Referenz

Setup and administration

NetApp
April 26, 2024

This PDF was generated from https://docs.netapp.com/de-de/bluexp-setup-admin/reference-permissions.html on April 26, 2024. Always check docs.netapp.com for the latest.

Inhalt

Referenz

Berechtigungen

Zusammenfassung der Berechtigungen für BlueXP

Um Funktionen und Services von BlueXP nutzen zu können, müssen Sie Berechtigungen bereitstellen, damit BlueXP Vorgänge 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

BlueXP erfordert AWS Berechtigungen für den Connector und für einzelne Services.

Anschlüsse

Ziel	Beschreibung	Verlinken
Implementieren Sie den Connector von BlueXP	Der Benutzer, der einen Connector von BlueXP erstellt, benötigt spezielle Berechtigungen, um die Instanz in AWS bereitzustellen.	"AWS-Berechtigungen einrichten"
Geben Sie Berechtigungen für den Connector an	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 einen Connector vom AWS Marketplace starten, den Connector manuell installieren oder wenn Sie ihn starten "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"

Backup und Recovery

Ziel	Beschreibung	Verlinken
Sichern Sie On-Premises-ONTAP-Cluster in Amazon S3	Bei der Aktivierung von Backups auf Ihren ONTAP Volumes werden Sie von BlueXP Backup und Recovery aufgefordert, einen Zugriffsschlüssel und einen Schlüssel für einen IAM-Benutzer mit spezifischen Berechtigungen einzugeben.	"Richten Sie S3-Berechtigungen für Backups ein"

Cloud Volumes ONTAP

Ziel	Beschreibung	Verlinken
Stellen Sie Berechtigungen für Cloud Volumes ONTAP-Knoten bereit	Eine IAM-Rolle muss mit jedem Cloud Volumes ONTAP-Node in AWS verbunden sein. Das gleiche gilt für den HA Mediator. Die Standardeinstellung ist, dass BlueXP die IAM-Rollen für Sie erstellen lässt. Sie können jedoch Ihre eigenen beim Erstellen der Arbeitsumgebung verwenden.	"Erfahren Sie, wie Sie die IAM-Rollen selbst einrichten"

Kopieren und Synchronisieren

Ziel	Beschreibung	Verlinken
Implementieren Sie den Daten-Broker in AWS	Das AWS-Benutzerkonto, mit dem Sie den Daten-Broker bereitstellen, muss über spezielle Berechtigungen verfügen.	"Erforderliche Berechtigungen für die Bereitstellung des Data Brokers in AWS"
Geben Sie Berechtigungen für den Daten-Broker an	Wenn der Daten-Broker durch BlueXP Kopier- und Synchronisierungsfunktion implementiert wird, wird eine IAM-Rolle für die Daten-Broker-Instanz erstellt. Sie können den Data Broker auf Wunsch mit Ihrer eigenen IAM-Rolle bereitstellen.	"Anforderungen für die Nutzung Ihrer eigenen IAM-Rolle mit dem AWS Data Broker"
Aktivieren Sie AWS Zugriff für einen manuell installierten Daten-Broker	Wenn Sie den Daten-Broker mit einer Synchronisierungsbeziehung nutzen, die einen S3-Bucket umfasst, sollten Sie den Linux Host auf AWS-Zugriff vorbereiten. Wenn Sie den Daten-Broker installieren, müssen Sie AWS-Schlüssel für einen IAM-Benutzer bereitstellen, der programmatischen Zugriff und bestimmte Berechtigungen hat.	"Zugriff auf AWS wird ermöglicht"

FSX für ONTAP

Ziel	Beschreibung	Verlinken
FSX für ONTAP erstellen und managen	Zum Erstellen oder Managen einer Arbeitsumgebung von Amazon FSX for NetApp ONTAP müssen Sie AWS-Zugangsdaten zu BlueXP hinzufügen. Hierfür stellen Sie den ARN einer IAM-Rolle bereit, die BlueXP die Berechtigungen gibt, die zum Erstellen der Arbeitsumgebung erforderlich sind.	"Erfahren Sie, wie Sie AWS Zugangsdaten für FSX einrichten"

Tiering

Ziel	Beschreibung	Verlinken
Das Tiering lokaler ONTAP Cluster zu Amazon S3	Wenn Sie BlueXP Tiering zu AWS aktivieren, werden Sie vom Assistenten aufgefordert, einen Zugriffsschlüssel und einen geheimen Schlüssel einzugeben. Diese Anmeldedaten werden an den ONTAP Cluster weitergeleitet, sodass ONTAP Daten-Tiering in den S3-Bucket durchführen kann.	"S3-Berechtigungen für Tiering einrichten"

Azure-Berechtigungen

BlueXP erfordert für den Connector und einzelne Services Azure Berechtigungen.

Anschlüsse

Ziel	Beschreibung	Verlinken
Implementieren Sie den Connector von BlueXP	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.	"Azure-Berechtigungen einrichten"
Geben Sie Berechtigungen für den Connector an	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 einen Connector vom Marktplatz starten, wenn Sie den Connector manuell installieren oder wenn Sie dies tun "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"

Kopieren und Synchronisieren

Ziel	Beschreibung	Verlinken
Implementieren Sie den Daten-Broker in Azure	Das Azure-Benutzerkonto, mit dem Sie den Daten-Broker bereitstellen, muss über die erforderlichen Berechtigungen verfügen.	"Erforderliche Berechtigungen für die Bereitstellung des Daten-Brokers in Azure"

Google Cloud-Berechtigungen

BlueXP erfordert für den Connector und einzelne Services Google Cloud-Berechtigungen.

Anschlüsse

Ziel	Beschreibung	Verlinken
Implementieren Sie den Connector von BlueXP	Der Google Cloud-Benutzer, der einen Connector von BlueXP bereitstellt, benötigt spezielle Berechtigungen, um den Connector in Google Cloud bereitzustellen.	"Richten Sie Berechtigungen zum Erstellen des Connectors ein"
Geben Sie Berechtigungen für den Connector an	Das Servicekonto für die Connector-VM-Instanz muss über spezielle Berechtigungen für den täglichen Betrieb verfügen. Sie müssen das Dienstkonto während der Bereitstellung dem Connector zuordnen. Außerdem müssen Sie sicherstellen, dass die Richtlinie aktuell ist, wenn neue Berechtigungen in nachfolgenden Releases hinzugefügt werden.	"Richten Sie die Berechtigungen für den Connector ein"

Backup und Recovery

Ziel	Beschreibung	Verlinken
Backup von Cloud Volumes ONTAP in der Google Cloud	Wenn Sie BlueXP Backup und Recovery für ein Backup von Cloud Volumes ONTAP verwenden, müssen Sie in den folgenden Szenarien Berechtigungen zum Connector hinzufügen: • Sie möchten die Funktion „Suchen & Wiederherstellen“ verwenden • Sie möchten vom Kunden gemanagte Verschlüsselungsschlüssel (CMEK) verwenden.	• "Berechtigungen für die Funktion Suchen Wiederherstellen " • "Berechtigungen für CMEKs"
Backup von lokalen ONTAP Clustern in Google Cloud	Wenn Sie Backup und Recovery von lokalen ONTAP-Clustern mit BlueXP nutzen, müssen Sie Berechtigungen zum Connector hinzufügen, um die Funktion „Suchen und Wiederherstellen“ nutzen zu können.	"Berechtigungen für die Funktion Suchen Wiederherstellen"

Cloud Volumes Service für Google Cloud

Ziel	Beschreibung	Verlinken
Cloud Volumes Service für Google Cloud entdecken	BlueXP benötigt Zugriff auf die Cloud Volumes Service API und die richtigen Berechtigungen über ein Google Cloud-Dienstkonto.	"Erstellen eines Servicekontos"

Kopieren und Synchronisieren

Ziel	Beschreibung	Verlinken
Implementieren Sie den Daten-Broker in Google Cloud	Stellen Sie sicher, dass der Google Cloud-Benutzer, der den Daten-Broker bereitstellt, über die erforderlichen Berechtigungen verfügt.	"Erforderliche Berechtigungen für die Bereitstellung des Daten-Brokers in Google Cloud"
Aktivieren Sie Google Cloud-Zugriff für einen manuell installierten Daten-Broker	Wenn Sie den Daten-Broker mit einer Synchronisierungsbeziehung verwenden möchten, die einen Google Cloud Storage Bucket enthält, sollten Sie den Linux-Host für Google Cloud-Zugriff vorbereiten. Nach der Installation des Daten-Brokers müssen Sie einen Schlüssel für ein Servicekonto mit spezifischen Berechtigungen bereitstellen.	"Zugriff auf Google Cloud wird ermöglicht"

StorageGRID-Berechtigungen

BlueXP erfordert StorageGRID Berechtigungen für zwei Services.

Backup und Recovery

Ziel	Beschreibung	Verlinken
Sichern Sie On-Premises-ONTAP-Cluster in StorageGRID	Wenn Sie StorageGRID als Backup-Ziel für ONTAP Cluster vorbereiten, werden Sie beim BlueXP Backup und Recovery aufgefordert, einen Zugriffsschlüssel und einen Schlüssel für einen IAM-Benutzer mit spezifischen Berechtigungen einzugeben.	"StorageGRID als Backup-Ziel vorbereiten"

Tiering

Ziel	Beschreibung	Verlinken
Tiering von lokalen ONTAP Clustern zu StorageGRID	Wenn Sie BlueXP Tiering auf StorageGRID einrichten, müssen Sie für BlueXP Tiering einen S3 Zugriffsschlüssel und einen geheimen Schlüssel bereitstellen. BlueXP Tiering verwendet die Schlüssel für den Zugriff auf Ihre Buckets.	"Tiering in StorageGRID vorbereiten"

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.

Beachten Sie Folgendes:

- 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.
- Sie müssen die Richtlinien selbst einrichten, wenn Sie den Connector über AWS Marketplace implementieren, den Connector manuell auf einem Linux-Host installieren oder zusätzliche AWS-Anmeldedaten zu BlueXP hinzufügen möchten.
- Außerdem müssen Sie sicherstellen, dass die Richtlinien immer auf dem neuesten Stand sind, wenn neue Berechtigungen in nachfolgenden Releases hinzugefügt werden.
- Bei Bedarf können Sie die IAM-Richtlinien mit Hilfe des IAM einschränken `Condition` Element: "AWS-Dokumentation: Condition Element"
- Informationen zur schrittweisen Verwendung dieser Richtlinien finden Sie auf den folgenden Seiten:
  - "Richten Sie Berechtigungen für eine AWS Marketplace-Implementierung ein"
  - "Richten Sie Berechtigungen für On-Premises-Implementierungen ein"
  - "Richten Sie Berechtigungen für den eingeschränkten Modus ein"
  - "Richten Sie Berechtigungen für den privaten Modus ein"

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

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:

- Amazon S3 Bucket-Erkennung
- Backup und Recovery
- Klassifizierung
- Cloud Volumes ONTAP
- FSX für ONTAP
- Tiering

Die zweite Richtlinie bietet Berechtigungen für die folgenden Dienste:

- Edge-Caching
- Kubernetes

Richtlinie #1

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

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

```
                "s3:GetEncryptionConfiguration",
                "kms:List*",
                "kms:ReEncrypt*",
                "kms:Describe*",
                "kms:CreateGrant",
                "fsx:Describe*",
                "fsx:List*",
                "kms:GenerateDataKeyWithoutPlaintext"
            ],
            "Resource": "*",
            "Effect": "Allow",
            "Sid": "cvoServicePolicy"
        },
        {
            "Action": [
                "ec2:StartInstances",
                "ec2:StopInstances",
                "ec2:DescribeInstances",
                "ec2:DescribeInstanceStatus",
                "ec2:RunInstances",
                "ec2:TerminateInstances",
                "ec2:DescribeInstanceAttribute",
                "ec2:DescribeImages",
                "ec2:CreateTags",
                "ec2:CreateVolume",
                "ec2:CreateSecurityGroup",
                "ec2:DescribeSubnets",
                "ec2:DescribeVpcs",
                "ec2:DescribeRegions",
                "cloudformation:CreateStack",
                "cloudformation:DeleteStack",
                "cloudformation:DescribeStacks",
                "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": "*",
            "Effect": "Allow",
            "Sid": "backupPolicy"
        },
        {
            "Action": [
                "s3:GetBucketLocation",
                "s3:ListAllMyBuckets",
                "s3:ListBucket",
                "s3:CreateBucket",
                "s3:GetLifecycleConfiguration",
                "s3:PutLifecycleConfiguration",
                "s3:PutBucketTagging",
                "s3:ListBucketVersions",
                "s3:GetBucketAcl",
                "s3:PutBucketPublicAccessBlock",
                "s3:GetObject",
                "s3:PutEncryptionConfiguration",
                "s3:DeleteObject",
                "s3:DeleteObjectVersion",
                "s3:ListBucketMultipartUploads",
                "s3:PutObject",
                "s3:PutBucketAcl",
                "s3:AbortMultipartUpload",
                "s3:ListMultipartUploadParts",
                "s3:DeleteBucket",
                "s3:GetObjectVersionTagging",
                "s3:GetObjectVersionAcl",
                "s3:GetObjectRetention",
                "s3:GetObjectTagging",
                "s3:GetObjectVersion",
                "s3:PutObjectVersionTagging",
                "s3:PutObjectRetention",
                "s3:DeleteObjectTagging",
                "s3:DeleteObjectVersionTagging",
                "s3:GetBucketObjectLockConfiguration",
                "s3:GetBucketVersioning",
                "s3:PutBucketObjectLockConfiguration",
                "s3:PutBucketVersioning",
                "s3:BypassGovernanceRetention",
                "s3:PutBucketPolicy",
                "s3:PutBucketOwnershipControls"
            ],
            "Resource": [
                "arn:aws:s3:::netapp-backup-*"
```

```
            ],
            "Effect": "Allow",
            "Sid": "backupS3Policy"
        },
        {
            "Action": [
                "s3:CreateBucket",
                "s3:GetLifecycleConfiguration",
                "s3:PutLifecycleConfiguration",
                "s3:PutBucketTagging",
                "s3:ListBucketVersions",
                "s3:GetBucketPolicyStatus",
                "s3:GetBucketPublicAccessBlock",
                "s3:GetBucketAcl",
                "s3:GetBucketPolicy",
                "s3:PutBucketPublicAccessBlock",
                "s3:DeleteBucket"
            ],
            "Resource": [
                "arn:aws:s3:::fabric-pool*"
            ],
            "Effect": "Allow",
            "Sid": "fabricPoolS3Policy"
        },
        {
            "Action": [
                "ec2:DescribeRegions"
            ],
            "Resource": "*",
            "Effect": "Allow",
            "Sid": "fabricPoolPolicy"
        },
        {
            "Condition": {
                "StringLike": {
                    "ec2:ResourceTag/netapp-adc-manager": "*"
                }
            },
            "Action": [
                "ec2:StartInstances",
                "ec2:StopInstances",
                "ec2:TerminateInstances"
            ],
            "Resource": [
                "arn:aws:ec2:*:*:instance/*"
            ],
```

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

```
}
```

Richtlinie #2

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

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

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",
                "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/*"
            ]
        }
    ]
}
```

Geheime Regionen

```
{
    "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-b:s3:::fabric-pool*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:StartInstances",
                "ec2:StopInstances",
                "ec2:TerminateInstances",
                "ec2:AttachVolume",
```

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

Top Secret Regionen

```
{
    "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 jeden BlueXP Service beschrieben. Diese Informationen können hilfreich sein, wenn Ihre Unternehmensrichtlinien vorschreiben, dass Berechtigungen nur bei Bedarf bereitgestellt werden.

Amazon FSX für ONTAP

Der Connector stellt die folgenden API-Anforderungen für das Management von Amazon FSX für ONTAP bereit:

- 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:DescribeVpcEndpunkte
- ec2:DescribeVpcs
- ec2:DescribeVolumiesModified
- ec2:DescribePlacementGroups
- Km:Liste*
- Km:Beschreiben*
- Km:CreateGrant
- Km:ListAliase
- fsx:Beschreiben*
- fsx:Liste*

Amazon S3 Bucket-Erkennung

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

s3:GetVerschlüsselungKonfiguration

Backup und Recovery

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:DescribeVpcEndpunkte
- 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:StartQueryExecution
- 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

Klassifizierung

Der Connector macht die folgenden API-Anfragen zur Implementierung der BlueXP Klassifizierungsinstanz:

- 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 macht die folgenden API-Anfragen zum Scannen von S3-Buckets, wenn Sie die BlueXP-Klassifizierung verwenden:

- 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 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
Routingtabellen in einer VPC beschreiben (nur für HA-Paare erforderlich)	ec2:DescribeRouteTables	Ja.	Nein	Nein

Zweck	Aktion	Werden sie für die Implementierung verwendet?	Wird für den täglichen Betrieb verwendet?	Zum Löschen verwendet?
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
	Kms:GenerateDataKeyWithoutPlaintext	Ja.	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

Edge-Caching

Der Connector macht die folgenden API-Anfragen zur Implementierung von BlueXP Edge-Caching-Instanzen während der Implementierung:

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

Kubernetes

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

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

Änderungsprotokoll

Wenn Berechtigungen hinzugefügt und entfernt werden, werden wir diese in den folgenden Abschnitten zur Kenntnis nehmen.

8 März 2024

Die folgende Berechtigung ist jetzt in der Connector-Richtlinie enthalten:

ec2:DescribeAvailability Zones

Diese Berechtigung ist für eine kommende Version erforderlich. Wir werden die Versionshinweise mit weiteren Details aktualisieren, sobald diese Version verfügbar ist.

6 Juni 2023

Für Cloud Volumes ONTAP ist nun die folgende Berechtigung erforderlich:

Kms:GenerateDataKeyWithoutPlaintext

14 Februar 2023

Für BlueXP Tiering ist jetzt die folgende Berechtigung erforderlich:

ec2:DescribeVpcEndpunkte

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.

Informationen zur schrittweisen Verwendung dieser Richtlinien finden Sie auf den folgenden Seiten:

- "Richten Sie Berechtigungen für eine Azure Marketplace-Implementierung ein"
- "Richten Sie Berechtigungen für On-Premises-Implementierungen ein"
- "Richten Sie Berechtigungen für den eingeschränkten Modus ein"
- "Richten Sie Berechtigungen für den privaten Modus ein"

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/read",
                    "Microsoft.Network/locations/operationResults/read",
                    "Microsoft.Network/locations/operations/read",
                    "Microsoft.Network/networkInterfaces/read",
                    "Microsoft.Network/networkInterfaces/write",
                    "Microsoft.Network/networkInterfaces/join/action",
                    "Microsoft.Network/networkSecurityGroups/read",
                    "Microsoft.Network/networkSecurityGroups/write",
                    "Microsoft.Network/networkSecurityGroups/join/action",
                    "Microsoft.Network/virtualNetworks/read",

"Microsoft.Network/virtualNetworks/checkIpAddressAvailability/read",
                    "Microsoft.Network/virtualNetworks/subnets/read",
                    "Microsoft.Network/virtualNetworks/subnets/write",

"Microsoft.Network/virtualNetworks/subnets/virtualMachines/read",

"Microsoft.Network/virtualNetworks/virtualMachines/read",

"Microsoft.Network/virtualNetworks/subnets/join/action",
                    "Microsoft.Resources/deployments/operations/read",
                    "Microsoft.Resources/deployments/read",
                    "Microsoft.Resources/deployments/write",
                    "Microsoft.Resources/resources/read",

"Microsoft.Resources/subscriptions/operationresults/read",

"Microsoft.Resources/subscriptions/resourceGroups/delete",

"Microsoft.Resources/subscriptions/resourceGroups/read",

"Microsoft.Resources/subscriptions/resourcegroups/resources/read",

"Microsoft.Resources/subscriptions/resourceGroups/write",
                    "Microsoft.Storage/checknameavailability/read",
```

```
                    "Microsoft.Storage/operations/read",
                    "Microsoft.Storage/storageAccounts/listkeys/action",
                    "Microsoft.Storage/storageAccounts/read",
                    "Microsoft.Storage/storageAccounts/delete",
                    "Microsoft.Storage/storageAccounts/write",

"Microsoft.Storage/storageAccounts/blobServices/containers/read",

"Microsoft.Storage/storageAccounts/listAccountSas/action",
                    "Microsoft.Storage/usages/read",
                    "Microsoft.Compute/snapshots/write",
                    "Microsoft.Compute/snapshots/read",
                    "Microsoft.Compute/availabilitySets/write",
                    "Microsoft.Compute/availabilitySets/read",
                    "Microsoft.Compute/disks/beginGetAccess/action",

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

"Microsoft.MarketplaceOrdering/offertypes/publishers/offers/plans/agreemen
ts/write",
                    "Microsoft.Network/loadBalancers/read",
                    "Microsoft.Network/loadBalancers/write",
                    "Microsoft.Network/loadBalancers/delete",

"Microsoft.Network/loadBalancers/backendAddressPools/read",

"Microsoft.Network/loadBalancers/backendAddressPools/join/action",

"Microsoft.Network/loadBalancers/loadBalancingRules/read",
                    "Microsoft.Network/loadBalancers/probes/read",
                    "Microsoft.Network/loadBalancers/probes/join/action",
                    "Microsoft.Authorization/locks/*",
                    "Microsoft.Network/routeTables/join/action",
                    "Microsoft.NetApp/netAppAccounts/read",
                    "Microsoft.NetApp/netAppAccounts/capacityPools/read",

"Microsoft.NetApp/netAppAccounts/capacityPools/volumes/write",

"Microsoft.NetApp/netAppAccounts/capacityPools/volumes/read",

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

"Microsoft.Storage/storageAccounts/PrivateEndpointConnectionsApproval/acti
on",
```

```
"Microsoft.Storage/storageAccounts/privateEndpointConnections/read",

"Microsoft.Storage/storageAccounts/managementPolicies/read",

"Microsoft.Storage/storageAccounts/managementPolicies/write",
                    "Microsoft.Network/privateEndpoints/read",
                    "Microsoft.Network/privateDnsZones/write",

"Microsoft.Network/privateDnsZones/virtualNetworkLinks/write",
                    "Microsoft.Network/virtualNetworks/join/action",
                    "Microsoft.Network/privateDnsZones/A/write",
                    "Microsoft.Network/privateDnsZones/read",

"Microsoft.Network/privateDnsZones/virtualNetworkLinks/read",

"Microsoft.Resources/deployments/operationStatuses/read",
                    "Microsoft.Insights/Metrics/Read",
                    "Microsoft.Compute/virtualMachines/extensions/write",
                    "Microsoft.Compute/virtualMachines/extensions/delete",
                    "Microsoft.Compute/virtualMachines/extensions/read",
                    "Microsoft.Compute/virtualMachines/delete",
                    "Microsoft.Network/networkInterfaces/delete",
                    "Microsoft.Network/networkSecurityGroups/delete",
                    "Microsoft.Resources/deployments/delete",
                    "Microsoft.Compute/diskEncryptionSets/read",
                    "Microsoft.Compute/snapshots/delete",
                    "Microsoft.Network/privateEndpoints/delete",
                    "Microsoft.Compute/availabilitySets/delete",
                    "Microsoft.KeyVault/vaults/read",
                    "Microsoft.KeyVault/vaults/accessPolicies/write",
                    "Microsoft.Compute/diskEncryptionSets/write",
                    "Microsoft.KeyVault/vaults/deploy/action",
                    "Microsoft.Compute/diskEncryptionSets/delete",
                    "Microsoft.Resources/tags/read",
                    "Microsoft.Resources/tags/write",
                    "Microsoft.Resources/tags/delete",
                    "Microsoft.Network/applicationSecurityGroups/write",
                    "Microsoft.Network/applicationSecurityGroups/read",

"Microsoft.Network/applicationSecurityGroups/joinIpConfiguration/action",

"Microsoft.Network/networkSecurityGroups/securityRules/write",
                    "Microsoft.Network/applicationSecurityGroups/delete",

"Microsoft.Network/networkSecurityGroups/securityRules/delete",
```

```
"Microsoft.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.Synapse/workspaces/privateEndpointConnectionsApproval/action",

"Microsoft.ManagedIdentity/userAssignedIdentities/assign/action",
                    "Microsoft.Compute/images/write",

"Microsoft.Network/loadBalancers/frontendIPConfigurations/read"
    ],
    "NotActions": [],
    "AssignableScopes": [],
    "Description": "BlueXP Permissions",
    "IsCustom": "true"
}
```

Verwendung von Azure Berechtigungen

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

Azure NetApp Dateien

Wenn Sie die BlueXP Klassifizierung zum Scannen von Azure NetApp Files-Daten verwenden, stellt der Connector die folgenden API-Anforderungen:

- 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

Backup und Recovery

Der Connector macht die folgenden API-Anfragen für das Backup und Recovery von BlueXP:

- Microsoft.Storage/StorageAccounts/Listkeys/Action
- Microsoft.Storage/StorageAccounts/Lesevorgang
- Microsoft.Storage/StorageAccounts/write
- Microsoft.Storage/StorageAccounts/blobServices/Container/Lesevorgang
- Microsoft.Storage/storageAccounts/listeAccountActionSas/Action
- 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.Network/networkInterfaces/delete
- Microsoft.Network/networkSecurityGroups/delete
- Microsoft.Ressourcen/Bereitstellungen/löschen
- 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
- Microsoft.Synapse/Workspaces/private EndpointConnectionsGenehmigung/Aktion

Klassifizierung

Bei der Verwendung der BlueXP Klassifizierung macht der Connector die folgenden API-Anfragen.

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.
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.

Aktion	Wird zur Einrichtung verwendet?	Wird für den täglichen Betrieb verwendet?
Microsoft.Storage/StorageAccounts/write	Ja.	Nein
Microsoft.Storage/StorageAccounts/blobServices/Container/Lesevorgang	Ja.	Ja.
Microsoft.Network/networkInterfaces/read	Ja.	Ja.
Microsoft.Network/networkInterfaces/write	Ja.	Nein
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.

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

Cloud Volumes ONTAP

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

Zweck	Aktion	Werden sie für die Implementierung verwendet?	Wird für den täglichen Betrieb verwendet?	Zum Löschen verwendet?
Erstellen und Managen von VMs	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
	Microsoft.Compute/virtualMachines/delete	Ja.	Ja.	Ja.
	Microsoft.Ressourcen/Bereitstellungen/löschen	Ja.	Nein	Nein

Zweck	Aktion	Werden sie für die Implementierung verwendet?	Wird für den täglichen Betrieb verwendet?	Zum Löschen verwendet?
Implementierung über eine VHD ermöglichen	Microsoft.Compute/images/read	Ja.	Nein	Nein
	Microsoft.Compute/images/write	Ja.	Nein	Nein
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
	Microsoft.Network/networkInterfaces/delete	Ja.	Ja.	Nein
Erstellen und Verwalten von Netzwerksicherheitsgruppen	Microsoft.Network/networkSecurityGroups/read	Ja.	Ja.	Nein
	Microsoft.Network/networkSecurityGroups/write	Ja.	Ja.	Nein
	Microsoft.Network/networkSecurityGroups/join/action	Ja.	Nein	Nein
	Microsoft.Network/networkSecurityGroups/delete	Nein	Ja.	Ja.

Zweck	Aktion	Werden sie für die Implementierung verwendet?	Wird für den täglichen Betrieb verwendet?	Zum Löschen verwendet?
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/CheckknameVerfügbarkeit/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

Zweck	Aktion	Werden sie für die Implementierung verwendet?	Wird für den täglichen Betrieb verwendet?	Zum Löschen verwendet?
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.	Nein	Nein
	Microsoft.Network/loadBalancers/backendAddressPools/join/action	Ja.	Nein	Nein
	Microsoft.Network/loadBalancers/frontendIPConfigurations/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
Verwaltung von Sperren auf Azure Festplatten aktivieren	Microsoft.Authorization/Locks/*	Ja.	Ja.	Nein

Zweck	Aktion	Werden sie für die Implementierung verwendet?	Wird für den täglichen Betrieb verwendet?	Zum Löschen verwendet?
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-Bereitstellungen, abhängig von der zugrunde liegenden physischen Hardware	Microsoft.Ressourcen/Implementierungen/OperationStatuses/read	Ja.	Ja.	Nein
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

Zweck	Aktion	Werden sie für die Implementierung verwendet?	Wird für den täglichen Betrieb verwendet?	Zum Löschen verwendet?
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.	Nein
	Microsoft.Network/applicationSecurityGroups/joinIpConfiguration/action	Nein	Ja.	Nein
	Microsoft.Network/networkSecurityGroups/securityRules/write	Ja.	Ja.	Nein
	Microsoft.Network/applicationSecurityGroups/delete	Nein	Ja.	Ja.
	Microsoft.Network/networkSecurityGroups/securityRules/delete	Nein	Ja.	Ja.
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

Edge-Caching

Der Connector macht die folgenden API-Anfragen, wenn Sie BlueXP Edge Caching verwenden:

- 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

Tiering

Der Connector macht die folgenden API-Anfragen, wenn Sie BlueXP Tiering einrichten.

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

Änderungsprotokoll

Wenn Berechtigungen hinzugefügt und entfernt werden, werden wir diese in den folgenden Abschnitten zur Kenntnis nehmen.

5 Dezember 2023

Die folgenden Berechtigungen für das BlueXP Backup und Recovery beim Backup von Volume-Daten auf Azure Blob Storage sind nicht mehr erforderlich:

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

Diese Berechtigungen sind für andere BlueXP Storage-Services erforderlich, sodass sie weiterhin für den Connector relevant sind, wenn Sie diese anderen Storage-Services nutzen.

12 Mai 2023

Die folgenden Berechtigungen wurden der JSON-Richtlinie hinzugefügt, da sie für das Cloud Volumes ONTAP-Management erforderlich sind:

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

Die folgenden Berechtigungen wurden aus der JSON-Richtlinie entfernt, da sie nicht mehr erforderlich sind:

- Microsoft.Storage/StorageAccounts/blobServices/Container/write
- Microsoft.Network/publicIPAddresses/delete

23 März 2023

Die Berechtigung „Microsoft.Storage/storageAccounts/delete“ wird für die BlueXP Klassifizierung nicht mehr benötigt.

Diese Genehmigung ist für Cloud Volumes ONTAP weiterhin erforderlich.

5. Januar 2023

Die folgenden Berechtigungen wurden der JSON-Richtlinie hinzugefügt:

- Microsoft.Storage/storageAccounts/listeAccountActionSas/Action
- Microsoft.Synapse/Workspaces/private EndpointConnectionsGenehmigung/Aktion

  Diese Berechtigungen sind für das Backup und Recovery von BlueXP erforderlich.

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

  Diese Berechtigung ist für die Cloud Volumes ONTAP-Bereitstellung erforderlich.

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.

- "Richten Sie Google Cloud-Berechtigungen für den Standardmodus ein"
- "Richten Sie Berechtigungen für den eingeschränkten Modus ein"
- "Richten Sie Berechtigungen für den privaten Modus ein"

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.instanceGroups.get
- compute.addresses.get
- compute.instances.updateNetworkInterface
- 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
- cloudkms.cryptoKeys.getIamPolicy
- cloudkms.cryptoKeys.setIamPolicy
- cloudkms.keyRings.get
- cloudkms.keyRings.getIamPolicy
- cloudkms.keyRings.setIamPolicy
```

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.

Aktionen	Zweck
- 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.
- 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.

Aktionen	Zweck
- deploymentmanager.compositeTypes.get - deploymentmanager.compositeTypes.list - deploymentmanager.deployments.create - deploymentmanager.deployments.delete - deploymentmanager.deployments.get - deploymentmanager.deployments.list - Deploymentmanager.Manifeste.get - Deplomentmanager.Manifeste.list - Deploymentmanager.Operations.get - Deplomentmanager.Operations.list - Deploymentmanager.Resources.get - Deploymentmanager.Resources.list - Deploymentmanager.typProviders.get - Deplomentmanager.typProviders.list - Deplomentmanager.types.get - Deplomentmanager.types.list	Um die Cloud Volumes ONTAP VM-Instanz mithilfe von Google Cloud Deployment Manager bereitzustellen.
- Logging.logEinträge.list - Logging.privateLogEinträge.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.cryptkeys.get - Cloudkms.cryptkeys.list - Cloudkms.Keyrings.list	Verwenden von vom Kunden gemanagten Verschlüsselungen aus dem Cloud-Verschlüsselungsmanagement-Service mit Cloud Volumes ONTAP.
- 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	Um die BlueXP Klassifizierung zu aktivieren.

Aktionen	Zweck
- 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 - compute.instances.updateNetworkInterface	Um Storage VMs auf Cloud Volumes ONTAP HA-Paaren zu erstellen und zu managen.
- Monitoring.timeseries.list - Storage.Buckets.getIamPolicy	Um Informationen zu Google Cloud Storage Buckets zu erhalten.
- Cloudkms.cryptkeys.get - Cloudkms.cryptkeys.getIamPolicy - Cloudkms.cryptkeys.list - cloudkms.cryptoKeys.setIamPolicy - Cloudkms.Schlüsselanhänger.get - Cloudkms.Keyrings.getIamPolicy - Cloudkms.Keyrings.list - cloudkms.keyRings.setIamPolicy	So wählen Sie im BlueXP Aktivierungsassistenten für Backup und Recovery eigene vom Kunden gemanagte Schlüssel aus, statt die standardmäßigen, von Google gemanagten Schlüssel zu verwenden.

Änderungsprotokoll

Wenn Berechtigungen hinzugefügt und entfernt werden, werden wir diese in den folgenden Abschnitten zur Kenntnis nehmen.

6 Februar 2023

Die folgende Berechtigung wurde dieser Richtlinie hinzugefügt:

- compute.instances.updateNetworkInterface

Diese Erlaubnis ist für Cloud Volumes ONTAP erforderlich.

27 Januar 2023

Die Richtlinie hat folgende Berechtigungen hinzugefügt:

- Cloudkms.KryptoKeys.getIamPolicy
- cloudkms.cryptoKeys.setIamPolicy
- Cloudkms.Schlüsselanhänger.get
- Cloudkms.Keyrings.getIamPolicy
- cloudkms.keyRings.setIamPolicy

Diese Berechtigungen sind für das Backup und Recovery von BlueXP erforderlich.

Ports

Regeln für die Connector-Sicherheitsgruppe in AWS

Für die AWS Sicherheitsgruppe für den Connector sind sowohl ein- als auch ausgehende Regeln erforderlich. BlueXP erstellt diese Sicherheitsgruppe automatisch, wenn Sie einen

Connector aus BlueXP erstellen. Sie müssen diese Sicherheitsgruppe für alle anderen Installationsoptionen einrichten.

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 • Wird während des Cloud Volumes ONTAP-Upgrade-Prozesses verwendet
HTTPS	443	Bietet HTTPS-Zugriff von Client-Webbrowsern auf die lokale Benutzeroberfläche und Verbindungen von der BlueXP Klassifizierungsinstanz
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. "Erfahren Sie, wie der Connector als Proxy für AutoSupport-Nachrichten verwendet wird"
TCP	9060, 9061	BlueXP Klassifizierung und BlueXP Backup und Recovery in Regierungsregionen lassen sich aktivieren und nutzen.

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, ONTAP, BlueXP Klassifizierung und das Senden von AutoSupport Nachrichten an NetApp
API-Aufrufe	TCP	3000	ONTAP HA Mediator	Kommunikation mit dem ONTAP HA Mediator
	TCP	8080	BlueXP Klassifizierung	Durchführung von Prüfanfragen zur BlueXP Klassifizierungsinstanz während der Implementierung
DNS	UDP	53	DNS	Wird für DNS Resolve von BlueXP verwendet

Regeln für die Connector-Sicherheitsgruppe in Azure

Für die Azure-Sicherheitsgruppe für den Connector sind sowohl ein- als auch ausgehende Regeln erforderlich. BlueXP erstellt diese Sicherheitsgruppe automatisch, wenn Sie einen Connector aus BlueXP erstellen. Sie müssen diese Sicherheitsgruppe für alle anderen Installationsoptionen einrichten.

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 • Wird während des Cloud Volumes ONTAP-Upgrade-Prozesses verwendet
HTTPS	443	Bietet HTTPS-Zugriff von Client-Webbrowsern auf die lokale Benutzeroberfläche und Verbindungen von der BlueXP Klassifizierungsinstanz

Protokoll	Port	Zweck
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. "Erfahren Sie, wie der Connector als Proxy für AutoSupport-Nachrichten verwendet wird"
TCP	9060, 9061	BlueXP Klassifizierung und BlueXP Backup und Recovery in Regierungsregionen lassen sich aktivieren und nutzen.

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 zu Azure, zu ONTAP, zur BlueXP Klassifizierung und zum Senden von AutoSupport Nachrichten an NetApp

Service	Protokoll	Port	Ziel	Zweck
API-Aufrufe	TCP	8080	BlueXP Klassifizierung	Durchführung von Prüfanfragen zur BlueXP Klassifizierungsinstanz während der Implementierung
DNS	UDP	53	DNS	Wird für DNS Resolve von BlueXP verwendet

Connector-Firewall-Regeln in Google Cloud

Die Google Cloud Firewall-Regeln für den Connector erfordern sowohl ein- als auch ausgehende Regeln. BlueXP erstellt diese Sicherheitsgruppe automatisch, wenn Sie einen Connector aus BlueXP erstellen. Sie müssen diese Sicherheitsgruppe für alle anderen Installationsoptionen einrichten.

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 • Wird während des Cloud Volumes ONTAP-Upgrade-Prozesses verwendet
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. "Erfahren Sie, wie der Connector als Proxy für AutoSupport-Nachrichten verwendet wird"

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 an Google Cloud, an ONTAP, an BlueXP Klassifizierung und Senden von AutoSupport Nachrichten an NetApp
API-Aufrufe	TCP	8080	BlueXP Klassifizierung	Durchführung von Prüfanfragen zur BlueXP Klassifizierungsinstanz während der Implementierung
DNS	UDP	53	DNS	Wird für DNS Resolve von BlueXP verwendet

Anschlüsse für den On-Prem Connector

Der Connector verwendet *Inbound*-Ports, wenn er manuell auf einem lokalen Linux-Host installiert wird. Möglicherweise müssen Sie diese Ports zu Planungszwecken verwenden.

Diese Inbound Regeln gelten für alle BlueXP Implementierungsmodelle.

Protokoll	Port	Zweck
HTTP	80	• Bietet HTTP-Zugriff von Client-Webbrowsern auf die lokale Benutzeroberfläche • Wird während des Cloud Volumes ONTAP-Upgrade-Prozesses verwendet
HTTPS	443	Bietet HTTPS-Zugriff von Client-Webbrowsern auf die lokale Benutzeroberfläche

Copyright-Informationen

Copyright © 2024 NetApp. Alle Rechte vorbehalten. Gedruckt in den USA. Dieses urheberrechtlich geschützte Dokument darf ohne die vorherige schriftliche Genehmigung des Urheberrechtsinhabers in keiner Form und durch keine Mittel – weder grafische noch elektronische oder mechanische, einschließlich Fotokopieren, Aufnehmen oder Speichern in einem elektronischen Abrufsystem – auch nicht in Teilen, vervielfältigt werden.

Software, die von urheberrechtlich geschütztem NetApp Material abgeleitet wird, unterliegt der folgenden Lizenz und dem folgenden Haftungsausschluss:

DIE VORLIEGENDE SOFTWARE WIRD IN DER VORLIEGENDEN FORM VON NETAPP ZUR VERFÜGUNG GESTELLT, D. H. OHNE JEGLICHE EXPLIZITE ODER IMPLIZITE GEWÄHRLEISTUNG, EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKT AUF DIE STILLSCHWEIGENDE GEWÄHRLEISTUNG DER MARKTGÄNGIGKEIT UND EIGNUNG FÜR EINEN BESTIMMTEN ZWECK, DIE HIERMIT AUSGESCHLOSSEN WERDEN. NETAPP ÜBERNIMMT KEINERLEI HAFTUNG FÜR DIREKTE, INDIREKTE, ZUFÄLLIGE, BESONDERE, BEISPIELHAFTE SCHÄDEN ODER FOLGESCHÄDEN (EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKT AUF DIE BESCHAFFUNG VON ERSATZWAREN ODER -DIENSTLEISTUNGEN, NUTZUNGS-, DATEN- ODER GEWINNVERLUSTE ODER UNTERBRECHUNG DES GESCHÄFTSBETRIEBS), UNABHÄNGIG DAVON, WIE SIE VERURSACHT WURDEN UND AUF WELCHER HAFTUNGSTHEORIE SIE BERUHEN, OB AUS VERTRAGLICH FESTGELEGTER HAFTUNG, VERSCHULDENSUNABHÄNGIGER HAFTUNG ODER DELIKTSHAFTUNG (EINSCHLIESSLICH FAHRLÄSSIGKEIT ODER AUF ANDEREM WEGE), DIE IN IRGENDEINER WEISE AUS DER NUTZUNG DIESER SOFTWARE RESULTIEREN, SELBST WENN AUF DIE MÖGLICHKEIT DERARTIGER SCHÄDEN HINGEWIESEN WURDE.

NetApp behält sich das Recht vor, die hierin beschriebenen Produkte jederzeit und ohne Vorankündigung zu ändern. NetApp übernimmt keine Verantwortung oder Haftung, die sich aus der Verwendung der hier beschriebenen Produkte ergibt, es sei denn, NetApp hat dem ausdrücklich in schriftlicher Form zugestimmt. Die Verwendung oder der Erwerb dieses Produkts stellt keine Lizenzierung im Rahmen eines Patentrechts, Markenrechts oder eines anderen Rechts an geistigem Eigentum von NetApp dar.

Das in diesem Dokument beschriebene Produkt kann durch ein oder mehrere US-amerikanische Patente, ausländische Patente oder anhängige Patentanmeldungen geschützt sein.

ERLÄUTERUNG ZU „RESTRICTED RIGHTS“: Nutzung, Vervielfältigung oder Offenlegung durch die US-Regierung unterliegt den Einschränkungen gemäß Unterabschnitt (b)(3) der Klausel „Rights in Technical Data – Noncommercial Items“ in DFARS 252.227-7013 (Februar 2014) und FAR 52.227-19 (Dezember 2007).

Die hierin enthaltenen Daten beziehen sich auf ein kommerzielles Produkt und/oder einen kommerziellen Service (wie in FAR 2.101 definiert) und sind Eigentum von NetApp, Inc. Alle technischen Daten und die Computersoftware von NetApp, die unter diesem Vertrag bereitgestellt werden, sind gewerblicher Natur und wurden ausschließlich unter Verwendung privater Mittel entwickelt. Die US-Regierung besitzt eine nicht ausschließliche, nicht übertragbare, nicht unterlizenzierbare, weltweite, limitierte unwiderrufliche Lizenz zur Nutzung der Daten nur in Verbindung mit und zur Unterstützung des Vertrags der US-Regierung, unter dem die Daten bereitgestellt wurden. Sofern in den vorliegenden Bedingungen nicht anders angegeben, dürfen die Daten ohne vorherige schriftliche Genehmigung von NetApp, Inc. nicht verwendet, offengelegt, vervielfältigt, geändert, aufgeführt oder angezeigt werden. Die Lizenzrechte der US-Regierung für das US-Verteidigungsministerium sind auf die in DFARS-Klausel 252.227-7015(b) (Februar 2014) genannten Rechte beschränkt.

Markeninformationen

NETAPP, das NETAPP Logo und die unter http://www.netapp.com/TM aufgeführten Marken sind Marken von NetApp, Inc. Andere Firmen und Produktnamen können Marken der jeweiligen Eigentümer sein.