



Reference

Setup and administration

NetApp
July 31, 2023

This PDF was generated from <https://docs.netapp.com/us-en/bluexp-setup-admin/reference-permissions.html> on July 31, 2023. Always check docs.netapp.com for the latest.

Table of Contents

| | |
|-------------------|----|
| Reference | 1 |
| Permissions | 1 |
| Ports | 55 |

Reference

Permissions

Permissions summary for BlueXP

To use BlueXP features and services, you'll need to provide permissions so that BlueXP can perform operations in your cloud environment. Use the links on this page to quickly access the permissions that you need based on your goal.

AWS permissions

| Purpose | Description | Link |
|---|--|--|
| Connector deployment from BlueXP | The user who creates a Connector from BlueXP needs specific permissions to deploy the instance in AWS. | Set up AWS permissions |
| Connector operation | <p>When BlueXP launches the Connector, it attaches a policy to the instance that provides the permissions required to manage resources and processes in your AWS account.</p> <p>You need to set up the policy yourself if you launch a Connector from the marketplace, manually install the Connector, or if you add more AWS credentials to a Connector.</p> <p>You also need to ensure that the policy is up to date as new permissions are added in subsequent releases.</p> | AWS permissions for the Connector |
| Cloud Volumes ONTAP operation | An IAM role must be attached to each Cloud Volumes ONTAP node in AWS. The same is true for the HA mediator. The default option is to let BlueXP create the IAM roles for you, but you can use your own. | Learn how to set up the IAM roles yourself |
| Back up on-premises ONTAP clusters to Amazon S3 | When activating backups on your ONTAP volumes, BlueXP backup and recovery prompts you to enter an access key and secret for an IAM user that has specific permissions. | Set up S3 permissions for backups |
| Tier on-premises ONTAP clusters to Amazon S3 | When you enable BlueXP tiering to AWS, the wizard prompts you to enter an access key and secret key. These credentials are passed to the ONTAP cluster so that ONTAP can tier data to the S3 bucket. | Set up S3 permissions for tiering |

Azure permissions

| Purpose | Description | Link |
|----------------------------------|---|---|
| Connector deployment from BlueXP | When you deploy a Connector from BlueXP, you need to use an Azure account or service principal that has permissions to deploy the Connector VM in Azure. | Set up Azure permissions |
| Connector operation | <p>When BlueXP deploys the Connector VM in Azure, it creates a custom role that provides the permissions required to manage resources and processes within that Azure subscription.</p> <p>You need to set up the custom role yourself if you launch a Connector from the marketplace, manually install the Connector, or if you add more Azure credentials to a Connector.</p> <p>You also need to ensure that the policy is up to date as new permissions are added in subsequent releases.</p> | Azure permissions for the Connector |

Google Cloud permissions

| Purpose | Description | Link |
|--|---|---|
| Connector deployment | The Google Cloud user who deploys a Connector from BlueXP needs specific permissions to deploy the Connector in Google Cloud. | Set up permissions to deploy the Connector |
| Connector operation | <p>The service account for the Connector VM instance must have specific permissions for day-to-day operations. You need to associate the service account with the Connector when you deploy it from BlueXP.</p> <p>You also need to ensure that the policy is up to date as new permissions are added in subsequent releases.</p> | Google Cloud permissions for the Connector |
| Back up Cloud Volumes ONTAP to Google Cloud | <p>When using BlueXP backup and recovery to back up Cloud Volumes ONTAP, you need to add permissions to the Connector in the following scenarios:</p> <ul style="list-style-type: none"> You want to use "Search & Restore" functionality You want to use customer-managed encryption keys (CMEK) | <ul style="list-style-type: none"> Permissions for Search & Restore functionality Permissions for CMEKs |
| Back up on-premises ONTAP clusters to Google Cloud | When using BlueXP backup and recovery to back up on-prem ONTAP clusters, you need to add permissions to the Connector in order to use the "Search & Restore" functionality. | Permissions for Search & Restore functionality |

StorageGRID permissions

| Purpose | Description | Link |
|---|---|---|
| Back up on-premises ONTAP clusters to StorageGRID | When you prepare StorageGRID as a backup target for ONTAP clusters, BlueXP backup and recovery prompts you to enter an access key and secret for an IAM user that has specific permissions. | Prepare StorageGRID as your backup target |
| Tier on-premises ONTAP clusters to StorageGRID | When you set up BlueXP tiering to StorageGRID, you need to provide BlueXP tiering with an S3 access key and secret key. BlueXP tiering uses the keys to access your buckets. | Prepare tiering to StorageGRID |

AWS permissions for the Connector

When BlueXP launches the Connector instance in AWS, it attaches a policy to the instance that provides the Connector with permissions to manage resources and processes within that AWS account. The Connector uses the permissions to make API calls to several AWS services, including EC2, S3, CloudFormation, IAM, the Key Management Service (KMS), and more.

IAM policies

The IAM policies available below provide the permissions that a Connector needs to manage resources and processes within your public cloud environment based on your AWS region.

Note the following:

- If you create a Connector in a standard AWS region directly from BlueXP, BlueXP automatically applies policies to the Connector. You don't need to do anything in this case.
- You need to set up the policies yourself if you deploy the Connector from the AWS Marketplace, if you manually install the Connector on a Linux host, or if you want to add additional AWS credentials to BlueXP.
- You also need to ensure that the policies are up to date as new permissions are added in subsequent releases.
- If needed, you can restrict the IAM policies by using the IAM `Condition` element. [AWS documentation: Condition element](#)
- To view step-by-step instructions for using these policies, refer to the following pages:
 - [Set up permissions for Connector installation in AWS \(standard mode\)](#)
 - [Set up permissions for Connector installation on premises \(standard mode\)](#)
 - [Set up permissions for restricted mode](#)
 - [Set up permissions for private mode](#)

Select your region to view the required policies:

Standard regions

For standard regions, the permissions are spread across two policies. Two policies are required due to a maximum character size limit for managed policies in AWS.

The first policy provides permissions for the following services:

- Amazon S3 bucket discovery
- Backup and recovery
- Classification
- Cloud Volumes ONTAP
- FSx for ONTAP
- Tiering

The second policy provides permissions for the following services:

- Edge caching
- Kubernetes
- Remediation

Policy #1

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

```
"ec2:DeleteSecurityGroup",
"ec2:DeleteNetworkInterface",
"ec2:DeleteSnapshot",
"ec2:DeleteTags",
"ec2:DeleteRoute",
"ec2:DeletePlacementGroup",
"ec2:DescribePlacementGroups",
"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",
        "ce:GetReservationUtilization",
        "ce:GetDimensionValues",
        "ce:GetCostAndUsage",
        "ce:GetTags",
        "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"
    }
]
}

```

Policy #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"
    }
]
```

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "iam:ListInstanceProfiles",
        "iam:CreateRole",
        "iam:DeleteRole",
        "iam:PutRolePolicy",
        "iam:CreateInstanceProfile",
        "iam:DeleteRolePolicy",
        "iam:AddRoleToInstanceProfile",
        "iam:RemoveRoleFromInstanceProfile",
        "iam:DeleteInstanceProfile",
        "ec2:ModifyVolumeAttribute",
        "sts:DecodeAuthorizationMessage",
        "ec2:DescribeImages",
        "ec2:DescribeRouteTables",
        "ec2:DescribeInstances",
        "iam:PassRole",
        "ec2:DescribeInstanceStatus",
        "ec2:RunInstances",
        "ec2:ModifyInstanceAttribute",
        "ec2:CreateTags",
        "ec2:CreateVolume",
        "ec2:DescribeVolumes",
        "ec2:DeleteVolume",
        "ec2:CreateSecurityGroup",
        "ec2:DeleteSecurityGroup",
        "ec2:DescribeSecurityGroups",
        "ec2:RevokeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:RevokeSecurityGroupIngress",
        "ec2:CreateNetworkInterface",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DeleteNetworkInterface",
        "ec2:ModifyNetworkInterfaceAttribute",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:DescribeDhcpOptions",
        "ec2:CreateSnapshot",
        "ec2:DeleteSnapshot",

```

```

        "ec2:DescribeSnapshots",
        "ec2:StopInstances",
        "ec2:GetConsoleOutput",
        "ec2:DescribeKeyPairs",
        "ec2:DescribeRegions",
        "ec2>DeleteTags",
        "ec2:DescribeTags",
        "cloudformation:CreateStack",
        "cloudformation>DeleteStack",
        "cloudformation:DescribeStacks",
        "cloudformation:DescribeStackEvents",
        "cloudformation:ValidateTemplate",
        "s3:GetObject",
        "s3:ListBucket",
        "s3:ListAllMyBuckets",
        "s3:GetBucketTagging",
        "s3:GetBucketLocation",
        "s3:CreateBucket",
        "s3:GetBucketPolicyStatus",
        "s3:GetBucketPublicAccessBlock",
        "s3:GetBucketAcl",
        "s3:GetBucketPolicy",
        "kms:List*",
        "kms:ReEncrypt*",
        "kms:Describe*",
        "kms:CreateGrant",
        "ec2:AssociateIamInstanceProfile",
        "ec2:DescribeIamInstanceProfileAssociations",
        "ec2:DisassociateIamInstanceProfile",
        "ec2:DescribeInstanceAttribute",
        "ce:GetReservationUtilization",
        "ce:GetDimensionValues",
        "ce:GetCostAndUsage",
        "ce:GetTags",
        "ec2:CreatePlacementGroup",
        "ec2>DeletePlacementGroup"
    ],
    "Resource": "*"
},
{
    "Sid": "fabricPoolPolicy",
    "Effect": "Allow",
    "Action": [
        "s3>DeleteBucket",
        "s3:GetLifecycleConfiguration",
        "s3:PutLifecycleConfiguration",

```



```

        "s3:PutBucketTagging",
        "s3:ListBucketVersions",
        "s3:GetBucketPolicyStatus",
        "s3:GetBucketPublicAccessBlock",
        "s3:GetBucketAcl",
        "s3:GetBucketPolicy",
        "s3:PutBucketPublicAccessBlock"
    ],
    "Resource": [
        "arn:aws-us-gov:s3:::fabric-pool*"
    ]
},
{
    "Sid": "backupPolicy",
    "Effect": "Allow",
    "Action": [
        "s3:DeleteBucket",
        "s3:GetLifecycleConfiguration",
        "s3:PutLifecycleConfiguration",
        "s3:PutBucketTagging",
        "s3:ListBucketVersions",
        "s3:GetObject",
        "s3:ListBucket",
        "s3:ListAllMyBuckets",
        "s3:GetBucketTagging",
        "s3:GetBucketLocation",
        "s3:GetBucketPolicyStatus",
        "s3:GetBucketPublicAccessBlock",
        "s3:GetBucketAcl",
        "s3:GetBucketPolicy",
        "s3:PutBucketPublicAccessBlock"
    ],
    "Resource": [
        "arn:aws-us-gov:s3:::netapp-backup-*"
    ]
},
{
    "Effect": "Allow",
    "Action": [
        "ec2:StartInstances",
        "ec2:TerminateInstances",
        "ec2:AttachVolume",
        "ec2:DetachVolume"
    ],
    "Condition": {
        "StringLike": {

```

```

        "ec2:ResourceTag/WorkingEnvironment": "*"
    },
    "Resource": [
        "arn:aws-us-gov:ec2:*:*:instance/*"
    ],
    {
        "Effect": "Allow",
        "Action": [
            "ec2:AttachVolume",
            "ec2:DetachVolume"
        ],
        "Resource": [
            "arn:aws-us-gov:ec2:*:*:volume/*"
        ]
    }
]
}

```

```

{
  "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/*"
    ]
}
]
}

```

How the AWS permissions are used

The following sections describe how the permissions are used for each BlueXP service. This information can be helpful if your corporate policies dictate that permissions are only provided as needed.

Amazon FSx for ONTAP

The Connector makes the following API requests to manage Amazon FSx for ONTAP:

- ec2:DescribeInstances
- ec2:DescribeInstanceStatus
- ec2:DescribeInstanceAttribute
- ec2:DescribeRouteTables
- ec2:DescribeImages
- ec2:CreateTags
- ec2:DescribeVolumes
- ec2:DescribeSecurityGroups
- ec2:DescribeNetworkInterfaces
- ec2:DescribeSubnets
- ec2:DescribeVpcs

- ec2:DescribeDhcpOptions
- ec2:DescribeSnapshots
- ec2:DescribeKeyPairs
- ec2:DescribeRegions
- ec2:DescribeTags
- ec2:DescribeIamInstanceProfileAssociations
- ec2:DescribeReservedInstancesOfferings
- ec2:DescribeVpcEndpoints
- ec2:DescribeVpcs
- ec2:DescribeVolumesModifications
- ec2:DescribePlacementGroups
- kms:List*
- kms:Describe*
- kms:CreateGrant
- kms:ListAliases
- fsx:Describe*
- fsx:List*

Amazon S3 bucket discovery

The Connector makes the following API request to discover Amazon S3 buckets:

s3:GetEncryptionConfiguration

Backup and recovery

The Connector makes the following API requests to manage backups in Amazon S3:

- s3:GetBucketLocation
- s3:ListAllMyBuckets
- s3:ListBucket
- s3>CreateBucket
- s3:GetLifecycleConfiguration
- s3:PutLifecycleConfiguration
- s3:PutBucketTagging
- s3:ListBucketVersions
- s3:GetBucketAcl
- s3:PutBucketPublicAccessBlock
- kms:List*
- kms:Describe*
- s3:GetObject

- ec2:DescribeVpcEndpoints
- kms:ListAliases
- s3:PutEncryptionConfiguration

The Connector makes the following API requests when you use the Search & Restore method to restore volumes and files:

- s3:CreateBucket
- s3:DeleteObject
- s3:DeleteObjectVersion
- s3:GetBucketAcl
- s3:ListBucket
- s3:ListBucketVersions
- s3:ListBucketMultipartUploads
- s3:PutObject
- s3:PutBucketAcl
- s3:PutLifecycleConfiguration
- s3:PutBucketPublicAccessBlock
- s3:AbortMultipartUpload
- s3:ListMultipartUploadParts
- athena:StartQueryExecution
- athena:GetQueryResults
- athena:GetQueryExecution
- athena:StopQueryExecution
- glue:CreateDatabase
- glue:CreateTable
- glue:BatchDeletePartition

The Connector makes the following API requests when you use DataLock and Ransomware protection for your volume backups:

- s3:GetObjectVersionTagging
- s3:GetBucketObjectLockConfiguration
- s3:GetObjectVersionAcl
- s3:PutObjectTagging
- s3:DeleteObject
- s3:DeleteObjectTagging
- s3:GetObjectRetention
- s3:DeleteObjectVersionTagging
- s3:PutObject

- s3:GetObject
- s3:PutBucketObjectLockConfiguration
- s3:GetLifecycleConfiguration
- s3:ListBucketByTags
- s3:GetBucketTagging
- s3:DeleteObjectVersion
- s3:ListBucketVersions
- s3:ListBucket
- s3:PutBucketTagging
- s3:GetObjectTagging
- s3:PutBucketVersioning
- s3:PutObjectVersionTagging
- s3:GetBucketVersioning
- s3:GetBucketAcl
- s3:BypassGovernanceRetention
- s3:PutObjectRetention
- s3:GetBucketLocation
- s3:GetObjectVersion

The Connector makes the following API requests if you use a different AWS account for your Cloud Volumes ONTAP backups than you're using for the source volumes:

- s3:PutBucketPolicy
- s3:PutBucketOwnershipControls

Classification

The Connector makes the following API requests to deploy the BlueXP classification instance:

- 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:DescribeRegions
- cloudformation:CreateStack
- cloudformation>DeleteStack
- cloudformation:DescribeStacks
- cloudformation:DescribeStackEvents
- iam:AddRoleToInstanceProfile
- ec2:AssociateIamInstanceProfile
- ec2:DescribeIamInstanceProfileAssociations

The Connector makes the following API requests to scan S3 buckets when you use BlueXP classification:

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

Cloud Volumes ONTAP

The Connector makes the following API requests to deploy and manage Cloud Volumes ONTAP in AWS.

| Purpose | Action | Used for deployment? | Used for daily operations? | Used for deletion? |
|---|--|----------------------|----------------------------|--------------------|
| Create and manage IAM roles and instance profiles for Cloud Volumes ONTAP instances | iam:ListInstanceProfiles | Yes | Yes | No |
| | iam:CreateRole | Yes | No | No |
| | iam:DeleteRole | No | Yes | Yes |
| | iam:PutRolePolicy | Yes | No | No |
| | iam:CreateInstanceProfile | Yes | No | No |
| | iam:DeleteRolePolicy | No | Yes | Yes |
| | iam:AddRoleToInstanceProfile | Yes | No | No |
| | iam:RemoveRoleFromInstanceProfile | No | Yes | Yes |
| | iam:DeleteInstanceProfile | No | Yes | Yes |
| | iam:PassRole | Yes | No | No |
| | ec2:AssociateIamInstanceProfile | Yes | Yes | No |
| | ec2:DescribeIamInstanceProfileAssociations | Yes | Yes | No |
| | ec2:DisassociateIamInstanceProfile | No | Yes | No |
| Decode authorization status messages | sts:DecodeAuthorizationMessage | Yes | Yes | No |
| Describe the specified images (AMIs) available to the account | ec2:DescribeImages | Yes | Yes | No |
| Describe the route tables in a VPC (required for HA pairs only) | ec2:DescribeRouteTables | Yes | No | No |

| Purpose | Action | Used for deployment? | Used for daily operations? | Used for deletion? |
|--|-------------------------------|----------------------|----------------------------|--------------------|
| Stop, start, and monitor instances | ec2:StartInstances | Yes | Yes | No |
| | ec2:StopInstances | Yes | Yes | No |
| | ec2:DescribeInstances | Yes | Yes | No |
| | ec2:DescribeInstanceStatus | Yes | Yes | No |
| | ec2:RunInstances | Yes | No | No |
| | ec2:TerminateInstances | No | No | Yes |
| | ec2:ModifyInstanceAttribute | No | Yes | No |
| Verify that enhanced networking is enabled for supported instance types | ec2:DescribeInstanceAttribute | No | Yes | No |
| Tag resources with the "WorkingEnvironment" and "WorkingEnvironmentId" tags which are used for maintenance and cost allocation | ec2:CreateTags | Yes | Yes | No |
| Manage EBS volumes that Cloud Volumes ONTAP uses as back-end storage | ec2:CreateVolume | Yes | Yes | No |
| | ec2:DescribeVolumes | Yes | Yes | Yes |
| | ec2:ModifyVolumeAttribute | No | Yes | Yes |
| | ec2:AttachVolume | Yes | Yes | No |
| | ec2>DeleteVolume | No | Yes | Yes |
| | ec2:DetachVolume | No | Yes | Yes |

| Purpose | Action | Used for deployment? | Used for daily operations? | Used for deletion? |
|--|-------------------------------------|----------------------|----------------------------|--------------------|
| Create and manage security groups for Cloud Volumes ONTAP | ec2:CreateSecurityGroup | Yes | No | No |
| | ec2:DeleteSecurityGroup | No | Yes | Yes |
| | ec2:DescribeSecurityGroups | Yes | Yes | Yes |
| | ec2:RevokeSecurityGroupEgress | Yes | No | No |
| | ec2:AuthorizeSecurityGroupEgress | Yes | No | No |
| | ec2:AuthorizeSecurityGroupIngress | Yes | No | No |
| | ec2:RevokeSecurityGroupIngress | Yes | Yes | No |
| Create and manage network interfaces for Cloud Volumes ONTAP in the target subnet | ec2:CreateNetworkInterface | Yes | No | No |
| | ec2:DescribeNetworkInterfaces | Yes | Yes | No |
| | ec2>DeleteNetworkInterface | No | Yes | Yes |
| | ec2:ModifyNetworkInterfaceAttribute | No | Yes | No |
| Get the list of destination subnets and security groups | ec2:DescribeSubnets | Yes | Yes | No |
| | ec2:DescribeVpcs | Yes | Yes | No |
| Get DNS servers and the default domain name for Cloud Volumes ONTAP instances | ec2:DescribeDhcpOptions | Yes | No | No |
| Take snapshots of EBS volumes for Cloud Volumes ONTAP | ec2:CreateSnapshot | Yes | Yes | No |
| | ec2>DeleteSnapshot | No | Yes | Yes |
| | ec2:DescribeSnapshots | No | Yes | No |
| Capture the Cloud Volumes ONTAP console, which is attached to AutoSupport messages | ec2:GetConsoleOutput | Yes | Yes | No |

| Purpose | Action | Used for deployment? | Used for daily operations? | Used for deletion? |
|---|------------------------------------|----------------------|----------------------------|--------------------|
| Get the list of available key pairs | ec2:DescribeKeyPairs | Yes | No | No |
| Get the list of available AWS regions | ec2:DescribeRegions | Yes | Yes | No |
| Manage tags for resources associated with Cloud Volumes ONTAP instances | ec2:DeleteTags | No | Yes | Yes |
| | ec2:DescribeTags | No | Yes | No |
| Create and manage stacks for AWS CloudFormation templates | cloudformation:CreateStack | Yes | No | No |
| | cloudformation:DeleteStack | Yes | No | No |
| | cloudformation:DescribeStacks | Yes | Yes | No |
| | cloudformation:DescribeStackEvents | Yes | No | No |
| | cloudformation:ValidateTemplate | Yes | No | No |

| Purpose | Action | Used for deployment? | Used for daily operations? | Used for deletion? |
|---|-------------------------------------|----------------------|----------------------------|--------------------|
| Create and manage an S3 bucket that a Cloud Volumes ONTAP system uses as a capacity tier for data tiering | s3:CreateBucket | Yes | Yes | No |
| | s3>DeleteBucket | No | Yes | Yes |
| | s3:GetLifecycleConfiguration | No | Yes | No |
| | s3:PutLifecycleConfiguration | No | Yes | No |
| | s3:PutBucketTagging | No | Yes | No |
| | s3:ListBucketVersions | No | Yes | No |
| | s3:GetBucketPolicyStatus | No | Yes | No |
| | s3:GetBucketPublicAccessBlock | No | Yes | No |
| | s3:GetBucketAcl | No | Yes | No |
| | s3:GetBucketPolicy | No | Yes | No |
| | s3:PutBucketPublicAccessBlock | No | Yes | No |
| | s3:GetBucketTagging | No | Yes | No |
| | s3:GetBucketLocation | No | Yes | No |
| | s3:ListAllMyBuckets | No | No | No |
| | s3:ListBucket | No | Yes | No |
| Enable data encryption of Cloud Volumes ONTAP using the AWS Key Management Service (KMS) | kms:List* | Yes | Yes | No |
| | kms:ReEncrypt* | Yes | No | No |
| | kms:Describe* | Yes | Yes | No |
| | kms>CreateGrant | Yes | Yes | No |
| | kms:GenerateDataKeyWithoutPlaintext | Yes | Yes | No |
| Obtain AWS cost data for Cloud Volumes ONTAP | ce:GetReservationUtilization | No | Yes | No |
| | ce:GetDimensionValues | No | Yes | No |
| | ce:GetCostAndUsage | No | Yes | No |
| | ce:GetTags | No | Yes | No |

| Purpose | Action | Used for deployment? | Used for daily operations? | Used for deletion? |
|---|---------------------------------|----------------------|----------------------------|--------------------|
| Create and manage an AWS spread placement group for two HA nodes and the mediator in a single AWS Availability Zone | ec2:CreatePlacementGroup | Yes | No | No |
| | ec2:DeletePlacementGroup | No | Yes | Yes |
| Create reports | fsx:Describe* | No | Yes | No |
| | fsx:List* | No | Yes | No |
| Create and manage aggregates that support the Amazon EBS Elastic Volumes feature | ec2:DescribeVolumeModifications | No | Yes | No |
| | ec2:ModifyVolume | No | Yes | No |

Edge caching

The Connector makes the following API requests to deploy BlueXP edge caching instances during deployment:

- cloudformation:DescribeStacks
- cloudwatch:GetMetricStatistics
- cloudformation:ListStacks

Kubernetes

The Connector makes the following API requests to discover and manage Amazon EKS clusters:

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

Remediation

The Connector makes the following API requests to manage tags on AWS resources when you use BlueXP remediation:

- ec2:CreateTags
- ec2:DeleteTags
- ec2:DescribeTags
- tag:getResources
- tag:getTagKeys
- tag:getTagValues
- tag:TagResources

- tag:UntagResources

Change log

As permissions are added and removed, we'll note them in the sections below.

6 June, 2023

The following permission is now required for Cloud Volumes ONTAP:

kms:GenerateDataKeyWithoutPlaintext

14 February, 2023

The following permission is now required for BlueXP tiering:

ec2:DescribeVpcEndpoints

Azure permissions for the Connector

When BlueXP launches the Connector VM in Azure, it attaches a custom role to the VM that provides the Connector with permissions to manage resources and processes within that Azure subscription. The Connector uses the permissions to make API calls to several Azure services.

Custom role permissions

The custom role shown below provides the permissions that a Connector needs to manage resources and processes within your Azure network.

When you create a Connector directly from BlueXP, BlueXP automatically applies this custom role to the Connector.

If you deploy the Connector from the Azure Marketplace or if you manually install the Connector on a Linux host, then you'll need to set up the custom role yourself.

- [Set up permissions for Connector installation in Azure \(standard mode\)](#)
- [Set up permissions for Connector installation on premises \(standard mode\)](#)
- [Set up permissions for restricted mode](#)
- [Set up permissions for private mode](#)

You also need to ensure that the role is up to date as new permissions are added in subsequent releases.

```
{
  "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/agreements/read",

"Microsoft.MarketplaceOrdering/offertypes/publishers/offers/plans/agreements/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/action",

```

```
"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/action",
    "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"
}

```

How Azure permissions are used

The following sections describe how the permissions are used for each BlueXP service. This information can be helpful if your corporate policies dictate that permissions are only provided as needed.

Azure NetApp Files

The Connector makes the following API requests when you use BlueXP classification to scan Azure NetApp Files data:

- 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 and recovery

The Connector makes the following API requests for BlueXP backup and recovery:

- Microsoft.Compute/virtualMachines/read
- Microsoft.Compute/virtualMachines/start/action
- Microsoft.Compute/virtualMachines/deallocate/action
- Microsoft.Storage/storageAccounts/listkeys/action
- Microsoft.Storage/storageAccounts/read
- Microsoft.Storage/storageAccounts/write
- Microsoft.Storage/storageAccounts/blobServices/containers/read
- Microsoft.Storage/storageAccounts/listAccountSas/action
- Microsoft.KeyVault/vaults/read
- Microsoft.KeyVault/vaults/accessPolicies/write
- Microsoft.Network/networkInterfaces/read
- Microsoft.Resources/subscriptions/locations/read
- Microsoft.Network/virtualNetworks/read
- Microsoft.Network/virtualNetworks/subnets/read
- Microsoft.Resources/subscriptions/resourceGroups/read
- Microsoft.Resources/subscriptions/resourcegroups/resources/read
- Microsoft.Resources/subscriptions/resourceGroups/write
- Microsoft.Authorization/locks/*
- Microsoft.Network/privateEndpoints/write
- Microsoft.Network/privateEndpoints/read
- Microsoft.Network/privateDnsZones/virtualNetworkLinks/write
- Microsoft.Network/virtualNetworks/join/action
- Microsoft.Network/privateDnsZones/A/write
- Microsoft.Network/privateDnsZones/read
- Microsoft.Network/privateDnsZones/virtualNetworkLinks/read
- Microsoft.Compute/virtualMachines/extensions/delete
- Microsoft.Compute/virtualMachines/delete
- Microsoft.Network/networkInterfaces/delete
- Microsoft.Network/networkSecurityGroups/delete
- Microsoft.Resources/deployments/delete
- Microsoft.ManagedIdentity/userAssignedIdentities/assign/action

The Connector makes the following API requests when you use the Search & Restore functionality:

- 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

Classification

The Connector makes the following API requests when you use BlueXP classification.

| Action | Used for set up? | Used for daily operations? |
|---|------------------|----------------------------|
| Microsoft.Compute/locations/operations/read | Yes | Yes |
| Microsoft.Compute/locations/vmSizes/read | Yes | Yes |
| Microsoft.Compute/operations/read | Yes | Yes |
| Microsoft.Compute/virtualMachines/instanceView/read | Yes | Yes |
| Microsoft.Compute/virtualMachines/powerOff/action | Yes | No |
| Microsoft.Compute/virtualMachines/read | Yes | Yes |
| Microsoft.Compute/virtualMachines/restart/action | Yes | No |
| Microsoft.Compute/virtualMachines/start/action | Yes | No |
| Microsoft.Compute/virtualMachines/vmSizes/read | No | Yes |
| Microsoft.Compute/virtualMachines/write | Yes | No |
| Microsoft.Compute/images/read | Yes | Yes |
| Microsoft.Compute/disks/delete | Yes | No |
| Microsoft.Compute/disks/read | Yes | Yes |
| Microsoft.Compute/disks/write | Yes | No |
| Microsoft.Storage/checknameavailability/read | Yes | Yes |
| Microsoft.Storage/operations/read | Yes | Yes |
| Microsoft.Storage/storageAccounts/listkeys/action | Yes | No |

| Action | Used for set up? | Used for daily operations? |
|---|------------------|----------------------------|
| Microsoft.Storage/storageAccounts/read | Yes | Yes |
| Microsoft.Storage/storageAccounts/write | Yes | No |
| Microsoft.Storage/storageAccounts/blobServices/containers/read | Yes | Yes |
| Microsoft.Network/networkInterfaces/read | Yes | Yes |
| Microsoft.Network/networkInterfaces/write | Yes | No |
| Microsoft.Network/networkInterfaces/join/action | Yes | No |
| Microsoft.Network/networkSecurityGroups/read | Yes | Yes |
| Microsoft.Network/networkSecurityGroups/write | Yes | No |
| Microsoft.Resources/subscriptions/locations/read | Yes | Yes |
| Microsoft.Network/locations/operationResults/read | Yes | Yes |
| Microsoft.Network/locations/operations/read | Yes | Yes |
| Microsoft.Network/virtualNetworks/read | Yes | Yes |
| Microsoft.Network/virtualNetworks/checkIpAddressAvailability/read | Yes | Yes |
| Microsoft.Network/virtualNetworks/subnets/read | Yes | Yes |
| Microsoft.Network/virtualNetworks/subnets/virtualMachines/read | Yes | Yes |
| Microsoft.Network/virtualNetworks/virtualMachines/read | Yes | Yes |
| Microsoft.Network/virtualNetworks/subnets/join/action | Yes | No |
| Microsoft.Network/virtualNetworks/subnets/write | Yes | No |
| Microsoft.Network/routeTables/join/action | Yes | No |
| Microsoft.Resources/deployments/operations/read | Yes | Yes |

| Action | Used for set up? | Used for daily operations? |
|---|------------------|----------------------------|
| Microsoft.Resources/deployments/read | Yes | Yes |
| Microsoft.Resources/deployments/write | Yes | No |
| Microsoft.Resources/resources/read | Yes | Yes |
| Microsoft.Resources/subscriptions/operationresults/read | Yes | Yes |
| Microsoft.Resources/subscriptions/resourceGroups/delete | Yes | No |
| Microsoft.Resources/subscriptions/resourceGroups/read | Yes | Yes |
| Microsoft.Resources/subscriptions/resourcegroups/resources/read | Yes | Yes |
| Microsoft.Resources/subscriptions/resourceGroups/write | Yes | No |

Cloud Volumes ONTAP

The Connector makes the following API requests to deploy and manage Cloud Volumes ONTAP in Azure.

| Purpose | Action | Used for deployment? | Used for daily operations? | Used for deletion? |
|------------------------------|---|----------------------|----------------------------|--------------------|
| Create and manage VMs | Microsoft.Compute/locations/operations/read | Yes | Yes | No |
| | Microsoft.Compute/locations/vmSizes/read | Yes | Yes | No |
| | Microsoft.Resources/subscriptions/locations/read | Yes | No | No |
| | Microsoft.Compute/operations/read | Yes | Yes | No |
| | Microsoft.Compute/virtualMachines/instanceView/read | Yes | Yes | No |
| | Microsoft.Compute/virtualMachines/powerOff/action | Yes | Yes | No |
| | Microsoft.Compute/virtualMachines/read | Yes | Yes | No |
| | Microsoft.Compute/virtualMachines/restart/action | Yes | Yes | No |
| | Microsoft.Compute/virtualMachines/start/action | Yes | Yes | No |
| | Microsoft.Compute/virtualMachines/deallocate/action | No | Yes | Yes |
| | Microsoft.Compute/virtualMachines/vmSizes/read | No | Yes | No |
| | Microsoft.Compute/virtualMachines/write | Yes | Yes | No |
| | Microsoft.Compute/virtualMachines/delete | Yes | Yes | Yes |
| | Microsoft.Resources/deployments/delete | Yes | No | No |
| Enable deployment from a VHD | Microsoft.Compute/images/read | Yes | No | No |
| | Microsoft.Compute/images/write | Yes | No | No |

| Purpose | Action | Used for deployment? | Used for daily operations? | Used for deletion? |
|---|---|----------------------|----------------------------|--------------------|
| Create and manage network interfaces in the target subnet | Microsoft.Network/networkInterfaces/read | Yes | Yes | No |
| | Microsoft.Network/networkInterfaces/write | Yes | Yes | No |
| | Microsoft.Network/networkInterfaces/join/action | Yes | Yes | No |
| | Microsoft.Network/networkInterfaces/delete | Yes | Yes | No |
| Create and manage network security groups | Microsoft.Network/networkSecurityGroups/read | Yes | Yes | No |
| | Microsoft.Network/networkSecurityGroups/write | Yes | Yes | No |
| | Microsoft.Network/networkSecurityGroups/join/action | Yes | No | No |
| | Microsoft.Network/networkSecurityGroups/delete | No | Yes | Yes |

| Purpose | Action | Used for deployment? | Used for daily operations? | Used for deletion? |
|---|---|----------------------|----------------------------|--------------------|
| Get network information about regions, the target VNet and subnet, and add the VMs to VNets | Microsoft.Network/locations/operationResults/read | Yes | Yes | No |
| | Microsoft.Network/locations/operations/read | Yes | Yes | No |
| | Microsoft.Network/virtualNetworks/read | Yes | No | No |
| | Microsoft.Network/virtualNetworks/checkIpAddressAvailability/read | Yes | No | No |
| | Microsoft.Network/virtualNetworks/subnets/read | Yes | Yes | No |
| | Microsoft.Network/virtualNetworks/subnets/virtualMachines/read | Yes | Yes | No |
| | Microsoft.Network/virtualNetworks/virtualMachines/read | Yes | Yes | No |
| | Microsoft.Network/virtualNetworks/subnets/join/action | Yes | Yes | No |

| Purpose | Action | Used for deployment? | Used for daily operations? | Used for deletion? |
|-----------------------------------|---|----------------------|----------------------------|--------------------|
| Create and manage resource groups | Microsoft.Resources/deployments/operations/read | Yes | Yes | No |
| | Microsoft.Resources/deployments/read | Yes | Yes | No |
| | Microsoft.Resources/deployments/write | Yes | Yes | No |
| | Microsoft.Resources/resources/read | Yes | Yes | No |
| | Microsoft.Resources/subscriptions/operationresults/read | Yes | Yes | No |
| | Microsoft.Resources/subscriptions/resourceGroups/delete | Yes | Yes | Yes |
| | Microsoft.Resources/subscriptions/resourceGroups/read | No | Yes | No |
| | Microsoft.Resources/subscriptions/resourcegroups/resources/read | Yes | Yes | No |
| | Microsoft.Resources/subscriptions/resourceGroups/write | Yes | Yes | No |

| Purpose | Action | Used for deployment? | Used for daily operations? | Used for deletion? |
|---|--|----------------------|----------------------------|--------------------|
| Manage Azure storage accounts and disks | Microsoft.Compute/disks/read | Yes | Yes | Yes |
| | Microsoft.Compute/disks/write | Yes | Yes | No |
| | Microsoft.Compute/disks/delete | Yes | Yes | Yes |
| | Microsoft.Storage/checknameavailability/read | Yes | Yes | No |
| | Microsoft.Storage/operations/read | Yes | Yes | No |
| | Microsoft.Storage/storageAccounts/listkeys/action | Yes | Yes | No |
| | Microsoft.Storage/storageAccounts/read | Yes | Yes | No |
| | Microsoft.Storage/storageAccounts/delete | No | Yes | Yes |
| | Microsoft.Storage/storageAccounts/write | Yes | Yes | No |
| | Microsoft.Storage/usage/read | No | Yes | No |
| Enable backups to Blob storage and encryption of storage accounts | Microsoft.Storage/storageAccounts/blobServices/containers/read | Yes | Yes | No |
| | Microsoft.KeyVault/vaults/read | Yes | Yes | No |
| | Microsoft.KeyVault/vaults/accessPolicies/write | Yes | Yes | No |
| Enable VNet service endpoints for data tiering | Microsoft.Network/virtualNetworks/subnets/write | Yes | Yes | No |
| | Microsoft.Network/routeTables/join/action | Yes | Yes | No |

| Purpose | Action | Used for deployment? | Used for daily operations? | Used for deletion? |
|--|---|----------------------|----------------------------|--------------------|
| Create and manage Azure managed snapshots | Microsoft.Compute/snapshots/write | Yes | Yes | No |
| | Microsoft.Compute/snapshots/read | Yes | Yes | No |
| | Microsoft.Compute/snapshots/delete | No | Yes | Yes |
| | Microsoft.Compute/disks/beginGetAccess/action | No | Yes | No |
| Create and manage availability sets | Microsoft.Compute/availabilitySets/write | Yes | No | No |
| | Microsoft.Compute/availabilitySets/read | Yes | No | No |
| Enable programmatic deployments from the marketplace | Microsoft.MarketplaceOrdering/offertypes/publishers/offers/plans/agreements/read | Yes | No | No |
| | Microsoft.MarketplaceOrdering/offertypes/publishers/offers/plans/agreements/write | Yes | Yes | No |

| Purpose | Action | Used for deployment? | Used for daily operations? | Used for deletion? |
|---|---|----------------------|----------------------------|--------------------|
| Manage a load balancer for HA pairs | Microsoft.Network/loadBalancers/read | Yes | Yes | No |
| | Microsoft.Network/loadBalancers/write | Yes | No | No |
| | Microsoft.Network/loadBalancers/delete | No | Yes | Yes |
| | Microsoft.Network/loadBalancers/backendAddressPools/read | Yes | No | No |
| | Microsoft.Network/loadBalancers/backendAddressPools/join/action | Yes | No | No |
| | Microsoft.Network/loadBalancers/frontendIPConfigurations/read | Yes | Yes | No |
| | Microsoft.Network/loadBalancers/loadBalancingRules/read | Yes | No | No |
| | Microsoft.Network/loadBalancers/probes/read | Yes | No | No |
| | Microsoft.Network/loadBalancers/probes/join/action | Yes | No | No |
| | Microsoft.Authorization/locks/* | Yes | Yes | No |
| Enable management of locks on Azure disks | | | | |

| Purpose | Action | Used for deployment? | Used for daily operations? | Used for deletion? |
|---|---|----------------------|----------------------------|--------------------|
| Enable private endpoints for HA pairs when there's no connectivity outside the subnet | Microsoft.Network/privateEndpoints/write | Yes | Yes | No |
| | Microsoft.Storage/storageAccounts/PrivateEndpointConnectionsApproval/action | Yes | No | No |
| | Microsoft.Storage/storageAccounts/privateEndpointConnections/read | Yes | Yes | Yes |
| | Microsoft.Network/privateEndpoints/read | Yes | Yes | Yes |
| | Microsoft.Network/privateDnsZones/write | Yes | Yes | No |
| | Microsoft.Network/privateDnsZones/virtualNetworkLinks/write | Yes | Yes | No |
| | Microsoft.Network/virtualNetworks/join/action | Yes | Yes | No |
| | Microsoft.Network/privateDnsZones/A/write | Yes | Yes | No |
| | Microsoft.Network/privateDnsZones/read | Yes | Yes | No |
| | Microsoft.Network/privateDnsZones/virtualNetworkLinks/read | Yes | Yes | No |
| Required for some VM deployments, depending on the underlying physical hardware | Microsoft.Resources/deployments/operationStatuses/read | Yes | Yes | No |
| Remove resources from a resource group in case of deployment failure or deletion | Microsoft.Network/privateEndpoints/delete | Yes | Yes | No |
| | Microsoft.Compute/availabilitySets/delete | Yes | Yes | No |

| Purpose | Action | Used for deployment? | Used for daily operations? | Used for deletion? |
|--|--|----------------------|----------------------------|--------------------|
| Enable the use of customer-managed encryption keys when using the API | Microsoft.Compute/diskEncryptionSets/read | Yes | Yes | Yes |
| | Microsoft.Compute/diskEncryptionSets/write | Yes | Yes | No |
| | Microsoft.KeyVault/vaults/deploy/action | Yes | No | No |
| | Microsoft.Compute/diskEncryptionSets/delete | Yes | Yes | Yes |
| Configure an application security group for an HA pair to isolate the HA interconnect and cluster network NICs | Microsoft.Network/applicationSecurityGroups/write | No | Yes | No |
| | Microsoft.Network/applicationSecurityGroups/read | No | Yes | No |
| | Microsoft.Network/applicationSecurityGroups/joinIpConfiguration/action | No | Yes | No |
| | Microsoft.Network/networkSecurityGroups/securityRules/write | Yes | Yes | No |
| | Microsoft.Network/applicationSecurityGroups/delete | No | Yes | Yes |
| | Microsoft.Network/networkSecurityGroups/securityRules/delete | No | Yes | Yes |
| Read, write, and delete tags associated with Cloud Volumes ONTAP resources | Microsoft.Resources/tags/read | No | Yes | No |
| | Microsoft.Resources/tags/write | Yes | Yes | No |
| | Microsoft.Resources/tags/delete | Yes | No | No |
| Encrypt storage accounts during creation | Microsoft.ManagedIdentity/userAssignedIdentities/assign/action | Yes | Yes | No |

Edge caching

The Connector makes the following API requests when you use BlueXP edge caching:

- Microsoft.Insights/Metrics/Read
- Microsoft.Compute/virtualMachines/extensions/write
- Microsoft.Compute/virtualMachines/extensions/read
- Microsoft.Compute/virtualMachines/extensions/delete
- Microsoft.Compute/virtualMachines/delete
- Microsoft.Network/networkInterfaces/delete
- Microsoft.Network/networkSecurityGroups/delete
- Microsoft.Resources/deployments/delete

Kubernetes

The Connector makes the following API requests to discover and manage clusters running in Azure Kubernetes Service (AKS):

- Microsoft.Compute/virtualMachines/read
- Microsoft.Resources/subscriptions/locations/read
- Microsoft.Resources/subscriptions/operationresults/read
- Microsoft.Resources/subscriptions/resourceGroups/read
- Microsoft.Resources/subscriptions/resourcegroups/resources/read
- Microsoft.ContainerService/managedClusters/read
- Microsoft.ContainerService/managedClusters/listClusterUserCredential/action

Remediation

The Connector makes the following API requests to manage tags on Azure resources when you use BlueXP remediation:

- Microsoft.Resources/resources/read
- Microsoft.Resources/subscriptions/operationresults/read
- Microsoft.Resources/subscriptions/resourceGroups/read
- Microsoft.Resources/subscriptions/resourcegroups/resources/read
- Microsoft.Resources/tags/read
- Microsoft.Resources/tags/write

Tiering

The Connector makes the following API requests when you set up BlueXP tiering.

- Microsoft.Storage/storageAccounts/listkeys/action
- Microsoft.Resources/subscriptions/resourceGroups/read
- Microsoft.Resources/subscriptions/locations/read

The Connector makes the following API requests for daily operations.

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

Change log

As permissions are added and removed, we'll note them in the sections below.

12 May, 2023

The following permissions were added to the JSON policy because they are required for Cloud Volumes ONTAP management:

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

The following permissions were removed from the JSON policy because they are no longer required:

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

23 March, 2023

The "Microsoft.Storage/storageAccounts/delete" permission is no longer needed for BlueXP classification.

This permission is still required for Cloud Volumes ONTAP.

5 January, 2023

The following permissions were added to the JSON policy:

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

These permissions are required for BlueXP backup and recovery.

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

This permission is required for Cloud Volumes ONTAP deployment.

Google Cloud permissions for the Connector

BlueXP requires permissions to perform actions in Google Cloud. These permissions are included in a custom role provided by NetApp. You might want to understand what BlueXP does with these permissions.

Service account permissions

The custom role shown below provides the permissions that a Connector needs to manage resources and processes within your Google Cloud network.

You'll need to apply this custom role to a service account that gets attached to the Connector VM.

- [Set up permissions for standard mode](#)
- [Set up permissions for restricted mode](#)
- [Set up permissions for private mode](#)

You also need to ensure that the role is up to date as new permissions are added in subsequent releases.

```
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

How Google Cloud permissions are used

| Actions | Purpose |
|---|---|
| <ul style="list-style-type: none"> - compute.disks.create - compute.disks.createSnapshot - compute.disks.delete - compute.disks.get - compute.disks.list - compute.disks.setLabels - compute.disks.use | To create and manage disks for Cloud Volumes ONTAP. |
| <ul style="list-style-type: none"> - compute.firewalls.create - compute.firewalls.delete - compute.firewalls.get - compute.firewalls.list | To create firewall rules for Cloud Volumes ONTAP. |
| <ul style="list-style-type: none"> - compute.globalOperations.get | To get the status of operations. |
| <ul style="list-style-type: none"> - compute.images.get - compute.images.getFromFamily - compute.images.list - compute.images.useReadOnly | To get images for VM instances. |

| Actions | Purpose |
|--|--|
| <ul style="list-style-type: none"> - compute.instances.attachDisk - compute.instances.detachDisk | To attach and detach disks to Cloud Volumes ONTAP. |
| <ul style="list-style-type: none"> - compute.instances.create - compute.instances.delete | To create and delete Cloud Volumes ONTAP VM instances. |
| <ul style="list-style-type: none"> - compute.instances.get | To list VM instances. |
| <ul style="list-style-type: none"> - compute.instances.getSerialPortOutput | To get console logs. |
| <ul style="list-style-type: none"> - compute.instances.list | To retrieve the list of instances in a zone. |
| <ul style="list-style-type: none"> - compute.instances.setDeletionProtection | To set deletion protection on the instance. |
| <ul style="list-style-type: none"> - compute.instances.setLabels | To add labels. |
| <ul style="list-style-type: none"> - compute.instances.setMachineType - compute.instances.setMinCpuPlatform | To change the machine type for Cloud Volumes ONTAP. |
| <ul style="list-style-type: none"> - compute.instances.setMetadata | To add metadata. |
| <ul style="list-style-type: none"> - compute.instances.setTags | To add tags for firewall rules. |
| <ul style="list-style-type: none"> - compute.instances.start - compute.instances.stop - compute.instances.updateDisplayDevice | To start and stop Cloud Volumes ONTAP. |
| <ul style="list-style-type: none"> - compute.machineTypes.get | To get the numbers of cores to check quotas. |
| <ul style="list-style-type: none"> - compute.projects.get | To support multi-projects. |
| <ul style="list-style-type: none"> - compute.snapshots.create - compute.snapshots.delete - compute.snapshots.get - compute.snapshots.list - compute.snapshots.setLabels | To create and manage persistent disk snapshots. |
| <ul style="list-style-type: none"> - 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 | To get the networking information needed to create a new Cloud Volumes ONTAP virtual machine instance. |

| Actions | Purpose |
|---|--|
| <ul style="list-style-type: none"> - 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 | To deploy the Cloud Volumes ONTAP virtual machine instance using Google Cloud Deployment Manager. |
| <ul style="list-style-type: none"> - logging.logEntries.list - logging.privateLogEntries.list | To get stack log drives. |
| <ul style="list-style-type: none"> - resourcemanager.projects.get | To support multi-projects. |
| <ul style="list-style-type: none"> - storage.buckets.create - storage.buckets.delete - storage.buckets.get - storage.buckets.list - storage.buckets.update | To create and manage a Google Cloud Storage bucket for data tiering. |
| <ul style="list-style-type: none"> - cloudkms.cryptoKeyVersions.useToEncrypt - cloudkms.cryptoKeys.get - cloudkms.cryptoKeys.list - cloudkms.keyRings.list | To use customer-managed encryption keys from the Cloud Key Management Service with Cloud Volumes ONTAP. |
| <ul style="list-style-type: none"> - compute.instances.setServiceAccount - iam.serviceAccounts.actAs - iam.serviceAccounts.getIamPolicy - iam.serviceAccounts.list - storage.objects.get - storage.objects.list | To set a service account on the Cloud Volumes ONTAP instance. This service account provides permissions for data tiering to a Google Cloud Storage bucket. |
| <ul style="list-style-type: none"> - compute.addresses.list | To retrieve the addresses in a region when deploying an HA pair. |
| <ul style="list-style-type: none"> - compute.backendServices.create - compute.regionBackendServices.create - compute.regionBackendServices.get - compute.regionBackendServices.list | To configure a backend service for distributing traffic in an HA pair. |
| <ul style="list-style-type: none"> - compute.networks.updatePolicy | To apply firewall rules on the VPCs and subnets for an HA pair. |
| <ul style="list-style-type: none"> - compute.subnetworks.use - compute.subnetworks.useExternalIp - compute.instances.addAccessConfig | To enable BlueXP classification. |

| Actions | Purpose |
|--|---|
| <ul style="list-style-type: none"> - container.clusters.get - container.clusters.list | To discover Kubernetes clusters running in Google Kubernetes Engine. |
| <ul style="list-style-type: none"> - compute.instanceGroups.get - compute.addresses.get - compute.instances.updateNetworkInterface | To create and manage storage VMs on Cloud Volumes ONTAP HA pairs. |
| <ul style="list-style-type: none"> - monitoring.timeSeries.list - storage.buckets.getIamPolicy | To discover information about Google Cloud Storage buckets. |
| <ul style="list-style-type: none"> - cloudkms.cryptoKeys.get - cloudkms.cryptoKeys.getIamPolicy - cloudkms.cryptoKeys.list - cloudkms.cryptoKeys.setIamPolicy - cloudkms.keyRings.get - cloudkms.keyRings.getIamPolicy - cloudkms.keyRings.list - cloudkms.keyRings.setIamPolicy | To select your own customer-managed keys in the BlueXP backup and recovery activation wizard instead of using the default Google-managed encryption keys. |

Change log

As permissions are added and removed, we'll note them in the sections below.

6 February, 2023

The following permission was added to this policy:

- compute.instances.updateNetworkInterface

This permission is required for Cloud Volumes ONTAP.

27 January, 2023

The following permissions were added to the policy:

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

These permissions are required for BlueXP backup and recovery.

Ports

Security group rules in AWS

The AWS security group for the Connector requires both inbound and outbound rules. BlueXP automatically creates this security group when you create a Connector from BlueXP. You need to set up this security group for all other installation options.

Inbound rules

| Protocol | Port | Purpose |
|----------|------------|--|
| SSH | 22 | Provides SSH access to the Connector host |
| HTTP | 80 | Provides HTTP access from client web browsers to the local user interface |
| HTTPS | 443 | Provides HTTPS access from client web browsers to the local user interface, and connections from the BlueXP classification instance |
| TCP | 3128 | Provides Cloud Volumes ONTAP with internet access to send AutoSupport messages to NetApp Support. You must manually open this port after deployment. Learn how the Connector is used as a proxy for AutoSupport messages |
| TCP | 9060, 9061 | Provides the ability to enable and use BlueXP classification and BlueXP backup and recovery in Government regions. |

Outbound rules

The predefined security group for the Connector opens all outbound traffic. If that is acceptable, follow the basic outbound rules. If you need more rigid rules, use the advanced outbound rules.

Basic outbound rules

The predefined security group for the Connector includes the following outbound rules.

| Protocol | Port | Purpose |
|----------|------|----------------------|
| All TCP | All | All outbound traffic |
| All UDP | All | All outbound traffic |

Advanced outbound rules

If you need rigid rules for outbound traffic, you can use the following information to open only those ports that are required for outbound communication by the Connector.



The source IP address is the Connector host.

| Service | Protocol | Port | Destination | Purpose |
|---------------------------|----------|------|--|---|
| API calls and AutoSupport | HTTPS | 443 | Outbound internet and ONTAP cluster management LIF | API calls to AWS, to ONTAP, to BlueXP classification, to BlueXP ransomware protection, and sending AutoSupport messages to NetApp |
| API calls | TCP | 3000 | ONTAP HA mediator | Communication with the ONTAP HA mediator |
| | TCP | 8080 | BlueXP classification | Probe to BlueXP classification instance during deployment |
| DNS | UDP | 53 | DNS | Used for DNS resolve by BlueXP |

Security group rules in Azure

The Azure security group for the Connector requires both inbound and outbound rules. BlueXP automatically creates this security group when you create a Connector from BlueXP. You need to set up this security group for all other installation options.

Inbound rules

| Protocol | Port | Purpose |
|----------|------------|--|
| SSH | 22 | Provides SSH access to the Connector host |
| HTTP | 80 | Provides HTTP access from client web browsers to the local user interface |
| HTTPS | 443 | Provides HTTPS access from client web browsers to the local user interface, and connections from the BlueXP classification instance |
| TCP | 3128 | Provides Cloud Volumes ONTAP with internet access to send AutoSupport messages to NetApp Support. You must manually open this port after deployment. Learn how the Connector is used as a proxy for AutoSupport messages |
| TCP | 9060, 9061 | Provides the ability to enable and use BlueXP classification and BlueXP backup and recovery in Government regions. |

Outbound rules

The predefined security group for the Connector opens all outbound traffic. If that is acceptable, follow the basic outbound rules. If you need more rigid rules, use the advanced outbound rules.

Basic outbound rules

The predefined security group for the Connector includes the following outbound rules.

| Protocol | Port | Purpose |
|----------|------|----------------------|
| All TCP | All | All outbound traffic |
| All UDP | All | All outbound traffic |

Advanced outbound rules

If you need rigid rules for outbound traffic, you can use the following information to open only those ports that are required for outbound communication by the Connector.



The source IP address is the Connector host.

| Service | Protocol | Port | Destination | Purpose |
|---------------------------|----------|------|--|---|
| API calls and AutoSupport | HTTPS | 443 | Outbound internet and ONTAP cluster management LIF | API calls to Azure, to ONTAP, to BlueXP classification, to BlueXP ransomware protection, and sending AutoSupport messages to NetApp |

| Service | Protocol | Port | Destination | Purpose |
|-----------|----------|------|-----------------------|---|
| API calls | TCP | 8080 | BlueXP classification | Probe to BlueXP classification instance during deployment |
| DNS | UDP | 53 | DNS | Used for DNS resolve by BlueXP |

Firewall rules in Google Cloud

The Google Cloud firewall rules for the Connector requires both inbound and outbound rules. BlueXP automatically creates this security group when you create a Connector from BlueXP. You need to set up this security group for all other installation options.

Inbound rules

| Protocol | Port | Purpose |
|----------|------|--|
| SSH | 22 | Provides SSH access to the Connector host |
| HTTP | 80 | Provides HTTP access from client web browsers to the local user interface |
| HTTPS | 443 | Provides HTTPS access from client web browsers to the local user interface |
| TCP | 3128 | Provides Cloud Volumes ONTAP with internet access to send AutoSupport messages to NetApp Support. You must manually open this port after deployment. Learn how the Connector is used as a proxy for AutoSupport messages |

Outbound rules

The predefined firewall rules for the Connector opens all outbound traffic. If that is acceptable, follow the basic outbound rules. If you need more rigid rules, use the advanced outbound rules.

Basic outbound rules

The predefined firewall rules for the Connector includes the following outbound rules.

| Protocol | Port | Purpose |
|----------|------|----------------------|
| All TCP | All | All outbound traffic |
| All UDP | All | All outbound traffic |

Advanced outbound rules

If you need rigid rules for outbound traffic, you can use the following information to open only those ports that are required for outbound communication by the Connector.



The source IP address is the Connector host.

| Service | Protocol | Port | Destination | Purpose |
|---------------------------|----------|------|--|--|
| API calls and AutoSupport | HTTPS | 443 | Outbound internet and ONTAP cluster management LIF | API calls to Google Cloud, to ONTAP, to BlueXP classification, to BlueXP ransomware protection, and sending AutoSupport messages to NetApp |
| API calls | TCP | 8080 | BlueXP classification | Probe to BlueXP classification instance during deployment |
| DNS | UDP | 53 | DNS | Used for DNS resolve by BlueXP |

Ports for the on-prem Connector

The Connector uses *inbound* ports when installed manually on an on-premises Linux host. You might need to refer to these ports for planning purposes.

These inbound rules apply to all BlueXP deployment models.

| Protocol | Port | Purpose |
|----------|------|--|
| HTTP | 80 | Provides HTTP access from client web browsers to the local user interface |
| HTTPS | 443 | Provides HTTPS access from client web browsers to the local user interface |

Copyright information

Copyright © 2023 NetApp, Inc. All Rights Reserved. Printed in the U.S. No part of this document covered by copyright may be reproduced in any form or by any means—graphic, electronic, or mechanical, including photocopying, recording, taping, or storage in an electronic retrieval system—without prior written permission of the copyright owner.

Software derived from copyrighted NetApp material is subject to the following license and disclaimer:

THIS SOFTWARE IS PROVIDED BY NETAPP “AS IS” AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, WHICH ARE HEREBY DISCLAIMED. IN NO EVENT SHALL NETAPP BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

NetApp reserves the right to change any products described herein at any time, and without notice. NetApp assumes no responsibility or liability arising from the use of products described herein, except as expressly agreed to in writing by NetApp. The use or purchase of this product does not convey a license under any patent rights, trademark rights, or any other intellectual property rights of NetApp.

The product described in this manual may be protected by one or more U.S. patents, foreign patents, or pending applications.

LIMITED RIGHTS LEGEND: Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (b)(3) of the Rights in Technical Data -Noncommercial Items at DFARS 252.227-7013 (FEB 2014) and FAR 52.227-19 (DEC 2007).

Data contained herein pertains to a commercial product and/or commercial service (as defined in FAR 2.101) and is proprietary to NetApp, Inc. All NetApp technical data and computer software provided under this Agreement is commercial in nature and developed solely at private expense. The U.S. Government has a non-exclusive, non-transferrable, nonsublicensable, worldwide, limited irrevocable license to use the Data only in connection with and in support of the U.S. Government contract under which the Data was delivered. Except as provided herein, the Data may not be used, disclosed, reproduced, modified, performed, or displayed without the prior written approval of NetApp, Inc. United States Government license rights for the Department of Defense are limited to those rights identified in DFARS clause 252.227-7015(b) (FEB 2014).

Trademark information

NETAPP, the NETAPP logo, and the marks listed at <http://www.netapp.com/TM> are trademarks of NetApp, Inc. Other company and product names may be trademarks of their respective owners.