Referenz

Set up and administration

NetApp
November 23, 2022

Inhaltsverzeichnis

Referenz

Berechtigungen

Zusammenfassung der Berechtigungen für BlueXP

Um die Funktionen und Services in BlueXP nutzen zu können, müssen Sie Berechtigungen bereitstellen, damit BlueXP die Abläufe in Ihrer Cloud-Umgebung ausführen kann. Über die Links auf dieser Seite können Sie schnell auf die Berechtigungen zugreifen, die Sie basierend auf Ihrem Ziel benötigen.

AWS Berechtigungen

Zweck	Beschreibung	Verlinken
Connector-Bereitstellung	Der Benutzer, der einen Connector von BlueXP erstellt, benötigt spezielle Berechtigungen, um die Instanz in AWS bereitzustellen.	"Erstellen Sie einen Connector in AWS von BlueXP"
Verbindungsbetrieb	Beim Start des Connectors durch BlueXP wird eine Richtlinie an die Instanz angehängt, die die erforderlichen Berechtigungen für das Management von Ressourcen und Prozessen in Ihrem AWS-Konto bereitstellt. Sie müssen die Richtlinie selbst einrichten, wenn Sie dies tun "Starten Sie einen Connector vom Markt aus" Oder wenn Sie "Fügen Sie weitere AWS Zugangsdaten zu einem Connector hinzu". Außerdem müssen Sie sicherstellen, dass die Richtlinie aktuell ist, wenn neue Berechtigungen in nachfolgenden Releases hinzugefügt werden.	"AWS-Berechtigungen für den Connector"
Cloud Volumes ONTAP Betrieb	Eine IAM-Rolle muss mit jedem Cloud Volumes ONTAP-Node in AWS verbunden sein. Das gleiche gilt für den HA Mediator. Standardmäßig können BlueXP die IAM-Rollen für Sie erstellen lassen, Sie können jedoch Ihre eigenen Funktionen verwenden.	"Erfahren Sie, wie Sie die IAM-Rollen selbst einrichten"

Azure-Berechtigungen

Zweck	Beschreibung	Verlinken
Connector-Bereitstellung	Wenn Sie einen Connector von BlueXP bereitstellen, müssen Sie ein Azure-Konto oder einen Service-Principal verwenden, der über die Berechtigungen zum Bereitstellen der Connector-VM in Azure verfügt.	"Erstellen Sie einen Connector in Azure von BlueXP"

Zweck	Beschreibung	Verlinken
Verbindungsbetrieb	Wenn BlueXP die Connector VM in Azure implementiert, wird eine benutzerdefinierte Rolle erstellt, die die erforderlichen Berechtigungen für das Management von Ressourcen und Prozessen im Azure Abonnement bietet. Sie müssen die benutzerdefinierte Rolle selbst einrichten, wenn Sie "Starten Sie einen Connector vom Markt aus" Oder wenn Sie "Fügen Sie weitere Azure Credentials zu einem Connector hinzu". Außerdem müssen Sie sicherstellen, dass die Richtlinie aktuell ist, wenn neue Berechtigungen in nachfolgenden Releases hinzugefügt werden.	"Azure-Berechtigungen für den Connector"

Google Cloud-Berechtigungen

Zweck	Beschreibung	Verlinken
Connector-Bereitstellung	Der Google Cloud-Benutzer, der einen Connector von BlueXP bereitstellt, benötigt spezielle Berechtigungen, um den Connector in Google Cloud bereitzustellen.	"Richten Sie Berechtigungen für die Bereitstellung des Connectors ein"
Verbindungsbetrieb	Das Servicekonto für die Connector-VM-Instanz muss über spezielle Berechtigungen für den täglichen Betrieb verfügen. Sie müssen das Servicekonto mit dem Connector verknüpfen, wenn Sie es über BlueXP bereitstellen. Außerdem müssen Sie sicherstellen, dass die Richtlinie aktuell ist, wenn neue Berechtigungen in nachfolgenden Releases hinzugefügt werden.	"Richten Sie ein Servicekonto für den Konnektor ein"

AWS-Berechtigungen für den Connector

Beim Start der Connector-Instanz in AWS hängt BlueXP eine Richtlinie an die Instanz an, die dem Connector Berechtigungen für das Management von Ressourcen und Prozessen innerhalb dieses AWS-Kontos bietet. Der Connector verwendet die Berechtigungen, um API-Aufrufe an verschiedene AWS Services wie EC2, S3, CloudFormation, IAM, Der Key Management Service (KMS) und vieles mehr.

IAM-Richtlinien

Die unten verfügbaren IAM-Richtlinien bieten die Berechtigungen, die ein Connector zur Verwaltung von Ressourcen und Prozessen innerhalb Ihrer Public-Cloud-Umgebung basierend auf Ihrer AWS-Region benötigt.

Wenn Sie einen Connector in einer standardmäßigen AWS-Region direkt aus BlueXP erstellen, wendet BlueXP automatisch Richtlinien auf den Connector an. Sie müssen in diesem Fall nichts tun.

Wenn Sie den Connector über den AWS Marketplace bereitstellen oder den Connector manuell auf einem

Linux-Host installieren, müssen Sie die Richtlinien selbst festlegen.

Außerdem müssen Sie sicherstellen, dass die Richtlinien immer auf dem neuesten Stand sind, wenn neue Berechtigungen in nachfolgenden Releases hinzugefügt werden.

Wählen Sie Ihre Region aus, um die erforderlichen Richtlinien anzuzeigen:

Beispiel 1. Standardregionen

Für Standardregionen werden die Berechtigungen auf zwei Richtlinien verteilt. Zwei Richtlinien sind aufgrund einer maximal zulässigen Zeichengröße für gemanagte Richtlinien in AWS erforderlich.

Die erste Richtlinie bietet Berechtigungen für folgende Dienste:

- Cloud-Backup
- Cloud-Daten Sinnvoll
- Cloud Tiering
- Cloud Volumes ONTAP
- FSX für ONTAP
- S3-Bucket-Erkennung

Die zweite Richtlinie bietet Berechtigungen für die folgenden Dienste:

- AppTemplate-Tagging
- Globaler Datei-Cache
- Kubernetes

Richtlinie #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/*"
            ]
        }
    ]
```

```
    }
```

Richtlinie #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": "*"
    }
  ]
}
```

Beispiel 2. GovCloud (USA) Regionen

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

Beispiel 3. C2S-Umgebung

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

Wie werden die AWS Berechtigungen verwendet

In den folgenden Abschnitten wird die Nutzung der Berechtigungen für den jeweiligen NetApp Cloud-Service beschrieben. Diese Informationen können hilfreich sein, wenn Ihre Unternehmensrichtlinien vorschreiben, dass Berechtigungen nur bei Bedarf bereitgestellt werden.

AppTemplate-Tags

Der Connector stellt die folgenden API-Anforderungen zur Verwaltung von Tags auf AWS-Ressourcen bereit, wenn Sie den AppTemplate Tagging-Service verwenden:

- ec2:CreateTags
- ec2:DeleteTags
- ec2:DescribeTags
- Tag:getResources
- Tag:getTagKeys
- Tag:getTagValues
- Tag:TagResources
- Tag:UntagRessourcen

Cloud-Backup

Der Connector stellt die folgenden API-Anfragen zur Bereitstellung der Wiederherstellungsinstanz für Cloud-Backup bereit:

- ec2:StartInstances
- ec2:StopInstances
- ec2:DescribeInstances
- ec2:DescribeInstanceStatus
- ec2:RunInstances
- ec2:TerminateInstances
- ec2:DescribeInstanceAttribut
- ec2:DescribeBilder
- ec2:CreateTags
- ec2:CreateVolume
- ec2:CreateSecurityGroup
- ec2:DescribeSubnets
- ec2:DescribeVpcs
- ec2:DescribeRegionen
- CloudFormation:CreateStack
- CloudFormation:DeleteStack
- Wolkenbildung:DescribeStacks

Der Connector stellt folgende API-Anforderungen zum Management von Backups in Amazon S3:

- s3:GetBucketLocation
- s3:ListAllMyBuchs
- s3:ListBucket
- s3:CreateBucket
- s3:GetLifecycleKonfiguration
- s3:PutLifecycleKonfiguration
- s3:PutBucketTagging
- s3:ListBucketVersions
- s3:GetBucketAcl
- s3:PutBucketPublicAccessBlock
- Km:Liste*
- Km:Beschreiben*
- s3:GetObject
- ec2:descbeVpcEndpunkte
- Km:ListAliase

- s3:PutVerschlüsselungKonfiguration

Der Connector stellt folgende API-Anforderungen vor, wenn Sie die Methode Suchen und Wiederherstellen verwenden, um Volumes und Dateien wiederherzustellen:

- s3:CreateBucket
- s3:DeleteObject
- s3:DeleteObjectVersion
- s3:GetBucketAcl
- s3:ListBucket
- s3:ListBucketVersions
- s3:ListBucketMultipartUploads
- s3:PutObject
- s3:PutBucketAcl
- s3:PutLifecycleKonfiguration
- s3:PutBucketPublicAccessBlock
- s3:AbortMehrteilaUpload
- s3:ListeMultipartUploadParts
- athena:StartQueryExecutionc
- athena:GetQueryResults
- athena:GetQueryExecution
- athena:StoppQueryExecution
- Kleber:CreateDatabase
- Kleber:CreateTable
- Kleber:BatchDeletePartition

Der Connector macht die folgenden API-Anforderungen, wenn Sie DataLock und Ransomware-Schutz für Ihre Volume-Backups verwenden:

- s3:GetObjectVersionTagging
- s3:GetBucketObjectLockConfiguration
- s3:GetObjectVersionAkl
- s3:PuttObjectTagging
- s3:DeleteObject
- s3:DeleteObjectTagging
- s3:GetObjectRetention
- s3:DeleteObjectVersionTagging
- s3:PutObject
- s3:GetObject
- s3:PutBucketObjectLockConfiguration

- s3:GetLifecycleKonfiguration
- s3:ListBucketByTags
- s3:GetBucketTagging
- s3:DeleteObjectVersion
- s3:ListBucketVersions
- s3:ListBucket
- s3:PutBucketTagging
- s3:GetObjectTagging
- s3:PutBucketVersionierung
- s3:PuttObjectVersionTagging
- s3:GetBucketVersionierung
- s3:GetBucketAcl
- s3:BypassGovernanceAufbewahrung
- s3:PutObjectRetention
- s3:GetBucketLocation
- s3:GetObjectVersion

Der Connector macht die folgenden API-Anforderungen, wenn Sie ein anderes AWS-Konto für Ihre Cloud Volumes ONTAP-Backups verwenden, als Sie für die Quell-Volumes verwenden:

- s3:PutBucketPolicy
- s3:PutBucketEigentümerControls

Cloud-Daten Sinnvoll

Der Connector stellt die folgenden API-Anforderungen zur Bereitstellung der Cloud Data Sense Instanz:

- ec2:DescribeInstances
- ec2:DescribeInstanceStatus
- ec2:RunInstances
- ec2:TerminateInstances
- ec2:CreateTags
- ec2:CreateVolume
- ec2:AttachVolume
- ec2:CreateSecurityGroup
- ec2:DeleteSecurityGroup
- ec2:DescribeSecurityGroups
- ec2:CreateNetworkInterface
- ec2:DescribeNetworkInterfaces
- ec2:DeleteNetworkInterface
- ec2:DescribeSubnets

- ec2:DescribeVpcs
- ec2:CreateSnapshot
- ec2:DescribeRegionen
- CloudFormation:CreateStack
- CloudFormation:DeleteStack
- Wolkenbildung:DescribeStacks
- Molkenbildung:DescribeStackEvents
- iam:AddRoleToInstanceProfile
- ec2:AssociateIamInstanceProfil
- ec2:DescribeIamInstanceProfilVerbände

Der Connector erstellt bei Verwendung von Cloud Data Sense die folgenden API-Anforderungen zum Scannen von S3-Buckets:

- iam:AddRoleToInstanceProfile
- ec2:AssociateIamInstanceProfil
- ec2:DescribeIamInstanceProfilVerbände
- s3:GetBucketTagging
- s3:GetBucketLocation
- s3:ListAllMyBuchs
- s3:ListBucket
- s3:GetBucketPolicyStatus
- s3:GetBucketPolicy
- s3:GetBucketAcl
- s3:GetObject
- iam:GetRole
- s3:DeleteObject
- s3:DeleteObjectVersion
- s3:PutObject
- STS:AssumeRole

Cloud Tiering

Der Connector erstellt bei Verwendung von Cloud Tiering die folgenden API-Anforderungen an das Tiering von Daten in Amazon S3.

Aktion	Wird zur Einrichtung verwendet?	Wird für den täglichen Betrieb verwendet?
s3:CreateBucket	Ja.	Nein
s3:PutLifecycleKonfiguration	Ja.	Nein
s3:GetLifecycleKonfiguration	Ja.	Ja.

Aktion	Wird zur Einrichtung verwendet?	Wird für den täglichen Betrieb verwendet?
ec2:DescribeRegionen	Ja.	Ja.

Cloud Volumes ONTAP

Der Connector stellt die folgenden API-Anforderungen für die Implementierung und das Management von Cloud Volumes ONTAP in AWS.

Zweck	Aktion	Werden sie für die Implementierung verwendet?	Wird für den täglichen Betrieb verwendet?	Zum Löschen verwendet?
Erstellung und Management von IAM-Rollen und Instanzprofilen für Cloud Volumes ONTAP Instanzen	iam:ListInstanceProfiles	Ja.	Ja.	Nein
	iam:CreateRollenole	Ja.	Nein	Nein
	iam:DeleteRole	Nein	Ja.	Ja.
	iam:PuttePolicy	Ja.	Nein	Nein
	iam:CreateInstanceProfil	Ja.	Nein	Nein
	iam:DeleteRolePolicy	Nein	Ja.	Ja.
	iam:AddRoleToInstanceProfile	Ja.	Nein	Nein
	iam:RemoveRoleFromInstanceProfile	Nein	Ja.	Ja.
	iam:DeleteInstanceProfil	Nein	Ja.	Ja.
	iam:PassRole	Ja.	Nein	Nein
	ec2:AssociateIamInstanceProfil	Ja.	Ja.	Nein
	ec2:DescribeIamInstanceProfilVerbände	Ja.	Ja.	Nein
	ec2:DisassociateIamInstanceProfil	Nein	Ja.	Nein
Dekodieren von Autorisierungsstatusmeldungen	STS:DekodeAuthorisationNachricht	Ja.	Ja.	Nein
Beschreiben Sie die angegebenen Bilder (Amis), die dem Konto zur Verfügung stehen	ec2:DescribeBilder	Ja.	Ja.	Nein

Zweck	Aktion	Werden sie für die Implementierung verwendet?	Wird für den täglichen Betrieb verwendet?	Zum Löschen verwendet?
Routingtabellen in einer VPC beschreiben (nur für HA-Paare erforderlich)	ec2:DescribeRouteTables	Ja.	Nein	Nein
Beenden, starten und überwachen Sie Instanzen	ec2:StartInstances	Ja.	Ja.	Nein
	ec2:StopInstances	Ja.	Ja.	Nein
	ec2:DescribeInstances	Ja.	Ja.	Nein
	ec2:DescribeInstanceStatus	Ja.	Ja.	Nein
	ec2:RunInstances	Ja.	Nein	Nein
	ec2:TerminateInstances	Nein	Nein	Ja.
	ec2:ModifyInstanceAttribut	Nein	Ja.	Nein
Vergewissern Sie sich, dass erweitertes Networking für unterstützte Instanztypen aktiviert ist	ec2:DescribeInstanceAttribut	Nein	Ja.	Nein
Markieren Sie Ressourcen mit den Tags „WorkingEnvironment“ und „WorkingEnvironment ID“, die zur Wartung und Kostenverteilung verwendet werden	ec2:CreateTags	Ja.	Ja.	Nein
Management von EBS Volumes, die Cloud Volumes ONTAP als Back-End Storage verwendet	ec2:CreateVolume	Ja.	Ja.	Nein
	ec2:DescribeVolumes	Ja.	Ja.	Ja.
	ec2:ModifyVolumeAttribute	Nein	Ja.	Ja.
	ec2:AttachVolume	Ja.	Ja.	Nein
	ec2:DeleteVolume	Nein	Ja.	Ja.
	ec2:DetachVolume	Nein	Ja.	Ja.

Zweck	Aktion	Werden sie für die Implementierung verwendet?	Wird für den täglichen Betrieb verwendet?	Zum Löschen verwendet?
Erstellen und Managen von Sicherheitsgruppen für Cloud Volumes ONTAP	ec2:CreateSecurityGroup	Ja.	Nein	Nein
	ec2:DeleteSecurityGroup	Nein	Ja.	Ja.
	ec2:DescribeSecurityGroups	Ja.	Ja.	Ja.
	ec2:RevokeSecurityGroupEgress	Ja.	Nein	Nein
	ec2:AuthoriseSecurityGroupEgress	Ja.	Nein	Nein
	ec2:AuthoriseSecurityGroupIngress	Ja.	Nein	Nein
	ec2:RevokeSecurityGroupIngress	Ja.	Ja.	Nein
Netzwerkschnittstellen für Cloud Volumes ONTAP im Ziel-Subnetz erstellen und verwalten	ec2:CreateNetworkInterface	Ja.	Nein	Nein
	ec2:DescribeNetworkInterfaces	Ja.	Ja.	Nein
	ec2:DeleteNetworkInterface	Nein	Ja.	Ja.
	ec2:ModifyNetworkInterface Attribute	Nein	Ja.	Nein
Abrufen der Liste der Zielnetze und -Sicherheitsgruppen	ec2:DescribeSubnets	Ja.	Ja.	Nein
	ec2:DescribeVpcs	Ja.	Ja.	Nein
Abrufen der DNS-Server und des Standard-Domain-Namens für Cloud Volumes ONTAP-Instanzen	ec2:DescribeDhcpOptions	Ja.	Nein	Nein
Erstellen von Snapshots von EBS Volumes für Cloud Volumes ONTAP	ec2:CreateSnapshot	Ja.	Ja.	Nein
	ec2:DeleteSnapshot	Nein	Ja.	Ja.
	ec2:DescribeSnapshots	Nein	Ja.	Nein

Zweck	Aktion	Werden sie für die Implementierung verwendet?	Wird für den täglichen Betrieb verwendet?	Zum Löschen verwendet?
Erfassen Sie die Cloud Volumes ONTAP Konsole, die an AutoSupport Meldungen angeschlossen ist	ec2:GetConsoleOutput	Ja.	Ja.	Nein
Erhalten Sie die Liste der verfügbaren Schlüsselpaare	ec2:DescribeKeypairs	Ja.	Nein	Nein
Hier erhalten Sie eine Liste der verfügbaren AWS Regionen	ec2:DescribeRegionen	Ja.	Ja.	Nein
Verwalten von Tags für Ressourcen, die Cloud Volumes ONTAP Instanzen zugeordnet sind	ec2:DeleteTags	Nein	Ja.	Ja.
	ec2:DescribeTags	Nein	Ja.	Nein
Stacks für AWS CloudFormation-Vorlagen erstellen und managen	CloudFormation:CreateStack	Ja.	Nein	Nein
	CloudFormation:DeleteStack	Ja.	Nein	Nein
	Wolkenbildung:DescribeStacks	Ja.	Ja.	Nein
	Molkenbildung:DescribeStackEvents	Ja.	Nein	Nein
	Cloudformation:ValidierteVorlage	Ja.	Nein	Nein

Zweck	Aktion	Werden sie für die Implementierung verwendet?	Wird für den täglichen Betrieb verwendet?	Zum Löschen verwendet?
Es wird ein S3-Bucket erstellt und gemanagt, den ein Cloud Volumes ONTAP System als Kapazitäts-Tier für Daten-Tiering verwendet	s3:CreateBucket	Ja.	Ja.	Nein
	s3:DeleteBucket	Nein	Ja.	Ja.
	s3:GetLifecycleKonfiguration	Nein	Ja.	Nein
	s3:PutLifecycleKonfiguration	Nein	Ja.	Nein
	s3:PutBucketTagging	Nein	Ja.	Nein
	s3:ListBucketVersions	Nein	Ja.	Nein
	s3:GetBucketPolicyStatus	Nein	Ja.	Nein
	s3:GetBucketPublicAccessBlock	Nein	Ja.	Nein
	s3:GetBucketAcl	Nein	Ja.	Nein
	s3:GetBucketPolicy	Nein	Ja.	Nein
	s3:PutBucketPublicAccessBlock	Nein	Ja.	Nein
	s3:GetBucketTagging	Nein	Ja.	Nein
	s3:GetBucketLocation	Nein	Ja.	Nein
	s3:ListAllMyBuchs	Nein	Nein	Nein
	s3:ListBucket	Nein	Ja.	Nein
Datenverschlüsselung von Cloud Volumes ONTAP mithilfe des AWS KMS (Key Management Service)	Km:Liste*	Ja.	Ja.	Nein
	Km:ReVerschlüsseln*	Ja.	Nein	Nein
	Km:Beschreiben*	Ja.	Ja.	Nein
	Km:CreateGrant	Ja.	Ja.	Nein
AWS Kostendaten für Cloud Volumes ONTAP beziehen	ce:GetReservoirUtilisation	Nein	Ja.	Nein
	ce:GetDimensionValues	Nein	Ja.	Nein
	ce:GetCostAndUsage	Nein	Ja.	Nein
	ce:GetTags	Nein	Ja.	Nein

Zweck	Aktion	Werden sie für die Implementierung verwendet?	Wird für den täglichen Betrieb verwendet?	Zum Löschen verwendet?
Erstellen und managen Sie eine AWS Spread-Platzierungsgruppe für zwei HA-Nodes und den Mediator in einer einzigen AWS Availability Zone	ec2:CreatePlacementGroup	Ja.	Nein	Nein
	ec2:DeletePlacementGroup	Nein	Ja.	Ja.
Erstellen von Berichten	fsx:Beschreiben*	Nein	Ja.	Nein
	fsx:Liste*	Nein	Ja.	Nein
Aggregate erstellen und managen, die die Amazon EBS Elastic Volumes Funktion unterstützen	ec2:DescribeVolumiesModified	Nein	Ja.	Nein
	ec2:ModifyVolume	Nein	Ja.	Nein

Globaler Datei-Cache

Der Connector stellt folgende API-Anforderungen zur Bereitstellung von Global File Cache-Instanzen während der Bereitstellung bereit:

- Wolkenbildung:DescribeStacks
- cloudwatch:GetMetricStatistics
- CloudFormation:ListenStacks

FSX für ONTAP

Der Konnektor stellt die folgenden API-Anforderungen zur Verwaltung von FSX für ONTAP vor:

- ec2:DescribeInstances
- ec2:DescribeInstanceStatus
- ec2:DescribeInstanceAttribut
- ec2:DescribeRouteTables
- ec2:DescribeBilder
- ec2:CreateTags
- ec2:DescribeVolumes
- ec2:DescribeSecurityGroups
- ec2:DescribeNetworkInterfaces
- ec2:DescribeSubnets
- ec2:DescribeVpcs
- ec2:DescribeDhcpOptions

- ec2:DescribeSnapshots
- ec2:DescribeKeypairs
- ec2:DescribeRegionen
- ec2:DescribeTags
- ec2:DescribeIamInstanceProfilVerbände
- ec2:DescribeReserviertInstanceAngebote
- ec2:descbeVpcEndpunkte
- ec2:DescribeVpcs
- ec2:DescribeVolumiesModified
- ec2:DescribePlacementGroups
- Km:Liste*
- Km:Beschreiben*
- Km:CreateGrant
- Km:ListAliase
- fsx:Beschreiben*
- fsx:Liste*

Kubernetes

Der Connector stellt folgende API-Anforderungen zur Erkennung und Verwaltung von Amazon EKS-Clustern vor:

- ec2:DescribeRegionen
- eks:ListClusters
- eks:DescribeCluster
- iam:GetInstanceProfile

S3-Bucket-Erkennung

Der Connector stellt folgende API-Anforderung vor, Amazon S3 Buckets zu erkennen:

s3:GetVerschlüsselungKonfiguration

Azure-Berechtigungen für den Connector

Beim Start der Connector-VM in Azure wird von BlueXP eine benutzerdefinierte Rolle an die VM angehängt, die dem Connector Berechtigungen für das Management von Ressourcen und Prozessen innerhalb des Azure-Abonnements bietet. Der Connector nutzt die Berechtigungen, um API-Aufrufe an mehrere Azure-Services durchzuführen.

Berechtigungen für benutzerdefinierte Rollen

Die unten aufgeführte benutzerdefinierte Rolle stellt die Berechtigungen bereit, die ein Connector zur Verwaltung von Ressourcen und Prozessen in Ihrem Azure-Netzwerk benötigt.

Wenn Sie einen Connector direkt aus BlueXP erstellen, wendet BlueXP diese benutzerdefinierte Rolle automatisch auf den Connector an.

Wenn Sie den Connector über den Azure Marketplace bereitstellen oder den Connector manuell auf einem Linux-Host installieren, müssen Sie die benutzerdefinierte Rolle selbst einrichten.

Außerdem müssen Sie sicherstellen, dass die Rolle auf dem neuesten Stand ist, wenn neue Berechtigungen in nachfolgenden Releases hinzugefügt werden.

```
{
    "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/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/regeneratekey/action",
                    "Microsoft.Storage/storageAccounts/write",

"Microsoft.Storage/storageAccounts/blobServices/containers/read",
                    "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/frontendIPConfigurations/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"
}
```

Verwendung von Azure Berechtigungen

In den folgenden Abschnitten wird die Nutzung der Berechtigungen für den jeweiligen NetApp Cloud-Service beschrieben. Diese Informationen können hilfreich sein, wenn Ihre Unternehmensrichtlinien vorschreiben, dass

Berechtigungen nur bei Bedarf bereitgestellt werden.

AppTemplate-Tags

Der Connector stellt bei Verwendung des AppTemplate Tagging-Dienstes folgende API-Anforderungen zur Verwaltung von Tags auf Azure-Ressourcen bereit:

- Microsoft.Ressourcen/Ressourcen/Lesen
- Microsoft.Ressourcen/Abonnements/Operationsergebnisse/Lesen
- Microsoft.Resources/Subskriptionen/resourceGroups/read
- Microsoft.Ressourcen/Abonnements/Ressourcengruppen/Ressourcen/Lesen
- Microsoft.Ressourcen/Tags/lesen
- Microsoft.Ressourcen/Tags/schreiben

Azure NetApp Dateien

Der Connector stellt folgende API-Anforderungen zur Verwaltung von Azure NetApp Files-Arbeitsumgebungen vor:

- 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

Cloud-Backup

Der Connector stellt die folgenden API-Anforderungen für Backup- und Wiederherstellungsvorgänge:

- Microsoft.Compute/virtualMachines/read
- Microsoft.Compute/virtualMachines/start/action
- Microsoft.Compute/virtualMachines/deallocate/action
- Microsoft.Storage/StorageAccounts/Listkeys/Action
- Microsoft.Storage/StorageAccounts/Lesevorgang
- Microsoft.Storage/StorageAccounts/write
- Microsoft.Storage/StorageAccounts/blobServices/Container/Lesevorgang
- Microsoft.KeyVault/Vaults/read
- Microsoft.KeyVault/Vaults/accessPolicies/write
- Microsoft.Network/networkInterfaces/read
- Microsoft.Ressourcen/Abonnements/Standorte/gelesen
- Microsoft.Network/virtualNetworks/read
- Microsoft.Network/virtualNetworks/subnets/read
- Microsoft.Resources/Subskriptionen/resourceGroups/read
- Microsoft.Ressourcen/Abonnements/Ressourcengruppen/Ressourcen/Lesen

- Microsoft.Resources/Subskriptionen/resourceGroups/write
- Microsoft.Authorization/Locks/*
- 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.Ressourcen/Bereitstellungen/löschen
- Microsoft.Network/publicIPAddresses/delete
- Microsoft.Storage/StorageAccounts/blobServices/Container/write
- Microsoft.ManagedIdentity/userAssignetIdentities/assign/Action

Der Konnektor stellt folgende API-Anforderungen zur Verfügung, wenn Sie die Funktion Suchen & Wiederherstellen verwenden:

- Microsoft.Synapse/Workspaces/schreiben
- Microsoft.Synapse/Workspaces/Lesen
- Microsoft.Synapse/Workspaces/delete
- Microsoft.Synapse/Register/Aktion
- Microsoft.Synapse/CheckNameVerfügbarkeit/Aktion
- Microsoft.Synapse/Workspaces/OperationStatus/Lesen
- Microsoft.Synapse/Workspaces/Firewall Regeln/lesen
- Microsoft.Synapse/Workspaces/ersetzenAllIpFirewallRegeln/Aktion
- Microsoft.Synapse/Workspaces/OperationResults/read

Cloud-Daten Sinnvoll

Der Connector stellt bei der Verwendung von Cloud Data Sense die folgenden API-Anforderungen vor.

Aktion	Wird zur Einrichtung verwendet?	Wird für den täglichen Betrieb verwendet?
Microsoft.Compute/locations/operations/read	Ja.	Ja.
Microsoft.Compute/locations/vmSizes/read	Ja.	Ja.

Aktion	Wird zur Einrichtung verwendet?	Wird für den täglichen Betrieb verwendet?
Microsoft.Compute/operations/read	Ja.	Ja.
Microsoft.Compute/virtualMachines/instanceView/read	Ja.	Ja.
Microsoft.Compute/virtualMachines/powerOff/action	Ja.	Nein
Microsoft.Compute/virtualMachines/read	Ja.	Ja.
Microsoft.Compute/virtualMachines/restart/action	Ja.	Nein
Microsoft.Compute/virtualMachines/start/action	Ja.	Nein
Microsoft.Compute/virtualMachines/vmSizes/read	Nein	Ja.
Microsoft.Compute/virtualMachines/write	Ja.	Nein
Microsoft.Compute/images/read	Ja.	Ja.
Microsoft.Compute/disks/delete	Ja.	Nein
Microsoft.Compute/disks/read	Ja.	Ja.
Microsoft.Compute/disks/write	Ja.	Nein
Microsoft.Storage/ChecknameVerfügbarkeit/Lesevorgang	Ja.	Ja.
Microsoft.Storage/Operations/Lesevorgang	Ja.	Ja.
Microsoft.Storage/StorageAccounts/Listkeys/Action	Ja.	Nein
Microsoft.Storage/StorageAccounts/Lesevorgang	Ja.	Ja.
Microsoft.Storage/StorageAccounts/write	Ja.	Nein
Microsoft.Storage/StorageAccounts/delete	Nein	Ja.
Microsoft.Storage/StorageAccounts/blobServices/Container/Lesevorgang	Ja.	Ja.
Microsoft.Network/networkInterfaces/read	Ja.	Ja.
Microsoft.Network/networkInterfaces/write	Ja.	Nein

Aktion	Wird zur Einrichtung verwendet?	Wird für den täglichen Betrieb verwendet?
Microsoft.Network/networkInterfaces/join/action	Ja.	Nein
Microsoft.Network/networkSecurityGroups/read	Ja.	Ja.
Microsoft.Network/networkSecurityGroups/write	Ja.	Nein
Microsoft.Ressourcen/Abonnements/Standorte/gelesen	Ja.	Ja.
Microsoft.Network/locations/operationResults/read	Ja.	Ja.
Microsoft.Network/locations/operations/read	Ja.	Ja.
Microsoft.Network/virtualNetworks/read	Ja.	Ja.
Microsoft.Network/virtualNetworks/checkIpAddressAvailability/read	Ja.	Ja.
Microsoft.Network/virtualNetworks/subnets/read	Ja.	Ja.
Microsoft.Network/virtualNetworks/subnets/virtualMachines/read	Ja.	Ja.
Microsoft.Network/virtualNetworks/virtualMachines/read	Ja.	Ja.
Microsoft.Network/virtualNetworks/subnets/join/action	Ja.	Nein
Microsoft.Network/virtualNetworks/subnets/write	Ja.	Nein
Microsoft.Network/routeTables/join/action	Ja.	Nein
Microsoft.Ressourcen/Implementierungen/Betrieb/Lesevorgang	Ja.	Ja.
Microsoft.Ressourcen/Implementierungen/lesen	Ja.	Ja.
Microsoft.Ressourcen/Implementierungen/schreiben	Ja.	Nein
Microsoft.Ressourcen/Ressourcen/Lesen	Ja.	Ja.
Microsoft.Ressourcen/Abonnements/Operationsergebnisse/Lesen	Ja.	Ja.
Microsoft.Resources/Subskriptionen/resourceGroups/delete	Ja.	Nein

Aktion	Wird zur Einrichtung verwendet?	Wird für den täglichen Betrieb verwendet?
Microsoft.Resources/Subskriptionen/resourceGroups/read	Ja.	Ja.
Microsoft.Ressourcen/Abonnements/Ressourcengruppen/Ressourcen/Lesen	Ja.	Ja.
Microsoft.Resources/Subskriptionen/resourceGroups/write	Ja.	Nein

Cloud Tiering

Der Connector stellt bei der Einrichtung von Cloud Tiering die folgenden API-Anforderungen vor.

- Microsoft.Storage/StorageAccounts/Listkeys/Action
- Microsoft.Resources/Subskriptionen/resourceGroups/read
- Microsoft.Ressourcen/Abonnements/Standorte/gelesen

Der Connector stellt folgende API-Anforderungen für den täglichen Betrieb.

- Microsoft.Storage/StorageAccounts/blobServices/Container/Lesevorgang
- Microsoft.Storage/StorageAccounts/blobServices/Container/write
- Microsoft.Storage/StorageAccounts/Management Policies/read
- Microsoft.Storage/StorageAccounts/Management Richtlinien/schreiben
- Microsoft.Storage/StorageAccounts/Lesevorgang

Cloud Volumes ONTAP

Der Connector stellt die folgenden API-Anforderungen für die Implementierung und das Management von Cloud Volumes ONTAP in AWS.

Zweck	Aktion	Werden sie für die Implementierung verwendet?	Wird für den täglichen Betrieb verwendet?	Zum Löschen verwendet?
Erstellen Sie VMs, stoppen, starten, löschen und erhalten Sie den Status des Systems	Microsoft.Compute/locations/operations/read	Ja.	Ja.	Nein
	Microsoft.Compute/locations/vmSizes/read	Ja.	Ja.	Nein
	Microsoft.Ressourcen/Abonnements/Standorte/gelesen	Ja.	Nein	Nein
	Microsoft.Compute/operations/read	Ja.	Ja.	Nein
	Microsoft.Compute/virtualMachines/instanceView/read	Ja.	Ja.	Nein
	Microsoft.Compute/virtualMachines/powerOff/action	Ja.	Ja.	Nein
	Microsoft.Compute/virtualMachines/read	Ja.	Ja.	Nein
	Microsoft.Compute/virtualMachines/restart/action	Ja.	Ja.	Nein
	Microsoft.Compute/virtualMachines/start/action	Ja.	Ja.	Nein
	Microsoft.Compute/virtualMachines/deallocate/action	Nein	Ja.	Ja.
	Microsoft.Compute/virtualMachines/vmSizes/read	Nein	Ja.	Nein
	Microsoft.Compute/virtualMachines/write	Ja.	Ja.	Nein
Implementierung über eine VHD ermöglichen	Microsoft.Compute/images/read	Ja.	Nein	Nein

Zweck	Aktion	Werden sie für die Implementierung verwendet?	Wird für den täglichen Betrieb verwendet?	Zum Löschen verwendet?
Netzwerkschnittstellen im Ziel-Subnetz erstellen und verwalten	Microsoft.Network/networkInterfaces/read	Ja.	Ja.	Nein
	Microsoft.Network/networkInterfaces/write	Ja.	Ja.	Nein
	Microsoft.Network/networkInterfaces/join/action	Ja.	Ja.	Nein
Erstellen Sie vordefinierte Netzwerksicherheitsgruppen	Microsoft.Network/networkSecurityGroups/read	Ja.	Ja.	Nein
	Microsoft.Network/networkSecurityGroups/write	Ja.	Ja.	Nein
	Microsoft.Network/networkSecurityGroups/join/action	Ja.	Nein	Nein
Abrufen der Netzwerkinformationen zu Regionen, Ziel-vnet und Subnetz, und Hinzufügen der VMs zu VNets	Microsoft.Network/locations/operationResults/read	Ja.	Ja.	Nein
	Microsoft.Network/locations/operations/read	Ja.	Ja.	Nein
	Microsoft.Network/virtualNetworks/read	Ja.	Nein	Nein
	Microsoft.Network/virtualNetworks/checkIpAddressAvailability/read	Ja.	Nein	Nein
	Microsoft.Network/virtualNetworks/subnets/read	Ja.	Ja.	Nein
	Microsoft.Network/virtualNetworks/subnets/virtualMachines/read	Ja.	Ja.	Nein
	Microsoft.Network/virtualNetworks/virtualMachines/read	Ja.	Ja.	Nein
	Microsoft.Network/virtualNetworks/subnets/join/action	Ja.	Ja.	Nein

Zweck	Aktion	Werden sie für die Implementierung verwendet?	Wird für den täglichen Betrieb verwendet?	Zum Löschen verwendet?
Erstellen und Verwalten von Ressourcengruppen	Microsoft.Ressourcen/Implementierungen/Betrieb/Lesevorgang	Ja.	Ja.	Nein
	Microsoft.Ressourcen/Implementierungen/lesen	Ja.	Ja.	Nein
	Microsoft.Ressourcen/Implementierungen/schreiben	Ja.	Ja.	Nein
	Microsoft.Ressourcen/Ressourcen/Lesen	Ja.	Ja.	Nein
	Microsoft.Ressourcen/Abonnements/Operationsergebnisse/Lesen	Ja.	Ja.	Nein
	Microsoft.Resources/Subskriptionen/resourceGroups/delete	Ja.	Ja.	Ja.
	Microsoft.Resources/Subskriptionen/resourceGroups/read	Nein	Ja.	Nein
	Microsoft.Ressourcen/Abonnements/Ressourcengruppen/Ressourcen/Lesen	Ja.	Ja.	Nein
	Microsoft.Resources/Subskriptionen/resourceGroups/write	Ja.	Ja.	Nein

Zweck	Aktion	Werden sie für die Implementierung verwendet?	Wird für den täglichen Betrieb verwendet?	Zum Löschen verwendet?
Azure-Storage-Konten und -Festplatten managen	Microsoft.Compute/disks/read	Ja.	Ja.	Ja.
	Microsoft.Compute/disks/write	Ja.	Ja.	Nein
	Microsoft.Compute/disks/delete	Ja.	Ja.	Ja.
	Microsoft.Storage/ChecknameVerfügbarkeit/Lesevorgang	Ja.	Ja.	Nein
	Microsoft.Storage/Operations/Lesevorgang	Ja.	Ja.	Nein
	Microsoft.Storage/StorageAccounts/Listkeys/Action	Ja.	Ja.	Nein
	Microsoft.Storage/StorageAccounts/Lesevorgang	Ja.	Ja.	Nein
	Microsoft.Storage/StorageAccounts/delete	Nein	Ja.	Ja.
	Microsoft.Storage/StorageAccounts/write	Ja.	Ja.	Nein
	Microsoft.Speicherung/Verwendung/Lesen	Nein	Ja.	Nein
Ermöglichen von Backups auf Blob Storage und Verschlüsselung von Storage-Konten	Microsoft.Storage/StorageAccounts/blobServices/Container/Lesevorgang	Ja.	Ja.	Nein
	Microsoft.KeyVault/Vaults/read	Ja.	Ja.	Nein
	Microsoft.KeyVault/Vaults/accessPolicies/write	Ja.	Ja.	Nein
Vnet-Service-Endpunkte für Daten-Tiering aktivieren	Microsoft.Network/virtualNetworks/subnets/write	Ja.	Ja.	Nein
	Microsoft.Network/routeTables/join/action	Ja.	Ja.	Nein

Zweck	Aktion	Werden sie für die Implementierung verwendet?	Wird für den täglichen Betrieb verwendet?	Zum Löschen verwendet?
Erstellen und managen Sie über Azure gemanagte Snapshots	Microsoft.Compute/snapshots/write	Ja.	Ja.	Nein
	Microsoft.Compute/snapshots/read	Ja.	Ja.	Nein
	Microsoft.Compute/snapshots/delete	Nein	Ja.	Ja.
	Microsoft.Compute/disks/beginGetAccess/action	Nein	Ja.	Nein
Erstellung und Management von Verfügbarkeitsgruppen	Microsoft.Compute/availabilitySets/write	Ja.	Nein	Nein
	Microsoft.Compute/availabilitySets/read	Ja.	Nein	Nein
Programmatische Implementierungen über den Markt ermöglichen	Microsoft.MarketplaceOrdering/offertypes/Publisher/Offers/Plans/Agreements/read	Ja.	Nein	Nein
	Microsoft.MarketplaceOrdering/offertypes/Publisher/Offers/Plans/Agreements/write	Ja.	Ja.	Nein
Managen Sie einen Load Balancer für HA-Paare	Microsoft.Network/loadBalancers/read	Ja.	Ja.	Nein
	Microsoft.Network/loadBalancers/write	Ja.	Nein	Nein
	Microsoft.Network/loadBalancers/delete	Nein	Ja.	Ja.
	Microsoft.Network/loadBalancers/backendAddressPools/read	Ja.	Ja.	Nein
	Microsoft.Network/loadBalancers/loadBalancingRules/read	Ja.	Nein	Nein
	Microsoft.Network/loadBalancers/probes/read	Ja.	Nein	Nein
	Microsoft.Network/loadBalancers/probes/join/action	Ja.	Nein	Nein

Zweck	Aktion	Werden sie für die Implementierung verwendet?	Wird für den täglichen Betrieb verwendet?	Zum Löschen verwendet?
Verwaltung von Sperren auf Azure Festplatten aktivieren	Microsoft.Authorization/Locks/*	Ja.	Ja.	Nein
Aktivieren Sie private Endpunkte für HA-Paare, wenn sich keine Verbindung außerhalb des Subnetzes befindet	Microsoft.Network/privateEndpoints/write	Ja.	Ja.	Nein
	Microsoft.Speicherung/Speicherkonten/PrivateEndpointConnectionsGenehmigung/Aktion	Ja.	Nein	Nein
	Microsoft.Storage/StorageAccounts/private EndpointConnections/Lesevorgang	Ja.	Ja.	Ja.
	Microsoft.Network/privateEndpoints/read	Ja.	Ja.	Ja.
	Microsoft.Network/privateDnsZones/write	Ja.	Ja.	Nein
	Microsoft.Network/privateDnsZones/virtualNetworkLinks/write	Ja.	Ja.	Nein
	Microsoft.Network/virtualNetworks/join/action	Ja.	Ja.	Nein
	Microsoft.Network/privateDnsZones/A/write	Ja.	Ja.	Nein
	Microsoft.Network/privateDnsZones/read	Ja.	Ja.	Nein
	Microsoft.Network/privateDnsZones/virtualNetworkLinks/read	Ja.	Ja.	Nein
Erforderlich für einige VM-Implementierungen, abhängig von der zugrunde liegenden physischen Hardware	Microsoft.Ressourcen/Implementierungen/OperationStatuses/read	Ja.	Ja.	Nein

Zweck	Aktion	Werden sie für die Implementierung verwendet?	Wird für den täglichen Betrieb verwendet?	Zum Löschen verwendet?
Entfernen von Ressourcen aus einer Ressourcengruppe bei Ausfall oder Löschen der Bereitstellung	Microsoft.Network/privateEndpoints/delete	Ja.	Ja.	Nein
	Microsoft.Compute/availabilitySets/delete	Ja.	Ja.	Nein
Nutzen Sie die API, wenn Sie die vom Kunden gemanagten Schlüssel verwenden	Microsoft.Compute/diskEncryptionSets/read	Ja.	Ja.	Ja.
	Microsoft.Compute/diskEncryptionSets/write	Ja.	Ja.	Nein
	Microsoft.KeyVault/Vaults/Deploy/Action	Ja.	Nein	Nein
	Microsoft.Compute/diskEncryptionSets/delete	Ja.	Ja.	Ja.
Konfigurieren Sie eine Applikationssicherheitsgruppe für ein HA-Paar, um die HA Interconnect- und Cluster-Netzwerk-NICs zu isolieren	Microsoft.Network/applicationSecurityGroups/write	Nein	Ja.	Nein
	Microsoft.Network/applicationSecurityGroups/read	Nein	Ja.	Ja.
	Microsoft.Network/applicationSecurityGroups/joinIpConfiguration/action	Nein	Ja.	Nein
	Microsoft.Network/networkSecurityGroups/securityRules/write	Ja.	Ja.	Nein
	Microsoft.Network/applicationSecurityGroups/delete	Nein	Ja.	Nein
	Microsoft.Network/networkSecurityGroups/securityRules/delete	Nein	Ja.	Ja.

Zweck	Aktion	Werden sie für die Implementierung verwendet?	Wird für den täglichen Betrieb verwendet?	Zum Löschen verwendet?
Lesen, Schreiben und Löschen von Tags im Zusammenhang mit Cloud Volumes ONTAP Ressourcen	Microsoft.Ressourcen/Tags/lesen	Nein	Ja.	Nein
	Microsoft.Ressourcen/Tags/schreiben	Ja.	Ja.	Nein
	Microsoft.Ressourcen/Tags/delete	Ja.	Nein	Nein
Verschlüsselung von Speicherkonten bei der Erstellung	Microsoft.ManagedIdentity/userAssignetIdentities/assign/Action	Ja.	Ja.	Nein

Globaler Datei-Cache

Der Connector stellt bei Verwendung des globalen Datei-Caches folgende API-Anforderungen vor:

- Microsoft.Insights/Metriken/Lesevorgang
- 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.Ressourcen/Bereitstellungen/löschen

Kubernetes

Der Connector stellt folgende API-Anforderungen zur Erkennung und Verwaltung von Clustern in Azure Kubernetes Service (AKS):

- Microsoft.Compute/virtualMachines/read
- Microsoft.Ressourcen/Abonnements/Standorte/gelesen
- Microsoft.Ressourcen/Abonnements/Operationsergebnisse/Lesen
- Microsoft.Resources/Subskriptionen/resourceGroups/read
- Microsoft.Ressourcen/Abonnements/Ressourcengruppen/Ressourcen/Lesen
- Microsoft.ContainerService/manageCluster/lesen
- Microsoft.ContainerService/verwaltungCluster/listClusterUserCredential/Action

Google Cloud-Berechtigungen für den Connector

Für Aktionen in Google Cloud sind für BlueXP Berechtigungen erforderlich. Diese Berechtigungen sind Bestandteil einer benutzerdefinierten Rolle, die NetApp zur Verfügung stellt. Vielleicht möchten Sie wissen, was BlueXP mit diesen Berechtigungen

macht.

Berechtigungen für Dienstkonto

Die unten abgebildete benutzerdefinierte Rolle bietet die Berechtigungen, die ein Connector zur Verwaltung von Ressourcen und Prozessen in Ihrem Google Cloud-Netzwerk benötigt.

Sie müssen diese benutzerdefinierte Rolle auf ein Servicekonto anwenden, das mit der Connector-VM verbunden ist. "Schritt-für-Schritt-Anleitungen anzeigen".

Außerdem müssen Sie sicherstellen, dass die Rolle auf dem neuesten Stand ist, wenn neue Berechtigungen in nachfolgenden Releases hinzugefügt werden.

```
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
```

Verwendung von Google Cloud-Berechtigungen

Aktionen	Zweck
- Compute.Disks.create - Compute.Disks.createSnapshot - compute.disks.delete - Compute.Disks.get - Compute.Disks.list - compute.disks.setLabels - compute.disks.use	Zum Erstellen und Verwalten von Festplatten für Cloud Volumes ONTAP.
- Compute.Firewalls.create - compute.firewalls.delete - Compute.Firewalls.get - Compute.Firewalls.list	Um Firewall-Regeln für Cloud Volumes ONTAP zu erstellen.
- Compute.globalOperations.get	Um den Status von Vorgängen anzuzeigen.
- Compute.images.get - Compute.images.getFromFamily - Compute.images.list - compute.images.useReadOnly	Um Images für VM-Instanzen zu erhalten.
- compute.instances.attachDisk - compute.instances.detachDisk	Zum Verbinden und Trennen von Festplatten mit Cloud Volumes ONTAP.
- compute.instances.create - compute.instances.delete	Um Cloud Volumes ONTAP VM-Instanzen zu erstellen und zu löschen.
- compute.instances.get	Um VM-Instanzen aufzulisten.
- compute.instances.getSerialPortOutput	Um Konsolenprotokolle zu erhalten.
- compute.instances.list	Um die Liste der Instanzen in einer Zone abzurufen.
- compute.instances.setDeletionProtection	So legen Sie den Löschschutz für die Instanz fest:
- compute.instances.setLabels	So fügen Sie Etiketten hinzu:
- compute.instances.setMachineType - compute.instances.setMinCpuPlatform	So ändern Sie den Maschinentyp für Cloud Volumes ONTAP.

Aktionen	Zweck
- compute.instances.setMetadata	Um Metadaten hinzuzufügen.
- compute.instances.setTags	Um Tags für Firewall-Regeln hinzuzufügen.
- compute.instances.start - compute.instances.stop - compute.instances.updateDisplayDevice	Um Cloud Volumes ONTAP zu starten und anzuhalten.
- Compute.machineTypes.get	Um die Anzahl der Kerne zu erhalten, um qouten zu überprüfen.
- compute.projects.get	Zur Unterstützung mehrerer Projekte.
- Compute.Snapshots.create - compute.snapshots.delete - Compute.Snapshots.get - Compute.Snapshots.list - compute.snapshots.setLabels	Um persistente Festplatten-Snapshots zu erstellen und zu managen.
- compute.networks.get - compute.networks.list - Compute.Regions.get - Compute.Regions.list - Compute.subNetworks.get - Compute.subNetworks.list - Compute.zoneOperations.get - Compute.Zones.get - Compute.Zones.list	Um die Netzwerkinformationen zu erhalten, die für die Erstellung einer neuen Instanz einer Cloud Volumes ONTAP Virtual Machine erforderlich sind.
- deploymentmanager.compositeTypes.get - deploymentmanager.compositeTypes.list - deploymentmanager.deployments.create - deploymentmanager.deployments.delete - deploymentmanager.deployments.get - deploymentmanager.deployments.list - istmentmanager.Manifeste.get - istmentmanager.manifeste.list - istmentmanager.Operations.get - istmentmanager.Operations.list - bereitsmanager.Resources.get - bereitsmanager.Resources.list - Bereitstellungmanager.typeProviders.get - istmentmanager.tyArten.list	Um die Cloud Volumes ONTAP VM-Instanz mithilfe von Google Cloud Deployment Manager bereitzustellen.
- Logging.logEntries.list - Logging.privateLogEntries.list	Zum Abrufen von Stack-Protokolllaufwerken.
- resourcemanager.projects.get	Zur Unterstützung mehrerer Projekte.
- Storage.Buckets.create - storage.buckets.delete - Storage.Buckets.get - Storage.Buckets.list - Storage.Buckets.Update	Zur Erstellung und Verwaltung eines Google Cloud Storage Buckets für Daten-Tiering
- cloudkms.cryptoKeyVersions.useToEncrypt - cloudkms.kryptoKeys.get - cloudkms.kryptoKeys.list - cloudkms.Keyrings.list	Verwenden von vom Kunden gemanagten Verschlüsselungen aus dem Cloud-Verschlüsselungsmanagement-Service mit Cloud Volumes ONTAP.

Aktionen	Zweck
- compute.instances.setServiceAccount - iam.serviceAccounts.actAs - iam.serviceAccounts.getIamPolicy - iam.serviceAccounts.list - Storage.objects.get - Storage.objects.list	So legen Sie ein Servicekonto für die Cloud Volumes ONTAP-Instanz fest: Dieses Servicekonto bietet Berechtigungen für Daten-Tiering zu einem Google Cloud Storage Bucket.
- Compute.Addresses.list	So rufen Sie die Adressen in einer Region ab, wenn Sie ein HA-Paar bereitstellen.
- Compute.backendServices.create - Compute.regionBackendServices.create - Compute.regionBackendServices.get - Compute.regionBackendServices.list	Um einen Backend-Service für die Verteilung von Datenverkehr in einem HA-Paar zu konfigurieren
- compute.networks.updatePolicy	So wenden Sie Firewall-Regeln auf die VPCs und Subnetze für ein HA-Paar an.
- compute.subnetworks.use - compute.subnetworks.useExternalIp - compute.instances.addAccessConfig	Und Cloud-Daten sinnvoll nutzen.
- Container.Clusters.get - Container.Clusters.list	Um Kubernetes Cluster zu erkennen, die in der Google Kubernetes Engine ausgeführt werden.
- compute.instanceGroups.get - Compute.Addresses.get	Um Storage VMs auf HA-Paaren zu erstellen und zu managen.
- Monitoring.Timeeries.list - Storage.Buckets.getIamPolicy	Um Informationen zu Google Cloud Storage Buckets zu erhalten.

Ports

Sicherheitsgruppenregeln in AWS

Für die AWS Sicherheitsgruppe für den Connector sind sowohl ein- als auch ausgehende Regeln erforderlich.

Regeln für eingehende Anrufe

Protokoll	Port	Zweck
SSH	22	Bietet SSH-Zugriff auf den Connector-Host
HTTP	80	Bietet HTTP-Zugriff von Client-Webbrowsern auf die lokale Benutzeroberfläche
HTTPS	443	Bietet HTTPS-Zugriff von Client-Webbrowsern zur lokalen Benutzeroberfläche und Verbindungen aus der Cloud Data Sense Instanz
TCP	3128	Ermöglicht Cloud Volumes ONTAP den Zugang zum Internet, um AutoSupport-Nachrichten an den NetApp Support zu senden. Nach der Bereitstellung müssen Sie diesen Port manuell öffnen. server for AutoSupport messages,Erfahren Sie mehr über den Proxy-Server des Connectors.

Protokoll	Port	Zweck
TCP	9060	Ermöglicht die Aktivierung und Nutzung von Cloud Data Sense und Cloud Backup in öffentlicher Cloud-Implementierungen. Dieser Port ist auch für Cloud Backup erforderlich, wenn Sie die SaaS-Schnittstelle in Ihrem BlueXP-Konto deaktivieren.

Regeln für ausgehende Anrufe

Die vordefinierte Sicherheitsgruppe für den Konnektor öffnet den gesamten ausgehenden Datenverkehr. Wenn dies akzeptabel ist, befolgen Sie die grundlegenden Regeln für ausgehende Anrufe. Wenn Sie strengere Regeln benötigen, verwenden Sie die erweiterten Outbound-Regeln.

Grundlegende Regeln für ausgehende Anrufe

Die vordefinierte Sicherheitsgruppe für den Connector enthält die folgenden ausgehenden Regeln.

Protokoll	Port	Zweck
Alle TCP	Alle	Gesamter abgehender Datenverkehr
Alle UDP-Protokolle	Alle	Gesamter abgehender Datenverkehr

Erweiterte Outbound-Regeln

Wenn Sie starre Regeln für ausgehenden Datenverkehr benötigen, können Sie die folgenden Informationen verwenden, um nur die Ports zu öffnen, die für die ausgehende Kommunikation durch den Konnektor erforderlich sind.

Die Quell-IP-Adresse ist der Connector-Host.

Service	Protokoll	Port	Ziel	Zweck
API-Aufrufe und AutoSupport	HTTPS	443	Outbound-Internet und ONTAP Cluster Management LIF	API-Aufrufe an AWS und ONTAP, Cloud Data Sense, zum Ransomware-Service und dem Senden von AutoSupport-Nachrichten an NetApp
API-Aufrufe	TCP	3000	ONTAP HA Mediator	Kommunikation mit dem ONTAP HA Mediator
	TCP	8088	Backup auf S3	API-Aufrufe zur Sicherung in S3
DNS	UDP	53	DNS	Wird für DNS Resolve von BlueXP verwendet

Für Sicherheitsgruppen gibt es in Azure Regeln

Für die Azure-Sicherheitsgruppe für den Connector sind sowohl ein- als auch ausgehende Regeln erforderlich.

Regeln für eingehende Anrufe

Protokoll	Port	Zweck
SSH	22	Bietet SSH-Zugriff auf den Connector-Host
HTTP	80	Bietet HTTP-Zugriff von Client-Webbrowsern auf die lokale Benutzeroberfläche
HTTPS	443	Bietet HTTPS-Zugriff von Client-Webbrowsern zur lokalen Benutzeroberfläche und Verbindungen aus der Cloud Data Sense Instanz
TCP	3128	Ermöglicht Cloud Volumes ONTAP den Zugang zum Internet, um AutoSupport-Nachrichten an den NetApp Support zu senden. Nach der Bereitstellung müssen Sie diesen Port manuell öffnen. server for AutoSupport messages,Erfahren Sie mehr über den Proxy-Server des Connectors.
TCP	9060	Ermöglicht die Aktivierung und Nutzung von Cloud Data Sense und Cloud Backup in öffentlicher Cloud-Implementierungen. Dieser Port ist auch für Cloud Backup erforderlich, wenn Sie die SaaS-Schnittstelle in Ihrem BlueXP-Konto deaktivieren.

Regeln für ausgehende Anrufe

Die vordefinierte Sicherheitsgruppe für den Konnektor öffnet den gesamten ausgehenden Datenverkehr. Wenn dies akzeptabel ist, befolgen Sie die grundlegenden Regeln für ausgehende Anrufe. Wenn Sie strengere Regeln benötigen, verwenden Sie die erweiterten Outbound-Regeln.

Grundlegende Regeln für ausgehende Anrufe

Die vordefinierte Sicherheitsgruppe für den Connector enthält die folgenden ausgehenden Regeln.

Protokoll	Port	Zweck
Alle TCP	Alle	Gesamter abgehender Datenverkehr

Protokoll	Port	Zweck
Alle UDP-Protokolle	Alle	Gesamter abgehender Datenverkehr

Erweiterte Outbound-Regeln

Wenn Sie starre Regeln für ausgehenden Datenverkehr benötigen, können Sie die folgenden Informationen verwenden, um nur die Ports zu öffnen, die für die ausgehende Kommunikation durch den Konnektor erforderlich sind.

Die Quell-IP-Adresse ist der Connector-Host.

Service	Protokoll	Port	Ziel	Zweck
API-Aufrufe und AutoSupport	HTTPS	443	Outbound-Internet und ONTAP Cluster Management LIF	API-Aufrufe an Azure und ONTAP, Cloud Data Sense, zum Ransomware-Service und Senden von AutoSupport-Nachrichten an NetApp
DNS	UDP	53	DNS	Wird für DNS Resolve von BlueXP verwendet

Firewall-Regeln in Google Cloud

Die Google Cloud Firewall-Regeln für den Connector erfordern sowohl ein- als auch ausgehende Regeln.

Regeln für eingehende Anrufe

Protokoll	Port	Zweck
SSH	22	Bietet SSH-Zugriff auf den Connector-Host
HTTP	80	Bietet HTTP-Zugriff von Client-Webbrowsern auf die lokale Benutzeroberfläche
HTTPS	443	Bietet HTTPS-Zugriff von Client-Webbrowsern auf die lokale Benutzeroberfläche
TCP	3128	Ermöglicht Cloud Volumes ONTAP den Zugang zum Internet, um AutoSupport-Nachrichten an den NetApp Support zu senden. Nach der Bereitstellung müssen Sie diesen Port manuell öffnen. server for AutoSupport messages,Erfahren Sie mehr über den Proxy-Server des Connectors.

Regeln für ausgehende Anrufe

Die vordefinierten Firewall-Regeln für den Connector öffnen den gesamten ausgehenden Datenverkehr. Wenn dies akzeptabel ist, befolgen Sie die grundlegenden Regeln für ausgehende Anrufe. Wenn Sie strengere Regeln benötigen, verwenden Sie die erweiterten Outbound-Regeln.

Grundlegende Regeln für ausgehende Anrufe

Die vordefinierten Firewall-Regeln für den Connector enthalten die folgenden ausgehenden Regeln.

Protokoll	Port	Zweck
Alle TCP	Alle	Gesamter abgehender Datenverkehr
Alle UDP-Protokolle	Alle	Gesamter abgehender Datenverkehr

Erweiterte Outbound-Regeln

Wenn Sie starre Regeln für ausgehenden Datenverkehr benötigen, können Sie die folgenden Informationen verwenden, um nur die Ports zu öffnen, die für die ausgehende Kommunikation durch den Konnektor erforderlich sind.

Die Quell-IP-Adresse ist der Connector-Host.

Service	Protokoll	Port	Ziel	Zweck
API-Aufrufe und AutoSupport	HTTPS	443	Outbound-Internet und ONTAP Cluster Management LIF	API-Aufrufe bei GCP und ONTAP, Cloud Data Sense, zum Ransomware-Service und dem Senden von AutoSupport Nachrichten an NetApp
DNS	UDP	53	DNS	Wird für DNS Resolve von BlueXP verwendet

Anschlüsse für den On-Prem Connector

Der Connector verwendet die folgenden *Inbound*-Ports, wenn er manuell auf einem lokalen Linux-Host installiert wird.

Diese eingehenden Regeln gelten für beide Bereitstellungsmodelle für den On-Prem Connector: Installiert mit Internetzugang oder ohne Internetzugang.

Protokoll	Port	Zweck
HTTP	80	Bietet HTTP-Zugriff von Client-Webbrowsern auf die lokale Benutzeroberfläche
HTTPS	443	Bietet HTTPS-Zugriff von Client-Webbrowsern auf die lokale Benutzeroberfläche