Reference

NetApp Console setup and administration

NetApp
January 27, 2026

Table of Contents

Reference

Agent maintenance console

Agent validation with the maintenance console

You can use the Console agent maintenance console to validate the installation and configuration of a Console agent.

Access the agent maintenance console

You can access the maintenance Console from the Console agent host. Navigate to the following directory:

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

config-checker validate

The `config-checker validate` command allows you to validate the configuration of a Console agent.

Parameters

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

Choose one or more services to validate. Valid service names are:
*`PLATFORM` which validates network connectivity to required Console endpoints.

`--validationTypes <comma-separated list validation types to run>` **--REQUIRED--**
Choose from one or more validation types to run. Valid validation types are:
* `NETWORK` which validates network connectivity to required Console endpoints.

`--proxy <url>` **--OPTIONAL--**

Specifies the proxy server URL to use for the validation. Required if your agent is configured to use a proxy server.

`--certs <paths>` **--OPTIONAL--**

Specifies the path to one or more certificate files to use for the validation. The certificate files must be in PEM format. Separate multiple paths with commas. This parameter is required if your agent uses a custom certificate.

Config-checker validate examples

Basic validation:

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

Validation where a proxy server is used for the agent:

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

Validation where a certificate is used for the agent:

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

View help for any command

To view help for any command, append `--help` to the command. For example, to view help for the `proxy add` command, use the following command:

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

Transparent proxy commands

You can use the Console agent maintenance console to configure a Console agent to use a transparent proxy server.

Access the agent maintenance console

You can access the maintenance Console from the Console agent host. Navigate to the following directory:

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

View help for any command

To view help for any command, append `--help` to the command. For example, to view help for the `proxy add` command, use the following command:

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

proxy get

The `proxy get` command displays information about the current transparent proxy server configuration. To view the current transparent proxy server configuration, use the following command:

Proxy get example

To view the current transparent proxy server configuration, use the following command:

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

proxy add

The `proxy add` command configures the agent to use a transparent proxy server.

Parameters

`-c <certificate file>`

Specifies the path to the certificate file for the proxy server. The certificate file must be in PEM format. Ensure that the certificate file is in the same directory as the command or specify the full path to the certificate file.

Proxy add example

To add a transparent proxy server, use the following command, where `/home/ubuntu/myCA1.pem` is the path to the certificate file for the proxy server. The certificate file must be in PEM format:

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

proxy update

The `proxy update` command allows you to update the certificate of a transparent proxy.

Parameters

`-c <certificate file>` specifies the path to the certificate file for the proxy server. The certificate file must be in PEM format.

Ensure that the certificate file is in the same directory as the command or specify the full path to the certificate file.

Proxy update example

To update the certificate for a transparent proxy server, use the following command, where `/home/ubuntu/myCA1.pem` is the path to the new certificate file for the proxy server. The certificate file must be in PEM format:

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

proxy remove

The `proxy remove` command removes the transparent proxy server configuration from the agent.

Proxy remove example

To remove transparent proxy server, use the following command:

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

Cloud Provider agent permissions and network requirements

Permissions summary for NetApp Console

You'll need to provide the Console agent appropriate permissions so that it 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

The NetApp Console requires AWS permissions for a Console agent and for individual services.

Console agents

Goal	Description	Link
Deploy a Console agent from the Console To deploy a Console agent in AWS, the user needs specific permissions.	Set up AWS permissions	Provide permissions for a Console agent

NetApp Backup and Recovery

Goal	Description	Link
Back up on-premises ONTAP clusters to Amazon S3 with NetApp Backup and Recovery	When activating backups on your ONTAP volumes, NetApp 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

Cloud Volumes ONTAP

Goal	Description	Link
Provide permissions for Cloud Volumes ONTAP nodes	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 the Console create the IAM roles for you, but you can use your own when creating the system in the Console.	Learn how to set up the IAM roles yourself

NetApp Copy and Sync

Goal	Description	Link
Deploy the data broker in AWS	The AWS user account you use to deploy the data broker must have the needed permissions.	Permissions required to deploy the data broker in AWS
Provide permissions for the data broker	When NetApp Copy and Sync deploys the data broker, it creates an IAM role for the data broker instance. You can deploy the data broker using your own IAM role, if you prefer.	Requirements to use your own IAM role with the AWS data broker
Enable AWS access for a manually installed data broker	If you use the data broker with a sync relationship that includes an S3 bucket, then you should prepare the Linux host for AWS access. When you install the data broker, you'll need to provide AWS keys for an IAM user that has programmatic access and specific permissions.	Enabling access to AWS

FSx for ONTAP

Goal	Description	Link
Create and manage FSx for ONTAP	To create or manage an Amazon FSx for NetApp ONTAP system, you need to add AWS credentials to the Console by providing the ARN of an IAM role that gives the Console the permissions needed.	Learn how to set up AWS credentials for FSx

NetApp Cloud Tiering

Goal	Description	Link
Tier on-premises ONTAP clusters to Amazon S3	When you enable NetApp Cloud Tiering to AWS, you 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

The Console requires Azure permissions for a Console agent and for individual services.

Console agent

Goal	Description	Link
Deploy a Console agent from the Console	When you deploy a Console agent from the Console, you need to use an Azure account or service principal that has permissions to deploy a Console agent VM in Azure.	Set up Azure permissions

Goal	Description	Link
Provide permissions for a Console agent	When the Console deploys a Console agent VM in Azure, it creates a custom role that provides the permissions required to manage resources and processes within that Azure subscription. You need to set up the custom role yourself if you launch a Console agent from the marketplace, if you manually install a Console agent, or if you add more Azure credentials to a Console agent. Keep the policy up to date as new permissions are added in later releases.	Azure permissions for a Console agent

NetApp Backup and Recovery

Goal	Description	Link
Back up Cloud Volumes ONTAP to Azure blob storage	When using NetApp Backup and Recovery to back up Cloud Volumes ONTAP, you need to add permissions to a Console agent in the following scenarios: • You want to use "Search & Restore" functionality • You want to use customer-managed encryption keys (CMEK)	• Back up Cloud Volumes ONTAP data to Azure Blob storage with Backup and Recovery
Back up on-premises ONTAP clusters to Azure blob storage	When using NetApp Backup and Recovery to back up on-premises ONTAP clusters, you need to add permissions to a Console agent to use the "Search & Restore" functionality.	Back up on-premises ONTAP data to Azure Blob storage with Backup and Recovery

NetApp Copy and sync

Goal	Description	Link
Deploy the data broker in Azure	The Azure user account that you use to deploy the data broker must have the required permissions.	Permissions required to deploy the data broker in Azure

Google Cloud permissions

The Console requires Google Cloud permissions for a Console agent and for individual services.

Console agents

Goal	Description	Link
Deploy a Console agent from the Console	The Google Cloud user who deploys a Console agent from the Console needs specific permissions to deploy a Console agent in Google Cloud.	Set up permissions to create a Console agent

Goal	Description	Link
Provide permissions for a Console agent	The service account for a Console agent must have specific permissions for day-to-day operations. You need to associate the service account with a Console agent during deployment. Keep the policy up to date as new permissions are added in later releases.	Set up permissions for a Console agent

NetApp Backup and Recovery

Goal	Description	Link
Back up Cloud Volumes ONTAP to Google Cloud	When using NetApp Backup and Recovery to back up Cloud Volumes ONTAP, you need to add permissions to a Console agent in the following scenarios: • You want to use "Search & Restore" functionality • You want to use customer-managed encryption keys (CMEK)	• Back up Cloud Volumes ONTAP data to Google Cloud Storage with Backup and Recovery • Permissions for CMEKs
Back up on-premises ONTAP clusters to Google Cloud	When using NetApp Backup and Recovery to back up on-premises ONTAP clusters, you need to add permissions to a Console agent to use the "Search & Restore" functionality.	Back up on-premises ONTAP data to Google Cloud Storage with Backup and Recovery

NetApp Copy and Sync

Goal	Description	Link
Deploy the data broker in Google Cloud	Ensure that the Google Cloud user who deploys the data broker has the required permissions.	Permissions required to deploy the data broker in Google Cloud
Enable Google Cloud access for a manually installed data broker	If you plan to use the data broker with a sync relationship that includes a Google Cloud Storage bucket, then you should prepare the Linux host for Google Cloud access. When you install the data broker, you'll need to provide a key for a service account that has specific permissions.	Enabling access to Google Cloud

StorageGRID permissions

The Console requires StorageGRID permissions for two services.

NetApp Backup and Recovery

Goal	Description	Link
Back up on-premises ONTAP clusters to StorageGRID	When you prepare StorageGRID as a backup target for ONTAP clusters, NetApp 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

NetApp Cloud Tiering

Goal	Description	Link
Tier on-premises ONTAP clusters to StorageGRID	When you set up NetApp Cloud Tiering to StorageGRID, you need to provide Cloud Tiering with an S3 access key and secret key. Cloud tiering uses the keys to access your buckets.	Prepare tiering to StorageGRID

AWS agent permissions and security rules

AWS permissions for the Console agent

When the NetApp Console launches a Console agent in AWS, it attaches a policy to the agent that provides the agent with permissions to manage resources and processes within that AWS account. The agent 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 Console agent needs to manage resources and processes within your public cloud environment based on your AWS region.

Note the following:

- If you create a Console agent in a standard AWS region directly from the Console, the Console automatically applies policies to the agent.
- You need to set up the policies yourself if you deploy the agent from the AWS Marketplace, if you manually install the agent on a Linux host, or if you want to add additional AWS credentials to the Console.
- In either case, you need to ensure that the policies are up to date as new permissions are added in subsequent releases. If new permissions are required, they will be listed in the release notes.
- 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 an AWS Marketplace deployment
  - Set up permissions for on-premises deployments
  - Set up permissions for restricted 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.

Policy #1

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

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

```
        "s3:GetEncryptionConfiguration",
        "kms:ReEncrypt*",
        "kms:CreateGrant",
        "fsx:Describe*",
        "fsx:List*",
        "kms:GenerateDataKeyWithoutPlaintext"
      ],
      "Resource": "*",
      "Effect": "Allow",
      "Sid": "cvoServicePolicy"
    },
    {
      "Action": [
        "ec2:StartInstances",
        "ec2:StopInstances",
        "ec2:DescribeInstances",
        "ec2:DescribeInstanceStatus",
        "ec2:RunInstances",
        "ec2:TerminateInstances",
        "ec2:DescribeInstanceAttribute",
        "ec2:DescribeImages",
        "ec2:CreateTags",
        "ec2:CreateVolume",
        "ec2:CreateSecurityGroup",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:DescribeRegions",
        "cloudformation:CreateStack",
        "cloudformation:DeleteStack",
        "cloudformation:DescribeStacks",
        "ec2:DescribeVpcEndpoints",
        "kms:ListAliases",
        "glue:GetDatabase",
        "glue:GetTable",
        "glue:GetPartitions"
      ],
      "Resource": "*",
      "Effect": "Allow",
      "Sid": "backupPolicy"
    },
    {
      "Action": [
        "s3:GetBucketLocation",
        "s3:ListAllMyBuckets",
        "s3:ListBucket",
        "s3:CreateBucket",
```

```
        "s3:GetLifecycleConfiguration",
        "s3:PutLifecycleConfiguration",
        "s3:PutBucketTagging",
        "s3:ListBucketVersions",
        "s3:GetBucketAcl",
        "s3:PutBucketPublicAccessBlock",
        "s3:GetObject",
        "s3:PutEncryptionConfiguration",
        "s3:DeleteObject",
        "s3:DeleteObjectVersion",
        "s3:ListBucketMultipartUploads",
        "s3:PutObject",
        "s3:PutBucketAcl",
        "s3:AbortMultipartUpload",
        "s3:ListMultipartUploadParts",
        "s3:DeleteBucket",
        "s3:GetObjectVersionTagging",
        "s3:GetObjectVersionAcl",
        "s3:GetObjectRetention",
        "s3:GetObjectTagging",
        "s3:GetObjectVersion",
        "s3:PutObjectVersionTagging",
        "s3:PutObjectRetention",
        "s3:DeleteObjectTagging",
        "s3:DeleteObjectVersionTagging",
        "s3:GetBucketObjectLockConfiguration",
        "s3:GetBucketVersioning",
        "s3:PutBucketObjectLockConfiguration",
        "s3:PutBucketVersioning",
        "s3:BypassGovernanceRetention",
        "s3:PutBucketPolicy",
        "s3:PutBucketOwnershipControls"
      ],
      "Resource": [
        "arn:aws:s3:::netapp-backup-*"
      ],
      "Effect": "Allow",
      "Sid": "backupS3Policy"
    },
    {
      "Action": [
        "s3:CreateBucket",
        "s3:GetLifecycleConfiguration",
        "s3:PutLifecycleConfiguration",
        "s3:PutBucketTagging",
        "s3:ListBucketVersions",
```

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

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

Policy #2

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": [
        "ec2:CreateTags",
        "ec2:DeleteTags",
        "ec2:DescribeTags",
        "tag:getResources",
        "tag:getTagKeys",
        "tag:getTagValues",
        "tag:TagResources",
        "tag:UntagResources"
      ],
      "Resource": "*",
      "Effect": "Allow",
      "Sid": "tagServicePolicy"
    }
  ]
}
```

GovCloud (US) regions

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

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

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

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

Secret regions

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "ec2:DescribeInstances",
        "ec2:DescribeInstanceStatus",
        "ec2:RunInstances",
        "ec2:ModifyInstanceAttribute",
        "ec2:DescribeRouteTables",
        "ec2:DescribeImages",
        "ec2:CreateTags",
        "ec2:CreateVolume",
        "ec2:DescribeVolumes",
        "ec2:ModifyVolumeAttribute",
        "ec2:DeleteVolume",
        "ec2:CreateSecurityGroup",
        "ec2:DeleteSecurityGroup",
        "ec2:DescribeSecurityGroups",
        "ec2:RevokeSecurityGroupEgress",
        "ec2:RevokeSecurityGroupIngress",
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:CreateNetworkInterface",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DeleteNetworkInterface",
        "ec2:ModifyNetworkInterfaceAttribute",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:DescribeDhcpOptions",
        "ec2:CreateSnapshot",
        "ec2:DeleteSnapshot",
        "ec2:DescribeSnapshots",
        "ec2:GetConsoleOutput",
        "ec2:DescribeKeyPairs",
        "ec2:DescribeRegions",
        "ec2:DeleteTags",
        "ec2:DescribeTags",
        "cloudformation:CreateStack",
        "cloudformation:DeleteStack",
        "cloudformation:DescribeStacks",
        "cloudformation:DescribeStackEvents",
        "cloudformation:ValidateTemplate",
```

```
        "iam:PassRole",
        "iam:CreateRole",
        "iam:DeleteRole",
        "iam:PutRolePolicy",
        "iam:CreateInstanceProfile",
        "iam:DeleteRolePolicy",
        "iam:AddRoleToInstanceProfile",
        "iam:RemoveRoleFromInstanceProfile",
        "iam:DeleteInstanceProfile",
        "s3:GetObject",
        "s3:ListBucket",
        "s3:GetBucketTagging",
        "s3:GetBucketLocation",
        "s3:ListAllMyBuckets",
        "ec2:AssociateIamInstanceProfile",
        "ec2:DescribeIamInstanceProfileAssociations",
        "ec2:DisassociateIamInstanceProfile",
        "ec2:DescribeInstanceAttribute",
        "ec2:CreatePlacementGroup",
        "ec2:DeletePlacementGroup",
        "iam:ListinstanceProfiles"
      ],
      "Resource": "*"
    },
    {
      "Sid": "fabricPoolPolicy",
      "Effect": "Allow",
      "Action": [
        "s3:DeleteBucket",
        "s3:GetLifecycleConfiguration",
        "s3:PutLifecycleConfiguration",
        "s3:PutBucketTagging",
        "s3:ListBucketVersions"
      ],
      "Resource": [
        "arn:aws-iso-b:s3:::fabric-pool*"
      ]
    },
    {
      "Effect": "Allow",
      "Action": [
        "ec2:StartInstances",
        "ec2:StopInstances",
        "ec2:TerminateInstances",
        "ec2:AttachVolume",
        "ec2:DetachVolume"
```

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

Top Secret regions

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "ec2:DescribeInstances",
        "ec2:DescribeInstanceStatus",
        "ec2:RunInstances",
        "ec2:ModifyInstanceAttribute",
        "ec2:DescribeRouteTables",
        "ec2:DescribeImages",
        "ec2:CreateTags",
        "ec2:CreateVolume",
        "ec2:DescribeVolumes",
        "ec2:ModifyVolumeAttribute",
        "ec2:DeleteVolume",
        "ec2:CreateSecurityGroup",
        "ec2:DeleteSecurityGroup",
        "ec2:DescribeSecurityGroups",
        "ec2:RevokeSecurityGroupEgress",
        "ec2:RevokeSecurityGroupIngress",
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:CreateNetworkInterface",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DeleteNetworkInterface",
        "ec2:ModifyNetworkInterfaceAttribute",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:DescribeDhcpOptions",
        "ec2:CreateSnapshot",
        "ec2:DeleteSnapshot",
        "ec2:DescribeSnapshots",
        "ec2:GetConsoleOutput",
        "ec2:DescribeKeyPairs",
        "ec2:DescribeRegions",
        "ec2:DeleteTags",
        "ec2:DescribeTags",
        "cloudformation:CreateStack",
        "cloudformation:DeleteStack",
        "cloudformation:DescribeStacks",
        "cloudformation:DescribeStackEvents",
        "cloudformation:ValidateTemplate",
```

```
        "iam:PassRole",
        "iam:CreateRole",
        "iam:DeleteRole",
        "iam:PutRolePolicy",
        "iam:CreateInstanceProfile",
        "iam:DeleteRolePolicy",
        "iam:AddRoleToInstanceProfile",
        "iam:RemoveRoleFromInstanceProfile",
        "iam:DeleteInstanceProfile",
        "s3:GetObject",
        "s3:ListBucket",
        "s3:GetBucketTagging",
        "s3:GetBucketLocation",
        "s3:ListAllMyBuckets",
        "ec2:AssociateIamInstanceProfile",
        "ec2:DescribeIamInstanceProfileAssociations",
        "ec2:DisassociateIamInstanceProfile",
        "ec2:DescribeInstanceAttribute",
        "ec2:CreatePlacementGroup",
        "ec2:DeletePlacementGroup",
        "iam:ListinstanceProfiles"
      ],
      "Resource": "*"
    },
    {
      "Sid": "fabricPoolPolicy",
      "Effect": "Allow",
      "Action": [
        "s3:DeleteBucket",
        "s3:GetLifecycleConfiguration",
        "s3:PutLifecycleConfiguration",
        "s3:PutBucketTagging",
        "s3:ListBucketVersions"
      ],
      "Resource": [
        "arn:aws-iso:s3:::fabric-pool*"
      ]
    },
    {
      "Effect": "Allow",
      "Action": [
        "ec2:StartInstances",
        "ec2:StopInstances",
        "ec2:TerminateInstances",
        "ec2:AttachVolume",
        "ec2:DetachVolume"
```

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

How the AWS permissions are used

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

Amazon FSx for ONTAP

The Console agent makes the following API requests to manage an Amazon FSx for ONTAP file system:

- 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:CreateGrant
- kms:ListAliases
- fsx:Describe*
- fsx:List*

Amazon S3 bucket discovery

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

s3:GetEncryptionConfiguration

NetApp Backup and Recovery

The agent 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
- s3:GetObject
- ec2:DescribeVpcEndpoints
- kms:ListAliases
- s3:PutEncryptionConfiguration

The agent 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

The agent makes the following API requests when you use DataLock and NetApp Ransomware Resilience 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 agent 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

Legacy permissions for Backup and Recovery

You only need the following permissions if you enabled legacy indexing features before the release of indexing v2:

- kms:List*
- kms:Describe*
- athena:StartQueryExecution
- athena:GetQueryResults
- athena:GetQueryExecution
- athena:StopQueryExecution
- glue:CreateDatabase
- glue:CreateTable
- glue:BatchDeletePartition

Classification

The agent makes the following API requests to deploy NetApp Data Classification:

- 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 agent makes the following API requests to scan S3 buckets when you use NetApp Data 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 agent 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 backend 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:ReEncrypt*	Yes	No	No
	kms:CreateGrant	Yes	Yes	No
	kms:GenerateDataKeyWithoutPlaintext	Yes	Yes	No
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

Purpose	Action	Used for deployment?	Used for daily operations?	Used for deletion?
Create and manage aggregates that support the Amazon EBS Elastic Volumes feature	ec2:DescribeVolumesModifications	No	Yes	No
	ec2:ModifyVolume	No	Yes	No
Check whether the Availability Zone is an AWS Local Zone and validates that all deployment parameters are compatible	ec2:DescribeAvailabilityZones	Yes	No	Yes

Change log

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

11 November 2025

The following permissions are no longer required for NetApp Backup and Recovery unless you use legacy indexing. These permissions have been removed from the policies on this page:

- kms:List*
- kms:Describe*
- athena:StartQueryExecution
- athena:GetQueryResults
- athena:GetQueryExecution
- athena:StopQueryExecution
- glue:CreateDatabase
- glue:CreateTable
- glue:BatchDeletePartition

9 September 2024

Permissions were removed from policy #2 for standard regions because the NetApp Console no longer supports NetApp edge caching and discovery and management of Kubernetes clusters.

View the permissions that were removed from the policy

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

9 May 2024

The following permission is now required for Cloud Volumes ONTAP:

ec2:DescribeAvailabilityZones

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 NetApp Cloud Tiering:

ec2:DescribeVpcEndpoints

Console agent security group rules in AWS

The AWS security group for the agent requires both inbound and outbound rules. The NetApp Console automatically creates this security group when you create a Console agent from the Console. 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 agent host
HTTP	80	• Provides HTTP access from client web browsers to the local user interface • Used during the Cloud Volumes ONTAP upgrade process
HTTPS	443	Provides HTTPS access to the local user interface and connections from the NetApp Data Classification instance
TCP	3128	Provides Cloud Volumes ONTAP with internet access. You must manually open this port after deployment.

Outbound rules

The predefined security group for the agent 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 agent 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 agent

The source IP address is the agent 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 NetApp Data Classification, and sending AutoSupport messages to NetApp
API calls	TCP	3000	ONTAP HA mediator	Communication with the ONTAP HA mediator
	TCP	8080	Data Classification	Probe to Data Classification instance during deployment
DNS	UDP	53	DNS	Used for DNS resolve by the Console

Azure permissions and required security rules

Azure permissions for the Console agent

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

Whether or not you need to create this custom role for the agent depends on how you deployed it.

Deploying from NetApp Console

When you use the Console to deploy the agent virtual machine in Azure, it enables a system-assigned managed identity on the virtual machine, creates a custom role, and assigns it to the virtual machine. The role provides the Console with the permissions required to manage resources and processes within that Azure subscription. The role's permissions are kept up-to-date when the agent is upgraded. You don't need to create this role for the agent or manage updates.

Deploying manually or from Azure marketplace

When you deploy the agent from the Azure Marketplace or if you manually install the agent on a Linux host, then you need to set up the custom role yourself and maintain its permissions with any changes.

You'll need to ensure that the role is up to date as new permissions are added in subsequent releases. If new permissions are required, they will be listed in the release notes.

- To view step-by-step instructions for using these policies, refer to the following pages:
  - Set up permissions for an Azure Marketplace deployment
  - Set up permissions for on-premises deployments
  - Set up permissions for restricted mode

```
{
  "Name": "Console Operator",
  "Actions": [
    "Microsoft.Compute/disks/delete",
    "Microsoft.Compute/disks/read",
    "Microsoft.Compute/disks/write",
    "Microsoft.Compute/locations/operations/read",
    "Microsoft.Compute/locations/vmSizes/read",
    "Microsoft.Resources/subscriptions/locations/read",
    "Microsoft.Compute/operations/read",
    "Microsoft.Compute/virtualMachines/instanceView/read",
    "Microsoft.Compute/virtualMachines/powerOff/action",
    "Microsoft.Compute/virtualMachines/read",
    "Microsoft.Compute/virtualMachines/restart/action",
    "Microsoft.Compute/virtualMachines/deallocate/action",
    "Microsoft.Compute/virtualMachines/start/action",
    "Microsoft.Compute/virtualMachines/vmSizes/read",
    "Microsoft.Compute/virtualMachines/write",
    "Microsoft.Compute/images/read",
    "Microsoft.Network/locations/operationResults/read",
    "Microsoft.Network/locations/operations/read",
    "Microsoft.Network/networkInterfaces/read",
    "Microsoft.Network/networkInterfaces/write",
    "Microsoft.Network/networkInterfaces/join/action",
    "Microsoft.Network/networkSecurityGroups/read",
    "Microsoft.Network/networkSecurityGroups/write",
    "Microsoft.Network/networkSecurityGroups/join/action",
    "Microsoft.Network/virtualNetworks/read",
    "Microsoft.Network/virtualNetworks/checkIpAddressAvailability/read",
    "Microsoft.Network/virtualNetworks/subnets/read",
    "Microsoft.Network/virtualNetworks/subnets/write",
    "Microsoft.Network/virtualNetworks/subnets/virtualMachines/read",
    "Microsoft.Network/virtualNetworks/virtualMachines/read",
    "Microsoft.Network/virtualNetworks/subnets/join/action",
    "Microsoft.Resources/deployments/operations/read",
    "Microsoft.Resources/deployments/read",
    "Microsoft.Resources/deployments/write",
    "Microsoft.Resources/resources/read",
    "Microsoft.Resources/subscriptions/operationresults/read",
    "Microsoft.Resources/subscriptions/resourceGroups/delete",
    "Microsoft.Resources/subscriptions/resourceGroups/read",
    "Microsoft.Resources/subscriptions/resourcegroups/resources/read",
    "Microsoft.Resources/subscriptions/resourceGroups/write",
    "Microsoft.Storage/checknameavailability/read",
    "Microsoft.Storage/operations/read",
    "Microsoft.Storage/storageAccounts/listkeys/action",
```

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

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

    "Microsoft.MarketplaceOrdering/offertypes/publishers/offers/plans/agreemen
    ts/write",
        "Microsoft.Network/loadBalancers/read",
        "Microsoft.Network/loadBalancers/write",
        "Microsoft.Network/loadBalancers/delete",
        "Microsoft.Network/loadBalancers/backendAddressPools/read",
        "Microsoft.Network/loadBalancers/backendAddressPools/join/action",
        "Microsoft.Network/loadBalancers/loadBalancingRules/read",
        "Microsoft.Network/loadBalancers/probes/read",
        "Microsoft.Network/loadBalancers/probes/join/action",
        "Microsoft.Authorization/locks/*",
        "Microsoft.Network/routeTables/join/action",
        "Microsoft.NetApp/netAppAccounts/read",
        "Microsoft.NetApp/netAppAccounts/capacityPools/read",
        "Microsoft.NetApp/netAppAccounts/capacityPools/volumes/write",
        "Microsoft.NetApp/netAppAccounts/capacityPools/volumes/read",
        "Microsoft.NetApp/netAppAccounts/capacityPools/volumes/delete",
        "Microsoft.Network/privateEndpoints/write",

    "Microsoft.Storage/storageAccounts/PrivateEndpointConnectionsApproval/acti
    on",
        "Microsoft.Storage/storageAccounts/privateEndpointConnections/read",
        "Microsoft.Storage/storageAccounts/managementPolicies/read",
        "Microsoft.Storage/storageAccounts/managementPolicies/write",
        "Microsoft.Network/privateEndpoints/read",
        "Microsoft.Network/privateDnsZones/write",
        "Microsoft.Network/privateDnsZones/virtualNetworkLinks/write",
        "Microsoft.Network/virtualNetworks/join/action",
        "Microsoft.Network/privateDnsZones/A/write",
        "Microsoft.Network/privateDnsZones/read",
        "Microsoft.Network/privateDnsZones/virtualNetworkLinks/read",
```

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

"Microsoft.Network/applicationSecurityGroups/joinIpConfiguration/action",
    "Microsoft.Network/networkSecurityGroups/securityRules/write",
    "Microsoft.Network/applicationSecurityGroups/delete",
    "Microsoft.Network/networkSecurityGroups/securityRules/delete",
    "Microsoft.Synapse/workspaces/write",
    "Microsoft.Synapse/workspaces/read",
    "Microsoft.Synapse/workspaces/delete",
    "Microsoft.Synapse/register/action",
    "Microsoft.Synapse/checkNameAvailability/action",
    "Microsoft.Synapse/workspaces/operationStatuses/read",
    "Microsoft.Synapse/workspaces/firewallRules/read",
    "Microsoft.Synapse/workspaces/replaceAllIpFirewallRules/action",
    "Microsoft.Synapse/workspaces/operationResults/read",

"Microsoft.Synapse/workspaces/privateEndpointConnectionsApproval/action",
    "Microsoft.ManagedIdentity/userAssignedIdentities/assign/action",
    "Microsoft.Compute/images/write",
    "Microsoft.Network/loadBalancers/frontendIPConfigurations/read",
    "Microsoft.Compute/virtualMachineScaleSets/write",
    "Microsoft.Compute/virtualMachineScaleSets/read",
    "Microsoft.Compute/virtualMachineScaleSets/delete"
  ],
```

```
  "NotActions": [],
  "AssignableScopes": [],
  "Description": "Console Permissions",
  "IsCustom": "true"
}
```

How Azure permissions are used

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

Azure NetApp Files

The agent makes the following API requests when you use NetApp Data 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

NetApp Backup and Recovery

The following sections describe how permissions are used for NetApp Backup and Recovery.

Minimal NetApp Backup and Recovery permissions

The Console agent makes the following API requests for basic NetApp Backup and Recovery functionality:

- Microsoft.Storage/storageAccounts/listkeys/action
- Microsoft.Storage/storageAccounts/read
- Microsoft.Storage/storageAccounts/write
- Microsoft.Storage/storageAccounts/blobServices/containers/read
- Microsoft.Storage/storageAccounts/listAccountSas/action
- Microsoft.Resources/subscriptions/locations/read
- Microsoft.Resources/subscriptions/resourceGroups/read
- Microsoft.Resources/subscriptions/resourcegroups/resources/read
- Microsoft.Resources/subscriptions/resourceGroups/write
- Microsoft.Storage/storageAccounts/managementPolicies/read
- Microsoft.Storage/storageAccounts/managementPolicies/write
- Microsoft.Authorization/locks/write
- Microsoft.Authorization/locks/read

The following is a custom policy for Backup and Recovery that uses the fewest possible permissions and the

narrowest possible scope:

```
{
  "id":
"/subscriptions/{subscriptionId}/providers/Microsoft.Authorization/roleDef
initions/{roleDefinitionGuid}",
  "properties": {
    "roleName": "Custom Role",
    "description": "Minimal permissions required for Backup and
Recovery.",
    "assignableScopes": [
      "/subscriptions/{subscriptionId}",

"/subscriptions/{subscriptionId}/resourceGroups/{resourceGroupNameContaini
ngConnectorAndStorageAccount}",

"/subscriptions/{subscriptionId}/resourceGroups/{resourceGroupNameContaini
ngConnectorAndStorageAccount}/providers/Microsoft.Storage/storageAccounts/
{storageAccountNameWithObjectLockPreprovisioned}"
    ],
    "permissions": [
      {
        "actions": [
          "Microsoft.Storage/storageAccounts/listkeys/action",
          "Microsoft.Storage/storageAccounts/read",
          "Microsoft.Storage/storageAccounts/write",

"Microsoft.Storage/storageAccounts/blobServices/containers/read",
          "Microsoft.Storage/storageAccounts/listAccountSas/action",
          "Microsoft.Resources/subscriptions/locations/read",

"Microsoft.Resources/subscriptions/resourcegroups/resources/read",
          "Microsoft.Resources/subscriptions/resourceGroups/write",
          "Microsoft.Resources/subscriptions/resourceGroups/read",
          "Microsoft.Storage/storageAccounts/managementPolicies/read",
          "Microsoft.Storage/storageAccounts/managementPolicies/write",
          "Microsoft.Authorization/locks/write",
          "Microsoft.Authorization/locks/read"
        ],
        "notActions": [],
        "dataActions": [],
        "notDataActions": []
      }
    ]
  }
}
```

Advanced Backup and Recovery permissions

The console agent makes the following API requests for advanced Backup and Recovery operations and Search & Restore features. These permissions enable management of networking, key vaults, and managed identities:

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

Legacy permissions for Backup and Recovery

The agent makes the following API requests when you use the Search & Restore functionality. You only need these permissions if you enabled legacy indexing features before the release of indexing v2 in February 2025:

- 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

NetApp Data Classification

The agent makes the following API requests when you use Data Classification.

Action	Used for set up?	Used for daily operations?
Microsoft.Compute/locations/operations/read	Yes	Yes
Microsoft.Compute/locations/vmSizes/read	Yes	Yes

Action	Used for set up?	Used for daily operations?
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
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

Action	Used for set up?	Used for daily operations?
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
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

Action	Used for set up?	Used for daily operations?
Microsoft.Resources/subscriptions/resourceGroups/write	Yes	No

Cloud Volumes ONTAP

The agent 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/usages/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
Enable management of locks on Azure disks	Microsoft.Authorization/locks/*	Yes	Yes	No

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

Purpose	Action	Used for deployment?	Used for daily operations?	Used for deletion?
Use Virtual Machine Scale Sets in Flexible orchestration mode in order to specify specific zones for Cloud Volumes ONTAP	Microsoft.Compute/virtualMachineScaleSets/write	Yes	No	No
	Microsoft.Compute/virtualMachineScaleSets/read	Yes	No	No
	Microsoft.Compute/virtualMachineScaleSets/delete	No	No	Yes

Tiering

The agent makes the following API requests when you set up NetApp Cloud Tiering.

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

The Console agent 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.

11 November 2025

A custom JSON policy was added that reflects the fewest possible permissions and narrowest possible scope.

The following permissions were added to the minimal Backup and Recovery permissions list:

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

The following permissions are no longer needed for Backup and Recovery unless you are using legacy indexing:

- 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

The following permissions were moved to the "Additional Backup and Recovery permissions" section because they are not required for a minimal configuration:

- Microsoft.Storage/storageAccounts/listkeys/action
- Microsoft.Storage/storageAccounts/read
- Microsoft.Storage/storageAccounts/write
- Microsoft.Storage/storageAccounts/blobServices/containers/read
- Microsoft.Storage/storageAccounts/listAccountSas/action
- Microsoft.Resources/subscriptions/locations/read
- Microsoft.Resources/subscriptions/resourceGroups/read
- Microsoft.Resources/subscriptions/resourcegroups/resources/read
- Microsoft.Resources/subscriptions/resourceGroups/write
- Microsoft.Storage/storageAccounts/managementPolicies/read
- Microsoft.Storage/storageAccounts/managementPolicies/write

9 September 2024

The following permissions were removed from the JSON policy because the Console no longer supports discovery and management of Kubernetes clusters:

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

22 August 2024

The following permissions were added to the JSON policy because they are required for Cloud Volumes ONTAP support of Virtual Machine Scale Sets:

- Microsoft.Compute/virtualMachineScaleSets/write
- Microsoft.Compute/virtualMachineScaleSets/read
- Microsoft.Compute/virtualMachineScaleSets/delete

5 December 2023

The following permissions are no longer needed for NetApp Backup and Recovery when backing up volume data to Azure Blob storage:

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

- Microsoft.Compute/virtualMachines/extensions/delete
- Microsoft.Compute/virtualMachines/delete

These permissions are required for other Console storage services, so they'll still remain in the custom role for the agent if you're using those other storage services.

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 Data 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 NetApp Backup and Recovery.

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

  This permission is required for Cloud Volumes ONTAP deployment.

Console agent security group rules in Azure

The Azure security group for the agent requires both inbound and outbound rules. The NetApp Console automatically creates this security group when you create a Console agent from the Console. for other installation options, You need to set up this security group manually.

Inbound rules

Protocol	Port	Purpose
SSH	22	Provides SSH access to the agent host

Protocol	Port	Purpose
HTTP	80	• Provides HTTP access from client web browsers to the local user interface • Used during the Cloud Volumes ONTAP upgrade process
HTTPS	443	Provides HTTPS access from client web browsers to the local user interface, and connections from the NetApp Data 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 agent is used as a proxy for AutoSupport messages

Outbound rules

The predefined security group for the agent 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 agent 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 agent.

The source IP address is the agent 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 NetApp Data Classification, and sending AutoSupport messages to NetApp
API calls	TCP	8080	Data Classification	Probe to Data Classification instance during deployment
DNS	UDP	53	DNS	Used for DNS resolve by the Console

Google Cloud permissions and required firewall rules

Google Cloud permissions for the Console agent

The Console agent requires permissions to perform actions in Google Cloud. These permissions are included in a custom role provided by NetApp. You should understand

what the agent does with these permissions.

Google Cloud user account permissions

The custom role below gives a Google Cloud user the permissions needed to deploy an agent. Apply this custom role to the user who will deploy the agent.

View Google Cloud user account permissions

```
title: Console agent deployment policy
description: Permissions for the user who deploys the Console agent
stage: GA
includedPermissions:

- cloudbuild.builds.get
- compute.disks.create
- compute.disks.get
- compute.disks.list
- compute.disks.setLabels
- compute.disks.use
- compute.firewalls.create
- compute.firewalls.delete
- compute.firewalls.get
- compute.firewalls.list
- compute.globalOperations.get
- compute.images.get
- compute.images.getFromFamily
- compute.images.list
- compute.images.useReadOnly
- compute.instances.attachDisk
- compute.instances.create
- compute.instances.get
- compute.instances.list
- compute.instances.setDeletionProtection
- compute.instances.setLabels
- compute.instances.setMachineType
- compute.instances.setMetadata
- compute.instances.setTags
- compute.instances.start
- compute.instances.updateDisplayDevice
- compute.machineTypes.get
- compute.networks.get
- compute.networks.list
- compute.networks.updatePolicy
- compute.projects.get
- compute.regions.get
- compute.regions.list
- compute.subnetworks.get
- compute.subnetworks.list
- compute.zoneOperations.get
- compute.zones.get
- compute.zones.list
- config.deployments.create
```

```
- config.operations.get
- config.deployments.delete
- config.deployments.deleteState
- config.deployments.get
- config.deployments.getState
- config.deployments.list
- config.deployments.update
- config.deployments.updateState
- config.previews.get
- config.previews.list
- config.revisions.get
- config.resources.list
- deploymentmanager.compositeTypes.get
- deploymentmanager.compositeTypes.list
- deploymentmanager.deployments.create
- deploymentmanager.deployments.delete
- deploymentmanager.deployments.get
- deploymentmanager.deployments.list
- deploymentmanager.manifests.get
- deploymentmanager.manifests.list
- deploymentmanager.operations.get
- deploymentmanager.operations.list
- deploymentmanager.resources.get
- deploymentmanager.resources.list
- deploymentmanager.typeProviders.get
- deploymentmanager.typeProviders.list
- deploymentmanager.types.get
- deploymentmanager.types.list
- resourcemanager.projects.get
- compute.instances.setServiceAccount
- iam.serviceAccounts.actAs
- iam.serviceAccounts.create
- iam.serviceAccounts.list
- iam.serviceAccountKeys.create
- storage.buckets.create
- storage.buckets.get
- storage.objects.create
- storage.folders.create
- storage.objects.list
```

Service account permissions

The custom role below gives the Google Cloud service account attached to the Console agent the permissions needed to manage resources and processes in your Google Cloud network.

Apply this custom role to a service account attached to the Console agent VM.

- Set up Google Cloud permissions for standard mode
- Set up permissions for restricted mode

View Google service account permissions

Ensure the role is up to date as new permissions are added or removed in subsequent releases. The change log lists any required new permissions. Review the Google permissions change log Review how to add Google Cloud service accounts

```
title: NetApp Console agent
description: Permissions for the service account associated with the
Console agent.
stage: GA
includedPermissions:
- cloudbuild.builds.get
- cloudbuild.connections.list
- cloudbuild.repositories.accessReadToken
- cloudbuild.repositories.list
- cloudquotas.quotas.get
- cloudkms.cryptoKeys.getIamPolicy
- cloudkms.cryptoKeys.setIamPolicy
- cloudkms.keyRings.get
- cloudkms.keyRings.getIamPolicy
- cloudkms.keyRings.setIamPolicy
- config.artifacts.import
- config.deployments.create
- config.deployments.delete
- config.deployments.deleteState
- config.deployments.get
- config.deployments.getLock
- config.deployments.getState
- config.deployments.update
- config.deployments.updateState
- config.previews.upload
- config.revisions.get
- config.revisions.getState
- config.deployments.getLock
- config.deployments.list
- config.deployments.lock
- config.operations.get
- config.previews.get
- config.previews.list
- config.resources.list
- compute.regionBackendServices.create
- compute.regionBackendServices.get
- compute.regionBackendServices.list
- compute.regionBackendServices.update
- compute.networks.updatePolicy
- compute.addresses.createInternal
```

```
- compute.addresses.deleteInternal
- compute.addresses.list
- compute.addresses.setLabels
- compute.addresses.useInternal
- compute.backendServices.create
- compute.disks.create
- compute.disks.createSnapshot
- compute.disks.delete
- compute.disks.get
- compute.disks.list
- compute.disks.setLabels
- compute.disks.use
- compute.firewalls.create
- compute.firewalls.delete
- compute.firewalls.get
- compute.firewalls.list
- compute.forwardingRules.create
- compute.forwardingRules.delete
- compute.forwardingRules.get
- compute.forwardingRules.setLabels
- compute.globalOperations.get
- compute.healthChecks.create
- compute.healthChecks.delete
- compute.healthChecks.get
- compute.healthChecks.useReadOnly
- compute.images.get
- compute.images.getFromFamily
- compute.images.list
- compute.images.useReadOnly
- compute.instances.addAccessConfig
- compute.instances.attachDisk
- compute.instances.create
- compute.instances.delete
- compute.instances.detachDisk
- compute.instances.get
- compute.instances.getSerialPortOutput
- compute.instances.list
- compute.instances.setDeletionProtection
- compute.instances.setLabels
- compute.instances.setMachineType
- compute.instances.setMetadata
- compute.instances.setTags
- compute.instances.start
- compute.instances.stop
- compute.instances.updateDisplayDevice
- compute.instances.use
```

```
- compute.instanceGroups.create
- compute.instanceGroups.delete
- compute.instanceGroups.get
- compute.instanceGroups.update
- compute.instanceGroups.use
- compute.addresses.get
- compute.instances.updateNetworkInterface
- compute.instances.setMinCpuPlatform
- compute.machineTypes.get
- compute.networks.get
- compute.networks.list
- compute.projects.get
- compute.regions.get
- compute.regions.list
- compute.regionBackendServices.delete
- compute.regionBackendServices.use
- compute.resourcePolicies.create
- compute.resourcePolicies.delete
- compute.resourcePolicies.get
- compute.snapshots.create
- compute.snapshots.delete
- compute.snapshots.get
- compute.snapshots.list
- compute.snapshots.setLabels
- compute.subnetworks.get
- compute.subnetworks.list
- compute.subnetworks.use
- compute.subnetworks.useExternalIp
- compute.zoneOperations.get
- compute.zones.get
- compute.zones.list
- compute.instances.setServiceAccount
- deploymentmanager.compositeTypes.get
- deploymentmanager.compositeTypes.list
- deploymentmanager.deployments.create
- deploymentmanager.deployments.delete
- deploymentmanager.deployments.get
- deploymentmanager.deployments.list
- deploymentmanager.manifests.get
- deploymentmanager.manifests.list
- deploymentmanager.operations.get
- deploymentmanager.operations.list
- deploymentmanager.resources.get
- deploymentmanager.resources.list
- deploymentmanager.typeProviders.get
- deploymentmanager.typeProviders.list
```

```
- deploymentmanager.types.get
- deploymentmanager.types.list
- logging.logEntries.list
- logging.privateLogEntries.list
- logging.logEntries.create
- logging.logEntries.route
- monitoring.timeSeries.list
- resourcemanager.projects.get
- storage.buckets.create
- storage.buckets.delete
- storage.buckets.get
- storage.buckets.list
- storage.objects.create
- storage.objects.delete
- storage.objects.list
- storage.objects.update
- cloudkms.cryptoKeyVersions.useToEncrypt
- cloudkms.cryptoKeys.get
- cloudkms.cryptoKeys.list
- cloudkms.keyRings.list
- storage.buckets.update
- iam.serviceAccounts.actAs
- iam.serviceAccounts.create
- iam.serviceAccounts.get
- iam.serviceAccounts.getIamPolicy
- iam.serviceAccounts.list
- iam.serviceAccountKeys.create
- storage.objects.get
- storage.objects.list
- storage.buckets.getIamPolicy
```

How Google Cloud permissions are used

The Console agent uses the permissions in the custom role to manage Cloud Volumes ONTAP resources and NetApp data services processes in your Google Cloud network. The following sections describe how the agent uses these permissions.

Permissions used for Cloud Volumes ONTAP

The Console agent uses the permissions in the custom role to manage Cloud Volumes ONTAP resources and processes in your Google Cloud network. The following sections describe how the agent uses these permissions.

Permissions for Cloud Volumes ONTAP

Actions	Purpose	Used for deployment?	Used for daily operations?	Used for deletion?
config.deployments.create	To deploy the Cloud Volumes ONTAP virtual machine instance using Google Cloud Infrastructure Manager.	Yes	No	No
config.deployments.delete		No	No	Yes
config.deployments.deleteState		No	No	Yes
config.deployments.get		No	Yes	No
config.deployments.getLock		No	Yes	No
config.deployments.getState		No	Yes	No
config.deployments.list		No	Yes	No
config.deployments.lock		No	Yes	No
config.deployments.update		No	Yes	No
config.deployments.updateState		No	Yes	No
config.operations.get		No	Yes	No
config.previews.get		No	Yes	No
config.previews.list		No	Yes	No
config.resources.list		No	Yes	No
config.revisions.get		No	Yes	No
compute.disks.create	To create and manage disks for Cloud Volumes ONTAP.	Yes	Yes	No
compute.disks.createSnapshot		No	Yes	No
compute.disks.delete		No	Yes	Yes
compute.disks.get		No	Yes	No
compute.disks.list		Yes	Yes	No
compute.disks.setLabels		Yes	Yes	No
compute.disks.use		No	Yes	No

Actions	Purpose	Used for deployment?	Used for daily operations?	Used for deletion?
compute.firewalls.create	To create firewall rules for Cloud Volumes ONTAP.	Yes	No	No
compute.firewalls.delete		No	Yes	Yes
compute.firewalls.get		Yes	Yes	No
compute.firewalls.list		Yes	Yes	No
compute.forwardingRules.create	Create forwarding rules for traffic routing to backend services.	No	Yes	No
compute.forwardingRules.delete	Delete existing forwarding rules.	No	Yes	No
compute.forwardingRules.get	Retrieve details about existing forwarding rules.	No	Yes	No
compute.forwardingRules.setLabels	Set or update labels on forwarding rules for organization.	No	Yes	No
compute.globalOperations.get	To get the status of operations.	Yes	Yes	No
compute.healthChecks.create	Create and manage health checks to monitor backend service health.	No	Yes	No
compute.healthChecks.delete		No	Yes	No
compute.healthChecks.get		No	Yes	No
compute.healthChecks.useReadOnly		No	Yes	No
compute.images.get	To get images for VM instances.	Yes	No	No
compute.images.getFromFamily		Yes	No	No
compute.images.list		Yes	No	No
compute.images.useReadOnly		Yes	No	No

Actions	Purpose	Used for deployment?	Used for daily operations?	Used for deletion?
compute.instances.attachDisk	To attach and detach disks to Cloud Volumes ONTAP.	Yes	Yes	No
compute.instances.detachDisk		No	Yes	Yes
compute.instances.create	To create and delete Cloud Volumes ONTAP VM instances.	Yes	No	No
compute.instances.delete		No	No	Yes
compute.instances.get	To list VM instances.	Yes	Yes	No
compute.instances.getSerialPortOutput	To get console logs.	Yes	Yes	No
compute.instances.list	To retrieve the list of instances in a zone.	Yes	Yes	No
compute.instances.setDeletionProtection	To set deletion protection on the instance.	Yes	No	No
compute.instances.setLabels	To add labels.	Yes	No	No
compute.instances.setMachineType	To change the machine type for Cloud Volumes ONTAP.	Yes	Yes	No
compute.instances.setMinCpuPlatform		Yes	Yes	No
compute.instances.setMetadata	To add metadata.	Yes	Yes	No
compute.instances.setTags	To add tags for firewall rules.	Yes	Yes	No
compute.instances.start	To start and stop Cloud Volumes ONTAP.	Yes	Yes	No
compute.instances.stop		Yes	Yes	No
compute.instances.updateDisplayDevice		Yes	Yes	No
compute.instances.use	Use virtual machine instances (start, stop, connect operations).	No	Yes	No

Actions	Purpose	Used for deployment?	Used for daily operations?	Used for deletion?
compute.machineTypes.get	To get the numbers of cores to check quotas.	Yes	No	No
compute.projects.get	To support multi-projects.	Yes	No	No
compute.resourcePolicies.create	Create and manage resource policies for automated resource management.	No	Yes	No
compute.resourcePolicies.delete		No	Yes	No
compute.resourcePolicies.get		No	Yes	No
compute.snapshots.create	To create and manage persistent disk snapshots.	Yes	Yes	No
compute.snapshots.delete		No	Yes	Yes
compute.snapshots.get		No	Yes	No
compute.snapshots.list		No	Yes	No
compute.snapshots.setLabels		Yes	Yes	No
compute.networks.get	To get the networking information needed to create a new Cloud Volumes ONTAP virtual machine instance.	Yes	Yes	No
compute.networks.list		Yes	Yes	No
compute.regions.get		Yes	Yes	No
compute.regions.list		Yes	Yes	No
compute.subnetworks.get		Yes	Yes	No
compute.subnetworks.list		Yes	Yes	No
compute.zoneOperations.get		Yes	Yes	No
compute.zones.get		Yes	Yes	No
compute.zones.list		Yes	Yes	No

Actions	Purpose	Used for deployment?	Used for daily operations?	Used for deletion?
deploymentmanager.compositeTypes.get	To deploy the Cloud Volumes ONTAP virtual machine instance using Google Cloud Deployment Manager.	Yes	No	No
deploymentmanager.compositeTypes.list		Yes	No	No
deploymentmanager.deployments.create		Yes	No	No
deploymentmanager.deployments.delete		Yes	No	No
deploymentmanager.deployments.get		Yes	No	No
deploymentmanager.deployments.list		Yes	No	No
deploymentmanager.manifests.get		Yes	No	No
deploymentmanager.manifests.list		Yes	No	No
deploymentmanager.operations.get		Yes	No	No
deploymentmanager.operations.list		Yes	No	No
deploymentmanager.resources.get		Yes	No	No
deploymentmanager.resources.list		Yes	No	No
deploymentmanager.typeProviders.get		Yes	No	No
deploymentmanager.typeProviders.list		Yes	No	No
deploymentmanager.types.get		Yes	No	No
deploymentmanager.types.list		Yes	No	No
logging.logEntries.list	To get stack log drives.	Yes	Yes	No
logging.privateLogEntries.list		Yes	Yes	No

Actions	Purpose	Used for deployment?	Used for daily operations?	Used for deletion?
logging.logEntries.create	Create and route log entires for monitoring, debugging, and auditing.	Yes	Yes	No
logging.logEntries.route		Yes	Yes	No
resourcemanager.projects.get	To support multi-projects.	Yes	Yes	No
storage.buckets.create	To create and manage a Google Cloud Storage bucket for data tiering.	Yes	Yes	No
storage.buckets.delete		No	Yes	Yes
storage.buckets.get		No	Yes	No
storage.buckets.list		No	Yes	No
storage.buckets.update		No	Yes	No
cloudkms.cryptoKeyVersions.useToEncrypt	To use customer-managed encryption keys from the Cloud Key Management Service with Cloud Volumes ONTAP.	Yes	Yes	No
cloudkms.cryptoKeys.get		Yes	Yes	No
cloudkms.cryptoKeys.list		Yes	Yes	No
cloudkms.keyRings.list		Yes	Yes	No
cloudbuild.builds.get		Yes	No	No
compute.instances.setServiceAccount	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.	Yes	Yes	No
iam.serviceAccounts.actAs		Yes	No	No
iam.serviceAccounts.create		Yes	No	No
iam.serviceAccounts.getIamPolicy		Yes	Yes	No
iam.serviceAccounts.list		Yes	Yes	No
iam.serviceAccountKeys.create		Yes	No	No

Actions	Purpose	Used for deployment?	Used for daily operations?	Used for deletion?
storage.objects.create	Create and manage objects (files) in Google Cloud Storage bucket.	Yes	Yes	No
storage.objects.delete		No	No	Yes
storage.objects.get		Yes	Yes	No
storage.objects.list		Yes	Yes	No
compute.addresses.list	To retrieve the addresses in a region when deploying an HA pair.	Yes	No	No
compute.addresses.createInternal	Create internal IP addresses within VPC network for resource allocation.	No	Yes	No
compute.addresses.deleteInternal	Delete internal IP addresses for resource cleanup.	No	Yes	No
compute.addresses.setLabels	Update labels on Address resource.	No	Yes	No
compute.addresses.useInternal	Use internal IP addresses for network communication.	No	Yes	No
compute.backendServices.create	To configure a backend service for distributing traffic in an HA pair.	Yes	No	No

Actions	Purpose	Used for deployment?	Used for daily operations?	Used for deletion?
compute.regionBackendServices.create	Create and manage backend services for traffic routing.	Yes	No	No
compute.regionBackendServices.delete		No	Yes	No
compute.regionBackendServices.get		Yes	No	No
compute.regionBackendServices.update		Yes	Yes	No
compute.regionBackendServices.list		Yes	No	No
compute.regionBackendServices.use		No	Yes	No
compute.networks.updatePolicy	To apply firewall rules on the VPCs and subnets for an HA pair.	Yes	No	No
compute.instanceGroups.get	To create and manage storage VMs on Cloud Volumes ONTAP HA pairs.	Yes	Yes	No
compute.addresses.get		Yes	Yes	No
compute.instances.updateNetworkInterface		Yes	Yes	No
compute.instanceGroups.create		No	Yes	No
compute.instanceGroups.delete		No	Yes	No
compute.instanceGroups.update		No	Yes	No
compute.instanceGroups.use		No	Yes	No
monitoring.timeSeries.list	To discover information about Google Cloud Storage buckets.	Yes	Yes	No
storage.buckets.getIamPolicy		Yes	Yes	No

Permissions used for NetApp Backup and Recovery

The Console agent uses the permissions in the custom role to manage NetApp Backup and Recovery resources and processes in your Google Cloud network. The following sections describe how the agent uses these permissions.

View permissions for NetApp Backup and Recovery

Actions	Purpose	Used for deployment?	Used for daily operations?	Used for deletion?
• 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 NetApp Backup and Recovery activation wizard instead of using the default Google-managed encryption keys.	Yes	Yes	No

Permissions used for NetApp Data Classification

The Console agent uses the permissions in the custom role to manage NetApp Data Classification resources and processes in your Google Cloud network. The following sections describe how the agent uses these permissions.

View permissions for NetApp Data Classification

Actions	Purpose	Used for deployment?	Used for daily operations?	Used for deletion?
• compute.subnetworks.use • compute.subnetworks.useExternalIp • compute.instances.addAccessConfig	To enable NetApp Data Classification.	Yes	No	No

Change log

Added and removed permissions are noted below.

08 December 2025

NetApp is moving from Google Cloud Deployment Manager to Google Cloud Infrastructure Manager (IM) to deploy and run the Console agent in Google Cloud. The following permissions were added to support this change.

The following added permissions are required for the Google Cloud user who deploys the agent:

- storage.buckets.create
- storage.buckets.get
- storage.objects.create
- storage.folders.create
- storage.objects.list
- iam.serviceAccount.actAs
- config.deployments.create
- config.operations.get

The following additional permissions are required for the service account in Google Cloud used for day-to-day operations:

- cloudbuild.connections.list
- cloudbuild.repositories.accessReadToken
- cloudbuild.repositories.list
- cloudquotas.quotas.get
- config.artifacts.import

- config.deployments.deleteState
- config.deployments.getLock
- config.deployments.getState
- config.deployments.updateState
- config.previews.upload
- config.revisions.getState
- logging.logEntries.create
- storage.objects.create
- storage.objects.delete
- storage.objects.update
- iam.serviceAccounts.get

The following added permissions are required to deploy Cloud Volumes ONTAP:

- cloudbuild.builds.get
- config.deployments.delete
- config.deployments.deleteState
- config.deployments.get
- config.deployments.getState
- config.deployments.list
- config.deployments.update
- config.deployments.updateState
- config.previews.get
- config.previews.list
- config.revisions.get
- config.resources.list
- iam.serviceAccountKeys.create
- iam.serviceAccounts.create

The following added permissions are required for the service account used for day-to-day operations of Cloud Volumes ONTAP.

- compute.addresses.createInternal
- compute.addresses.deleteInternal
- compute.addresses.setLabels
- compute.addresses.useInternal
- compute.forwardingRules.create
- compute.forwardingRules.delete
- compute.forwardingRules.get
- compute.forwardingRules.setLabels

- compute.healthChecks.create
- compute.healthChecks.delete
- compute.healthChecks.get
- compute.healthChecks.useReadOnly
- compute.instanceGroups.create
- compute.instanceGroups.delete
- compute.instanceGroups.update
- compute.instanceGroups.use
- compute.instances.use
- compute.regionBackendServices.delete
- compute.regionBackendServices.update
- compute.regionBackendServices.use
- compute.resourcePolicies.create
- compute.resourcePolicies.delete
- compute.resourcePolicies.get
- logging.logEntries.route
- config.deployments.create
- config.deployments.delete
- config.deployments.get
- config.deployments.update
- config.revisions.get
- config.deployments.lock
- config.operations.get

26 November 2025

The permissions are updated to add clarity about their usage, but no permissions were added or removed. Three columns are added to indicate whether each permission is used for deployment, daily operations, or deletion. Apart from this, a few permissions are segregated based on their use for NetApp Data Classification and NetApp Backup and Recovery.

06 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 this policy:

- cloudkms.cryptoKeys.getIamPolicy

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

These permissions are required for NetApp Backup and Recovery.

Agent firewall rules in Google Cloud

The Google Cloud firewall rules for the agent requires both inbound and outbound rules. The NetApp Console automatically creates this security group when you create a Console agent from the Console. for other installation options, you need to set up this security group manually.

Inbound rules

Protocol	Port	Purpose
SSH	22	Provides SSH access to the agent host
HTTP	80	• Provides HTTP access from client web browsers to the local user interface • Used during the Cloud Volumes ONTAP upgrade process
HTTPS	443	Provides HTTPS access from client web browsers to the local user interface
TCP	3128	Provides Cloud Volumes ONTAP with internet access. You must manually open this port after deployment.

Outbound rules

The agent's predefined firewall rules open all outbound traffic. Follow basic outbound rules if acceptable, or use advanced outbound rules for stricter requirements.

Basic outbound rules

The predefined firewall rules for the agent include 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 agent.

The source IP address is the agent 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 NetApp Data Classification, and sending AutoSupport messages to NetApp
API calls	TCP	8080	Data Classification	Probe to Data Classification instance during deployment
DNS	UDP	53	DNS	Used for DNS resolve by Data Classification

Required network access for 3.9.55 and below

NetApp Console, the NetApp Console agent, and NetApp data services require outbound internet access to contact necessary endpoints.

This topic documents the network access required for versions of the NetApp Console standard mode 3.9.55 and below. For required endpoints for 4.0.0 and above, review the required endpoints for 4.0.0 and higher.

You need to set up network access for the following:

- Computers that access the NetApp Console as software as a service (SaaS)
- Console agents you install on-premises or in the cloud.

Update your endpoint list to the revised list for 4.0.0 and higher

Starting with version 4.0.0, Console agents require fewer endpoints. Existing deployments before 4.0.0 remain supported. After upgrading to 4.0.0 or later, you may remove the old endpoints from your allow list when convenient.

NetApp recommends updating firewall rules to use the revised endpoint list, which is smaller, more secure, and easier to manage. NetApp removes the need for wildcard entries, and endpoints for agent upgrades support all data services.

Endpoints for 3.9.55 and below	Endpoints for 4.0.0 and above	Purpose
• https://support.netapp.com • https://mysupport.netapp.com	• https://mysupport.netapp.com • https://signin.b2c.netapp.com • https://support.netapp.com	For licensing and contacting NetApp Support.

Endpoints for 3.9.55 and below	Endpoints for 4.0.0 and above	Purpose
• https://*.api.bluexp.netapp.com • https://api.bluexp.netapp.com • https://*.cloudmanager.cloud.netapp.com • https://cloudmanager.cloud.netapp.com • https://netapp-cloud-account.auth0.com • https://netapp-cloud-account.us.auth0.com • https://console.bluexp.netapp.com • https://*.console.bluexp.netapp.com	• https://api.bluexp.netapp.com • https://netapp-cloud-account.auth0.com • https://netapp-cloud-account.us.auth0.com • https://console.netapp.com • https://components.console.bluexp.netapp.com • https://cdn.auth0.com	For day-to-day operations.
• https://*.blob.core.windows.net • https://cloudmanagerinfraprod.azurecr.io	• https://bluexpinfraprod.eastus2.data.azurecr.io • https://bluexpinfraprod.azurecr.io	To obtain images for Console agent upgrades.

Steps

1. Verify that your agent is version 4.0.0 or higher. View agent version.
2. Whitelist the endpoints in Supported endpoints for 4.0.0 and higher.
3. Restart the service manager 2 service on each agent by running the following command:

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

4. Run the following command and verify that the agent's status shows as *active(running)*:

–

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

5. Remove the old endpoints from your firewall allow list.

Endpoints for NetApp Console and Console agents for 3.9.55 and below

These endpoints are used for Console agents 3.9.55 and below.

Endpoints	Purpose
https://support.netapp.com https://mysupport.netapp.com	To obtain licensing information and to send AutoSupport messages to NetApp support.
https://*.api.bluexp.netapp.com https://api.bluexp.netapp.com https://*.cloudmanager.cloud.netapp.com https://cloudmanager.cloud.netapp.com https://netapp-cloud-account.auth0.com https://netapp-cloud-account.us.auth0.com	To provide features and services within the NetApp Console.
Choose between two sets of endpoints: • Option 1 (recommended) https://bluexpinfraprod.eastus2.data.azurecr.io https://bluexpinfraprod.azurecr.io • Option 2 https://*.blob.core.windows.net https://cloudmanagerinfraprod.azurecr.io	To obtain images for Console agent upgrades. NetApp recommends allowing Option 1 endpoints in your firewall as they are more secure and disallowing Option 2 endpoints, unless you are using Ransomware Resilience or Backup and Recovery. Note the following about these endpoints: • Option 1 endpoints are supported in 3.9.47 and higher. Releases previous to 3.9.47 do not support backwards compatibility. • The Console agent initiates contact with the endpoints in option 2 first. If those endpoints are not accessible, it automatically contacts the endpoints in option 1. • If you use the Console agent with NetApp Backup and Recovery or Ransomware Resilience, the system does not support Option 1 endpoints. Allow Option 2 endpoints and disallow Option 1.

Cloud provider endpoints contacted by the Console agent

Console agents must have access to additional endpoints if they are deployed in your cloud provider.

Enable access to the cloud provider endpoints before installing the Console agent.

- Set up AWS network access for a Console agent
- Set up Azure network access for a Console agent
- Set up Google Cloud network access for a Console agent

Cloud provider endpoints are the same for all versions.

Data services endpoints contacted by the Console agent

The Console agent requires additional outbound internet access to support some NetApp data services and Cloud Volumes ONTAP.

Endpoints for Cloud Volumes ONTAP

- Endpoints for Cloud Volumes ONTAP in AWS
- Endpoints for Cloud Volumes ONTAP in Azure
- Endpoints for Cloud Volumes ONTAP in Google Cloud

Require the use of IMDSv2 on Amazon EC2 instances

The NetApp Console supports the Amazon EC2 Instance Metadata Service Version 2 (IMDSv2) with the Console agent and with Cloud Volumes ONTAP (including the mediator for HA deployments). In most cases, IMDSv2 is automatically configured on new EC2 instances. IMDSv1 was enabled prior to March 2024. If required by your security policies, you might need to manually configure IMDSv2 on your EC2 instances.

Before you begin

- The Console agent version must be 3.9.38 or later.
- Cloud Volumes ONTAP must be running one of the following versions:
  - 9.12.1 P2 (or any subsequent patch)
  - 9.13.0 P4 (or any subsequent patch)
  - 9.13.1 or any version after this release
- This change requires you to restart the Cloud Volumes ONTAP instances.
- These steps require the use of the AWS CLI because you must change the response hop limit to 3.

About this task

IMDSv2 provides enhanced protection against vulnerabilities. Learn more about IMDSv2 from the AWS Security Blog

The Instance Metadata Service (IMDS) is enabled as follows on EC2 instances:

- For new Console agent deployments from the Console or using Terraform scripts, IMDSv2 is enabled by default on the EC2 instance.
- If you launch a new EC2 instance in AWS and then manually install the Console agent software, IMDSv2 is also enabled by default.
- If you launch the Console agent from the AWS Marketplace, IMDSv1 is enabled by default. You can manually configure IMDSv2 on the EC2 instance.
- For existing Console agents, IMDSv1 is still supported but you can manually configure IMDSv2 on the EC2 instance if you prefer.
- For Cloud Volumes ONTAP, IMDSv1 is enabled by default on new and existing instances. You can manually configure IMDSv2 on the EC2 instances if you prefer.

Steps

1. Require the use of IMDSv2 on the Console agent instance:
   a. Connect to the Linux VM for the Console agent.

      When you created the Console agent instance in AWS, you provided an AWS access key and secret key. You can use this key pair to SSH to the instance. The user name for the EC2 Linux instance is ubuntu (for Console agents created prior to May 2023, the user name was ec2-user).

      AWS Docs: Connect to your Linux instance

   b. Install the AWS CLI.

      AWS Docs: Install or update to the latest version of the AWS CLI

   c. Use the `aws ec2 modify-instance-metadata-options` command to require the use of IMDSv2 and to change the PUT response hop limit to 3.

      Example

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

      The `http-tokens` parameter sets IMDSv2 to required. When `http-tokens` is required, you must also set `http-endpoint` to enabled.

2. Require the use of IMDSv2 on Cloud Volumes ONTAP instances:
   a. Go to the Amazon EC2 console
   b. From the navigation pane, select **Instances**.
   c. Select a Cloud Volumes ONTAP instance.
   d. Select **Actions > Instance settings > Modify instance metadata options**.
   e. On the **Modify instance metadata options** dialog box, select the following:
      - For **Instance metadata service**, select **Enable**.
      - For **IMDSv2**, select **Required**.
      - Select **Save**.
   f. Repeat these steps for other Cloud Volumes ONTAP instances, including the HA mediator.
   g. Stop and start the Cloud Volumes ONTAP instances

Result

The Console agent instance and Cloud Volumes ONTAP instances are now configured to use IMDSv2.

Default configuration for the Console agent

Learn about Console agent default configurations for standard deployments (with internet

access) across AWS, Azure, and Google Cloud, as well as restricted deployments (without internet access) for on-premises environments.

Default configuration with internet access

The following configuration details apply if you deployed a Console agent from the NetApp Console, from your cloud provider's marketplace, or if you manually installed a Console agent on an on-premises Linux host that has internet access.

Console agent VM details for AWS

If you deployed a Console agent from the Console or from the cloud provider's marketplace, note the following:

- The EC2 instance type is t3.2xlarge.
- The operating system for the image is Ubuntu 22.04 LTS.

  The operating system does not include a GUI. You must use a terminal to access the system.

- The installation includes Docker Engine, which is the required container orchestration tool.
- The user name for the EC2 Linux instance is ubuntu (for agents created prior to May 2023, the user name is ec2-user).
- The default system disk is a 100 GiB gp2 disk.

Console agent VM details for Azure

If you deployed a Console agent from the Console or from the cloud provider's marketplace, note the following:

- The VM type is Standard_D8s_v3.
- The operating system for the image is Ubuntu 22.04 LTS.

  The operating system does not include a GUI. You must use a terminal to access the system.

- The installation includes Docker Engine, which is the required container orchestration tool.
- The default system disk is a 100 GiB premium SSD disk.

Console agent VM details for Google Cloud

If you deployed a Console agent from the Console, note the following:

- The VM instance is n2-standard-8.
- The operating system for the image is Ubuntu 22.04 LTS.

  The operating system does not include a GUI. You must use a terminal to access the system.

- The installation includes Docker Engine, which is the required container orchestration tool.
- The default system disk is a 100 GiB SSD persistent disk.

Installation folder

The agent installation folder is in the following location:

`/opt/application/netapp/cloudmanager`

Log files

Log files are contained in the following folders:

- `/opt/application/netapp/cloudmanager/log`
  or
- `/opt/application/netapp/service-manager-2/logs` (starting with new 3.9.23 installations)

  The logs in these folders provide details about the Console agent.

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

  The logs in this folder provide details about cloud services and the Console service that runs on the Console agent.

Console agent service

- The Console agent service is named occm.
- The occm service is dependent on the MySQL service.

  If the MySQL service is down, then the occm service is down too.

Ports

The agent uses the following ports on the Linux host:

- 80 for HTTP access
- 443 for HTTPS access

Default configuration without internet access

The following configuration applies if you manually installed the Console agent on an on-premises Linux host that doesn't have internet access. Learn more about this installation option.

- The agent installation folder is in the following location:

  `/opt/application/netapp/ds`

- Log files are contained in the following folders:

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

  The logs in this folder provide details about the Console agent and docker images.

- All services are running inside docker containers

  The services are dependent on the docker runtime service running

- The agent uses the following ports on the Linux host:

- 80 for HTTP access
- 443 for HTTPS access

Copyright information

Trademark information