Oui.	Non	Non
	ec2:AuthoreSecurityGroupIngress	Oui.	Non	Non
	ec2 : RevokeSecurityGroupIngress	Oui.	Oui.	Non
Créez et gérez des interfaces réseau pour Cloud Volumes ONTAP dans le sous-réseau cible	ec2:CreateNetworkinterface	Oui.	Non	Non
	ec2:DescribeNetworkinterfaces	Oui.	Oui.	Non
	ec2:DeleteNetworkinterface	Non	Oui.	Oui.
	ec2:ModilyNetworkInterfaceAttribute	Non	Oui.	Non
Obtenir la liste des sous-réseaux et groupes de sécurité de destination	ec2:DescribeSubnets	Oui.	Oui.	Non
	ec2 : descriptif	Oui.	Oui.	Non
Obtenir les serveurs DNS et le nom de domaine par défaut pour les instances Cloud Volumes ONTAP	ec2:DescribeDhcpOptions	Oui.	Non	Non
Prise de snapshots de volumes EBS pour Cloud Volumes ONTAP	ec2 : CreateSnapshot	Oui.	Oui.	Non
	ec2:DeleteSnapshot	Non	Oui.	Oui.
	ec2:snapshots descriptifs	Non	Oui.	Non

Objectif	Action	Utilisé pour le déploiement ?	Utilisé pour les opérations quotidiennes ?	Utilisé pour la suppression ?
Capturez la console Cloud Volumes ONTAP, qui est attachée aux messages AutoSupport	ec2:GetConsoleOutput	Oui.	Oui.	Non
Consultez la liste des paires de clés disponibles	ec2:Décrivez des Keypaires	Oui.	Non	Non
Consultez la liste des régions AWS disponibles	ec2:régions descriptives	Oui.	Oui.	Non
Gérez les balises des ressources associées aux instances Cloud Volumes ONTAP	ec2:DeleteTags	Non	Oui.	Oui.
	ec2:Etiquettes descriptives	Non	Oui.	Non
Créez et gérez des piles pour les modèles AWS CloudFormation	Cloudformation:CreateStack	Oui.	Non	Non
	Cloudformation:DeleteStack	Oui.	Non	Non
	Cloudformation:DescribeSacks	Oui.	Oui.	Non
	Cloudformation:DescribeStackEvents	Oui.	Non	Non
	Déformation:Validée Template	Oui.	Non	Non

Objectif	Action	Utilisé pour le déploiement ?	Utilisé pour les opérations quotidiennes ?	Utilisé pour la suppression ?
Créez et gérez un compartiment S3 utilisé par un système Cloud Volumes ONTAP comme Tier de capacité pour le Tiering des données	s3:CreateBucket	Oui.	Oui.	Non
	s3:DeleteBucket	Non	Oui.	Oui.
	s3:GetLifecyclConfiguration	Non	Oui.	Non
	s3:PutLifecyclConfiguration	Non	Oui.	Non
	s3:PutBuckeTagging	Non	Oui.	Non
	s3:ListBuckeVersions	Non	Oui.	Non
	s3:GetBucketPolicyStatus	Non	Oui.	Non
	s3:GetBuckePublicAccessBlock	Non	Oui.	Non
	s3:GetBucketAcl	Non	Oui.	Non
	s3:GetBucketPolicy	Non	Oui.	Non
	s3:PutBuckePublicAccessBlock	Non	Oui.	Non
	s3:GetBucketTaggin g	Non	Oui.	Non
	s3:GetBucketLocation	Non	Oui.	Non
	s3:ListAllMyseaux	Non	Non	Non
	s3:ListBucket	Non	Oui.	Non
Chiffrement des données Cloud Volumes ONTAP possible à l'aide du service AWS Key Management Service (KMS)	Km:liste*	Oui.	Oui.	Non
	Kms:Recrypter*	Oui.	Non	Non
	Km:décrire*	Oui.	Oui.	Non
	Kms:CreateGrant	Oui.	Oui.	Non
Obtenez des données de coût AWS pour Cloud Volumes ONTAP	ce:GetReservationUtilization	Non	Oui.	Non
	ce:GetDimensionTMValues	Non	Oui.	Non
	ce : GetCostAndUtisage	Non	Oui.	Non
	ce:GetTags	Non	Oui.	Non

Objectif	Action	Utilisé pour le déploiement ?	Utilisé pour les opérations quotidiennes ?	Utilisé pour la suppression ?
Créez et gérez un groupe de placement AWS réparti sur deux nœuds HA et le médiateur dans une seule zone de disponibilité AWS	ec2:CreatePlaceGroup	Oui.	Non	Non
	ec2:Deleteplacer dans le groupe	Non	Oui.	Oui.
Créer des rapports	fsx:décrire*	Non	Oui.	Non
	fsx:liste*	Non	Oui.	Non
Créez et gérez des agrégats prenant en charge la fonctionnalité Amazon EBS Elastic volumes	ec2:Describvolumes modificateurs	Non	Oui.	Non
	ec2 : Modifier le volume	Non	Oui.	Non

Cache global de fichiers

Le connecteur effectue les demandes d'API suivantes pour déployer des instances de cache de fichier global pendant le déploiement :

- Cloudformation:DescribeSacks
- cloudwatch:GetMetricStatistics
- Cloudformation:ListSacks

FSX pour ONTAP

Le connecteur effectue les requêtes API suivantes pour gérer FSX pour ONTAP :

- ec2:descriptifs
- ec2:DécriesInstanceStatus
- ec2:DescribeInstanceAttribute
- ec2:DescribeRoutetables
- ec2:descriptifs
- ec2:CreateTags
- ec2:Describvolumes
- ec2:descriptifs des groupes de sécurité
- ec2:DescribeNetworkinterfaces
- ec2:DescribeSubnets
- ec2 : descriptif
- ec2:DescribeDhcpOptions

- ec2:snapshots descriptifs
- ec2:Décrivez des Keypaires
- ec2:régions descriptives
- ec2:Etiquettes descriptives
- ec2:DéciesIamInstanceProfileassociations
- ec2:DescribeReserveInstanciesOfferings
- ec2:descriptionVpcEndpoints
- ec2 : descriptif
- ec2:Describvolumesmodificateurs
- ec2:descriptifs des groupes
- Km:liste*
- Km:décrire*
- Kms:CreateGrant
- Kms:Listalas
- fsx:décrire*
- fsx:liste*

Kubernetes

Le connecteur effectue les requêtes API suivantes pour détecter et gérer les clusters Amazon EKS :

- ec2:régions descriptives
- eks:Listclusters
- eks:DescribeCluster
- iam:GetInstanceProfile

Découverte des compartiments S3

Il effectue la demande d'API suivante pour détecter les compartiments Amazon S3 :

s3:GetEncryptionConfiguration

Autorisations Azure pour le connecteur

Lorsque BlueXP lance la machine virtuelle Connector dans Azure, il attache un rôle personnalisé à la machine virtuelle qui fournit au connecteur les autorisations nécessaires pour gérer les ressources et les processus au sein de cet abonnement Azure. Le connecteur utilise les autorisations pour effectuer des appels API vers plusieurs services Azure.

Autorisations de rôles personnalisées

Le rôle personnalisé illustré ci-dessous fournit les autorisations dont un connecteur a besoin pour gérer les ressources et les processus de votre réseau Azure.

Lorsque vous créez un connecteur directement à partir de BlueXP, BlueXP applique automatiquement ce rôle personnalisé au connecteur.

Si vous déployez le connecteur à partir d'Azure Marketplace ou si vous installez manuellement le connecteur sur un hôte Linux, vous devrez définir vous-même le rôle personnalisé.

Vous devez également vous assurer que le rôle est à jour lorsque de nouvelles autorisations sont ajoutées dans les versions suivantes.

```
{
    "Name": "BlueXP 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/blobServices/containers/write",
                    "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/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.Network/loadBalancers/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.ContainerService/managedClusters/listClusterUserCredential/acti
on",
                    "Microsoft.ContainerService/managedClusters/read",
                    "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.ManagedIdentity/userAssignedIdentities/assign/action"
    ],
    "NotActions": [],
    "AssignableScopes": [],
    "Description": "BlueXP Permissions",
    "IsCustom": "true"
}
```

Utilisation des autorisations Azure

Les sections suivantes décrivent la manière dont les autorisations sont utilisées pour chaque service cloud NetApp. Ces informations peuvent être utiles si vos stratégies d'entreprise exigent que les autorisations ne sont fournies que si nécessaire.

Balises AppTemplate

Le connecteur effectue les requêtes API suivantes pour gérer les balises sur les ressources Azure lorsque vous utilisez le service de balisage AppTemplate :

- Microsoft.Ressources/ressources/lecture
- Microsoft.Ressources/abonnements/résultats d'opération/lecture
- Microsoft.Ressources/abonnements/resourceGroups/read
- Microsoft.Ressources/abonnements/groupes de ressources/ressources/lecture
- Microsoft.Ressources/balises/lecture
- Microsoft.Ressources/balises/écrire

Azure NetApp Files

Il effectue les requêtes d'API suivantes pour gérer les environnements de travail Azure NetApp Files :

- 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

La sauvegarde dans le cloud

Il effectue les demandes d'API suivantes pour les opérations de sauvegarde et de restauration :

- Microsoft.Compute/virtualMachines/read
- Microsoft.Compute/virtualMachines/start/action
- Microsoft.Compute/virtualMachines/deallocate/action
- Microsoft.Storage/storageAccounts/listkeys/action
- Microsoft.Storage/storageAccounts/read
- Microsoft.Storage/storageAccounts/write
- Microsoft.Storage/storageAccounts/blobServices/containers/read
- Microsoft.KeyVault/coffres-forts/lecture
- Microsoft.KeyVault/coffres-forts/Access Policies/write
- Microsoft.Network/networkInterfaces/read
- Microsoft.Ressources/abonnements/emplacements/lecture
- Microsoft.Network/virtualNetworks/read
- Microsoft.Network/virtualNetworks/subnets/read
- Microsoft.Ressources/abonnements/resourceGroups/read
- Microsoft.Ressources/abonnements/groupes de ressources/ressources/lecture
- Microsoft.Ressources/abonnements/resourceGroups/write
- Microsoft.autorisation/verrous/*
- Microsoft.Network/privateEndpoints/write
- Microsoft.Network/privateEndpoints/read
- 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.Compute/virtualMachines/extensions/delete
- Microsoft.Compute/virtualMachines/delete
- Microsoft.Network/networkInterfaces/delete
- Microsoft.Network/networkSecurityGroups/delete
- Microsoft.Ressources/déploiements/suppression
- Microsoft.Network/publicIPAddresses/delete
- Microsoft.Storage/storageAccounts/blobServices/containers/write
- Microsoft.ManagedIdentity/userAssignedIdentities/attributable/action

Le connecteur effectue les demandes d'API suivantes lorsque vous utilisez la fonction de recherche et de restauration :

- Microsoft.Synapse/espaces de travail/écriture
- Microsoft.Synapse/espaces de travail/lecture
- Microsoft.Synapse/espaces de travail/supprimer
- Microsoft.Synapse/registre/action
- Microsoft.Synapse/checkNameAvailability/action
- Microsoft.Synapse/espaces de travail/opérationnalStatenses/lecture
- Microsoft.Synapse/espaces de travail/firewallRules/read
- Microsoft.Synapse/espaces de travail/replace AllIpFirewallRules/action
- Microsoft.Synapse/espaces de travail/opérationnalizResults/read

Sens des données cloud

Lorsque vous utilisez Cloud Data Sense, il effectue les requêtes d'API suivantes.

Action	Utilisé pour la configuration ?	Utilisé pour les opérations quotidiennes ?
Microsoft.Compute/locations/operations/read	Oui.	Oui.
Microsoft.Compute/locations/vmSizes/read	Oui.	Oui.
Microsoft.Compute/operations/read	Oui.	Oui.
Microsoft.Compute/virtualMachines/instanceView/read	Oui.	Oui.
Microsoft.Compute/virtualMachines/powerOff/action	Oui.	Non

Action	Utilisé pour la configuration ?	Utilisé pour les opérations quotidiennes ?
Microsoft.Compute/virtualMachines/read	Oui.	Oui.
Microsoft.Compute/virtualMachines/restart/action	Oui.	Non
Microsoft.Compute/virtualMachines/start/action	Oui.	Non
Microsoft.Compute/virtualMachines/vmSizes/read	Non	Oui.
Microsoft.Compute/virtualMachines/write	Oui.	Non
Microsoft.Compute/images/read	Oui.	Oui.
Microsoft.Compute/disks/delete	Oui.	Non
Microsoft.Compute/disks/read	Oui.	Oui.
Microsoft.Compute/disks/write	Oui.	Non
Microsoft.Storage/checkkamedisponibilité/read	Oui.	Oui.
Microsoft.stockage/opérations/lecture	Oui.	Oui.
Microsoft.Storage/storageAccounts/listkeys/action	Oui.	Non
Microsoft.Storage/storageAccounts/read	Oui.	Oui.
Microsoft.Storage/storageAccounts/write	Oui.	Non
Microsoft.Storage/storageAccounts/delete	Non	Oui.
Microsoft.Storage/storageAccounts/blobServices/containers/read	Oui.	Oui.
Microsoft.Network/networkInterfaces/read	Oui.	Oui.
Microsoft.Network/networkInterfaces/write	Oui.	Non
Microsoft.Network/networkInterfaces/join/action	Oui.	Non
Microsoft.Network/networkSecurityGroups/read	Oui.	Oui.
Microsoft.Network/networkSecurityGroups/write	Oui.	Non

Action	Utilisé pour la configuration ?	Utilisé pour les opérations quotidiennes ?
Microsoft.Ressources/abonnements/emplacements/lecture	Oui.	Oui.
Microsoft.Network/locations/operationResults/read	Oui.	Oui.
Microsoft.Network/locations/operations/read	Oui.	Oui.
Microsoft.Network/virtualNetworks/read	Oui.	Oui.
Microsoft.Network/virtualNetworks/checkIpAddressAvailability/read	Oui.	Oui.
Microsoft.Network/virtualNetworks/subnets/read	Oui.	Oui.
Microsoft.Network/virtualNetworks/subnets/virtualMachines/read	Oui.	Oui.
Microsoft.Network/virtualNetworks/virtualMachines/read	Oui.	Oui.
Microsoft.Network/virtualNetworks/subnets/join/action	Oui.	Non
Microsoft.Network/virtualNetworks/subnets/write	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.Ressources/ressources/lecture	Oui.	Oui.
Microsoft.Ressources/abonnements/résultats d’opération/lecture	Oui.	Oui.
Microsoft.Ressources/abonnements/resourceGroups/delete	Oui.	Non
Microsoft.Ressources/abonnements/resourceGroups/read	Oui.	Oui.
Microsoft.Ressources/abonnements/groupes de ressources/ressources/lecture	Oui.	Oui.

Action	Utilisé pour la configuration ?	Utilisé pour les opérations quotidiennes ?
Microsoft.Ressources/abonnements/resourceGroups/write	Oui.	Non

Tiering dans le cloud

Lors de la configuration de Cloud Tiering, il effectue les requêtes d'API suivantes.

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

Le connecteur effectue les demandes d'API suivantes pour les opérations quotidiennes.

- Microsoft.Storage/storageAccounts/blobServices/containers/read
- Microsoft.Storage/storageAccounts/blobServices/containers/write
- Microsoft.Storage/storageAccounts/managePolicies/read
- Microsoft.Storage/storageAccounts/managePolicies/write
- Microsoft.Storage/storageAccounts/read

Cloud Volumes ONTAP

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

Objectif	Action	Utilisé pour le déploiement ?	Utilisé pour les opérations quotidiennes ?	Utilisé pour la suppression ?
Créer des VM, arrêter, démarrer, supprimer et obtenir l'état du système	Microsoft.Compute/locations/operations/read	Oui.	Oui.	Non
	Microsoft.Compute/locations/vmSizes/read	Oui.	Oui.	Non
	Microsoft.Ressources/abonnements/emplacements/lecture	Oui.	Non	Non
	Microsoft.Compute/operations/read	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/read	Non	Oui.	Non
	Microsoft.Compute/virtualMachines/write	Oui.	Oui.	Non
Déployez à partir d'un VHD	Microsoft.Compute/images/read	Oui.	Non	Non

Objectif	Action	Utilisé pour le déploiement ?	Utilisé pour les opérations quotidiennes ?	Utilisé pour la suppression ?
Créez et gérez des interfaces réseau dans le sous-réseau cible	Microsoft.Network/networkInterfaces/read	Oui.	Oui.	Non
	Microsoft.Network/networkInterfaces/write	Oui.	Oui.	Non
	Microsoft.Network/networkInterfaces/join/action	Oui.	Oui.	Non
Créez des groupes de sécurité réseau prédéfinis	Microsoft.Network/networkSecurityGroups/read	Oui.	Oui.	Non
	Microsoft.Network/networkSecurityGroups/write	Oui.	Oui.	Non
	Microsoft.Network/networkSecurityGroups/join/action	Oui.	Non	Non
Obtenez des informations réseau sur les régions, le vnet cible et le sous-réseau, et ajoutez les machines virtuelles à VNets	Microsoft.Network/locations/operationResults/read	Oui.	Oui.	Non
	Microsoft.Network/locations/operations/read	Oui.	Oui.	Non
	Microsoft.Network/virtualNetworks/read	Oui.	Non	Non
	Microsoft.Network/virtualNetworks/checkIpAddressAvailability/read	Oui.	Non	Non
	Microsoft.Network/virtualNetworks/subnets/read	Oui.	Oui.	Non
	Microsoft.Network/virtualNetworks/subnets/virtualMachines/read	Oui.	Oui.	Non
	Microsoft.Network/virtualNetworks/virtualMachines/read	Oui.	Oui.	Non
	Microsoft.Network/virtualNetworks/subnets/join/action	Oui.	Oui.	Non

Objectif	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.Ressources/ressources/lecture	Oui.	Oui.	Non
	Microsoft.Ressources/abonnements/résultats d'opération/lecture	Oui.	Oui.	Non
	Microsoft.Ressources/abonnements/resourceGroups/delete	Oui.	Oui.	Oui.
	Microsoft.Ressources/abonnements/resourceGroups/read	Non	Oui.	Non
	Microsoft.Ressources/abonnements/groupes de ressources/ressources/lecture	Oui.	Oui.	Non
	Microsoft.Ressources/abonnements/resourceGroups/write	Oui.	Oui.	Non

Objectif	Action	Utilisé pour le déploiement ?	Utilisé pour les opérations quotidiennes ?	Utilisé pour la suppression ?
Gérez les comptes et les disques de stockage Azure	Microsoft.Compute/disks/read	Oui.	Oui.	Oui.
	Microsoft.Compute/disks/write	Oui.	Oui.	Non
	Microsoft.Compute/disks/delete	Oui.	Oui.	Oui.
	Microsoft.Storage/checkkamedisponibilité/read	Oui.	Oui.	Non
	Microsoft.stockage/opérations/lecture	Oui.	Oui.	Non
	Microsoft.Storage/storageAccounts/listkeys/action	Oui.	Oui.	Non
	Microsoft.Storage/storageAccounts/read	Oui.	Oui.	Non
	Microsoft.Storage/storageAccounts/delete	Non	Oui.	Oui.
	Microsoft.Storage/storageAccounts/write	Oui.	Oui.	Non
	Microsoft.Storage/usages/lecture	Non	Oui.	Non
Activez les sauvegardes sur le stockage Blob et le chiffrement des comptes de stockage	Microsoft.Storage/storageAccounts/blobServices/containers/read	Oui.	Oui.	Non
	Microsoft.KeyVault/coffres-forts/lecture	Oui.	Oui.	Non
	Microsoft.KeyVault/coffres-forts/AccessPolicies/write	Oui.	Oui.	Non
Activez les terminaux du service vnet pour le Tiering des données	Microsoft.Network/virtualNetworks/subnets/write	Oui.	Oui.	Non
	Microsoft.Network/routeTables/join/action	Oui.	Oui.	Non

Objectif	Action	Utilisé pour le déploiement ?	Utilisé pour les opérations quotidiennes ?	Utilisé pour la suppression ?
Créez et gérez des snapshots 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/disks/beginGetAccess/action	Non	Oui.	Non
Créer et gérer des ensembles de disponibilité	Microsoft.Compute/availabilitySets/write	Oui.	Non	Non
	Microsoft.Compute/availabilitySets/read	Oui.	Non	Non
Mettez en place des déploiements de programmation sur le marché	Microsoft.MarketplaceOrdering/Offres/éditeurs/offres/plans/accords/lecture	Oui.	Non	Non
	Microsoft.MarketplaceOrdering/Offres/éditeurs/offres/plans/accords/écrire	Oui.	Oui.	Non
Gérer un équilibreur de charge pour les paires HA	Microsoft.Network/loadBalancers/read	Oui.	Oui.	Non
	Microsoft.Network/loadBalancers/write	Oui.	Non	Non
	Microsoft.Network/loadBalancers/delete	Non	Oui.	Oui.
	Microsoft.Network/loadBalancers/backendAddressPools/read	Oui.	Oui.	Non
	Microsoft.Network/loadBalancers/loadBalancingRules/read	Oui.	Non	Non
	Microsoft.Network/loadBalancers/probes/read	Oui.	Non	Non
	Microsoft.Network/loadBalancers/probes/join/action	Oui.	Non	Non

Objectif	Action	Utilisé pour le déploiement ?	Utilisé pour les opérations quotidiennes ?	Utilisé pour la suppression ?
Activez la gestion des verrouillages sur les disques Azure	Microsoft.autorisation/verrous/*	Oui.	Oui.	Non
Activez des terminaux privés pour les paires haute disponibilité lorsque aucune connectivité ne se trouve en dehors du sous-réseau	Microsoft.Network/privateEndpoints/write	Oui.	Oui.	Non
	Microsoft.Storage/storageAccounts/PrivateEndpointConnectionsApproval/action	Oui.	Non	Non
	Microsoft.Storage/storageAccounts/privateEndpointConnections/read	Oui.	Oui.	Oui.
	Microsoft.Network/privateEndpoints/read	Oui.	Oui.	Oui.
	Microsoft.Network/privateDnsZones/write	Oui.	Oui.	Non
	Microsoft.Network/privateDnsZones/virtualNetworkLinks/write	Oui.	Oui.	Non
	Microsoft.Network/virtualNetworks/join/action	Oui.	Oui.	Non
	Microsoft.Network/privateDnsZones/A/write	Oui.	Oui.	Non
	Microsoft.Network/privateDnsZones/read	Oui.	Oui.	Non
	Microsoft.Network/privateDnsZones/virtualNetworkLinks/read	Oui.	Oui.	Non
Requis par Azure pour certains déploiements de VM, en fonction du matériel physique sous-jacent	Microsoft.Ressources/déploiements/opérations Statelis/lecture	Oui.	Oui.	Non

Objectif	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 ou de suppression du déploiement	Microsoft.Network/privateEndpoints/delete	Oui.	Oui.	Non
	Microsoft.Compute/availabilitySets/delete	Oui.	Oui.	Non
Activez l'utilisation de clés de chiffrement gérées par le client lors de l'utilisation de l'API	Microsoft.Compute/diskEncryptionSets/read	Oui.	Oui.	Oui.
	Microsoft.Compute/diskEncryptionSets/write	Oui.	Oui.	Non
	Microsoft.KeyVault/coffres-forts/déploiement/action	Oui.	Non	Non
	Microsoft.Compute/diskEncryptionSets/delete	Oui.	Oui.	Oui.
Configurez un groupe de sécurité des applications pour une paire haute disponibilité afin d'isoler les cartes réseau d'interconnexion haute disponibilité et de cluster	Microsoft.Network/applicationSecurityGroups/write	Non	Oui.	Non
	Microsoft.Network/applicationSecurityGroups/read	Non	Oui.	Oui.
	Microsoft.Network/applicationSecurityGroups/joinIpConfiguration/action	Non	Oui.	Non
	Microsoft.Network/networkSecurityGroups/securityRules/write	Oui.	Oui.	Non
	Microsoft.Network/applicationSecurityGroups/delete	Non	Oui.	Non
	Microsoft.Network/networkSecurityGroups/securityRules/delete	Non	Oui.	Oui.

Objectif	Action	Utilisé pour le déploiement ?	Utilisé pour les opérations quotidiennes ?	Utilisé pour la suppression ?
Balises de lecture, d'écriture et de suppression associées aux ressources Cloud Volumes ONTAP	Microsoft.Ressources/balises/lecture	Non	Oui.	Non
	Microsoft.Ressources/balises/écrire	Oui.	Oui.	Non
	Microsoft.Ressources/balises/Supprimer	Oui.	Non	Non
Crypter les comptes de stockage pendant leur création	Microsoft.ManagedIdentity/userAssignedIdentities/attributable/action	Oui.	Oui.	Non

Cache global de fichiers

Lorsque vous utilisez Global File cache, le connecteur effectue les demandes d'API suivantes :

- Microsoft.Insights/Metrics/Read
- Microsoft.Compute/virtualMachines/extensions/write
- Microsoft.Compute/virtualMachines/extensions/read
- Microsoft.Compute/virtualMachines/extensions/delete
- Microsoft.Compute/virtualMachines/delete
- Microsoft.Network/networkInterfaces/delete
- Microsoft.Network/networkSecurityGroups/delete
- Microsoft.Ressources/déploiements/suppression

Kubernetes

Ce connecteur effectue les requêtes d'API suivantes pour détecter et gérer les clusters exécutés dans Azure Kubernetes Service (AKS) :

- Microsoft.Compute/virtualMachines/read
- Microsoft.Ressources/abonnements/emplacements/lecture
- Microsoft.Ressources/abonnements/résultats d'opération/lecture
- Microsoft.Ressources/abonnements/resourceGroups/read
- Microsoft.Ressources/abonnements/groupes de ressources/ressources/lecture
- Microsoft.ContainerService/manageClusters/lecture
- Microsoft.ContainerService/manageClusters/listClusterUserCredential/action

Journal des modifications

Lorsque des autorisations sont ajoutées et supprimées, nous les noterons dans les sections ci-dessous.

1er décembre 2022

L'autorisation suivante a été ajoutée à la politique JSON. Elle est requise pour la sauvegarde dans le cloud et NetApp Cloud Tiering.

Microsoft.Storage/storageAccounts/blobServices/containers/write

Les autorisations suivantes ont été supprimées de la politique JSON. Ils ne sont plus nécessaires.

- Microsoft.Compute/images/write
- Microsoft.Network/loadBalancers/backendAddressPools/join/action
- Microsoft.Network/loadBalancers/frontendIPConfigurations/read
- Microsoft.Storage/storageAccounts/regénérateur/action

Autorisations Google Cloud pour le connecteur

BlueXP requiert des autorisations pour effectuer des actions dans Google Cloud. Ces autorisations sont incluses dans un rôle personnalisé fourni par NetApp. Vous voudrez peut-être comprendre ce que BlueXP fait avec ces autorisations.

Autorisations de compte de service

Le rôle personnalisé illustré ci-dessous fournit les autorisations dont un connecteur a besoin pour gérer les ressources et les processus au sein de votre réseau Google Cloud.

Vous devez appliquer ce rôle personnalisé à un compte de service rattaché à la machine virtuelle Connector. "Affichez les instructions détaillées".

Vous devez également vous assurer que le rôle est à jour lorsque de nouvelles autorisations sont ajoutées dans les versions suivantes.

```
title: NetApp BlueXP
description: Permissions for the service account associated with the
Connector instance.
stage: GA
includedPermissions:
- iam.serviceAccounts.actAs
- compute.regionBackendServices.create
- compute.regionBackendServices.get
- compute.regionBackendServices.list
- compute.networks.updatePolicy
- compute.backendServices.create
- compute.addresses.list
- 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.globalOperations.get
- 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.machineTypes.get
- compute.networks.get
- compute.networks.list
- compute.projects.get
- compute.regions.get
- compute.regions.list
- 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
- resourcemanager.projects.get
- storage.buckets.create
- storage.buckets.delete
- storage.buckets.get
- storage.buckets.list
- cloudkms.cryptoKeyVersions.useToEncrypt
- cloudkms.cryptoKeys.get
- cloudkms.cryptoKeys.list
- cloudkms.keyRings.list
- storage.buckets.update
- iam.serviceAccounts.getIamPolicy
- iam.serviceAccounts.list
- storage.objects.get
- storage.objects.list
- monitoring.timeSeries.list
- storage.buckets.getIamPolicy
```

Utilisation des autorisations Google Cloud

Actions	Objectif
- Compute.disks.create - Compute.disks.createSnapshot - compute.disks.delete - Compute.disks.get - Compute.disks.list - compute.disks.setLabels - compute.disks.use	Pour créer et gérer des disques pour Cloud Volumes ONTAP.
- compute.firewalls.create - compute.firewalls.delete - compute.firewalls.get - compute.firewalls.list	Pour créer des règles de pare-feu pour Cloud Volumes ONTAP.
- Compute.globalOperations.get	Pour obtenir l'état des opérations.

Actions	Objectif
- Compute.images.get - Compute.images.getFromFamily - Compute.images.list - compute.images.useReadOnly	Pour obtenir les images des instances de VM.
- compute.instances.attachDisk - compute.instances.detachDisk	Pour attacher et détacher les disques à Cloud Volumes ONTAP.
- compute.instances.create - compute.instances.delete	Pour créer et supprimer des instances de VM Cloud Volumes ONTAP.
- compute.instances.get	Pour afficher la liste des instances de VM.
- compute.instances.getSerialPortOutput	Pour obtenir les journaux de la console.
- compute.instances.list	Pour récupérer la liste des instances dans une zone.
- compute.instances.setDeletionProtection	Pour définir la protection de suppression sur l'instance.
- compute.instances.setLabels	Pour ajouter des étiquettes.
- compute.instances.setMachineType - compute.instances.setMinCpuPlatform	Pour modifier le type de machine pour Cloud Volumes ONTAP.
- compute.instances.setMetadata	Pour ajouter des métadonnées.
- compute.instances.setTags	Pour ajouter des balises pour les règles de pare-feu.
- compute.instances.start - compute.instances.stop - compute.instances.updateDisplayDevice	Pour démarrer et arrêter Cloud Volumes ONTAP.
- Compute.machineTypes.get	Pour obtenir le nombre de cœurs à vérifier qoupas.
- compute.projects.get	Pour prendre en charge des projets multiples.
- Compute.snapshots.create - compute.snapshots.delete - Compute.snapshots.get - Compute.snapshots.list - compute.snapshots.setLabels	Pour créer et gérer des snapshots de disques persistants.
- compute.networks.get - compute.networks.list - Compute.rerégions.get - Compute.rerégions.list - Compute.subNetworks.get - Compute.subNetworks.list - Compute.zoneOperations.get - Compute.zones.get - Compute.zones.zones.list	Pour obtenir les informations de mise en réseau nécessaires à la création d'une nouvelle instance de machine virtuelle Cloud Volumes ONTAP.

Actions	Objectif
- deploymentmanager.compositeTypes.get - deploymentmanager.compositeTypes.list - deploymentmanager.deployments.create - deploymentmanager.deployments.delete - deploymentmanager.deployments.get - deploymentmanager.deployments.list - deploymentmanager.manifestes.get - deploymentmanager.manifestes.list - deploymentmanager.Operations.get - deploymentmanager.Operations.list - deploymentmanager.resources.get - deploymentmanager.resources.list - deploymentmanager.typeProviders.get.types.deploymentmanager.deploymentmanager.deploymentlist.types.deploymentmanager.deploymentlist.deploymentmanager.deploymentmanager.Deploymenttypes.DeploymentManager.Deploymentlist.Deploymenttypes.DeploymentManager.Deployment	Pour déployer l'instance de machine virtuelle Cloud Volumes ONTAP à l'aide de Google Cloud Deployment Manager.
- Logging.logEntries.list - logging.privateLogEntries.list	Pour obtenir les disques de consignation des piles.
- resourcemanager.projects.get	Pour prendre en charge des projets multiples.
- storage.seaux.create - storage.buckets.delete - storage.seaux.get - storage.seaux.list - storage.seaux.update	Pour créer et gérer un compartiment Google Cloud Storage pour le Tiering des données.
- cloudkms.cryptoKeyVersions.useToEncrypt - cloudkms.cryptoKeys.get - cloudkms.crypKeys.list - cloudkms.keyrings.list	Pour utiliser des clés de chiffrement gérées par le client à partir du service Cloud Key Management avec Cloud Volumes ONTAP.
- compute.instances.setServiceAccount - iam.serviceAccounts.actAs - iam.serviceAccounts.getIamPolicy - iam.serviceAccounts.list - Storage.objects.get - Storage.objects.list	Pour définir un compte de service sur l'instance Cloud Volumes ONTAP. Ce compte de service fournit des autorisations de Tiering des données vers un compartiment Google Cloud Storage.
- compute.adresses.list	Pour récupérer les adresses d'une région lors du déploiement d'une paire haute disponibilité.
- Compute.backendServices.create - Compute.régionBackendServices.create - Compute.régionBackendServices.get - Compute.régionBackendServices.list	Pour configurer un service back-end pour la distribution du trafic dans une paire HA.
- compute.networks.updatePolicy	Pour appliquer des règles de pare-feu sur les VPC et les sous-réseaux d'une paire HA.
- compute.subnetworks.use - compute.subnetworks.useExternalIp - compute.instances.addAccessConfig	Pour activer le sens des données du cloud.
- container.cluster.get - container.cluster.list	Pour détecter les clusters Kubernetes s'exécutant dans Google Kubernetes Engine.
- compute.instanceGroups.get - Compute.adresses.get	Pour créer et gérer des VM de stockage sur des paires haute disponibilité.

Actions	Objectif
- Monitoring.timeseries.list - Storage.seaux.getIamPolicy	Pour découvrir des compartiments Google Cloud Storage.

Ports

Règles de groupe de sécurité dans AWS

Le groupe de sécurité AWS du connecteur nécessite à la fois des règles entrantes et sortantes.

Règles entrantes

Protocole	Port	Objectif
SSH	22	Fournit un accès SSH à l'hôte du connecteur
HTTP	80	Fournit un accès HTTP à partir des navigateurs Web du client vers l'interface utilisateur locale
HTTPS	443	Fournit un accès HTTPS à partir des navigateurs Web du client vers l'interface utilisateur locale et des connexions à partir de l'instance Cloud Data Sense
TCP	3128	Permet à Cloud Volumes ONTAP d'accéder à Internet pour l'envoi des messages AutoSupport au support NetApp. Vous devez ouvrir ce port manuellement après le déploiement. server for AutoSupport messages,En savoir plus sur le serveur proxy du connecteur.
TCP	9060	Il est possible d'activer et d'utiliser Cloud Data Sense et Cloud Backup dans les déploiements dans le cloud pour les administrations publiques. Ce port est également requis pour Cloud Backup si vous désactivez l'interface SaaS dans votre compte BlueXP.

Règles de sortie

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

Règles de base pour les appels sortants

Le groupe de sécurité prédéfini pour le connecteur inclut les règles de trafic sortant suivantes.

Protocole	Port	Objectif
Tous les protocoles TCP	Tout	Tout le trafic sortant
Tous les protocoles UDP	Tout	Tout le trafic sortant

Règles de sortie 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 le connecteur.

L'adresse IP source est l'hôte du connecteur.

Service	Protocole	Port	Destination	Objectif
Appels API et AutoSupport	HTTPS	443	LIF de gestion de cluster ONTAP et Internet sortant	Appels d'API vers AWS et ONTAP, vers le cloud Data Sense, vers le service ransomware et envoi de messages AutoSupport à NetApp
Appels API	TCP	3000	ONTAP HA médiateur	Communication avec le médiateur ONTAP HA
	TCP	8088	Sauvegarde vers S3	Appels d'API vers Backup vers S3
DNS	UDP	53	DNS	Utilisé pour la résolution DNS par BlueXP

Règles de groupe de sécurité dans Azure

Le groupe de sécurité Azure pour le connecteur nécessite à la fois des règles entrantes et sortantes.

Règles entrantes

Protocole	Port	Objectif
SSH	22	Fournit un accès SSH à l'hôte du connecteur
HTTP	80	Fournit un accès HTTP à partir des navigateurs Web du client vers l'interface utilisateur locale
HTTPS	443	Fournit un accès HTTPS à partir des navigateurs Web du client vers l'interface utilisateur locale et des connexions à partir de l'instance Cloud Data Sense

Protocole	Port	Objectif
TCP	3128	Permet à Cloud Volumes ONTAP d'accéder à Internet pour l'envoi des messages AutoSupport au support NetApp. Vous devez ouvrir ce port manuellement après le déploiement. server for AutoSupport messages,En savoir plus sur le serveur proxy du connecteur.
TCP	9060	Il est possible d'activer et d'utiliser Cloud Data Sense et Cloud Backup dans les déploiements dans le cloud pour les administrations publiques. Ce port est également requis pour Cloud Backup si vous désactivez l'interface SaaS dans votre compte BlueXP.

Règles de sortie

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

Règles de base pour les appels sortants

Le groupe de sécurité prédéfini pour le connecteur inclut les règles de trafic sortant suivantes.

Protocole	Port	Objectif
Tous les protocoles TCP	Tout	Tout le trafic sortant
Tous les protocoles UDP	Tout	Tout le trafic sortant

Règles de sortie 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 le connecteur.

L'adresse IP source est l'hôte du connecteur.

Service	Protocole	Port	Destination	Objectif
Appels API et AutoSupport	HTTPS	443	LIF de gestion de cluster ONTAP et Internet sortant	Appels d'API vers Azure et ONTAP, vers le cloud Data Sense, vers le service ransomware et envoi de messages AutoSupport à NetApp
DNS	UDP	53	DNS	Utilisé pour la résolution DNS par BlueXP

Règles de pare-feu dans Google Cloud

Les règles de pare-feu Google Cloud pour le connecteur exigent à la fois des règles entrantes et sortantes.

Règles entrantes

Protocole	Port	Objectif
SSH	22	Fournit un accès SSH à l'hôte du connecteur
HTTP	80	Fournit un accès HTTP à partir des navigateurs Web du client vers l'interface utilisateur locale
HTTPS	443	Fournit un accès HTTPS à partir des navigateurs Web du client vers l'interface utilisateur locale
TCP	3128	Permet à Cloud Volumes ONTAP d'accéder à Internet pour l'envoi des messages AutoSupport au support NetApp. Vous devez ouvrir ce port manuellement après le déploiement. server for AutoSupport messages,En savoir plus sur le serveur proxy du connecteur.

Règles de sortie

Les règles de pare-feu prédéfinies pour le connecteur ouvrent tout le trafic sortant. Si cela est acceptable, suivez les règles de base de l'appel sortant. Si vous avez besoin de règles plus rigides, utilisez les règles de sortie avancées.

Règles de base pour les appels sortants

Les règles de pare-feu prédéfinies pour le connecteur comprennent les règles de trafic sortant suivantes.

Protocole	Port	Objectif
Tous les protocoles TCP	Tout	Tout le trafic sortant

Protocole	Port	Objectif
Tous les protocoles UDP	Tout	Tout le trafic sortant

Règles de sortie 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 le connecteur.

L'adresse IP source est l'hôte du connecteur.

Service	Protocole	Port	Destination	Objectif
Appels API et AutoSupport	HTTPS	443	LIF de gestion de cluster ONTAP et Internet sortant	Appels d'API vers GCP et ONTAP, vers le cloud Data Sense, vers le service ransomware et envoi de messages AutoSupport à NetApp
DNS	UDP	53	DNS	Utilisé pour la résolution DNS par BlueXP

Ports pour le connecteur sur site

Le connecteur utilise les ports *Inbound* suivants lorsqu'il est installé manuellement sur un hôte Linux sur site.

Ces règles entrantes s'appliquent aux deux modèles de déploiement du connecteur sur site, installé avec accès à Internet ou sans accès à Internet.

Protocole	Port	Objectif
HTTP	80	Fournit un accès HTTP à partir des navigateurs Web du client vers l'interface utilisateur locale
HTTPS	443	Fournit un accès HTTPS à partir des navigateurs Web du client vers l'interface utilisateur locale

Informations sur le copyright

Informations sur les marques commerciales