



# **Set up and administer BlueXP**

## **Set up and administration**

NetApp

February 20, 2023

# Table of Contents

|   |     |
|---|-----|
| Set up and administer BlueXP                          | 1   |
| Release notes   | 2   |
| What's new  | 2   |
| Known limitations                                     | 14  |
| Get started   | 16  |
| Learn about BlueXP                                    | 16  |
| Getting started checklist                             | 17  |
| Sign up to BlueXP                                     | 21  |
| Log in to BlueXP                                      | 22  |
| Set up a NetApp account                               | 23  |
| Set up a Connector                                    | 31  |
| Where to go next                                      | 71  |
| Administer BlueXP                                     | 73  |
| NetApp accounts                                       | 73  |
| Connectors  | 87  |
| Manage PAYGO subscriptions and contracts              | 115 |
| Discovered cloud storage                              | 117 |
| AWS credentials                                       | 122 |
| Azure credentials                                     | 130 |
| Google Cloud credentials                              | 143 |
| Add and manage NetApp Support Site accounts in BlueXP | 149 |
| My Opportunities                                      | 156 |
| Reference   | 157 |
| Permissions   | 157 |
| Ports   | 211 |
| Knowledge and support                                 | 215 |
| Register for support                                  | 215 |
| Get help  | 219 |
| Legal notices   | 222 |
| Copyright   | 222 |
| Trademarks  | 222 |
| Patents   | 222 |
| Privacy policy  | 222 |
| Open source   | 222 |

# Set up and administer BlueXP

# Release notes

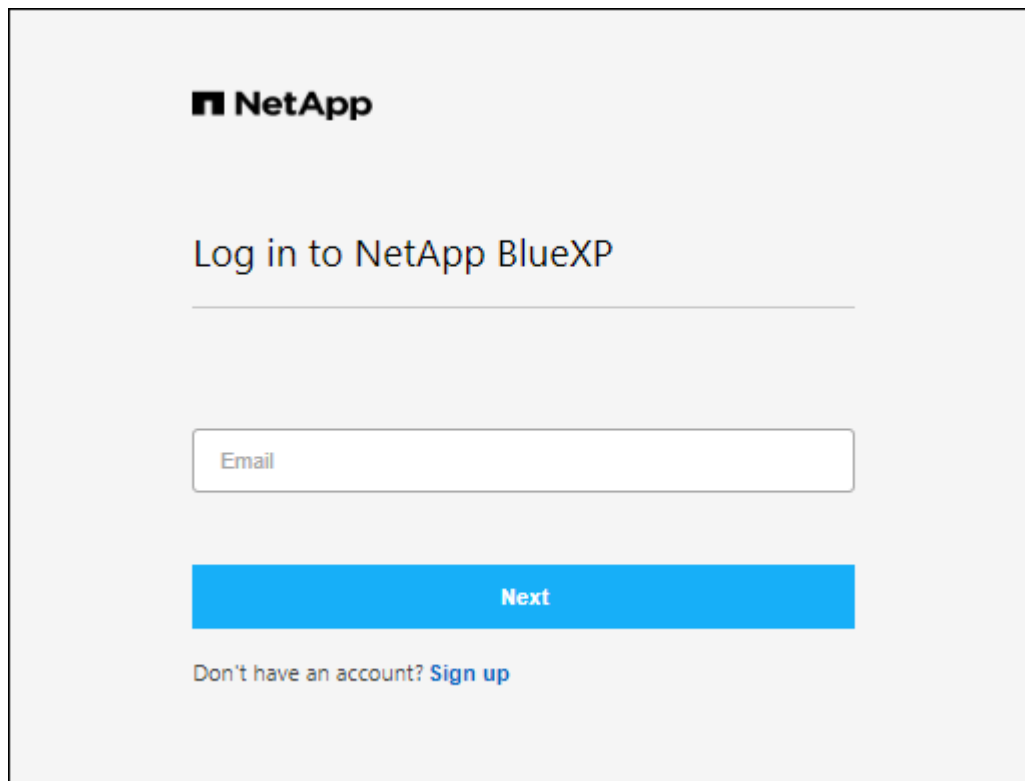
## What's new

Learn what's new with BlueXP (formerly Cloud Manager) administration features: NetApp accounts, Connectors, cloud provider credentials, and more.

### 5 February 2023

#### Connector 3.9.26

- On the **Log in** page, you're now prompted to enter the email address associated with your login. After you click **Next**, BlueXP then prompts you to authenticate using the authentication method associated with your login:
  - The password for your NetApp cloud credentials
  - Your federated identity credentials
  - Your NetApp Support Site credentials



NetApp

Log in to NetApp BlueXP

---

Email

Next

Don't have an account? [Sign up](#)

- If you're new to BlueXP and you have existing NetApp Support Site (NSS) credentials, then you can skip the sign up page and enter your email address directly in the log in page. BlueXP will sign you up as part of this initial login.
- When you subscribe to BlueXP from your cloud provider's marketplace, you now have the option to replace the existing subscription for one account with the new subscription.

Subscription Assignment

✓ Your subscription to BlueXP / Cloud Volumes ONTAP from the AWS Marketplace was created successfully.

Subscription name ⓘ

QAAccount\_Sub2Test-PAYGOByTheHourByCapacity

Select the NetApp accounts that you'd like to associate this subscription with. ⓘ

You can automatically replace the existing subscription for one account with this new subscription.

| Netapp account                                     | Replace existing subscription       |
|--|-------------------------------------|
| <input checked="" type="checkbox"/> MyAccount      | <input checked="" type="checkbox"/> |
| <input checked="" type="checkbox"/> Netapp-Kobi    | <input type="checkbox"/>            |
| <input checked="" type="checkbox"/> KeystoneTest01 | <input type="checkbox"/>            |
| <input checked="" type="checkbox"/> MyAccount      | <input type="checkbox"/>            |

Save

- [Learn how to associate an AWS subscription](#)
- [Learn how to associate an Azure subscription](#)
- [Learn how to associate a Google Cloud subscription](#)
- BlueXP will now notify you if your Connector has been powered down for 14 days or longer.
  - [Learn about BlueXP notifications](#)
  - [Learn why Connectors should remain running](#)
- We updated the Connector policy for Google Cloud to include a permission that's required to create and manage storage VMs on Cloud Volumes ONTAP HA pairs:

compute.instances.updateNetworkInterface

[View Google Cloud permissions for the Connector.](#)

- This release of the Connector includes Cloud Volumes ONTAP enhancements.

[Learn about Cloud Volumes ONTAP enhancements](#)

## 1 January 2023

### Connector 3.9.25

This release of the Connector includes Cloud Volumes ONTAP enhancements and bug fixes.

[Learn about Cloud Volumes ONTAP enhancements](#)

## 4 December 2022

### Connector 3.9.24

- We've updated the URL for the BlueXP console to <https://console.bluexp.netapp.com>
- The Connector is now supported in the Google Cloud Israel region.
- This release of the Connector also includes Cloud Volumes ONTAP enhancements and on-prem ONTAP cluster enhancements.
  - [Learn about Cloud Volumes ONTAP enhancements](#)
  - [Learn about ONTAP on-prem cluster enhancements](#)

## 6 November 2022

### Connector 3.9.23

- Your PAYGO subscriptions and annual contracts for BlueXP are now available to view and manage from the Digital Wallet.

[Learn how to manage your subscriptions](#)

- This release of the Connector also includes Cloud Volumes ONTAP enhancements.

[Learn about Cloud Volumes ONTAP enhancements](#)

## 1 November 2022

Cloud Manager now prompts you to update the credentials associated with your NetApp Support Site accounts when the refresh token associated with your account expires after 3 months. [Learn how to manage NSS accounts](#)

## 18 September 2022

### Connector 3.9.22

- We enhanced the Connector deployment wizard by adding an *in-product guide* that provides steps to meet the minimum requirements for Connector installation: permissions, authentication, and networking.
- You can now create a NetApp support case directly from Cloud Manager in the **Support Dashboard**.

[Learn how to create a case.](#)

- This release of the Connector also includes Cloud Volumes ONTAP enhancements.

[Learn about Cloud Volumes ONTAP enhancements](#)

## 31 July 2022

### Connector 3.9.21

- We've introduced a new way to discover the existing cloud resources that you're not yet managing in Cloud Manager.

On the Canvas, the **My Opportunities** tab provides a centralized location to discover existing resources that you can add to Cloud Manager for consistent data services and operations across your hybrid multicloud.

In this initial release, My Opportunities enables you to discover existing FSx for ONTAP file systems in your AWS account.

[Learn how to discover FSx for ONTAP using My Opportunities](#)

- This release of the Connector also includes Cloud Volumes ONTAP enhancements.

[Learn about Cloud Volumes ONTAP enhancements](#)

## 15 July 2022

### Policy changes

We updated the documentation by adding the Cloud Manager policies directly inside the docs. This means you can now view the required permissions for the Connector and Cloud Volumes ONTAP right alongside the steps that describe how to set them up. These policies were previously accessible from a page on the NetApp Support Site.

[Here's an example that shows the AWS IAM role permissions used to create a Connector.](#)

We also created a page that provides links to each of the policies. [View the permissions summary for Cloud Manager.](#)

## 3 July 2022

### Connector 3.9.20

- We've introduced a new way to navigate to the growing list of features in the Cloud Manager interface. All the familiar Cloud Manager capabilities can now be easily found by hovering over the left panel.



- You can now configure Cloud Manager to send notifications by email so you can be informed of important system activity even when you're not logged into the system.

[Learn more about monitoring operations in your account.](#)

- Cloud Manager now supports Azure Blob storage and Google Cloud Storage as working environments, similar to Amazon S3 support.

After you install a Connector in Azure or Google Cloud, Cloud Manager now automatically discovers information about Azure Blob storage in your Azure subscription or the Google Cloud Storage in the project where the Connector is installed. Cloud Manager displays the object storage as a working environment that you can open to view more detailed information.

Here's an example of an Azure Blob working environment:



1001

Azure blob

Overview

1001

637

Total Storage Accounts

1.5

TiB

Total Capacity

16

Total Locations

637

Storage Accounts

| Storage Account Name | Subscription | Location       | Creation Date     | Resource Group | Blob Capacity |
|----------------------|--------------|----------------|-------------------|----------------|---------------|
| ovu8llxvqdfypxn      | OCCM QA1     | West US        | June 24, 2021     | AdmAzureHa-rg  | 170 B         |
| rootsa9ktpjzcm       | OCCM QA1     | West US        | June 24, 2021     | AdmAzureHa-rg  | 950.22 GiB    |
| scvdwjcwehswli       | OCCM QA1     | West US        | June 24, 2021     | AdmAzureHa-rg  | 22.12 MiB     |
| 65qtx0smegmq2vt      | OCCM QA1     | West US        | June 24, 2021     | AdmAzureVsa-rg | 170 B         |
| bu9klxthymr1be       | OCCM QA1     | West US        | June 24, 2021     | AdmAzureVsa-rg | 1.01 MiB      |
| 8jzsvybvjiwieww8     | OCCM QA1     | Canada Central | December 12, 2019 | aff1-rg        | 170 B         |

- We redesigned the resources page for an Amazon S3 working environment by providing more detailed information about S3 buckets, such as capacity, encryption details, and more.
- The Connector is now supported in the following Google Cloud regions:
  - Madrid (europe-southwest1)
  - Paris (europe-west9)
  - Warsaw (europe-central2)
- The Connector is now supported in the Azure West US 3 region.

[View the full list of supported regions](#)

- This release of the Connector also includes Cloud Volumes ONTAP enhancements.

[Learn about Cloud Volumes ONTAP enhancements](#)

## 28 June 2022

### Log in with NetApp credentials

When new users sign up to Cloud Central, they can now select the **Log in with NetApp** option to log in with their NetApp Support Site credentials. This is an alternative to entering an email address and password.



Existing logins that use an email address and password need to keep using that login method. The Log in with NetApp option is available for new users who sign up.

## 7 June 2022

### Connector 3.9.19

- The Connector is now supported in the AWS Jakarta region (ap-southeast-3).
- The Connector is now supported in the Azure Brazil Southeast region.

[View the full list of supported regions](#)

- This release of the Connector also includes Cloud Volumes ONTAP enhancements and on-prem ONTAP cluster enhancements.
  - [Learn about Cloud Volumes ONTAP enhancements](#)
  - [Learn about ONTAP on-prem cluster enhancements](#)

## 12 May 2022

### Connector 3.9.18 patch

We updated the Connector to introduce bug fixes. The most notable fix is to an issue that affects Cloud Volumes ONTAP deployment in Google Cloud when the Connector is in a shared VPC.

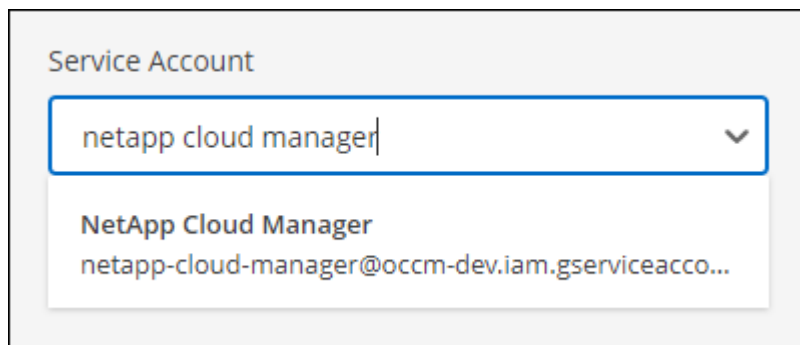
## 2 May 2022

### Connector 3.9.18

- The Connector is now supported in the following Google Cloud regions:
  - Delhi (asia-south2)
  - Melbourne (australia-southeast2)
  - Milan (europe-west8)
  - Santiago (southamerica-west1)

[View the full list of supported regions](#)

- When you select the Google Cloud service account to use with the Connector, Cloud Manager now displays the email address that's associated with each service account. Viewing the email address can make it easier to distinguish between service accounts that share the same name.



- We have certified the Connector in Google Cloud on a VM instance with an OS that supports [Shielded VM features](#)
- This release of the Connector also includes Cloud Volumes ONTAP enhancements. [Learn about those enhancements](#)
- New AWS permissions are required for the Connector to deploy Cloud Volumes ONTAP.

The following permissions are now required to create an AWS spread placement group when deploying an HA pair in a single Availability Zone (AZ):

```
"ec2:DescribePlacementGroups",  
"iam:GetRolePolicy"
```

These permissions are now required to optimize how Cloud Manager creates the placement group.

Be sure to provide these permissions to each set of AWS credentials that you've added to Cloud Manager.  
[View the latest IAM policy for the Connector.](#)

## 3 April 2022

### Connector 3.9.17

- You can now create a Connector by letting Cloud Manager assume an IAM role that you set up in your environment. This authentication method is more secure than sharing an AWS access key and secret key.

[Learn how to create a Connector using an IAM role.](#)

- This release of the Connector also includes Cloud Volumes ONTAP enhancements. [Learn about those enhancements](#)

## 27 February 2022

### Connector 3.9.16

- When you create a new Connector in Google Cloud, Cloud Manager will now display all of your existing firewall policies. Previously, Cloud Manager wouldn't display any policies that didn't have a target tag.
- This release of the Connector also includes Cloud Volumes ONTAP enhancements. [Learn about those enhancements](#)

## 30 January 2022

### Connector 3.9.15

This release of the Connector includes Cloud Volumes ONTAP enhancements. [Learn about those enhancements](#)

## 2 January 2022

### Reduced endpoints for the Connector

We reduced the number of endpoints that a Connector needs to contact in order to manage resources and processes within your public cloud environment.

[View the list of required endpoints](#)

### EBS disk encryption for the Connector

When you deploy a new Connector in AWS from Cloud Manager, you can now choose to encrypt the Connector's EBS disks using the default master key or a managed key.

✓ Get Ready

✓ AWS Credentials

3 Details

4 Network

5 Security Group

6 Review

Details

Connector Instance Name

Connector1

Connector Role

☒ Create Role ☐ Select an existing Role

Role Name

Cloud-Manager-Operator-9yils3K

+ Add Tags to Connector Instance

☒ AWS Managed Encryption

Master Key: aws/ebs (default) [Change Key](#)

### Email address for NSS accounts

Cloud Manager can now display the email address that's associated with a NetApp Support Site account.



**28 November 2021**

### **Update required for NetApp Support Site accounts**

Starting in December 2021, NetApp now uses Microsoft Azure Active Directory as the identity provider for authentication services specific to support and licensing. As a result of this update, Cloud Manager will prompt you to update the credentials for any existing NetApp Support Site accounts that you previously added.

If you haven't yet migrated your NSS account to IDaaS, you first need to migrate the account and then update your credentials in Cloud Manager.

- [Learn how to update an NSS account to the new authentication method.](#)
- [Learn more about NetApp's use of Microsoft Azure AD for identity management](#)

### **Change NSS accounts for Cloud Volumes ONTAP**

If your organization has multiple NetApp Support Site accounts, you can now change which account is associated with a Cloud Volumes ONTAP system.

[Learn how to attach a working environment to a different NSS account.](#)

## 4 November 2021

### SOC 2 Type 2 certification

An independent certified public accountant firm and services auditor examined Cloud Manager, Cloud Sync, Cloud Tiering, Cloud Data Sense, and Cloud Backup (Cloud Manager platform), and affirmed that they have achieved SOC 2 Type 2 reports based on the applicable Trust Services criteria.

[View NetApp's SOC 2 reports.](#)

### Connector no longer supported as a proxy

You can no longer use the Cloud Manager Connector as a proxy server to send AutoSupport messages from Cloud Volumes ONTAP. This functionality has been removed and is no longer supported. You will need to provide AutoSupport connectivity through a NAT instance or your environment's proxy services.

[Learn more about verifying AutoSupport with Cloud Volumes ONTAP](#)

## 31 October 2021

### Authentication with service principal

When you create a new Connector in Microsoft Azure, you can now authenticate with an Azure service principal, rather than with Azure account credentials.

[Learn how to authenticate with an Azure service principal.](#)

### Credentials enhancement

We redesigned the Credentials page for ease of use and to match the current look and feel of the Cloud Manager interface.

## 2 September 2021

### A new Notification Service has been added

The Notification service has been introduced so you can view the status of Cloud Manager operations that you have initiated during your current login session. You can verify whether the operation was successful, or if it failed. [See how to monitor operations in your account.](#)

## 1 August 2021

### RHEL 7.9 support with the Connector

The Connector is now supported on a host that's running Red Hat Enterprise Linux 7.9.

[View system requirements for the Connector.](#)

## 7 July 2021

### Enhancements to Add Connector wizard

We redesigned the **Add Connector** wizard to add new options and to make it easier to use. You can now add

tags, specify a role (for AWS or Azure), upload a root certificate for a proxy server, view code for Terraform automation, view progress details, and more.

- [Create a Connector in AWS](#)
- [Create a Connector in Azure](#)
- [Create a Connector in GCP](#)

## NSS account management from Support Dashboard

NetApp Support Site (NSS) accounts are now managed from the Support Dashboard, rather than from the Settings menu. This change makes it easier to find and manage all support-related information from a single location.

[Learn how to manage NSS accounts.](#)

Support Dashboard Resources **NSS Management** Connector

[Learn about NSS Accounts](#) [Add NSS Account](#)

1 Account

| NSS User Name | NSS User ID             | Attached Working Environments |
|---------------|-------------------------|-------------------------------|
| testcloud2    | 61e6b48b-371e-4681-a... | —                             |

## 5 May 2021

### Accounts in the Timeline

The Timeline in Cloud Manager now shows actions and events related to account management. The actions include things like associating users, creating workspaces, and creating Connectors. Checking the Timeline can be helpful if you need to identify who performed a specific action, or if you need to identify the status of an action.

[Learn how to filter the Timeline to the Tenancy service.](#)

## 11 April 2021

### API calls directly to Cloud Manager

If you configured a proxy server, you can now enable an option to send API calls directly to Cloud Manager without going through the proxy. This option is supported with Connectors that are running in AWS or in Google Cloud.

[Learn more about this setting.](#)

### Service account users

You can now create a service account user.

A service account acts as a "user" that can make authorized API calls to Cloud Manager for automation purposes. This makes it easier to manage automation because you don't need to build automation scripts based on a real person's user account who can leave the company at any time. And if you're using federation, you can create a token without generating a refresh token from the cloud.

[Learn more about using service accounts.](#)

### **Private previews**

You can now allow private previews in your account to get access to new NetApp cloud services as they are made available as a preview in Cloud Manager.

[Learn more about this option.](#)

### **Third-party services**

You can also allow third-party services in your account to get access to third-party services that are available in Cloud Manager.

[Learn more about this option.](#)

## **9 February 2021**

### **Support Dashboard improvements**

We've updated the Support Dashboard by enabling you to add your NetApp Support Site credentials, which registers you for support. You can also initiate a NetApp Support case directly from the dashboard. Just click the Help icon and then **Support**.

## **Known limitations**

Known limitations identify platforms, devices, or functions that are not supported by this release of the product, or that do not interoperate correctly with it. Review these limitations carefully.

These limitations are specific to BlueXP set up and administration: the Connector, the SaaS platform, and more.

### **Connector limitations**

#### **Possible conflict with IP addresses in the 172 range**

BlueXP deploys the Connector with two interfaces that have IP addresses in the 172.17.0.0/16 and 172.18.0.0/16 ranges.

If your network has a subnet configured with either of these ranges, then you might experience connectivity failures from BlueXP. For example, discovering on-prem ONTAP clusters in BlueXP might fail.

See Knowledge Base article [BlueXP Connector IP conflict with existing network](#) for instructions on how to change the IP address of the Connector's interfaces.



## SSL decryption isn't supported

BlueXP doesn't support firewall configurations that have SSL decryption enabled. If SSL decryption is enabled, error messages appear in BlueXP and the Connector instance displays as inactive.

For enhanced security, you have the option to [install an HTTPS certificate signed by a certificate authority \(CA\)](#).

## Blank page when loading the local UI

If you load the local user interface for a Connector, the UI might fail to display sometimes, and you just get a blank page.

This issue is related to a caching problem. The workaround is to use an incognito or private web browser session.

## Shared Linux hosts are not supported

The Connector isn't supported on a VM that is shared with other applications. The VM must be dedicated to the Connector software.

## 3rd-party agents and extensions

3rd-party agents or VM extensions are not supported on the Connector VM.

## SaaS limitations

### SaaS platform is disabled for Government regions

If you deploy a Connector in an AWS GovCloud region, an Azure Gov region, or an Azure DoD region, access to BlueXP is available only through a Connector's host IP address. Access to the SaaS platform is disabled for the entire account.

This means that only privileged users who can access the end-user internal VPC/VNet can use BlueXP's UI or API.

Note that the only services supported in these regions are Cloud Volumes ONTAP, Cloud Backup, Cloud Data Sense, and Replication. No other NetApp services are supported in Government regions.

[Learn how to access the local UI on the Connector.](#)

# Get started

## Learn about BlueXP

BlueXP (formerly Cloud Manager) enables IT experts and cloud architects to centrally manage their hybrid multi-cloud infrastructure using NetApp's cloud solutions.

### Features

BlueXP is an enterprise-class, SaaS-based management platform that keeps you in control of your data no matter where it is.

- Set up and use [Cloud Volumes ONTAP](#) for efficient, multi-protocol data management across clouds.
- Set up and use cloud file-storage services:
  - [Azure NetApp Files](#)
  - [Amazon FSx for ONTAP](#)
  - [Cloud Volumes Service for Google Cloud](#)
- Discover and manage [on-premises storage](#)
  - E-Series systems
  - ONTAP clusters
  - StorageGRID systems
- Use BlueXP's services for data mobility, data protection, and data analysis and control:
  - [Cloud Backup](#)
  - [Cloud Data Sense](#)
  - [Cloud Sync](#)
  - [Cloud Tiering](#)
  - [Digital Advisor](#)
  - [Global File Cache](#)
  - [Kubernetes](#)
  - [Ransomware Protection](#)
  - [Replication](#)

[Learn more about BlueXP](#)

### Supported cloud providers

BlueXP enables you to manage cloud storage and use cloud services in Amazon Web Services, Microsoft Azure, and Google Cloud.

### Cost

Pricing for BlueXP depends on the services that you plan to use. [Learn about BlueXP pricing](#).

## How BlueXP works

BlueXP includes a SaaS-based interface that is integrated with the BlueXP website, and Connectors that manage Cloud Volumes ONTAP and other cloud services.

### Software-as-a-service

BlueXP is accessible through a [SaaS-based user interface](#) and APIs. This SaaS experience enables you to automatically access the latest features as they're released and to easily switch between your NetApp accounts and Connectors.



If you're operating in an environment where outbound internet access isn't available, you can install the Connector software in that environment and access the local user interface that's available on the Connector. [Learn more about Connectors.](#)

### BlueXP website

The [BlueXP website](#) provides a centralized location to access and manage [NetApp cloud services](#). With centralized user authentication, you can use the same set of credentials to access BlueXP and other cloud services like Cloud Insights.

### NetApp account

When you log in to BlueXP for the first time, you're prompted to create a *NetApp account*. This account provides multi-tenancy and enables you to organize users and resources in isolated *workspaces*.

### Connectors

In most cases, a BlueXP Account Admin will need to deploy a *Connector* in your cloud or on-premises network. The Connector enables BlueXP to manage resources and processes within your public cloud environment.

[Learn more about when Connectors are required and how they work.](#)

## SOC 2 Type 2 certification

An independent certified public accountant firm and services auditor examined BlueXP, Cloud Sync, Cloud Tiering, Cloud Data Sense, and Cloud Backup (BlueXP platform), and affirmed that they have achieved SOC 2 Type 2 reports based on the applicable Trust Services criteria.

[View NetApp's SOC 2 reports](#)

## Getting started checklist

Use this checklist to understand what's needed to get up and running with BlueXP in a typical deployment where the Connector has outbound internet access.

### A login

To log in to BlueXP, you can use your NetApp Support Site credentials or you can sign up for a NetApp cloud login using your email and a password. [Learn more about logging in.](#)

### Network access from a web browser to several endpoints

The BlueXP user interface is accessible from a web browser. As you use the BlueXP user interface, it

contacts several endpoints to complete data management tasks. The machine running the web browser must have connections to the following endpoints.


| Endpoints  | Purpose  |
|--|--|
| <a href="https://console.bluexp.netapp.com">https://console.bluexp.netapp.com</a>  | Your web browser contacts this URL when using the SaaS UI.   |
| AWS services (amazonaws.com): <ul style="list-style-type: none"><li>• CloudFormation</li><li>• Cognito</li><li>• Elastic Compute Cloud (EC2)</li><li>• Key Management Service (KMS)</li><li>• Security Token Service (STS)</li><li>• Simple Storage Service (S3)</li></ul> | Required to deploy a Connector from BlueXP in AWS. The exact endpoint depends on the region in which you deploy the Connector. <a href="#">Refer to AWS documentation for details.</a> |
| <a href="https://management.azure.com">https://management.azure.com</a><br><a href="https://login.microsoftonline.com">https://login.microsoftonline.com</a>   | Required to deploy a Connector from BlueXP in most Azure regions.  |
| <a href="https://management.microsoftazure.de">https://management.microsoftazure.de</a><br><a href="https://login.microsoftonline.de">https://login.microsoftonline.de</a>   | Required to deploy a Connector from BlueXP in Azure Germany regions.   |
| <a href="https://management.usgovcloudapi.net">https://management.usgovcloudapi.net</a><br><a href="https://login.microsoftonline.com">https://login.microsoftonline.com</a>   | Required to deploy a Connector from BlueXP in Azure US Gov regions.  |
| <a href="https://www.googleapis.com">https://www.googleapis.com</a>  | Required to deploy a Connector from BlueXP in Google Cloud.  |
| <a href="https://signin.b2c.netapp.com">https://signin.b2c.netapp.com</a>  | Required to update NetApp Support Site (NSS) credentials or to add new NSS credentials to BlueXP.  |
| <a href="https://netapp-cloud-account.auth0.com">https://netapp-cloud-account.auth0.com</a><br><a href="https://cdn.auth0.com">https://cdn.auth0.com</a><br><a href="https://services.cloud.netapp.com">https://services.cloud.netapp.com</a>                              | Your web browser connects to these endpoints for centralized user authentication through BlueXP.   |
| <a href="https://widget.intercom.io">https://widget.intercom.io</a>  | For in-product chat that enables you to talk to NetApp cloud experts.  |

## Outbound networking for a Connector

After logging in to BlueXP, a BlueXP Account Admin will need to deploy a *Connector* in a cloud provider or in your on-premises network. The Connector enables BlueXP to manage resources and processes within your public cloud environment. Note that a Connector is required for most, but not all services and features in BlueXP. [Learn more about Connectors and how they work.](#)

- The network location where you deploy the Connector must have an outbound internet connection.

The Connector requires outbound internet access to contact the following endpoints in order to manage resources and processes within your public cloud environment.

| Endpoints   | Purpose  |
|---|--|
| https://<region>.amazonaws.com  | To manage resources in AWS.  |
| https://management.azure.com<br>https://login.microsoftonline.com   | To manage resources in Azure public regions.   |
| https://management.usgovcloudapi.net<br>https://login.microsoftonline.us  | To manage resources in Azure Government regions.   |
| https://management.azure.microsoft.scloud<br>https://login.microsoftonline.microsoft.scloud   | To manage resources in the Azure IL6 region.   |
| https://management.chinacloudapi.cn<br>https://login.chinacloudapi.cn   | To manage resources in Azure China regions.  |
| https://www.googleapis.com/compute/v1/<br>https://cloudresourcemanager.googleapis.com/v1/projects<br>https://www.googleapis.com/compute/beta<br>https://storage.googleapis.com/storage/v1<br>https://www.googleapis.com/storage/v1<br>https://iam.googleapis.com/v1<br>https://cloudkms.googleapis.com/v1<br>https://www.googleapis.com/deploymentmanager/v2/projects | To manage resources in Google Cloud.   |
| https://support.netapp.com  | To obtain licensing information and to send AutoSupport messages to NetApp support.  |
| https://*.api.bluexp.netapp.com<br><br>https://api.bluexp.netapp.com<br><br>https://*.cloudmanager.cloud.netapp.com<br><br>https://cloudmanager.cloud.netapp.com  | <div>  <p>The Connector is currently contacting "cloudmanager.cloud.netapp.com" but it will start contacting "api.bluexp.netapp.com" in an upcoming release.</p> </div> |
| https://cloudmanagerinfraprod.azurecr.io<br><br>https://*.blob.core.windows.net   | To upgrade the Connector and its Docker components.  |

- If you choose to manually install the Connector on your own Linux host (and not do so directly from the BlueXP interface), the installer for the Connector requires access to several endpoints during the installation process:

[Review the list of endpoints.](#)

- There's no incoming traffic to the Connector, unless you initiate it.

HTTP (80) and HTTPS (443) provide access to the local UI, which you'll use in rare circumstances. SSH (22) is only needed if you need to connect to the host for troubleshooting. Meanwhile, inbound connections over port 3128 are required if you deploy Cloud Volumes ONTAP systems in a subnet where an outbound internet connection isn't available.

## Cloud provider permissions

You need an account that has permissions to deploy the Connector in your cloud provider directly from BlueXP.



There are alternate ways to create a Connector: you can create a Connector from the [AWS Marketplace](#), the [Azure Marketplace](#), or you can [manually install the software](#).

| Location     | High-level steps   | Detailed steps                                     |
|--------------|--|--|
| AWS          | <ol style="list-style-type: none"><li>1. Use a JSON file that includes the required permissions to create an IAM policy in AWS.</li><li>2. Attach the policy to an IAM role or IAM user.</li><li>3. When you create the Connector, provide BlueXP with the ARN of the IAM role or the AWS access key and secret key for the IAM user.</li></ol>  | <a href="#">Click here to view detailed steps.</a> |
| Azure        | <ol style="list-style-type: none"><li>1. Use a JSON file that includes the required permissions to create a custom role in Azure.</li><li>2. Assign the role to the user who will create the Connector from BlueXP.</li><li>3. When you create the Connector, log in with the Microsoft account that has the required permissions (the login prompt that is owned and hosted by Microsoft).</li></ol>  | <a href="#">Click here to view detailed steps.</a> |
| Google Cloud | <ol style="list-style-type: none"><li>1. Use a YAML file that includes the required permissions to create a custom role in Google Cloud.</li><li>2. Attach that role to the user who will create the Connector from BlueXP.</li><li>3. If you plan to use Cloud Volumes ONTAP, set up a service account that has the required permissions.</li><li>4. Enable Google Cloud APIs.</li><li>5. When you create the Connector, log in with the Google account that has the required permissions (the login prompt is owned and hosted by Google).</li></ol> | <a href="#">Click here to view detailed steps.</a> |

## Networking for individual services

After setup is complete, you're ready to start using the services available from BlueXP. Note that each service has its own networking requirements. Refer to the following pages for more details.

- [Cloud Volumes ONTAP for AWS](#)
- [Cloud Volumes ONTAP for Azure](#)
- [Cloud Volumes ONTAP for GCP](#)
- [Data replication between ONTAP systems](#)
- [Deploying Cloud Data Sense](#)

- [On-prem ONTAP clusters](#)
- [Cloud Tiering](#)
- [Cloud Backup](#)

## Sign up to BlueXP

When you get started with BlueXP, your first step is to sign up. You'll be given the option to create an account, but you can skip that step if you're being invited to an existing account.

### A note about Government regions

If you need to access BlueXP from a Government region or a site that doesn't have outbound internet access, then you need to create a Connector and log in to the BlueXP user interface that runs locally on the Connector. [Learn how to access the local UI on the Connector.](#)

### Sign up options

BlueXP is accessible from your web browser through a SaaS-based user interface.

You can sign up to BlueXP using one of the following options:

- Your existing NetApp Support Site (NSS) credentials
- A NetApp cloud login by specifying your email address and a password

Both options support a federated connection, which enables single sign-on using credentials from your corporate directory (federated identity). After you sign up, you can set up a federated connection from the [BlueXP Help Center](#) by selecting **Cloud Central sign-in options**.

### Steps

1. Open a web browser and go to the [BlueXP console](#)
2. On the **Log in** page, select **Sign up**.



If you're planning to use your existing NSS credentials, then you can skip the sign up page and enter your email address directly in the log in page. BlueXP will sign you up as part of this initial login.

3. On the **Sign up** page, choose one of the login options:
  - If you have an existing NetApp Support Site (NSS) account, select **Sign up with your NetApp Support Site credentials**.  
  
When you use this option, your NetApp Support Site (NSS) credentials are not added to BlueXP in the Support Dashboard. [Learn how to add your NSS credentials to the Support Dashboard to enable key workflows.](#)
  - If you don't have an NSS account and you haven't created NetApp cloud credentials, enter the required information to create a NetApp cloud login.

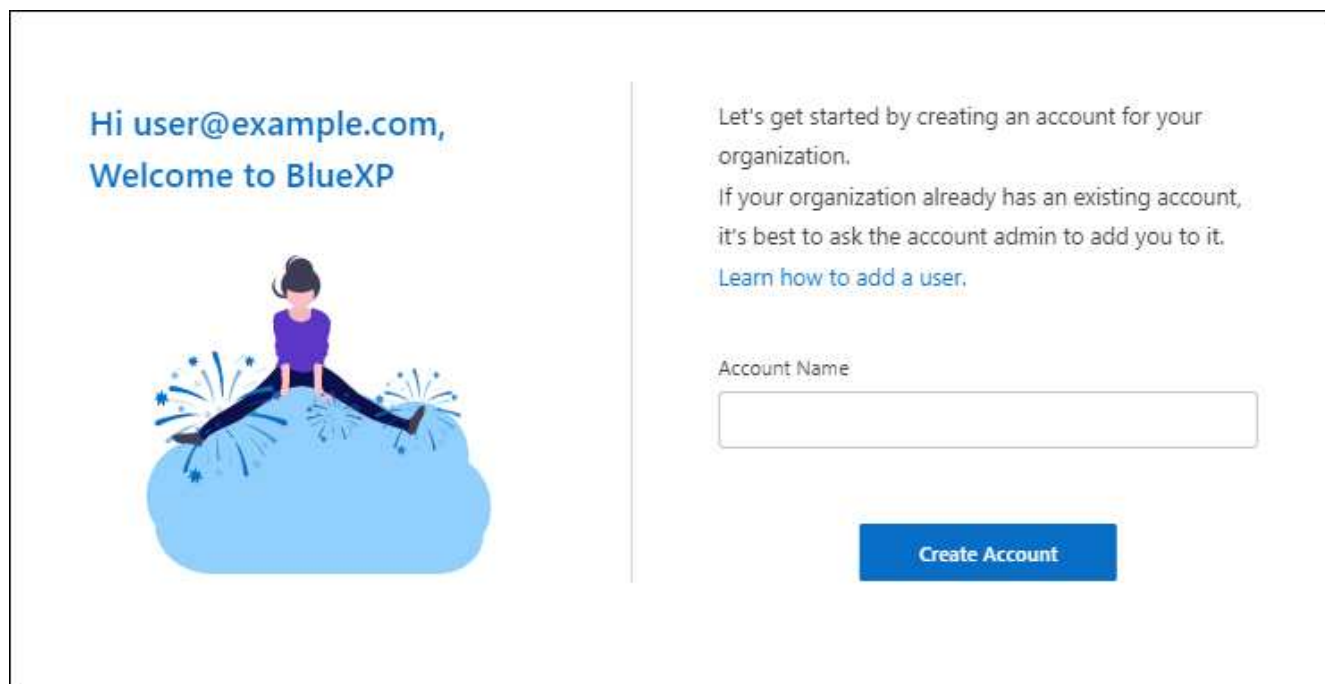
Note that only English characters are allowed in the sign up form.

4. When prompted, review the End User License Agreement and accept the terms.

5. On the **Welcome** page, enter a name for your account.

If your business already has an account and you want to join it, then you should skip this step and ask the owner to associate you with the account. After the owner adds you, you can log in and you'll have access to the account. [Learn how to add members to an existing account.](#)

An account is the top-level element in NetApp's identity platform. It enables you to add and manage users, roles, permissions, and working environments.



Hi user@example.com,  
Welcome to BlueXP

Let's get started by creating an account for your organization.  
If your organization already has an existing account, it's best to ask the account admin to add you to it.  
[Learn how to add a user.](#)

Account Name

Create Account

6. Select **Create Account**.

### Result

You now have a BlueXP login and an account. In most cases, the next step is to create a Connector, which connects BlueXP's services to your hybrid cloud environment.

## Log in to BlueXP

After you sign up to BlueXP, you can log in from your web browser through the SaaS-based user interface.

[Learn how to sign up to BlueXP and create an organization.](#)

If you're accessing BlueXP from a Government region or a site that doesn't have outbound internet access, then you need to log in to the BlueXP user interface that runs locally on the Connector. [Learn how to access the local UI on the Connector.](#)

### Log in options

You can log in to BlueXP using one of the following options:

- Your existing NetApp Support Site (NSS) credentials
- A NetApp cloud login using your email address and a password



- A federated connection

You can use single sign-on to log in using credentials from your corporate directory (federated identity). To learn more, go to the [BlueXP Help Center](#) and then click **sign-in options**.

### Steps

1. Open a web browser and go to the [BlueXP console](#)
2. On the **Log in** page, enter the email address that's associated with your login.
3. Depending on the authentication method associated with your login, you'll be prompted to enter your credentials:
  - NetApp cloud credentials: Enter your password
  - Federated user: Enter your federated identity credentials
  - NetApp Support Site account: Enter your NetApp Support Site credentials

### Result

You're now logged in and can start using BlueXP to manage your hybrid multi-cloud infrastructure.

## Set up a NetApp account


### Learn about NetApp accounts

A *NetApp account* provides multi-tenancy and enables you to organize users and resources in isolated workspaces from within BlueXP.

For example, multiple users can deploy and manage Cloud Volumes ONTAP systems in isolated environments called *workspaces*. These workspaces are invisible to other users, unless they are shared.

When you first access BlueXP, you're prompted to select or create a NetApp account:

Hi user@example.com,  
Welcome to BlueXP



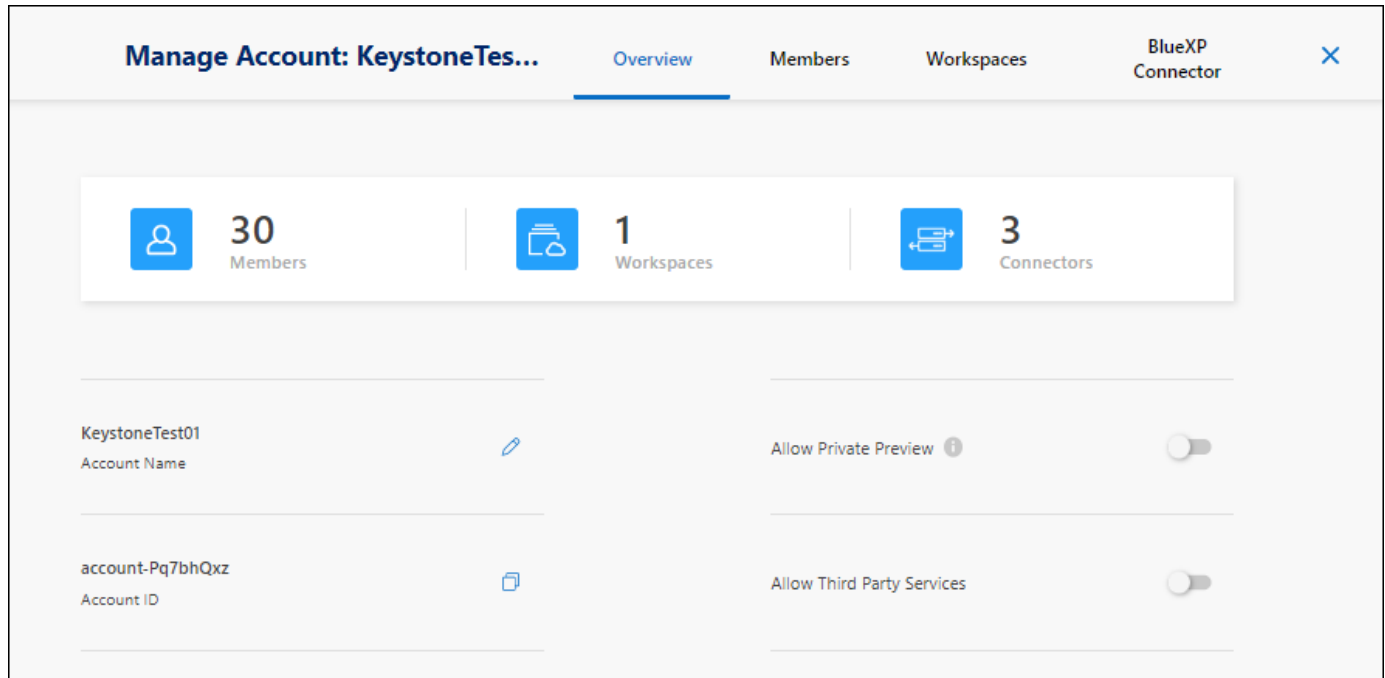
Let's get started by creating an account for your organization.

If your organization already has an existing account, it's best to ask the account admin to add you to it.  
[Learn how to add a user.](#)

Account Name

Create Account

BlueXP Account Admins can then modify the settings for this account by managing users (members), workspaces, and Connectors:



For step-by-step instructions, see [Setting up the NetApp account](#).

## Account Settings

The Manage Account widget in BlueXP enables Account Admins to manage a NetApp account. If you just created your account, then you'll start from scratch. But if you've already set up an account, then you'll see *all* the users, workspaces, and Connectors that are associated with the account.

### Overview

The Overview page shows the Account Name and the Account ID. You may need to provide your Account ID when registering some services. This page also includes some BlueXP configuration options.

### Members

The members are BlueXP users that you associate with your NetApp account. Associating a user with an account and one or more workspaces in that account enables those users to create and manage working environments in BlueXP.

When you associate a user, you assign them a role:

- **Account Admin:** Can perform any action in BlueXP.
- **Workspace Admin:** Can create and manage resources in the assigned workspace.
- **Compliance Viewer:** Can only view Cloud Data Sense compliance information and generate reports for systems that they have permission to access.
- **SnapCenter Admin:** Can use the SnapCenter Service to create application consistent backups and restore data using those backups. *This service is currently in Beta.*

[Learn more about these roles.](#)

## Workspaces

In BlueXP, a workspace isolates any number of *working environments* from other working environments. Workspace Admins can't access the working environments in a workspace unless the Account Admin associates the admin with that workspace.

A working environment represents a storage system. For example:

- A Cloud Volumes ONTAP system
- An on-premises ONTAP cluster
- A Kubernetes cluster

[Learn how to add a workspace.](#)

## Connectors

A Connector enables BlueXP to manage resources and processes within your public cloud environment. The Connector runs on a virtual machine instance that you deploy in your cloud provider, or on an on-prem host that you configured.

You can use a Connector with more than one NetApp cloud data service. For example, if you're using a Connector to manage Cloud Volumes ONTAP, you can use that same Connector with another service like Cloud Tiering.

[Learn more about Connectors.](#)

## Examples

The following examples depict how you might set up your accounts.

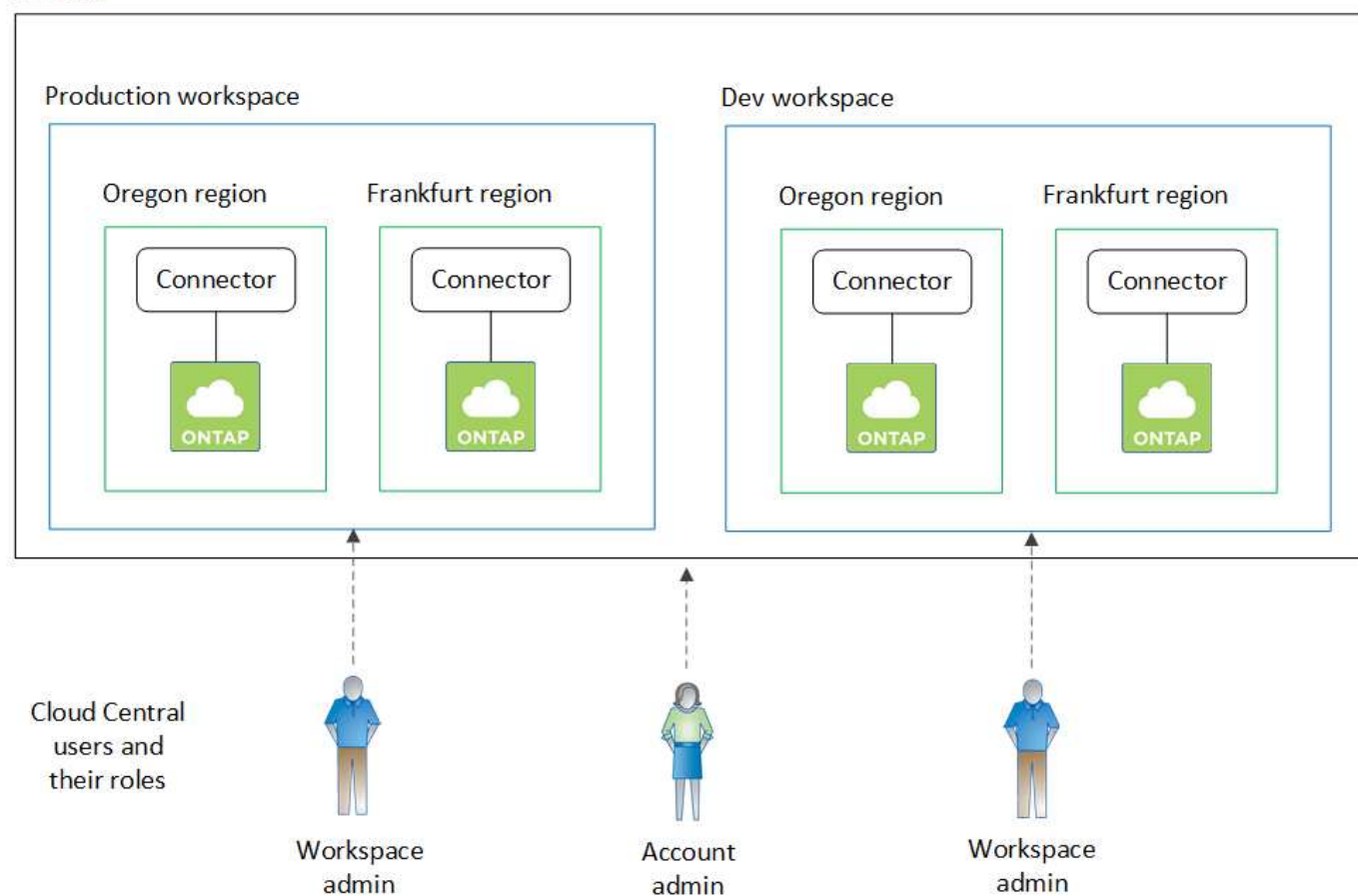


In both example images that follow, the Connector and the Cloud Volumes ONTAP systems don't actually reside *in* the NetApp account—they're running in a cloud provider. This is a conceptual representation of the relationship between each component.

### Example 1

The following example shows an account that uses two workspaces to create isolated environments. The first workspace is for a production environment and the second is for a dev environment.

## Account



### Example 2

Here's another example that shows the highest level of multi-tenancy by using two separate NetApp accounts. For example, a service provider might use BlueXP in one account to provide services for their customers, while using another account to provide disaster recovery for one of their business units.

Note that account 2 includes two separate Connectors. This might happen if you have systems in separate regions or in separate cloud providers.



## Set up workspaces and users in your NetApp account

When you log in to BlueXP for the first time, you're prompted to create a *NetApp account*. This account provides multi-tenancy and enables you to organize users and resources in isolated *workspaces*.

[Learn more about how NetApp accounts work.](#)

Set up your NetApp account so users can access BlueXP and access the working environments in a workspace. Just add a single user or add multiple users and workspaces.

### Add workspaces

In BlueXP, workspaces enable you to isolate a set of working environments from other working environments and from other users. For example, you can create two workspaces and associate separate users with each workspace.

#### Steps

1. From the top of [BlueXP](#), click the **Account** drop-down.



2. Click **Manage Account** next to the currently selected account.



3. Click **Workspaces**.
4. Click **Add New Workspace**.
5. Enter a name for the workspace and click **Add**.

#### After you finish

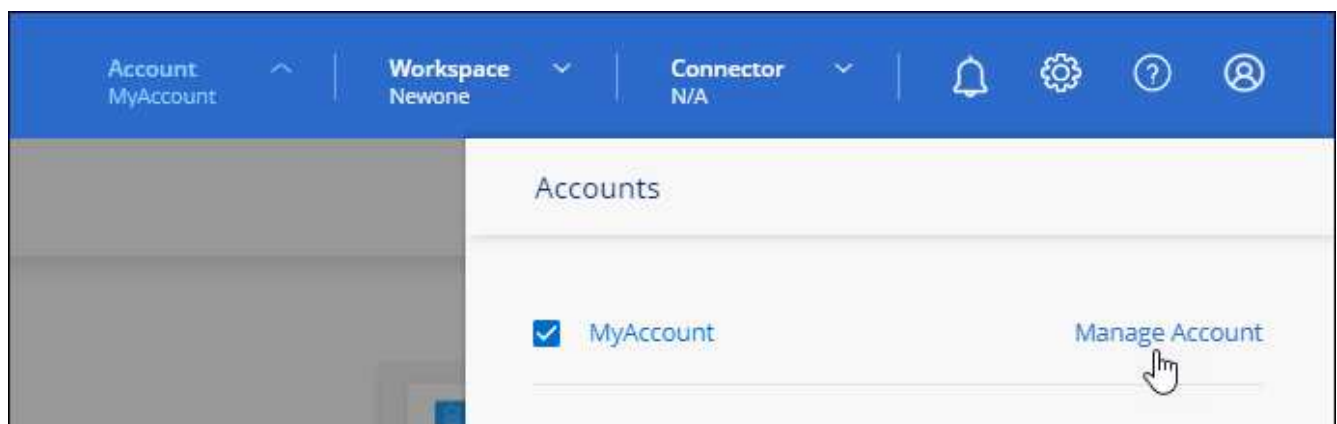
If a Workspace Admin needs access to this workspace, then you'll need to associate the user. You'll also need to associate Connectors with the workspace so Workspace Admins can use those Connectors.

#### Add users

Associate users with your NetApp account so those users can create and manage working environments in BlueXP.

#### Steps

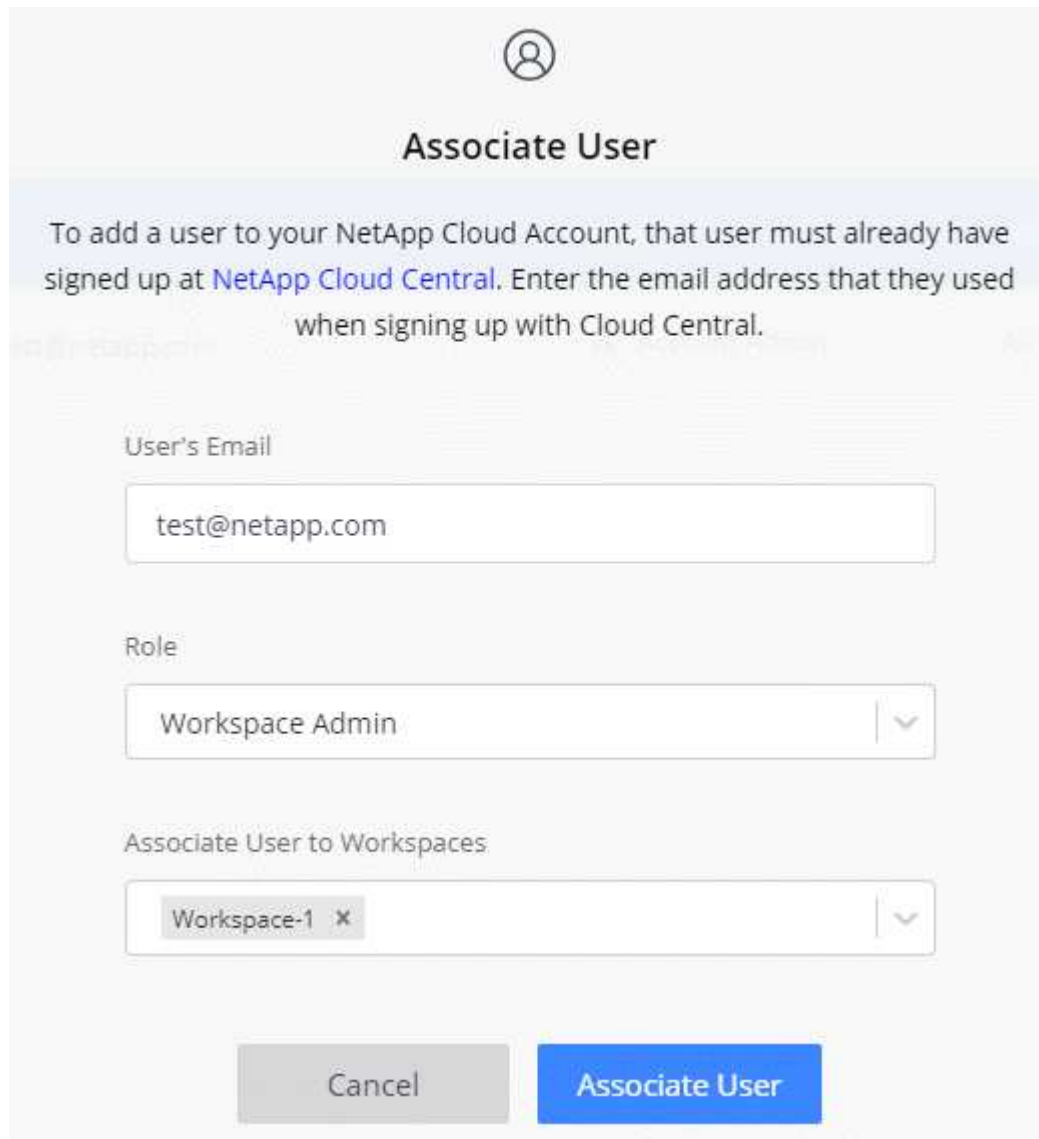
1. If the user hasn't already done so, ask the user to go to [NetApp BlueXP website](#) and sign up.
2. From the top of [BlueXP](#), click the **Account** drop-down and click **Manage Account**.



3. From the Members tab, click **Associate User**.
4. Enter the user's email address and select a role for the user:
  - **Account Admin:** Can perform any action in BlueXP.
  - **Workspace Admin:** Can create and manage resources in assigned workspaces.
  - **Compliance Viewer:** Can only view Cloud Data Sense governance and compliance information and generate reports for workspaces that they have permission to access.
  - **SnapCenter Admin:** Can use the SnapCenter Service to create application consistent backups and

restore data using those backups. This service is currently in Beta.

5. If you selected an account other than Account Admin, select one or more workspaces to associate with that user.



The image shows a dialog box titled "Associate User" with a user icon at the top. Below the title is a light blue banner with the text: "To add a user to your NetApp Cloud Account, that user must already have signed up at [NetApp Cloud Central](#). Enter the email address that they used when signing up with Cloud Central." Below this banner are three input fields: "User's Email" containing "test@netapp.com", "Role" with a dropdown menu showing "Workspace Admin", and "Associate User to Workspaces" with a dropdown menu showing "Workspace-1" and a close button (x). At the bottom are two buttons: "Cancel" and "Associate User".

6. Click **Associate**.

### Result

The user should receive an email from NetApp BlueXP website titled "Account Association." The email includes the information needed to access BlueXP.

### Associate Workspace Admins with workspaces

You can associate Workspace Admins with additional workspaces at any time. Associating the user enables them to create and view the working environments in that workspace.

### Steps

1. From the top of BlueXP, click the **Account** drop-down and click **Manage Account**.



2. From the Members tab, click the action menu in the row that corresponds to the user.



3. Click **Manage Workspaces**.
4. Select one or more workspaces and click **Apply**.

## Result

The user can now access those workspaces from BlueXP, as long as the Connector was also associated with the workspaces.

## Associate Connectors with workspaces

You need to associate a Connector with workspaces so Workspace Admins can use those Connectors to create Cloud Volumes ONTAP systems.

If you only have Account Admins, then associating the Connector with workspaces isn't required. Account Admins have the ability to access all workspaces in BlueXP by default.

[Learn more about users, workspaces, and Connectors.](#)

## Steps

1. From the top of BlueXP, click the **Account** drop-down and click **Manage Account**.





2. Click **Connector**.
3. Click **Manage Workspaces** for the Connector that you want to associate.
4. Select one or more workspaces and click **Apply**.

### Result

Workspace Admins can now use those Connectors to create Cloud Volumes ONTAP systems.

### What's next?

Now that you've set up your account, you can manage it any time by removing users, managing workspaces, and managing Connectors. [Learn how to manage your account](#).

## Set up a Connector

### Learn about Connectors

In most cases, a BlueXP Account Admin will need to deploy a *Connector* in your cloud or on-premises network. The Connector is a crucial component for the day-to-day use of BlueXP. It enables BlueXP to manage the resources and processes within your public cloud environment.

### When a Connector is required

A Connector is required for the following features and services in BlueXP:

- Amazon FSx for ONTAP management features
- Amazon S3 discovery
- Azure Blob discovery
- Cloud Backup
- Cloud Data Sense
- Cloud Tiering
- Cloud Volumes ONTAP
- E-Series systems
- Global File Cache

- Google Cloud Storage discovery
- Kubernetes clusters
- On-premises ONTAP cluster integration with BlueXP data services
- StorageGRID

A Connector is **not** required for the following services:

- Digital Advisor

In almost all cases, you can add a license to the Digital Wallet without a Connector.

The only time that a Connector is required to add a license to the Digital Wallet is for Cloud Volumes ONTAP *node-based* licenses. A Connector is required in this case because the data is taken from the licenses installed on Cloud Volumes ONTAP systems.

- Amazon FSx for ONTAP working environment creation

While a Connector isn't required to create a working environment, it is required to create and manage volumes, replicate data, and integrate FSx for ONTAP with NetApp cloud services, such as Data Sense and Cloud Sync.

- Azure NetApp Files

While a Connector isn't required to set up and manage Azure NetApp Files, a Connector is required if you want to use Cloud Data Sense to scan Azure NetApp Files data.

- Cloud Volumes Service for Google Cloud
- Cloud Sync
- Direct discovery of on-premises ONTAP clusters

While a Connector isn't required for direct discovery of an on-premises ONTAP cluster, a Connector is required if you want to take advantage of additional BlueXP features.

[Learn more about discovery and management options for on-prem ONTAP clusters](#)

## Supported locations

A Connector is supported in the following locations:

- Amazon Web Services
- Microsoft Azure
- Google Cloud
- On your premises
- On your premises, without internet access

### Note about Azure deployments

If you deploy the Connector in Azure, it should be deployed in the same Azure region as the Cloud Volumes ONTAP systems that it manages, or in the [Azure region pair](#) for the Cloud Volumes ONTAP systems. This requirement ensures that an Azure Private Link connection is used between Cloud Volumes ONTAP and its associated storage accounts. [Learn how Cloud Volumes ONTAP uses an Azure Private Link.](#)

## Note about Google Cloud deployments

If you want to create a Cloud Volumes ONTAP system in Google Cloud, then you must have a Connector that's running in Google Cloud as well. You can't use a Connector that's running in AWS, Azure, or on-prem.

## Connectors should remain running

A Connector should remain running at all times. It's important for the continued health and operation of the services that you enable.

For example, a Connector is a key component in the health and operation of Cloud Volumes ONTAP. If a Connector is powered down, Cloud Volumes ONTAP PAYGO systems and capacity-based BYOL systems shut down after losing communication with a Connector for longer than 14 days. This happens because the Connector refreshes licensing on the system each day.



If your Cloud Volumes ONTAP system has a node-based BYOL license, the system remains running after 14 days because the license is installed on the Cloud Volumes ONTAP system.

BlueXP will notify you if your Connector has been powered down for 14 days or longer. [Learn about BlueXP notifications.](#)

## How to create a Connector

A BlueXP Account Admin can create a Connector in a number of ways:

- Directly from BlueXP (recommended)
  - [Create in AWS](#)
  - [Create in Azure](#)
  - [Create in GCP](#)
- By manually installing the software on your own Linux host
  - [On a host that has internet access](#)
  - [On an on-prem host that doesn't have internet access](#)
- From your cloud provider's marketplace
  - [AWS Marketplace](#)
  - [Azure Marketplace](#)

If you are operating in a Government region, you need to deploy a Connector from your cloud provider's marketplace or by manually installing the Connector software on an existing Linux host. You can't deploy the Connector in a Government region from BlueXP's SaaS website.

## Permissions

Specific permissions are needed to create the Connector and another set of permissions are needed for the Connector instance itself.

### Permissions to create a Connector

The user who creates a Connector from BlueXP needs specific permissions to deploy the instance in your cloud provider of choice.

- [View the required AWS permissions](#)
- [View the required Azure permissions](#)
- [View the required Google Cloud permissions](#)

### **Permissions for the Connector instance**

The Connector needs specific cloud provider permissions to perform operations on your behalf. For example, to deploy and manage Cloud Volumes ONTAP.

When you create a Connector directly from BlueXP, BlueXP creates the Connector with the permissions that it needs. There's nothing that you need to do.

If you create the Connector yourself from the AWS Marketplace, the Azure Marketplace, or by manually installing the software, then you'll need to make sure that the right permissions are in place.

- [Learn how the Connector uses AWS permissions](#)
- [Learn how the Connector uses Azure permissions](#)
- [Learn how the Connector uses Google Cloud permissions](#)

### **Connector upgrades**

We typically update the Connector software each month to introduce new features and to provide stability improvements. While most of the services and features in the BlueXP platform are offered through SaaS-based software, a few features and functionalities are dependent on the version of the Connector. That includes Cloud Volumes ONTAP management, on-prem ONTAP cluster management, settings, and help.

The Connector automatically updates its software to the latest version, as long as it has outbound internet access to obtain the software update.

### **Number of working environments per Connector**

A Connector can manage multiple working environments in BlueXP. The maximum number of working environments that a single Connector should manage varies. It depends on the type of working environments, the number of volumes, the amount of capacity being managed, and the number of users.

If you have a large-scale deployment, work with your NetApp representative to size your environment. If you experience any issues along the way, reach out to us by using the in-product chat.

### **When to use multiple Connectors**

In some cases, you might only need one Connector, but you might find yourself needing two or more Connectors.

Here are a few examples:

- You're using a multi-cloud environment (AWS and Azure), so you have one Connector in AWS and another in Azure. Each manages the Cloud Volumes ONTAP systems running in those environments.
- A service provider might use one NetApp account to provide services for their customers, while using another account to provide disaster recovery for one of their business units. Each account would have separate Connectors.

## Using multiple Connectors with the same working environment

You can manage a working environment with multiple Connectors at the same time for disaster recovery purposes. If one Connector goes down, you can switch to the other Connector to immediately manage the working environment.

To set up this configuration:

1. [Switch to another Connector](#)
2. Discover the existing working environment.
  - [Add existing Cloud Volumes ONTAP systems to BlueXP](#)
  - [Discover ONTAP clusters](#)
3. Set the [Capacity Management Mode](#)

Only the main Connector should be set to **Automatic Mode**. If you switch to another Connector for DR purposes, then you can change the Capacity Management Mode as needed.

## When to switch between Connectors

When you create your first Connector, BlueXP automatically uses that Connector for each additional working environment that you create. Once you create an additional Connector, you'll need to switch between them to see the working environments that are specific to each Connector.

[Learn how to switch between Connectors.](#)

## The local user interface

While you should perform almost all tasks from the [SaaS user interface](#), a local user interface is still available on the Connector. This interface is needed if you install the Connector in an environment that doesn't have internet access (like a Government region), and for a few tasks that need to be performed from the Connector itself, instead of the SaaS interface:

- [Setting a proxy server](#)
- Installing a patch (you'll typically work with NetApp personnel to install a patch)
- Downloading AutoSupport messages (usually directed by NetApp personnel when you have issues)

[Learn how to access the local UI.](#)

## Create a Connector in AWS from BlueXP

A BlueXP Account Admin needs to deploy a *Connector* before you can use most BlueXP features. The Connector enables BlueXP to manage resources and processes within your public cloud environment.

These steps describe how to create a Connector in an AWS commercial region directly from the BlueXP SaaS website.

- [Learn how to deploy a Connector in a Government region](#)
- [Learn about other ways to deploy a Connector](#)

## Quick start

Get started quickly by following these steps, or scroll down to the remaining sections for full details.

1

### Set up authentication

To launch the Connector in AWS, BlueXP needs to authenticate with AWS by either assuming an IAM role or by using AWS access keys. With either option, an IAM policy is required.

[View the IAM role](#) or [follow step-by-step instructions](#).

2

### Set up networking

You'll need a VPC and subnet with outbound internet access to specific endpoints. If a proxy server is required for outbound internet, then you'll need the IP address, credentials, and HTTPS certificate.

[View networking requirements](#).

3

### Create the Connector

Click the Connector drop-down, select **Add Connector** and follow the prompts.

[Follow step-by-step instructions](#).

## Set up AWS authentication

BlueXP needs to authenticate with AWS before it can deploy the Connector instance in your VPC. You can choose one of these authentication methods:

- Let BlueXP assume an IAM role that has the required permissions
- Provide an AWS access key and secret key for an IAM user who has the required permissions

With either option, you first need to start by creating an IAM policy that includes the required permissions.

### Create an IAM policy

This policy contains only the permissions needed to launch the Connector instance in AWS from BlueXP. Don't use this policy for other situations.

When BlueXP creates the Connector, it applies a new set of permissions to the Connector instance that enables the Connector to manage the resources in your public cloud environment.

### Steps

1. Go to the AWS IAM console.
2. Click **Policies > Create policy**.
3. Click **JSON**.
4. Copy and paste the following policy:

```
{
```

```

"Version": "2012-10-17",
"Statement": [{
  "Effect": "Allow",
  "Action": [
    "iam:CreateRole",
    "iam:DeleteRole",
    "iam:PutRolePolicy",
    "iam:CreateInstanceProfile",
    "iam:DeleteRolePolicy",
    "iam:AddRoleToInstanceProfile",
    "iam:RemoveRoleFromInstanceProfile",
    "iam:DeleteInstanceProfile",
    "iam:PassRole",
    "ec2:DescribeInstanceStatus",
    "ec2:RunInstances",
    "ec2:ModifyInstanceAttribute",
    "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:DescribeKeyPairs",
    "ec2:DescribeRegions",
    "ec2:DescribeInstances",
    "ec2:CreateTags",
    "ec2:DescribeImages",
    "cloudformation:CreateStack",
    "cloudformation:DeleteStack",
    "cloudformation:DescribeStacks",
    "cloudformation:DescribeStackEvents",
    "cloudformation:ValidateTemplate",
    "ec2:AssociateIamInstanceProfile",
    "ec2:DescribeIamInstanceProfileAssociations",
    "ec2:DisassociateIamInstanceProfile",
    "iam:GetRole",
    "iam:TagRole",
    "iam:ListRoles",

```

```

        "kms:ListAliases"
      ],
      "Resource": "*"
    },
    {
      "Effect": "Allow",
      "Action": [
        "ec2:TerminateInstances"
      ],
      "Condition": {
        "StringLike": {
          "ec2:ResourceTag/OCCMInstance": "*"
        }
      },
      "Resource": [
        "arn:aws:ec2:*:*:instance/*"
      ]
    }
  ]
}

```

5. Click **Next** and add tags, if needed.
6. Click **Next** and enter a name and description.
7. Click **Create policy**.

### What's next?

Either attach the policy to an IAM role that BlueXP can assume or to an IAM user.

### Set up an IAM role

Set up an IAM role that BlueXP can assume in order to deploy the Connector in AWS.

### Steps

1. Go to the AWS IAM console in the target account.
2. Under Access Management, click **Roles > Create Role** and follow the steps to create the role.

Be sure to do the following:

- Under **Trusted entity type**, select **AWS account**.
  - Select **Another AWS account** and enter the ID of the BlueXP SaaS account: 952013314444
  - Select the policy that you created in the previous section.
3. After you create the role, copy the Role ARN so that you can paste it in BlueXP when you create the Connector.

### Result

The IAM role now has the required permissions.



## Set up permissions for an IAM user

When you create a Connector, you can provide an AWS access key and secret key for an IAM user who has the required permissions to deploy the Connector instance.

### Steps

1. From the AWS IAM console, click **Users** and then select the user name.
2. Click **Add permissions > Attach existing policies directly**.
3. Select the policy that you created.
4. Click **Next** and then click **Add permissions**.
5. Ensure that you have access to an access key and secret key for the IAM user.

### Result

The AWS user now has the permissions required to create the Connector from BlueXP. You'll need to specify AWS access keys for this user when you're prompted by BlueXP.

## Set up networking

Set up your networking so the Connector can manage resources and processes within your public cloud environment. Other than having a virtual network and subnet for the Connector, you'll need to ensure that the following requirements are met.


### Connection to target networks

A Connector requires a network connection to the type of working environment that you're creating and the services that you're planning to enable.

For example, if you install a Connector in your corporate network, then you must set up a VPN connection to the virtual network in which you launch Cloud Volumes ONTAP.

### Outbound internet access

The Connector requires outbound internet access to manage resources and processes within your public cloud environment.

| Endpoints  | Purpose   |
|--|---|
| https://<region>.amazonaws.com   | To manage resources in AWS.   |
| https://support.netapp.com   | To obtain licensing information and to send AutoSupport messages to NetApp support.   |
| https://*.api.bluexp.netapp.com<br>https://api.bluexp.netapp.com<br>https://*.cloudmanager.cloud.netapp.com<br>https://cloudmanager.cloud.netapp.com | <div> The Connector is currently contacting "cloudmanager.cloud.netapp.com" but it will start contacting "api.bluexp.netapp.com" in an upcoming release.</div> |

| Endpoints                                | Purpose   |
|--|---|
| https://cloudmanagerinfraprod.azurecr.io | To upgrade the Connector and its Docker components. |
| https://*.blob.core.windows.net          |   |

### Proxy server

If your organization requires deployment of a proxy server for all outgoing internet traffic, obtain the following information about your HTTP or HTTPS proxy:

- IP address
- Credentials
- HTTPS certificate

### Security group

There's no incoming traffic to the Connector, unless you initiate it or if the Connector is used as a proxy for AutoSupport messages. HTTP and HTTPS provide access to the [local UI](#), which you'll use in rare circumstances. SSH is only needed if you need to connect to the host for troubleshooting.

### IP address limitation

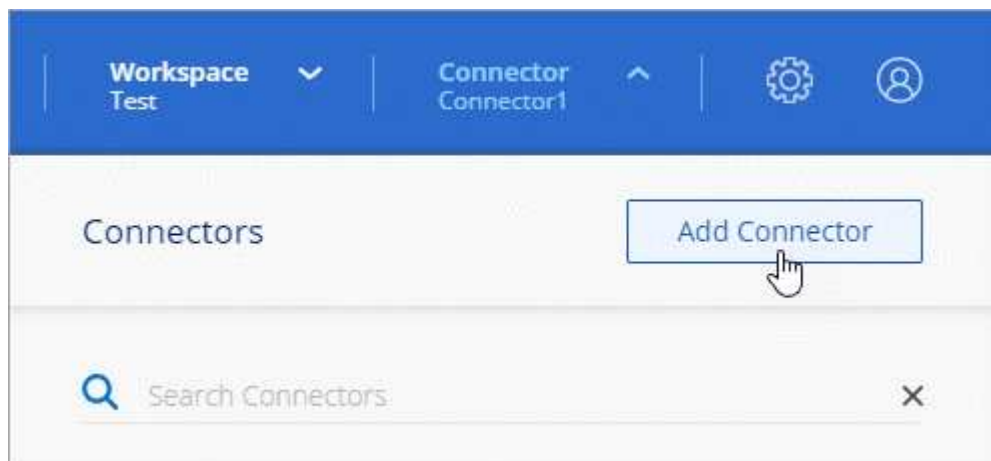
There's a possible conflict with IP addresses in the 172 range. [Learn more about this limitation.](#)

## Create a Connector

BlueXP enables you to create a Connector in AWS directly from its user interface.

### Steps

1. If you're creating your first Working Environment, click **Add Working Environment** and follow the prompts. Otherwise, click the **Connector** drop-down and select **Add Connector**.



2. Choose **Amazon Web Services** as your cloud provider and click **Continue**.
3. On the **Deploying a Connector** page, review the details about what you'll need. You have two options:
  - a. Click **Continue** to prepare for deployment by using the in-product guide. Each step in the in-product guide includes the information that's contained on this page of the documentation.

b. Click **Skip to Deployment** if you already prepared by following the steps on this page.

4. Follow the steps in the wizard to create the Connector:

- **Get Ready:** Review what you'll need.
- **AWS Credentials:** Specify your AWS region and then choose an authentication method, which is either an IAM role that BlueXP can assume or an AWS access key and secret key.



If you choose **Assume Role**, you can create the first set of credentials from the Connector deployment wizard. Any additional set of credentials must be created from the Credentials page. They will then be available from the wizard in a drop-down list. [Learn how to add additional credentials.](#)

- **Details:** Provide details about the Connector.
  - Enter a name for the instance.
  - Add custom tags (metadata) to the instance.
  - Choose whether you want BlueXP to create a new role that has the required permissions, or if you want to select an existing role that you set up with [the required permissions](#).
  - Choose whether you want to encrypt the Connector's EBS disks. You have the option to use the default encryption key or to use a custom key.
- **Network:** Specify a VPC, subnet, and key pair for the instance, choose whether to enable a public IP address, and optionally specify a proxy configuration (HTTP and HTTPS are supported).

Make sure that you have the correct key pair to use with the Connector. Without a key pair, you will not be able to access the Connector virtual machine.

- **Security Group:** Choose whether to create a new security group or whether to select an existing security group that allows inbound HTTP, HTTPS, and SSH access.
- **Review:** Review your selections to verify that your set up is correct.

5. Click **Add**.

The instance should be ready in about 7 minutes. You should stay on the page until the process is complete.

### After you finish

If you have Amazon S3 buckets in the same AWS account where you created the Connector, you'll see an Amazon S3 working environment appear on the Canvas automatically. [Learn more about what you can do with this working environment.](#)

### Open port 3128 for AutoSupport messages

If you plan to deploy Cloud Volumes ONTAP systems in a subnet where an outbound internet connection won't be available, then BlueXP automatically configures Cloud Volumes ONTAP to use the Connector as a proxy server.

The only requirement is to ensure that the Connector's security group allows *inbound* connections over port 3128. You'll need to open this port after you deploy the Connector.

If you use the default security group for Cloud Volumes ONTAP, then no changes are needed to its security group. But if you plan to define strict outbound rules for Cloud Volumes ONTAP, then you'll also need to ensure that the Cloud Volumes ONTAP security group allows *outbound* connections over port 3128.

## Create a Connector in Azure from BlueXP

A BlueXP Account Admin needs to deploy a *Connector* before you can use most BlueXP features. The Connector enables BlueXP to manage resources and processes within your public cloud environment.

These steps describe how to create a Connector in an Azure commercial region directly from the BlueXP SaaS website.

- [Learn how to deploy a Connector in a Government region](#)
- [Learn about other ways to deploy a Connector](#)

### Overview

To deploy a Connector, you need to provide BlueXP with a login that has the required permissions to create the Connector VM in Azure.

You have two options:

1. Sign in with your Microsoft account when prompted. This account must have specific Azure permissions. This is the default option.

[Follow the steps below to get started.](#)

2. Provide details about an Azure AD service principal. This service principal also requires specific permissions.

[Follow the steps below to get started.](#)

### A note about Azure regions

The Connector should be deployed in the same Azure region as the Cloud Volumes ONTAP systems that it manages, or in the [Azure region pair](#) for the Cloud Volumes ONTAP systems. This requirement ensures that an Azure Private Link connection is used between Cloud Volumes ONTAP and its associated storage accounts.

[Learn how Cloud Volumes ONTAP uses an Azure Private Link](#)

### Set up networking

Set up your networking so the Connector can manage resources and processes within your public cloud environment. Other than having a virtual network and subnet for the Connector, you'll need to ensure that the following requirements are met.


#### Connection to target networks

A Connector requires a network connection to the type of working environment that you're creating and the services that you're planning to enable.

For example, if you install a Connector in your corporate network, then you must set up a VPN connection to the virtual network in which you launch Cloud Volumes ONTAP.

## Outbound internet access

The Connector requires outbound internet access to manage resources and processes within your public cloud environment.

| Endpoints  | Purpose   |
|--|---|
| https://management.azure.com<br>https://login.microsoftonline.com  | To manage resources in Azure public regions.  |
| https://management.usgovcloudapi.net<br>https://login.microsoftonline.us   | To manage resources in Azure Government regions.  |
| https://management.azure.microsoft.scloud<br>https://login.microsoftonline.microsoft.scloud  | To manage resources in the Azure IL6 region.  |
| https://management.chinacloudapi.cn<br>https://login.chinacloudapi.cn  | To manage resources in Azure China regions.   |
| https://support.netapp.com   | To obtain licensing information and to send AutoSupport messages to NetApp support.   |
| https://*.api.bluexp.netapp.com<br>https://api.bluexp.netapp.com<br>https://*.cloudmanager.cloud.netapp.com<br>https://cloudmanager.cloud.netapp.com | <div>The Connector is currently contacting "cloudmanager.cloud.netapp.com" but it will start contacting "api.bluexp.netapp.com" in an upcoming release.</div> To provide SaaS features and services within BlueXP. |
| https://cloudmanagerinfraprod.azurecr.io<br>https://*.blob.core.windows.net  | To upgrade the Connector and its Docker components.   |

## Proxy server

If your organization requires deployment of a proxy server for all outgoing internet traffic, obtain the following information about your HTTP or HTTPS proxy:

- IP address
- Credentials
- HTTPS certificate

## Security group

There's no incoming traffic to the Connector, unless you initiate it or if the Connector is used as a proxy for AutoSupport messages. HTTP and HTTPS provide access to the [local UI](#), which you'll use in rare circumstances. SSH is only needed if you need to connect to the host for troubleshooting.

## IP address limitation

There's a possible conflict with IP addresses in the 172 range. [Learn more about this limitation.](#)

## Create a Connector using your Azure account

The default way to create a Connector in Azure is by logging in with your Azure account when prompted. The login form is owned and hosted by Microsoft. Your credentials are not provided to NetApp.

### Set up permissions for your Azure account

Before you can deploy a Connector from BlueXP, you need to ensure that your Azure account has the correct permissions.

#### Steps

1. Copy the required permissions for a new custom role in Azure and save them in a JSON file.



This policy contains only the permissions needed to launch the Connector VM in Azure from BlueXP. Don't use this policy for other situations. When BlueXP creates the Connector, it applies a new set of permissions to the Connector VM that enables the Connector to manage the resources in your public cloud environment.

```
{
  "Name": "Azure SetupAsService",
  "Actions": [
    "Microsoft.Compute/disks/delete",
    "Microsoft.Compute/disks/read",
    "Microsoft.Compute/disks/write",
    "Microsoft.Compute/locations/operations/read",
    "Microsoft.Compute/operations/read",
    "Microsoft.Compute/virtualMachines/instanceView/read",
    "Microsoft.Compute/virtualMachines/read",
    "Microsoft.Compute/virtualMachines/write",
    "Microsoft.Compute/virtualMachines/delete",
    "Microsoft.Compute/virtualMachines/extensions/write",
    "Microsoft.Compute/virtualMachines/extensions/read",
    "Microsoft.Compute/availabilitySets/read",
    "Microsoft.Network/locations/operationResults/read",
    "Microsoft.Network/locations/operations/read",
    "Microsoft.Network/networkInterfaces/join/action",
    "Microsoft.Network/networkInterfaces/read",
    "Microsoft.Network/networkInterfaces/write",
    "Microsoft.Network/networkInterfaces/delete",
    "Microsoft.Network/networkSecurityGroups/join/action",
    "Microsoft.Network/networkSecurityGroups/read",
    "Microsoft.Network/networkSecurityGroups/write",

    "Microsoft.Network/virtualNetworks/checkIpAddressAvailability/read",
    "Microsoft.Network/virtualNetworks/read",
    "Microsoft.Network/virtualNetworks/subnets/join/action",
    "Microsoft.Network/virtualNetworks/subnets/read",
```

```

"Microsoft.Network/virtualNetworks/subnets/virtualMachines/read",
    "Microsoft.Network/virtualNetworks/virtualMachines/read",
    "Microsoft.Network/publicIPAddresses/write",
    "Microsoft.Network/publicIPAddresses/read",
    "Microsoft.Network/publicIPAddresses/delete",
    "Microsoft.Network/networkSecurityGroups/securityRules/read",
    "Microsoft.Network/networkSecurityGroups/securityRules/write",
    "Microsoft.Network/networkSecurityGroups/securityRules/delete",
    "Microsoft.Network/publicIPAddresses/join/action",

"Microsoft.Network/locations/virtualNetworkAvailableEndpointServices/read",
    "Microsoft.Network/networkInterfaces/ipConfigurations/read",
    "Microsoft.Resources/deployments/operations/read",
    "Microsoft.Resources/deployments/read",
    "Microsoft.Resources/deployments/delete",
    "Microsoft.Resources/deployments/cancel/action",
    "Microsoft.Resources/deployments/validate/action",
    "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.Authorization/roleDefinitions/write",
    "Microsoft.Authorization/roleAssignments/write",

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

"Microsoft.MarketplaceOrdering/offertypes/publishers/offers/plans/agreements/write",
    "Microsoft.Network/networkSecurityGroups/delete",
    "Microsoft.Storage/storageAccounts/delete",
    "Microsoft.Storage/storageAccounts/write",
    "Microsoft.Resources/deployments/write",
    "Microsoft.Resources/deployments/operationStatuses/read",
    "Microsoft.Authorization/roleAssignments/read"
],
"NotActions": [],
"AssignableScopes": [],
"Description": "Azure SetupAsService",
"IsCustom": "true"
}

```

2. Modify the JSON by adding your Azure subscription ID to the assignable scope.

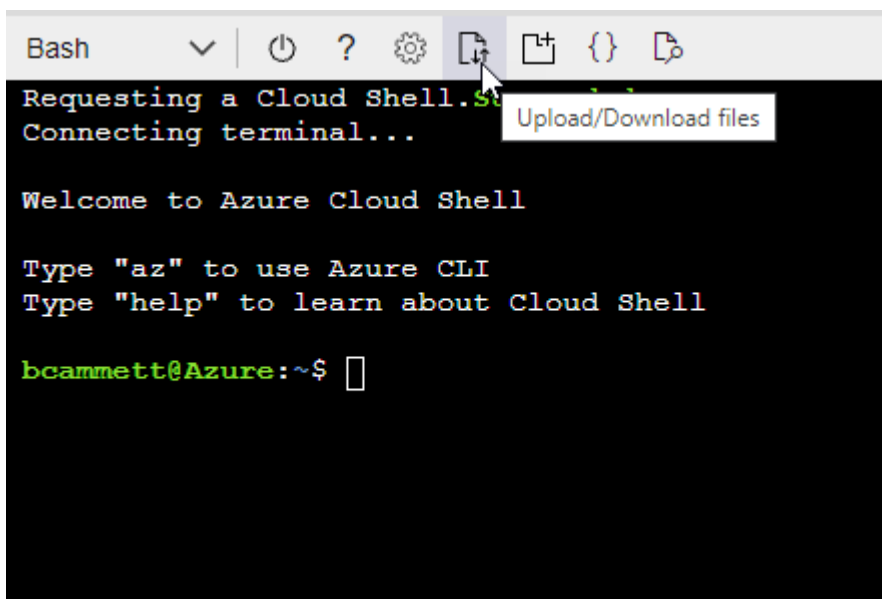
### Example

```
"AssignableScopes": [  
  "/subscriptions/d333af45-0d07-4154-943d-c25fbzzzzzzz"  
],
```

3. Use the JSON file to create a custom role in Azure.

The following steps describe how to create the role by using Bash in Azure Cloud Shell.

- a. Start [Azure Cloud Shell](#) and choose the Bash environment.
- b. Upload the JSON file.



- c. Enter the following Azure CLI command:

```
az role definition create --role-definition  
Policy_for_Setup_As_Service_Azure.json
```

You should now have a custom role called *Azure SetupAsService*.

4. Assign the role to the user who will deploy the Connector from BlueXP:
  - a. Open the **Subscriptions** service and select the user's subscription.
  - b. Click **Access control (IAM)**.
  - c. Click **Add > Add role assignment** and then add the permissions:
    - Select the **Azure SetupAsService** role and click **Next**.





Azure SetupAsService is the default name provided in the Connector deployment policy for Azure. If you chose a different name for the role, then select that name instead.

- Keep **User, group, or service principal** selected.
- Click **Select members**, choose your user account, and click **Select**.
- Click **Next**.
- Click **Review + assign**.

## Result

The Azure user now has the permissions required to deploy the Connector from BlueXP.

## Create the Connector by logging in with your Azure account

BlueXP enables you to create a Connector in Azure directly from its user interface.

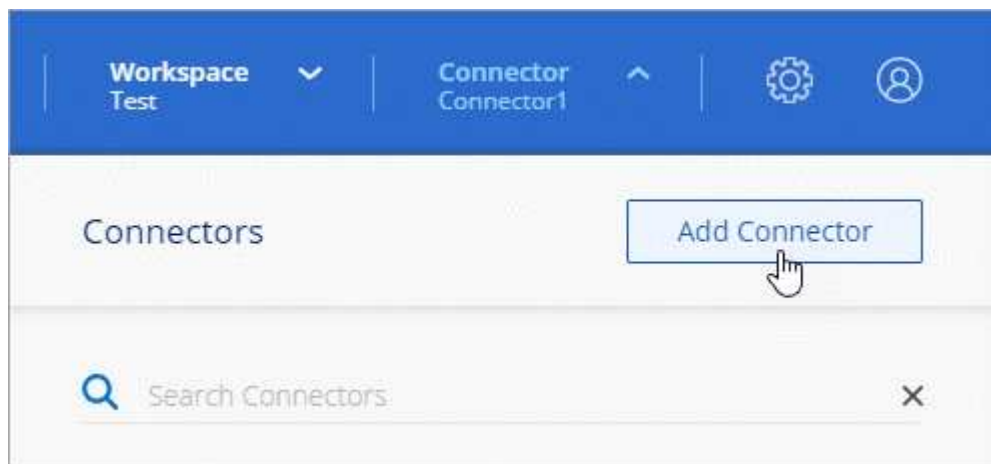
## What you'll need

- An Azure subscription.
- A VNet and subnet in your Azure region of choice.
- If you don't want BlueXP to automatically create an Azure role for the Connector, then you'll need to create your own [using the policy on this page](#).

These permissions are for the Connector instance itself. It's a different set of permissions than what you previously set up to simply deploy the Connector.

## Steps

1. If you're creating your first Working Environment, click **Add Working Environment** and follow the prompts. Otherwise, click the **Connector** drop-down and select **Add Connector**.



2. Choose **Microsoft Azure** as your cloud provider.
3. On the **Deploying a Connector** page, review the details about what you'll need. You have two options:
  - a. Click **Continue** to prepare for deployment by using the in-product guide. Each step include information contained on this page of the documentation.
  - b. Click **Skip to Deployment** if you already prepared by following the steps on this page.

#### 4. Follow the steps in the wizard to create the Connector:

- If you're prompted, log in to your Microsoft account, which should have the required permissions to create the virtual machine.

The form is owned and hosted by Microsoft. Your credentials are not provided to NetApp.



If you're already logged in to an Azure account, then BlueXP will automatically use that account. If you have multiple accounts, then you might need to log out first to ensure that you're using the right account.

- **VM Authentication:** Choose an Azure subscription, a location, a new resource group or an existing resource group, and then choose an authentication method.
- **Details:** Enter a name for the instance, specify tags, and choose whether you want BlueXP to create a new role that has the required permissions, or if you want to select an existing role that you set up with [the required permissions](#).

Note that you can choose the subscriptions associated with this role. Each subscription that you choose provides the Connector with permissions to deploy Cloud Volumes ONTAP in those subscriptions.

- **Network:** Choose a VNet and subnet, whether to enable a public IP address, and optionally specify a proxy configuration.
- **Security Group:** Choose whether to create a new security group or whether to select an existing security group that allows inbound HTTP, HTTPS, and SSH access.
- **Review:** Review your selections to verify that your set up is correct.

#### 5. Click **Add**.

The virtual machine should be ready in about 7 minutes. You should stay on the page until the process is complete.

### After you finish

You need to associate a Connector with workspaces so Workspace Admins can use those Connectors to create Cloud Volumes ONTAP systems. If you only have Account Admins, then associating the Connector with workspaces isn't required. Account Admins have the ability to access all workspaces in BlueXP by default. [Learn more](#).

If you have Azure Blob storage in the same Azure account where you created the Connector, you'll see an Azure Blob working environment appear on the Canvas automatically. [Learn more about what you can do with this working environment](#).

### Create a Connector using a service principal

Rather than logging in with your Azure account, you also have the option to provide BlueXP with the credentials for an Azure service principal that has the required permissions.

#### Granting Azure permissions using a service principal

Grant the required permissions to deploy a Connector in Azure by creating and setting up a service principal in Azure Active Directory and by obtaining the Azure credentials that BlueXP needs.

### Steps

1. [Create an Azure Active Directory application.](#)
2. [Assign the application to a role.](#)
3. [Add Windows Azure Service Management API permissions.](#)
4. [Get the application ID and directory ID.](#)
5. [Create a client secret.](#)

## Create an Azure Active Directory application

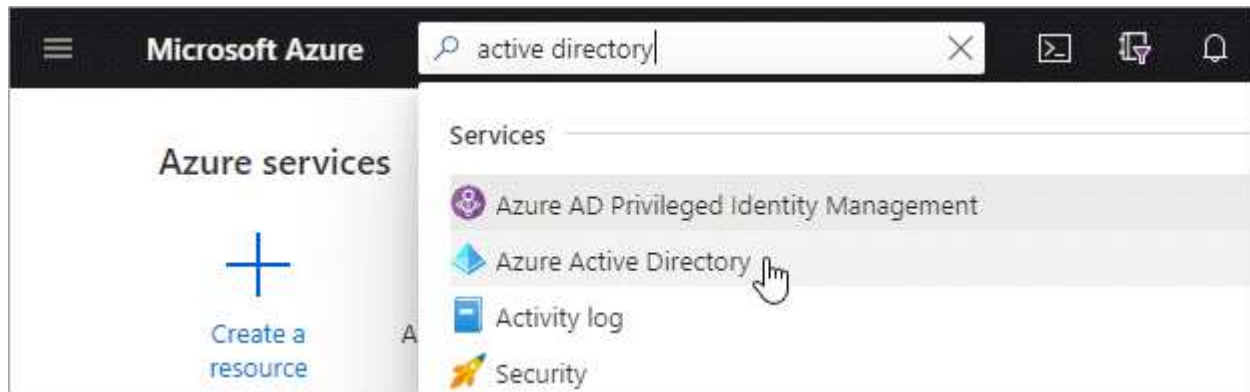
Create an Azure Active Directory (AD) application and service principal that BlueXP can use to deploy the Connector.

### Before you begin

You must have the right permissions in Azure to create an Active Directory application and to assign the application to a role. For details, refer to [Microsoft Azure Documentation: Required permissions](#).

### Steps

1. From the Azure portal, open the **Azure Active Directory** service.



2. In the menu, click **App registrations**.
3. Click **New registration**.
4. Specify details about the application:
  - **Name:** Enter a name for the application.
  - **Account type:** Select an account type (any will work with BlueXP).
  - **Redirect URI:** You can leave this field blank.
5. Click **Register**.

### Result

You've created the AD application and service principal.

## Assign the application to a role

You must bind the service principal to the Azure subscription in which you plan to deploy the Connector and assign it the custom "Azure SetupAsService" role.

### Steps

1. Copy the required permissions for a new custom role in Azure and save them in a JSON file.



This policy contains only the permissions needed to launch the Connector VM in Azure from BlueXP. Don't use this policy for other situations. When BlueXP creates the Connector, it applies a new set of permissions to the Connector VM that enables the Connector to manage the resources in your public cloud environment.

```
{
  "Name": "Azure SetupAsService",
  "Actions": [
    "Microsoft.Compute/disks/delete",
    "Microsoft.Compute/disks/read",
    "Microsoft.Compute/disks/write",
    "Microsoft.Compute/locations/operations/read",
    "Microsoft.Compute/operations/read",
    "Microsoft.Compute/virtualMachines/instanceView/read",
    "Microsoft.Compute/virtualMachines/read",
    "Microsoft.Compute/virtualMachines/write",
    "Microsoft.Compute/virtualMachines/delete",
    "Microsoft.Compute/virtualMachines/extensions/write",
    "Microsoft.Compute/virtualMachines/extensions/read",
    "Microsoft.Compute/availabilitySets/read",
    "Microsoft.Network/locations/operationResults/read",
    "Microsoft.Network/locations/operations/read",
    "Microsoft.Network/networkInterfaces/join/action",
    "Microsoft.Network/networkInterfaces/read",
    "Microsoft.Network/networkInterfaces/write",
    "Microsoft.Network/networkInterfaces/delete",
    "Microsoft.Network/networkSecurityGroups/join/action",
    "Microsoft.Network/networkSecurityGroups/read",
    "Microsoft.Network/networkSecurityGroups/write",

    "Microsoft.Network/virtualNetworks/checkIpAddressAvailability/read",
    "Microsoft.Network/virtualNetworks/read",
    "Microsoft.Network/virtualNetworks/subnets/join/action",
    "Microsoft.Network/virtualNetworks/subnets/read",

    "Microsoft.Network/virtualNetworks/subnets/virtualMachines/read",
    "Microsoft.Network/virtualNetworks/virtualMachines/read",
    "Microsoft.Network/publicIPAddresses/write",
    "Microsoft.Network/publicIPAddresses/read",
    "Microsoft.Network/publicIPAddresses/delete",
    "Microsoft.Network/networkSecurityGroups/securityRules/read",
    "Microsoft.Network/networkSecurityGroups/securityRules/write",
    "Microsoft.Network/networkSecurityGroups/securityRules/delete",
    "Microsoft.Network/publicIPAddresses/join/action",

    "Microsoft.Network/locations/virtualNetworkAvailableEndpointServices/rea
```

```

d",
    "Microsoft.Network/networkInterfaces/ipConfigurations/read",
    "Microsoft.Resources/deployments/operations/read",
    "Microsoft.Resources/deployments/read",
    "Microsoft.Resources/deployments/delete",
    "Microsoft.Resources/deployments/cancel/action",
    "Microsoft.Resources/deployments/validate/action",
    "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.Authorization/roleDefinitions/write",
    "Microsoft.Authorization/roleAssignments/write",

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

    "Microsoft.MarketplaceOrdering/offertypes/publishers/offers/plans/agreements/write",
    "Microsoft.Network/networkSecurityGroups/delete",
    "Microsoft.Storage/storageAccounts/delete",
    "Microsoft.Storage/storageAccounts/write",
    "Microsoft.Resources/deployments/write",
    "Microsoft.Resources/deployments/operationStatuses/read",
    "Microsoft.Authorization/roleAssignments/read"
],
    "NotActions": [],
    "AssignableScopes": [],
    "Description": "Azure SetupAsService",
    "IsCustom": "true"
}

```

2. Modify the JSON file by adding your Azure subscription ID to the assignable scope.

### Example

```

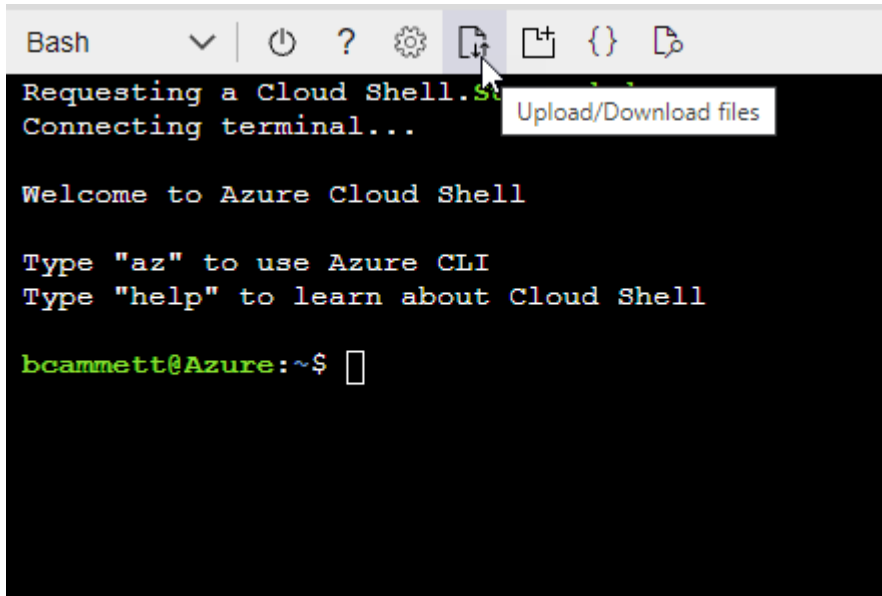
"AssignableScopes": [
    "/subscriptions/398e471c-3b42-4ae7-9b59-ce5bbzzzzzz"
]

```

3. Use the JSON file to create a custom role in Azure.

The following steps describe how to create the role by using Bash in Azure Cloud Shell.

- a. Start [Azure Cloud Shell](#) and choose the Bash environment.
- b. Upload the JSON file.



- c. Enter the following Azure CLI command:

```
az role definition create --role-definition  
Policy_for_Setup_As_Service_Azure.json
```

You should now have a custom role called *Azure SetupAsService*.

4. Assign the application to the role:
  - a. From the Azure portal, open the **Subscriptions** service.
  - b. Select the subscription.
  - c. Click **Access control (IAM) > Add > Add role assignment**.
  - d. In the **Role** tab, select the **Azure SetupAsService** role and click **Next**.
  - e. In the **Members** tab, complete the following steps:
    - Keep **User, group, or service principal** selected.
    - Click **Select members**.

**Add role assignment** ...

[Got feedback?](#)

**Role**   **Members**   [Review + assign](#)

**Selected role**   Cloud Manager Operator 3.9.12\_B

**Assign access to**   ☒ User, group, or service principal  
☐ Managed identity

**Members**   [+ Select members](#)

- Search for the name of the application.

Here's an example:

**Select members** ×

Select ⓘ

test-service-principal

test-service-principal

- Select the application and click **Select**.
  - Click **Next**.
- f. Click **Review + assign**.

The service principal now has the required Azure permissions to deploy the Connector.

## Add Windows Azure Service Management API permissions

The service principal must have "Windows Azure Service Management API" permissions.

### Steps

1. In the **Azure Active Directory** service, click **App registrations** and select the application.
2. Click **API permissions > Add a permission**.
3. Under **Microsoft APIs**, select **Azure Service Management**.

## Request API permissions

### Select an API

[Microsoft APIs](#) [APIs my organization uses](#) [My APIs](#)

#### Commonly used Microsoft APIs

**Microsoft Graph**  
Take advantage of the tremendous amount of data in Office 365, Enterprise Mobility + Security, and Windows 10. Access Azure AD, Excel, Intune, Outlook/Exchange, OneDrive, OneNote, SharePoint, Planner, and more through a single endpoint.



**Azure Batch**  
Schedule large-scale parallel and HPC applications in the cloud

**Azure Data Catalog**  
Programmatic access to Data Catalog resources to register, annotate and search data assets

**Azure Data Explorer**  
Perform ad-hoc queries on terabytes of data to build near real-time and complex analytics solutions

**Azure Data Lake**  
Access to storage and compute for big data analytic scenarios

**Azure DevOps**  
Integrate with Azure DevOps and Azure DevOps server

**Azure Import/Export**  
Programmatic control of import/export jobs

**Azure Key Vault**  
Manage your key vaults as well as the keys, secrets, and certificates within your Key Vaults

**Azure Rights Management Services**  
Allow validated users to read and write protected content

**Azure Service Management**  
Programmatic access to much of the functionality available through the Azure portal

**Azure Storage**  
Secure, massively scalable object and data lake storage for unstructured and semi-structured data

**Customer Insights**  
Create profile and interaction models for your products

**Data Export Service for Microsoft Dynamics 365**  
Export data from Microsoft Dynamics CRM organization to an external destination

- Click **Access Azure Service Management as organization users** and then click **Add permissions**.



## Request API permissions

[← All APIs](#)



Azure Service Management

<https://management.azure.com/> [Docs](#) [↗](#)

What type of permissions does your application require?

### Delegated permissions

Your application needs to access the API as the signed-in user.

### Application permissions

Your application runs as a background service or daemon without a signed-in user.

Select permissions

[expand all](#)

| Type to search   |                        |
|--|------------------------|
| PERMISSION   | ADMIN CONSENT REQUIRED |
| <input checked="" type="checkbox"/> <b>user_impersonation</b><br>Access Azure Service Management as organization users (preview) ⓘ | -                      |

## Get the application ID and directory ID

When you create the Connector from BlueXP, you need to provide the application (client) ID and the directory (tenant) ID for the application. BlueXP uses the IDs to programmatically sign in.

### Steps

1. In the **Azure Active Directory** service, click **App registrations** and select the application.
2. Copy the **Application (client) ID** and the **Directory (tenant) ID**.



## Create a client secret

You need to create a client secret and then provide BlueXP with the value of the secret so BlueXP can use it to authenticate with Azure AD.

### Steps

1. Open the **Azure Active Directory** service.
2. Click **App registrations** and select your application.
3. Click **Certificates & secrets > New client secret**.

4. Provide a description of the secret and a duration.
5. Click **Add**.
6. Copy the value of the client secret.

### Client secrets

A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.

[+ New client secret](#)

| DESCRIPTION | EXPIRES   | VALUE                            | Copy to clipboard |
|-------------|-----------|----------------------------------|-------------------|
| test secret | 8/16/2020 | *sZ1jSe2By:D*-ZRoV4NLfdAcY7:+0vA |                   |

### Result

Your service principal is now setup and you should have copied the application (client) ID, the directory (tenant) ID, and the value of the client secret. You need to enter this information in BlueXP when you create the Connector.

### Create the Connector by logging in with the service principal

BlueXP enables you to create a Connector in Azure directly from its user interface.

### What you'll need

- An Azure subscription.
- A VNet and subnet in your Azure region of choice.
- Details about a proxy server, if your organization requires a proxy for all outgoing internet traffic:
  - IP address
  - Credentials
  - HTTPS certificate
- If you don't want BlueXP to automatically create an Azure role for the Connector, then you'll need to create your own [using the policy on this page](#).

These permissions are for the Connector instance itself. It's a different set of permissions than what you previously set up to simply deploy the Connector.

### Steps

1. If you're creating your first Working Environment, click **Add Working Environment** and follow the prompts. Otherwise, click the **Connector** drop-down and select **Add Connector**.



2. Choose **Microsoft Azure** as your cloud provider.
3. On the **Deploying a Connector** page:
  - a. Under **Authentication**, click **Active Directory service principal** and enter information about the Azure Active Directory service principal that grants the required permissions:
    - Application (client) ID: See [Get the application ID and directory ID](#).
    - Directory (tenant) ID: See [Get the application ID and directory ID](#).
    - Client Secret: See [Create a client secret](#).
  - b. Click **Log in**.
  - c. You now have two options:
    - Click **Continue** to prepare for deployment by using the in-product guide. Each step in the in-product guide includes the information that's contained on this page of the documentation.
    - Click **Skip to Deployment** if you already prepared by following the steps on this page.
4. Follow the steps in the wizard to create the Connector:
  - **VM Authentication:** Choose an Azure subscription, a location, a new resource group or an existing resource group, and then choose an authentication method.
  - **Details:** Enter a name for the instance, specify tags, and choose whether you want BlueXP to create a new role that has the required permissions, or if you want to select an existing role that you set up with [the required permissions](#).

Note that you can choose the subscriptions associated with this role. Each subscription that you choose provides the Connector with permissions to deploy Cloud Volumes ONTAP in those subscriptions.

  - **Network:** Choose a VNet and subnet, whether to enable a public IP address, and optionally specify a proxy configuration.
  - **Security Group:** Choose whether to create a new security group or whether to select an existing security group that allows inbound HTTP, HTTPS, and SSH access.
  - **Review:** Review your selections to verify that your set up is correct.
5. Click **Add**.

The virtual machine should be ready in about 7 minutes. You should stay on the page until the process is complete.

## After you finish

You need to associate a Connector with workspaces so Workspace Admins can use those Connectors to create Cloud Volumes ONTAP systems. If you only have Account Admins, then associating the Connector with workspaces isn't required. Account Admins have the ability to access all workspaces in BlueXP by default. [Learn more](#).

If you have Azure Blob storage in the same Azure account where you created the Connector, you'll see an Azure Blob working environment appear on the Canvas automatically. [Learn more about what you can do with this working environment](#).

## Open port 3128 for AutoSupport messages

If you plan to deploy Cloud Volumes ONTAP systems in a subnet where an outbound internet connection won't be available, then BlueXP automatically configures Cloud Volumes ONTAP to use the Connector as a proxy server.

The only requirement is to ensure that the Connector's security group allows *inbound* connections over port 3128. You'll need to open this port after you deploy the Connector.

If you use the default security group for Cloud Volumes ONTAP, then no changes are needed to its security group. But if you plan to define strict outbound rules for Cloud Volumes ONTAP, then you'll also need to ensure that the Cloud Volumes ONTAP security group allows *outbound* connections over port 3128.

## Create a Connector in Google Cloud from BlueXP

A BlueXP Account Admin needs to deploy a *Connector* before you can use most BlueXP features. [Learn when a Connector is required](#). The Connector enables BlueXP to manage resources and processes within your public cloud environment.

This page describes how to create a Connector in Google Cloud directly from BlueXP. [Learn about other ways to deploy a Connector](#).

These steps must be completed by a user who has the Account Admin role. A Workspace Admin can't create a Connector.



When you create your first Cloud Volumes ONTAP working environment, BlueXP will prompt you to create a Connector if you don't have one yet.

## Quick start

Get started quickly by following these steps, or scroll down to the remaining sections for full details.

### 1

#### Set up permissions

- Ensure that your Google Cloud account has the correct permissions by creating and attaching a custom role.

[Set up permissions to deploy the Connector](#).

- When you create the Connector VM, you need to associate it with a service account. This service account must have a custom role that has permissions to manage resources in Google Cloud.

[Set up a service account for the Connector.](#)

- If you're deploying Cloud Volumes ONTAP across projects, ensure that the Connector has access to those projects.

[Set up permissions across projects.](#)

- If you're using a shared VPC, set up permissions in the service project and host project.

[Set up shared VPC permissions.](#)

2

## Set up networking

You'll need a VPC and subnet with outbound internet access to specific endpoints. If a proxy server is required for outbound internet, then you'll need the IP address, credentials, and HTTPS certificate.

[View networking requirements.](#)

3

## Enable Google Cloud APIs

- Cloud Deployment Manager V2 API
- Cloud Logging API
- Cloud Resource Manager API
- Compute Engine API
- Identity and Access Management (IAM) API

4

## Create the Connector

Click the Connector drop-down, select **Add Connector** and follow the prompts.

[Follow step-by-step instructions.](#)

## Set up permissions

Permissions are required for the following:

- The user who will deploy the Connector VM
- A service account that you need to attach to the Connector VM during deployment

Depending on your configuration, you might need to complete the following steps as well:

- Set up permissions across projects
- Set up permissions for a shared VPC

## Set up permissions to deploy the Connector

Before you can deploy a Connector, you need to ensure that your Google Cloud account has the correct permissions.

## Steps

1. [Create a custom role](#) that includes the following permissions:

```
title: Connector deployment policy
description: Permissions for the user who deploys the Connector from
BlueXP
stage: GA
includedPermissions:
- 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
- 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.list
```

2. Attach the custom role to the user who will deploy the Connector from BlueXP.

## Result

The Google Cloud user now has the permissions required to create the Connector.

## Set up a service account for the Connector

A service account is required to provide the Connector with the permission that it needs to manage resources in Google Cloud. You'll associate this service account with the Connector VM when you create it.

The permissions for the service account are different than the permissions that you set up in the previous section.

## Steps

1. [Create a custom role](#) that includes the following permissions:

```
title: NetApp BlueXP
description: Permissions for the service account associated with the
Connector instance.
stage: GA
includedPermissions:
- iam.serviceAccounts.actAs
- compute.regionBackendServices.create
- compute.regionBackendServices.get
- compute.regionBackendServices.list
- compute.networks.updatePolicy
- compute.backendServices.create
- compute.addresses.list
```

- `compute.disks.create`
- `compute.disks.createSnapshot`
- `compute.disks.delete`
- `compute.disks.get`
- `compute.disks.list`
- `compute.disks.setLabels`
- `compute.disks.use`
- `compute.firewalls.create`
- `compute.firewalls.delete`
- `compute.firewalls.get`
- `compute.firewalls.list`
- `compute.globalOperations.get`
- `compute.images.get`
- `compute.images.getFromFamily`
- `compute.images.list`
- `compute.images.useReadOnly`
- `compute.instances.addAccessConfig`
- `compute.instances.attachDisk`
- `compute.instances.create`
- `compute.instances.delete`
- `compute.instances.detachDisk`
- `compute.instances.get`
- `compute.instances.getSerialPortOutput`
- `compute.instances.list`
- `compute.instances.setDeletionProtection`
- `compute.instances.setLabels`
- `compute.instances.setMachineType`
- `compute.instances.setMetadata`
- `compute.instances.setTags`
- `compute.instances.start`
- `compute.instances.stop`
- `compute.instances.updateDisplayDevice`
- `compute.instanceGroups.get`
- `compute.addresses.get`
- `compute.instances.updateNetworkInterface`
- `compute.machineTypes.get`
- `compute.networks.get`
- `compute.networks.list`
- `compute.projects.get`
- `compute.regions.get`
- `compute.regions.list`
- `compute.snapshots.create`
- `compute.snapshots.delete`
- `compute.snapshots.get`
- `compute.snapshots.list`
- `compute.snapshots.setLabels`



- compute.subnetworks.get
- compute.subnetworks.list
- compute.subnetworks.use
- compute.subnetworks.useExternalIp
- compute.zoneOperations.get
- compute.zones.get
- compute.zones.list
- compute.instances.setServiceAccount
- deploymentmanager.compositeTypes.get
- deploymentmanager.compositeTypes.list
- deploymentmanager.deployments.create
- deploymentmanager.deployments.delete
- deploymentmanager.deployments.get
- deploymentmanager.deployments.list
- deploymentmanager.manifests.get
- deploymentmanager.manifests.list
- deploymentmanager.operations.get
- deploymentmanager.operations.list
- deploymentmanager.resources.get
- deploymentmanager.resources.list
- deploymentmanager.typeProviders.get
- deploymentmanager.typeProviders.list
- deploymentmanager.types.get
- deploymentmanager.types.list
- logging.logEntries.list
- logging.privateLogEntries.list
- resourcemanager.projects.get
- storage.buckets.create
- storage.buckets.delete
- storage.buckets.get
- storage.buckets.list
- cloudkms.cryptoKeyVersions.useToEncrypt
- cloudkms.cryptoKeys.get
- cloudkms.cryptoKeys.list
- cloudkms.keyRings.list
- storage.buckets.update
- iam.serviceAccounts.getIamPolicy
- iam.serviceAccounts.list
- storage.objects.get
- storage.objects.list
- monitoring.timeSeries.list
- storage.buckets.getIamPolicy
- cloudkms.cryptoKeys.getIamPolicy
- cloudkms.cryptoKeys.setIamPolicy
- cloudkms.keyRings.get
- cloudkms.keyRings.getIamPolicy

```
- cloudkms.keyRings.setIamPolicy
```

2. Create a Google Cloud service account and apply the custom role that you just created.
3. If you want to deploy Cloud Volumes ONTAP in other projects, [grant access by adding the service account with the BlueXP role to that project](#). You'll need to repeat this step for each project.

## Result

The service account for the Connector VM is set up.

## Set up permissions across projects

If you plan to deploy Cloud Volumes ONTAP systems in different projects than the project where the Connector resides, then you'll need to provide the Connector's service account with access to those projects.

For example, let's say the Connector is in project 1 and you want to create Cloud Volumes ONTAP systems in project 2. You'll need to grant access to the service account in project 2.

## Steps

1. In the Google Cloud console, go to the IAM service and select the project where you want to create Cloud Volumes ONTAP systems.
2. On the **IAM** page, select **Grant Access** and provide the required details.
  - Enter the email of the Connector's service account.
  - Select the Connector's custom role.
  - Click **Save**.

For more details, refer to [Google Cloud documentation](#)

## Set up shared VPC permissions

If you are using a shared VPC to deploy resources into a service project, then the following permissions are required. This table is for reference and your environment should reflect the permissions table when IAM configuration is complete.

| Identity                                    | Creator | Hosted in       | Service project permissions   | Host project permissions   | Purpose   |
|---|---------|-----------------|---|--|---|
| Google account used to deploy the Connector | Custom  | Service Project | <ul style="list-style-type: none"><li>• <a href="#">The permissions found in this section above</a></li></ul> | <ul style="list-style-type: none"><li>• compute.networkUser</li></ul>                                    | Deploying the Connector in the service project                                    |
| Connector service account                   | Custom  | Service project | <ul style="list-style-type: none"><li>• <a href="#">The permissions found in this section above</a></li></ul> | <ul style="list-style-type: none"><li>• compute.networkUser</li><li>• deploymentmanager.editor</li></ul> | Deploying and maintaining Cloud Volumes ONTAP and services in the service project |

| Identity                                      | Creator      | Hosted in       | Service project permissions  | Host project permissions  | Purpose   |
|---|--------------|-----------------|--|---|---|
| Cloud Volumes ONTAP service account           | Custom       | Service project | <ul style="list-style-type: none"> <li>storage.admin</li> <li>member: BlueXP service account as serviceAccount.user</li> </ul> | N/A   | (Optional) For data tiering and Cloud Backup  |
| Google APIs service agent                     | Google Cloud | Service project | <ul style="list-style-type: none"> <li>(Default) Editor</li> </ul>   | <ul style="list-style-type: none"> <li>compute.networkUser</li> </ul> | Interacts with Google Cloud APIs on behalf of deployment. Allows BlueXP to use the shared network.                          |
| Google Compute Engine default service account | Google Cloud | Service project | <ul style="list-style-type: none"> <li>(Default) Editor</li> </ul>   | <ul style="list-style-type: none"> <li>compute.networkUser</li> </ul> | Deploys Google Cloud instances and compute infrastructure on behalf of deployment. Allows BlueXP to use the shared network. |

#### Notes:

1. deploymentmanager.editor is only required at the host project if you are not passing firewall rules to the deployment and are choosing to let BlueXP create them for you. BlueXP will create a deployment in the host project which contains the VPC0 firewall rule if no rule is specified.
2. firewall.create and firewall.delete are only required if you are not passing firewall rules to the deployment and are choosing to let BlueXP create them for you. These permissions reside in the BlueXP account .yaml file. If you are deploying an HA pair using a shared VPC, these permissions will be used to create the firewall rules for VPC1, 2 and 3. For all other deployments, these permissions will also be used to create rules for VPC0.
3. For data tiering, the tiering service account must have the serviceAccount.user role on the service account, not just at the project level. Currently if you assign serviceAccount.user at the project level, the permissions don't show when you query the service account with getIAMPolicy.

## Set up networking

Set up your networking so the Connector can manage resources and processes within your public cloud environment. Other than having a virtual network and subnet for the Connector, you'll need to ensure that the following requirements are met.

### Connection to target networks


A Connector requires a network connection to the type of working environment that you're creating and the services that you're planning to enable.

For example, if you install a Connector in your corporate network, then you must set up a VPN connection to the virtual network in which you launch Cloud Volumes ONTAP.

### Outbound internet access

The Connector requires outbound internet access to manage resources and processes within your public cloud

environment.

| Endpoints  | Purpose   |
|--|---|
| <a href="https://www.googleapis.com/compute/v1/">https://www.googleapis.com/compute/v1/</a><br><a href="https://cloudresourcemanager.googleapis.com/v1/projects">https://cloudresourcemanager.googleapis.com/v1/projects</a><br><a href="https://www.googleapis.com/compute/beta">https://www.googleapis.com/compute/beta</a><br><a href="https://storage.googleapis.com/storage/v1">https://storage.googleapis.com/storage/v1</a><br><a href="https://www.googleapis.com/storage/v1">https://www.googleapis.com/storage/v1</a><br><a href="https://iam.googleapis.com/v1">https://iam.googleapis.com/v1</a><br><a href="https://cloudkms.googleapis.com/v1">https://cloudkms.googleapis.com/v1</a><br><a href="https://www.googleapis.com/deploymentmanager/v2/projects">https://www.googleapis.com/deploymentmanager/v2/projects</a> | To manage resources in Google Cloud.  |
| <a href="https://support.netapp.com">https://support.netapp.com</a>  | To obtain licensing information and to send AutoSupport messages to NetApp support.   |
| <a href="https://*.api.bluelxp.netapp.com">https://*.api.bluelxp.netapp.com</a><br><a href="https://api.bluelxp.netapp.com">https://api.bluelxp.netapp.com</a><br><a href="https://*.cloudmanager.cloud.netapp.com">https://*.cloudmanager.cloud.netapp.com</a><br><a href="https://cloudmanager.cloud.netapp.com">https://cloudmanager.cloud.netapp.com</a>   | To provide SaaS features and services within BlueXP.<br><br> The Connector is currently contacting "cloudmanager.cloud.netapp.com" but it will start contacting "api.bluelxp.netapp.com" in an upcoming release. |
| <a href="https://cloudmanagerinfraprod.azurecr.io">https://cloudmanagerinfraprod.azurecr.io</a><br><a href="https://*.blob.core.windows.net">https://*.blob.core.windows.net</a>   | To upgrade the Connector and its Docker components.   |

### Proxy server

If your organization requires deployment of a proxy server for all outgoing internet traffic, obtain the following information about your HTTP or HTTPS proxy:

- IP address
- Credentials
- HTTPS certificate

### Security group

There's no incoming traffic to the Connector, unless you initiate it or if the Connector is used as a proxy for AutoSupport messages. HTTP and HTTPS provide access to the [local UI](#), which you'll use in rare circumstances. SSH is only needed if you need to connect to the host for troubleshooting.

### IP address limitation

There's a possible conflict with IP addresses in the 172 range. [Learn more about this limitation.](#)

### Enable Google Cloud APIs

Several APIs are required to deploy the Connector and Cloud Volumes ONTAP.

### Step

1. [Enable the following Google Cloud APIs in your project.](#)

- Cloud Deployment Manager V2 API
- Cloud Logging API
- Cloud Resource Manager API
- Compute Engine API
- Identity and Access Management (IAM) API

### **Create a Connector**

Create a Connector in Google Cloud directly from the BlueXP user interface or by using gcloud.

## BlueXP

1. If you're creating your first Working Environment, click **Add Working Environment** and follow the prompts. Otherwise, click the **Connector** drop-down and select **Add Connector**.



2. Choose **Google Cloud Platform** as your cloud provider.
3. On the **Deploying a Connector** page, review the details about what you'll need. You have two options:
  - a. Click **Continue** to prepare for deployment by using the in-product guide. Each step in the in-product guide includes the information that's contained on this page of the documentation.
  - b. Click **Skip to Deployment** if you already prepared by following the steps on this page.
4. Follow the steps in the wizard to create the Connector:
  - If you're prompted, log in to your Google account, which should have the required permissions to create the virtual machine instance.

The form is owned and hosted by Google. Your credentials are not provided to NetApp.

- **Details:** Enter a name for the virtual machine instance, specify tags, select a project, and then select the service account that has the required permissions (refer to the section above for details).
  - **Location:** Specify a region, zone, VPC, and subnet for the instance.
  - **Network:** Choose whether to enable a public IP address and optionally specify a proxy configuration.
  - **Firewall Policy:** Choose whether to create a new firewall policy or whether to select an existing firewall policy that allows inbound HTTP, HTTPS, and SSH access.
  - **Review:** Review your selections to verify that your set up is correct.
5. Click **Add**.

The instance should be ready in about 7 minutes. You should stay on the page until the process is complete.

## gcloud

1. Log in to the gcloud SDK using your preferred methodology.

In our examples, we'll use a local shell with the gcloud SDK installed, but you could use the native

Google Cloud Shell in the Google Cloud console.

For more information about the Google Cloud SDK, visit the [Google Cloud SDK documentation page](#).

2. Verify that you are logged in as a user who has the required permissions that are defined in the section above:

```
gcloud auth list
```

The output should show the following where the \* user account is the desired user account to be logged in as:

```
Credentialed Accounts
ACTIVE ACCOUNT
    some_user_account@domain.com
*    desired_user_account@domain.com
To set the active account, run:
$ gcloud config set account `ACCOUNT`
Updates are available for some Cloud SDK components. To install
them,
please run:
$ gcloud components update
```

3. Run the `gcloud compute instances create` command:

```
gcloud compute instances create <instance-name>
  --machine-type=n2-standard-4
  --image-project=netapp-cloudmanager
  --image-family=cloudmanager
  --scopes=cloud-platform
  --project=<project>
  --service-account=<service-account>
  --zone=<zone>
  --no-address
  --tags <network-tag>
  --network <network-path>
  --subnet <subnet-path>
  --boot-disk-kms-key <kms-key-path>
```

**instance-name**

The desired instance name for the VM instance.

**project**

(Optional) The project where you want to deploy the VM.

**service-account**

The service account specified in the output from step 2.

**zone**

The zone where you want to deploy the VM

**no-address**

(Optional) No external IP address is used (you need a cloud NAT or proxy to route traffic to the public internet)

**network-tag**

(Optional) Add network tagging to link a firewall rule using tags to the Connector instance

**network-path**

(Optional) Add the name of the network to deploy the Connector into (for a Shared VPC, you need the full path)

**subnet-path**

(Optional) Add the name of the subnet to deploy the Connector into (for a Shared VPC, you need the full path)

**kms-key-path**

(Optional) Add a KMS key to encrypt the Connector's disks (IAM permissions also need to be applied)

For more information about these flags, visit the [Google Cloud compute SDK documentation](#).

Running the command deploys the Connector using the NetApp golden image. The Connector instance and software should be running in approximately five minutes.

4. Open a web browser from a host that has a connection to the Connector instance and enter the following URL:

`https://ipaddress`

5. After you log in, set up the Connector:
  - a. Specify the NetApp account to associate with the Connector.

[Learn about NetApp accounts](#).

- b. Enter a name for the system.

**Result**

The Connector is now installed and set up with your NetApp account. BlueXP will automatically use this Connector when you create new working environments. But if you have more than one Connector, you'll need to [switch between them](#).

If you have Google Cloud Storage buckets in the same Google Cloud account where you created the Connector, you'll see a Google Cloud Storage working environment appear on the Canvas automatically. [Learn more about what you can do with this working environment](#).



## Open port 3128 for AutoSupport messages

If you plan to deploy Cloud Volumes ONTAP systems in a subnet where an outbound internet connection won't be available, then BlueXP automatically configures Cloud Volumes ONTAP to use the Connector as a proxy server.

The only requirement is to ensure that the Connector's security group allows *inbound* connections over port 3128. You'll need to open this port after you deploy the Connector.

If you use the default security group for Cloud Volumes ONTAP, then no changes are needed to its security group. But if you plan to define strict outbound rules for Cloud Volumes ONTAP, then you'll also need to ensure that the Cloud Volumes ONTAP security group allows *outbound* connections over port 3128.

## Create a Connector in a Government region

If you are operating in a Government region, you need to deploy a Connector from your cloud provider's marketplace or by manually installing the Connector software on an existing Linux host. You can't deploy the Connector in a Government region from BlueXP's SaaS website.

Use one of the following links to view instructions for creating a Connector:

- [Create a Connector from the AWS Marketplace](#)
- [Create a Connector and Cloud Volumes ONTAP in the AWS C2S environment](#)
- [Create a Connector from the Azure Marketplace](#)
- [Install a Connector on your own Linux host](#)

For manual installations on your own Linux host, you must use the "online" installer to install the Connector on a host that has internet access. A separate "offline" installer is available for the Connector, but it's only supported with on-prem sites that don't have internet access. It's not supported with Government regions.

After you deploy the Connector, you can access BlueXP by opening your web browser and connecting to the IP address of the Connector instance: `https://ipaddress`

Since the Connector was deployed in a Government region, it's not accessible from <https://console.bluexp.netapp.com>.

## Where to go next

Now that you've logged in and set up BlueXP, users can start creating and discovering working environments.

- [Azure NetApp Files](#)
- [Amazon FSx for ONTAP](#)
- [Cloud Volumes ONTAP for AWS](#)
- [Cloud Volumes ONTAP for Azure](#)
- [Cloud Volumes ONTAP for Google Cloud](#)
- [Cloud Volumes Service for Google Cloud](#)

- E-Series systems
- Kubernetes clusters
- On-premises ONTAP clusters
- StorageGRID systems

# Administer BlueXP

## NetApp accounts

### Managing your NetApp account

After you perform initial setup, you can administer your account settings later by managing users, service accounts, workspaces, and Connectors.

[Learn more about how NetApp accounts work.](#)

### Managing your account with the Tenancy API

If you want to manage your account settings by sending API requests, then you'll need to use the *Tenancy* API. This API is different than the BlueXP API, which you use to create and manage Cloud Volumes ONTAP working environments.

[View endpoints for the Tenancy API](#)

### Creating and managing users

The user's in your account can access the manage the resources in your account's workspaces.

#### Adding users

Associate users with your NetApp account so those users can create and manage working environments in BlueXP.

#### Steps

1. If the user hasn't already done so, ask the user to go to [NetApp BlueXP website](#) and sign up.
2. From the top of BlueXP, click the **Account** drop-down.



3. Click **Manage Account** next to the currently selected account.



4. From the Members tab, click **Associate User**.
5. Enter the user's email address and select a role for the user:
  - **Account Admin**: Can perform any action in BlueXP.
  - **Workspace Admin**: Can create and manage resources in assigned workspaces.
  - **Compliance Viewer**: Can only view Cloud Data Sense compliance information and generate reports for workspaces that they have permission to access.
  - **SnapCenter Admin**: Can use the SnapCenter Service to create application consistent backups and restore data using those backups. *This service is currently in Beta.*
6. If you selected Workspace Admin or Compliance Viewer, select one or more workspaces to associate with that user.



## Associate User

To add a user to your NetApp Cloud Account, that user must already have signed up at [NetApp Cloud Central](#). Enter the email address that they used when signing up with Cloud Central.

User's Email

Role

Associate User to Workspaces

Cancel

Associate User

7. Click **Associate**.

### Result

The user should receive an email from NetApp BlueXP titled "Account Association." The email includes the information needed to access BlueXP.

### Removing users

Disassociating a user makes it so they can no longer access the resources in a NetApp account.

### Steps

1. From the top of BlueXP, click the **Account** drop-down and click **Manage Account**.



2. From the Members tab, click the action menu in the row that corresponds to the user.



3. Click **Disassociate User** and click **Disassociate** to confirm.

## Result

The user can no longer access the resources in this NetApp account.

## Managing a Workspace Admin's workspaces

You can associate and disassociate Workspace Admins with workspaces at any time. Associating the user enables them to create and view the working environments in that workspace.

## Steps

1. From the top of BlueXP, click the **Account** drop-down and click **Manage Account**.



2. From the Members tab, click the action menu in the row that corresponds to the user.

| 5 Members |      |       |                 |                |     |  |
|-----------|------|-------|-----------------|----------------|-----|--|
| Type      | Name | Email | Role            | Workspace      |     |  |
|           | Ben  |       | ☆ Account Admin | All Workspaces | ... |  |
|           | Tom  |       | ☆ Account Admin | All Workspaces | ... |  |
|           | Ben  |       | Workspace Admin | Newone         |     |  |

3. Click **Manage Workspaces**.

4. Select the workspaces to associate with the user and click **Apply**.

## Result

The user can now access those workspaces from BlueXP, as long as the Connector was also associated with the workspaces.

## Creating and managing service accounts

A service account acts as a "user" that can make authorized API calls to BlueXP for automation purposes. This makes it easier to manage automation because you don't need to build automation scripts based on a real person's user account who can leave the company at any time. And if you're using federation, you can create a token without generating a refresh token from the cloud.

You give permissions to a service account by assigning it a role, just like any other BlueXP user. You can also associate the service account with specific workspaces in order to control the working environments (resources) that the service can access.

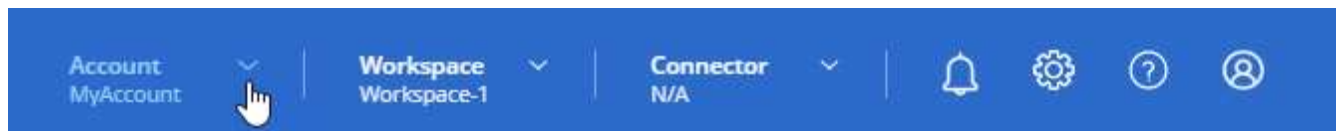
When you create the service account, BlueXP enables you to copy or download a client ID and client secret for the service account. This key pair is used for authentication with BlueXP.

### Creating a service account

Create as many service accounts as you need to manage the resources in your working environments.

### Steps

1. From the top of BlueXP, click the **Account** drop-down.



2. Click **Manage Account** next to the currently selected account.



3. From the Members tab, click **Create Service Account**.
4. Enter a name and select a role. If you chose a role other than Account Admin, choose the workspace to associate with this service account.
5. Click **Create**.
6. Copy or download the client ID and client secret.

The client secret is visible only once and is not stored anywhere by BlueXP. Copy or download the secret and store it safely.

7. Click **Close**.

#### Obtaining a bearer token for a service account

In order to make API calls to the [Tenancy API](#), you'll need to obtain a bearer token for a service account.

[Learn how to create a service account token](#)

#### Copying the client ID

You can copy a service account's client ID at any time.

#### Steps

1. From the Members tab, click the action menu in the row that corresponds to the service account.



2. Click **Client ID**.
3. The ID is copied to your clipboard.



## Recreating keys

Recreating the key will delete the existing key for this service account and then create a new key. You won't be able to use the previous key.

### Steps

1. From the Members tab, click the action menu in the row that corresponds to the service account.



2. Click **Recreate Key**.
3. Click **Recreate** to confirm.
4. Copy or download the client ID and client secret.

The client secret is visible only once and is not stored anywhere by BlueXP. Copy or download the secret and store it safely.

5. Click **Close**.

## Deleting a service account

Delete a service account if you no longer need to use it.

### Steps

1. From the Members tab, click the action menu in the row that corresponds to the service account.



2. Click **Delete**.
3. Click **Delete** again to confirm.

## Managing workspaces

Manage your workspaces by creating, renaming, and deleting them. Note that you can't delete a workspace if it contains any resources. It must be empty.

## Steps

1. From the top of BlueXP, click the **Account** drop-down and click **Manage Account**.
2. Click **Workspaces**.
3. Choose one of the following options:
  - Click **Add New Workspace** to create a new workspace.
  - Click **Rename** to rename the workspace.
  - Click **Delete** to delete the workspace.

## Managing a Connector's workspaces

You need to associate the Connector with workspaces so Workspace Admins can access those workspaces from BlueXP.

If you only have Account Admins, then associating the Connector with workspaces isn't required. Account Admins have the ability to access all workspaces in BlueXP by default.

[Learn more about users, workspaces, and Connectors.](#)

## Steps

1. From the top of BlueXP, click the **Account** drop-down and click **Manage Account**.
2. Click **Connector**.
3. Click **Manage Workspaces** for the Connector that you want to associate.
4. Select the workspaces to associate with the Connector and click **Apply**.

## Changing your account name

Change your account name at any time to change it to something meaningful for you.

## Steps

1. From the top of BlueXP, click the **Account** drop-down and click **Manage Account**.
2. In the **Overview** tab, click the edit icon next to the account name.
3. Type a new account name and click **Save**.

## Allowing private previews

Allow private previews in your account to get access to new NetApp cloud services that are made available as a preview in BlueXP.

Services in private preview are not guaranteed to behave as expected and might sustain outages and be missing functionality.

## Steps

1. From the top of BlueXP, click the **Account** drop-down and click **Manage Account**.
2. In the **Overview** tab, enable the **Allow Private Preview** setting.

## Allowing third-party services

Allow third-party services in your account to get access to third-party services that are available in BlueXP. Third-party services are cloud services similar to the services that NetApp offers, but they're managed and

supported by third-party companies.

**Steps**

1. From the top of BlueXP, click the **Account** drop-down and click **Manage Account**.
2. In the **Overview** tab, enable the **Allow Third Party Services** setting.

**Disabling the SaaS platform**

We don't recommend disabling the SaaS platform unless you need to in order to comply with your company's security policies. Disabling the SaaS platform limits your ability to use NetApp's integrated cloud services.

The following services aren't available from BlueXP if you disable the SaaS platform:

- Cloud Backup

Cloud Backup is supported in Government regions when the SaaS platform is disabled, but not in commercial regions when the SaaS platform is disabled

- Cloud Data Sense
- Kubernetes
- Cloud Tiering
- Global File Cache

If you do disable the SaaS platform, you'll need to perform all tasks from [the local user interface that is available on a Connector](#).



This is an irreversible action that will prevent you from using the BlueXP SaaS platform. You'll need to perform actions from the local Connector. You won't have the ability to use many of NetApp's integrated cloud services, and re-enabling the SaaS platform will require the help of NetApp support.

**Steps**

1. From the top of BlueXP, click the **Account** drop-down and click **Manage Account**.
2. In the Overview tab, toggle the option to disable use of the SaaS platform.

**Monitoring operations in your account**

You can monitor the status of the operations that BlueXP is performing to see if there are any issues that you need to address. You can view the status in the Notification Center, in the Timeline, or have notifications sent to your email.


This table provides a comparison of the Notification Center and the Timeline so you can understand what each has to offer.

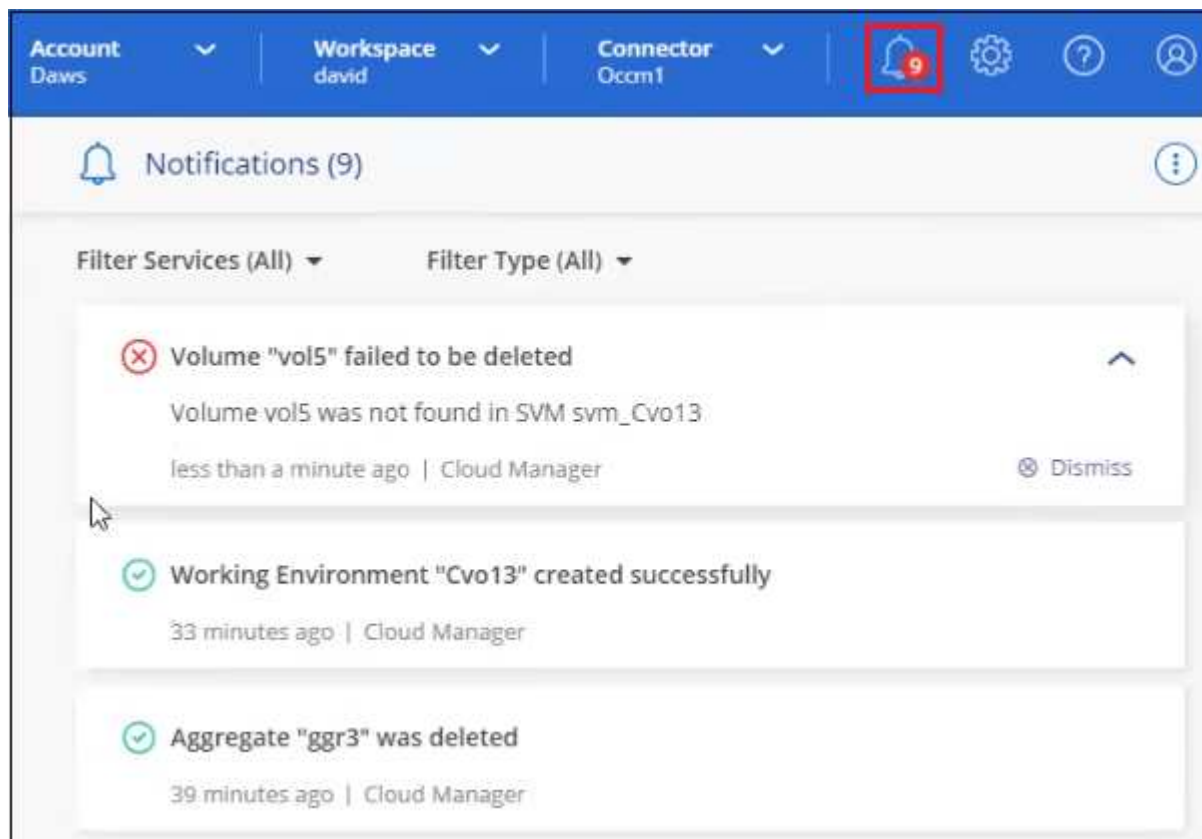
| Notification Center                            | Timeline  |
|--|---|
| Shows high level status for events and actions | Provides details for each event or action for further investigation |

| Notification Center  | Timeline  |
|--|---|
| Shows status for the current login session - the information won't appear in the Notification Center after you log off | Retains status for the last month                             |
| Shows only actions initiated in the user interface   | Shows all actions from the UI or APIs                         |
| Shows user-initiated actions   | Shows all actions, whether user-initiated or system-initiated |
| Filter results by importance   | Filter by service, action, user, status, and more             |
| Provides the ability to email notifications to Account users and to others   | No email capability   |

## Monitoring activities using the Notification Center

Notifications track the progress of operations that you've initiated in BlueXP so you can verify whether the operation was successful or not. They enable you to view the status for many BlueXP actions that you initiated during your current login session. Not all services report information into the Notification Center at this time.

You can display the notifications by clicking the notification bell  in the menu bar. The color of the little bubble in the bell indicates the highest level severity notification that is active. So if you see a red bubble, it means there's an important notification that you should look at.



You can also configure BlueXP to send notifications by email so you can be informed of important system activity even when you're not logged into the system. Emails can be sent to any users who are part of your NetApp Cloud Account, or to any other recipients who need to be aware of certain types of system activity. See [Setting email notification settings](#) below.

## Notification types

Notifications are classified in the following categories:

| Notification type | Description   |
|-------------------|---|
| Critical          | A problem occurred that might lead to service disruption if corrective action is not taken immediately.   |
| Error             | An action or process ended with failure, or could lead to failure if corrective action is not taken.  |
| Warning           | An issue that you should be aware of to make sure it does not reach the critical severity. Notifications of this severity do not cause service disruption, and immediate corrective action might not be required. |
| Recommendation    | A system recommendation for you to take an action to improve the system or a certain service; for example: costs saving, suggestion for new services, recommended security configuration, etc.                    |
| Information       | A message that provides additional information about an action or process.  |
| Success           | An action or process completed successfully.  |

## Filtering notifications

By default you'll see all notifications. You can filter the notifications that you see in the Notification Center to show only those notifications that are important to you. You can filter by BlueXP "Service" and by notification "Type".

The image shows a user interface for filtering notifications. It consists of two side-by-side panels, each with a title and a list of items with checkboxes, and buttons at the bottom.

**Filter Services (All) ▲**

- ☒ Digital Wallet (3)
- ☒ Active IQ (2)
- ☐ AppTemplate (1)

**Clear** **Apply**

**Filter Type (All) ▲**

- ☐ Information (0)
- ☐ Success (1)
- ☒ Warning (2)
- ☒ Error (1)
- ☒ Critical (0)
- ☐ Recommendation (0)

**Clear** **Apply**

For example, if you want to see only "Error" and "Warning" notifications for BlueXP operations, select those entries and you'll see only those types of notifications.

## Setting email notification settings

You can send specific types of notifications by email so you can be informed of important system activity even when you're not logged into BlueXP. Emails can be sent to any users who are part of your NetApp Account, or

to any other recipients who need to be aware of certain types of system activity.



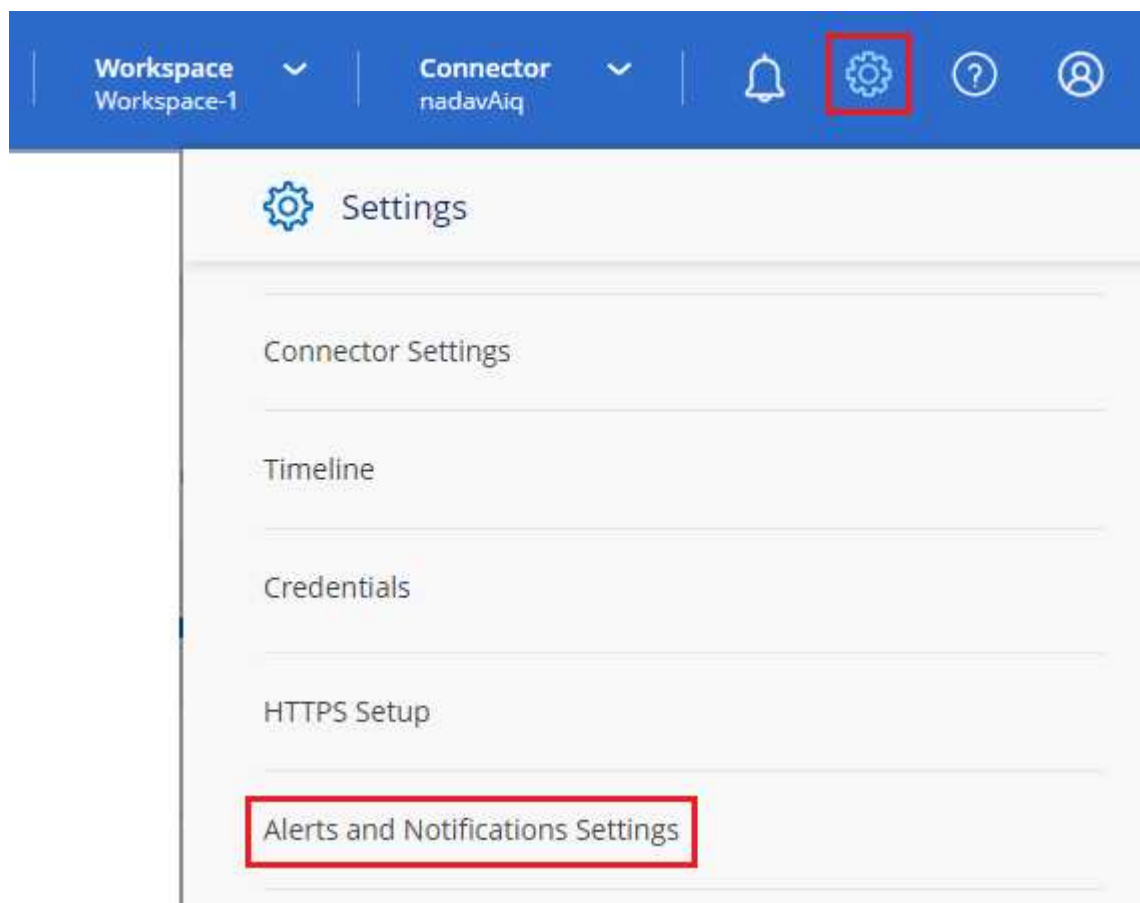
- At this time, notifications are sent by email for the following BlueXP features and services: Connectors, Cloud Sync, Cloud Backup, and Ransomware Protection. Additional services will be added in future releases.
- Sending email notifications is not supported when the Connector is installed in a site without internet access.

By default, BlueXP Account Admins will receive emails for all "Critical" and "Recommendation" notifications. All other users and recipients are configured, by default, not to receive any notification emails.

You must be an Account Admin to customize the notifications settings.

### Steps

1. From the BlueXP menu bar, click **Settings > Alerts and Notifications Settings**.



2. Select a user, or multiple users, from either the *Account Users* tab or the *Additional Recipients* tab, and choose the type of notifications to be sent:
  - To make changes for a single user, click the menu in the Notifications column for that user, check the types of Notifications to be sent, and click **Apply**.
  - To make changes for multiple users, check the box for each user, click **Manage Email Notifications**, check the types of Notifications to be sent, and click **Apply**.

| Email  | Name    | Role            |
|--|---------|-----------------|
| <input type="checkbox"/> Sabar@netapp.com                  | Sabar V | Account Admin   |
| <input checked="" type="checkbox"/> activeiq@netapp-st.com | nadav   | Account Admin   |
| <input checked="" type="checkbox"/> nand@netapp.com        | AnanK   | Account Admin   |
| <input type="checkbox"/> apra@netapp.com                   | Aradev  | Workspace Admin |
| <input type="checkbox"/> ash@netapp.com                    | AshG    | Account Admin   |

☒ Critical  
☐ Recommendation  
☐ Info  
☐ Warning  
☒ Error

Clear Apply

### Adding additional email recipients

The users who appear in the *Account Users* tab are populated automatically from the users in your NetApp Account (from the [Manage Account page](#)). You can add email addresses in the *Additional Recipients* tab for other people, or groups, who do not have access to BlueXP, but who need to be notified about certain types of alerts and notifications.

### Steps

1. From the Alerts and Notifications Settings page, click **Add New Recipients**.

### Add New Recipient

Email: saul.jenkin@gmail.com

Name: Saul Jenkin

Notification Type: Critical Recommendation Error

Add New Recipient Cancel

2. Enter the name, email address, and select the types of Notifications that recipient will receive, and click **Add New Recipient**.

### Dismissing notifications

You can remove notifications from the page if you no longer need to see them. You can dismiss all notifications at once, or you can dismiss individual notifications.

To dismiss all notifications, in the Notification Center, click and select **Dismiss All**.



To dismiss individual notifications, hover your cursor over the notification and click **Dismiss**.



## Auditing user activity in your account

The Timeline in BlueXP shows the actions that users completed to manage your account. This includes management actions such as associating users, creating workspaces, creating Connectors, and more.

Checking the Timeline can be helpful if you need to identify who performed a specific action, or if you need to identify the status of an action.

### Steps

1. From the BlueXP menu bar, click **Settings > Timeline**.
2. Under the Filters, click **Service**, enable **Tenancy**, and click **Apply**.

### Result

The Timeline updates to show you account management actions.

## Roles

The Account Admin, Workspace Admin, Compliance Viewer, and SnapCenter Admin roles provide specific permissions to users.

The Compliance Viewer role is for read-only Cloud Data Sense access.

| Task                                    | Account Admin | Workspace Admin | Compliance Viewer | SnapCenter Admin |
|---|---------------|-----------------|-------------------|------------------|
| Manage working environments             | Yes           | Yes             | No                | No               |
| Enable services on working environments | Yes           | Yes             | No                | No               |
| View data replication status            | Yes           | Yes             | No                | No               |
| View the timeline                       | Yes           | Yes             | No                | No               |
| Switch between workspaces               | Yes           | Yes             | Yes               | No               |



| Task  | Account Admin | Workspace Admin | Compliance Viewer | SnapCenter Admin |
|---|---------------|-----------------|-------------------|------------------|
| View Data Sense scan results                        | Yes           | Yes             | Yes               | No               |
| Delete working environments                         | Yes           | No              | No                | No               |
| Connect Kubernetes clusters to working environments | Yes           | No              | No                | No               |
| Receive the Cloud Volumes ONTAP report              | Yes           | No              | No                | No               |
| Create Connectors                                   | Yes           | No              | No                | No               |
| Manage NetApp accounts                              | Yes           | No              | No                | No               |
| Manage credentials                                  | Yes           | No              | No                | No               |
| Modify BlueXP settings                              | Yes           | No              | No                | No               |
| View and manage the Support Dashboard               | Yes           | No              | No                | No               |
| Remove working environments from BlueXP             | Yes           | No              | No                | No               |
| Install an HTTPS certificate                        | Yes           | No              | No                | No               |
| Use the SnapCenter Service                          | Yes           | Yes             | No                | Yes              |

#### Related links

- [Setting up workspaces and users in the NetApp account](#)
- [Managing workspaces and users in the NetApp account](#)

## Connectors

### Advanced deployment

#### Create a Connector from the AWS Marketplace

For an AWS commercial region, it's best to create a Connector directly from BlueXP, but you can launch a Connector from the AWS Marketplace, if you prefer. For AWS Government regions, you can't deploy the Connector in a Government region from the BlueXP SaaS website, so the next best option is to do so from the AWS Marketplace.



You can also download and install the Connector software on an existing Linux host in your network or in the cloud. [Learn how to install the Connector on an existing Linux host.](#)

## Create the Connector in an AWS commercial region

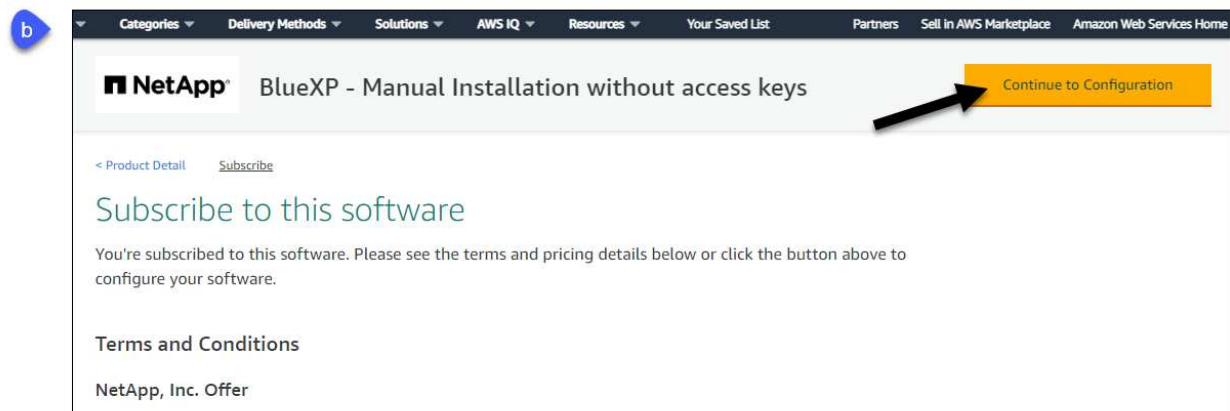
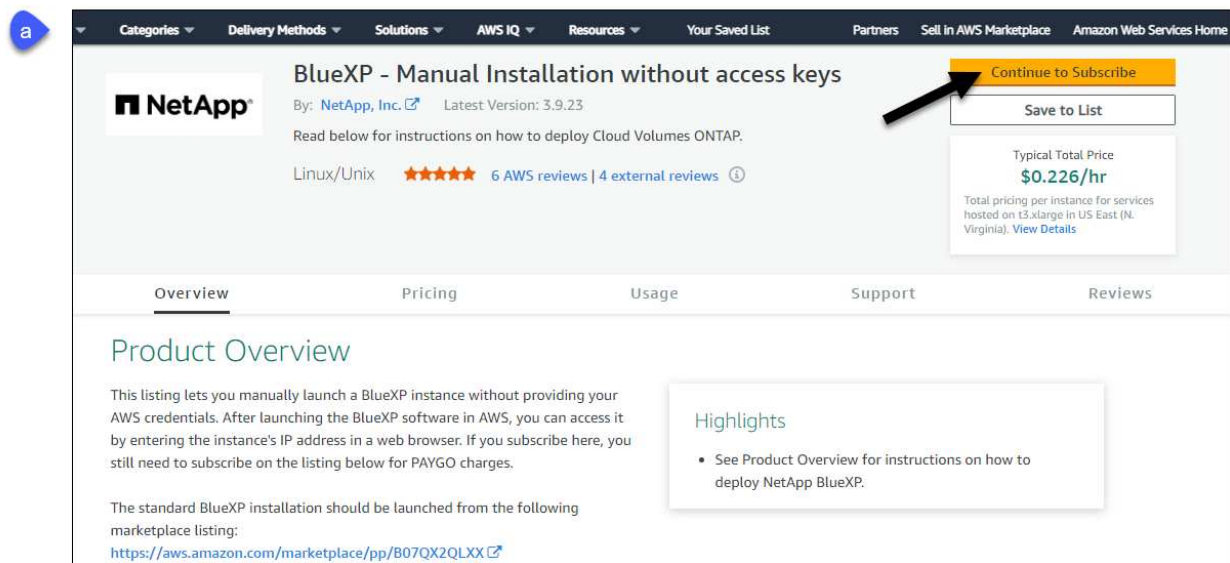
You can launch the Connector instance in an AWS commercial region directly from the AWS Marketplace offering for BlueXP.

### Before you get started

The IAM user who creates the Connector must have AWS Marketplace permissions to subscribe and unsubscribe.

### Steps

1. Set up permissions in AWS:
  - a. From the IAM console, create the required policies by copying and pasting the contents of [the IAM policies for the Connector](#).
  - b. Create an IAM role with the role type Amazon EC2 and attach the policies that you created in the previous step to the role.
2. Go to the [BlueXP page on the AWS Marketplace](#) to deploy the Connector from an AMI:
3. On the Marketplace page, click **Continue to Subscribe** and then click **Continue to Configuration**.



4. Change any of the default options and click **Continue to Launch**.
5. Under **Choose Action**, select **Launch through EC2** and then click **Launch**.

These steps describe how to launch the instance from the EC2 Console because the console enables you to attach an IAM role to the Connector instance. This isn't possible using the **Launch from Website** action.

6. Follow the prompts to configure and deploy the instance:

- **Name and tags:** Enter a name and tags for the instance.
- **Application and OS Image:** Skip this section. The Connector AMI is already selected.
- **Instance type:** Depending on region availability, choose one of the supported instance types (t3.xlarge is recommended).

[Review the instance requirements.](#)

- **Key pair (login):** Select the key pair that you want to use to securely connect to the instance.
- **Network settings:** Edit the network settings as needed:
  - Choose the desired VPC and subnet.
  - Specify whether the instance should have a public IP address.
  - Specify firewall settings that enable the required connection methods for the Connector instance: SSH, HTTP, and HTTPS.
- **Configure storage:** Keep the default storage options.
- **Advanced details:** Under **IAM instance profile**, choose the IAM role that you created in step 1.
- **Summary:** Review the summary and click **Launch instance**.

AWS launches the software with the specified settings. The Connector instance and software should be running in approximately five minutes.

7. Open a web browser from a host that has a connection to the Connector instance and enter the following URL:

`https://ipaddress`

8. After you log in, set up the Connector:

- a. Specify the NetApp account to associate with the Connector.

[Learn about NetApp accounts.](#)

- b. Enter a name for the system.

9. Open a web browser and go to <https://console.bluexp.netapp.com> to start using the Connector with BlueXP.

## Result

The Connector is now installed and set up with your NetApp account. BlueXP will automatically use this Connector when you create new working environments. But if you have more than one Connector, you'll need to [switch between them](#).

If you have Amazon S3 buckets in the same AWS account where you created the Connector, you'll see an Amazon S3 working environment appear on the Canvas automatically. [Learn more about what you can do with this working environment.](#)

## Create the Connector in an AWS Government region

To deploy the Connector in an AWS Government region, you need to go to the EC2 service and select the BlueXP offering from the AWS Marketplace.

### Steps

1. Set up permissions in AWS:
  - a. From the IAM console, create your own policy by copying and pasting the contents of [the IAM policy for the Connector](#).
  - b. Create an IAM role with the role type Amazon EC2 and attach the policy that you created in the previous step to the role.
2. Go to the BlueXP offering in the AWS Marketplace.

The IAM user must have AWS Marketplace permissions to subscribe and unsubscribe.

- a. Open the EC2 service and select **Launch instance**.
- b. Select **AWS Marketplace**.
- c. Search for BlueXP and select the offering.



- d. Click **Continue**.
3. Follow the prompts to configure and deploy the instance:
    - **Choose an Instance Type:** Depending on region availability, choose one of the supported instance types (t3.xlarge is recommended).
- [Review the instance requirements.](#)
- **Configure Instance Details:** Select a VPC and subnet, choose the IAM role that you created in step 1, enable termination protection (recommended), and choose any other configuration options that meet your requirements.

|                               |   |   |
|-------------------------------|---|---|
| Number of instances           | 1   | <a href="#">Launch into Auto Scaling Group</a>  |
| Purchasing option             | <input type="checkbox"/> Request Spot instances   |   |
| Network                       | vpc-a76d91c2   VPC4QA (default)   | <a href="#">Create new VPC</a>                  |
| Subnet                        | subnet-39536c13   QASubnet1   us-east-1b<br>155 IP Addresses available                                      | <a href="#">Create new subnet</a>               |
| Auto-assign Public IP         | Enable  |   |
| Placement group               | <input type="checkbox"/> Add instance to placement group  |   |
| Capacity Reservation          | Open  | <a href="#">Create new Capacity Reservation</a> |
| IAM role                      | Cloud_Manager   | <a href="#">Create new IAM role</a>             |
| CPU options                   | <input type="checkbox"/> Specify CPU options  |   |
| Shutdown behavior             | Stop  |   |
| Enable termination protection | <input checked="" type="checkbox"/> Protect against accidental termination                                  |   |
| Monitoring                    | <input type="checkbox"/> Enable CloudWatch detailed monitoring<br><a href="#">Additional charges apply.</a> |   |

- **Add Storage:** Keep the default storage options.
- **Add Tags:** Enter tags for the instance, if desired.
- **Configure Security Group:** Specify the required connection methods for the Connector instance: SSH, HTTP, and HTTPS.
- **Review:** Review your selections and click **Launch**.

AWS launches the software with the specified settings. The Connector instance and software should be running in approximately five minutes.

4. Open a web browser from a host that has a connection to the Connector instance and enter the following URL:

`https://ipaddress`

5. After you log in, set up the Connector:
  - a. Specify the NetApp account to associate with the Connector.

[Learn about NetApp accounts.](#)

- b. Enter a name for the system.

## Result

The Connector is now installed and set up with your NetApp account.

Any time that you want to use BlueXP, open your web browser and connect to the IP address of the Connector instance: `https://ipaddress`

Since the Connector was deployed in a Government region, it's not accessible from <https://console.bluexp.netapp.com>.

## Open port 3128 for AutoSupport messages

If you plan to deploy Cloud Volumes ONTAP systems in a subnet where an outbound internet connection won't be available, then BlueXP automatically configures Cloud Volumes ONTAP to use the Connector as a proxy server.

The only requirement is to ensure that the Connector's security group allows *inbound* connections over port 3128. You'll need to open this port after you deploy the Connector.

If you use the default security group for Cloud Volumes ONTAP, then no changes are needed to its security group. But if you plan to define strict outbound rules for Cloud Volumes ONTAP, then you'll also need to ensure that the Cloud Volumes ONTAP security group allows *outbound* connections over port 3128.

## Create a Connector from the Azure Marketplace

For an Azure commercial region, it's best to create a Connector directly from BlueXP, but you can launch a Connector from the Azure Marketplace, if you prefer. For Azure Government regions, you can't deploy the Connector in a Government region from the BlueXP SaaS website, so the next best option is to do so from the Azure Marketplace.



You can also download and install the Connector software on an existing Linux host in your network or in the cloud. [Learn how to install the Connector on an existing Linux host.](#)

## Creating a Connector in Azure

Deploy the Connector in Azure using the image in the Azure Marketplace and then log in to the Connector to specify your NetApp account.

### Steps

1. Go to the NetApp Connector VM page in the Azure Marketplace.
  - [Azure Marketplace page for commercial regions](#)
  - [Azure Marketplace page for Azure Government regions](#)
2. Click **Get it now** and then click **Continue**.
3. From the Azure portal, click **Create** and follow the steps to configure the virtual machine.

Note the following as you configure the VM:

- The Connector can perform optimally with either HDD or SSD disks.
- Choose a VM size that meets CPU and RAM requirements. We recommend DS3 v2.

[Review the VM requirements.](#)

- For the network security group, the Connector requires inbound connections using SSH, HTTP, and HTTPS.

[Learn more about security group rules for the Connector.](#)

- Under **Management**, enable **System assigned managed identity** for the Connector by selecting **On**.

This setting is important because a managed identity allows the Connector virtual machine to identify itself to Azure Active Directory without providing any credentials. [Learn more about managed identities](#)

for [Azure resources](#).

4. On the **Review + create** page, review your selections and click **Create** to start the deployment.

Azure deploys the virtual machine with the specified settings. The virtual machine and Connector software should be running in approximately five minutes.

5. Open a web browser from a host that has a connection to the Connector virtual machine and enter the following URL:

`https://ipaddress`

6. After you log in, set up the Connector:

- a. Specify the NetApp account to associate with the Connector.

[Learn about NetApp accounts](#).

- b. Enter a name for the system.

## Result

The Connector is now installed and set up with your NetApp account.

If the Connector is in an Azure commercial region, open a web browser and go to <https://console.blueexp.netapp.com> to start using the Connector with BlueXP.

If the Connector is in an Azure Government region, you can use BlueXP by opening your web browser and connecting to the IP address of the Connector instance: `https://ipaddress`

Since the Connector was deployed in a Government region, it's not accessible from <https://console.blueexp.netapp.com>.

## Granting Azure permissions

When you deployed the Connector in Azure, you should have enabled a [system-assigned managed identity](#). You must now grant the required Azure permissions by creating a custom role and then by assigning the role to the Connector virtual machine for one or more subscriptions.

## Steps

1. Create a custom role:
  - a. Copy the contents of the [custom role permissions for the Connector](#) and save them in a JSON file.
  - b. Modify the JSON file by adding Azure subscription IDs to the assignable scope.

You should add the ID for each Azure subscription from which users will create Cloud Volumes ONTAP systems.

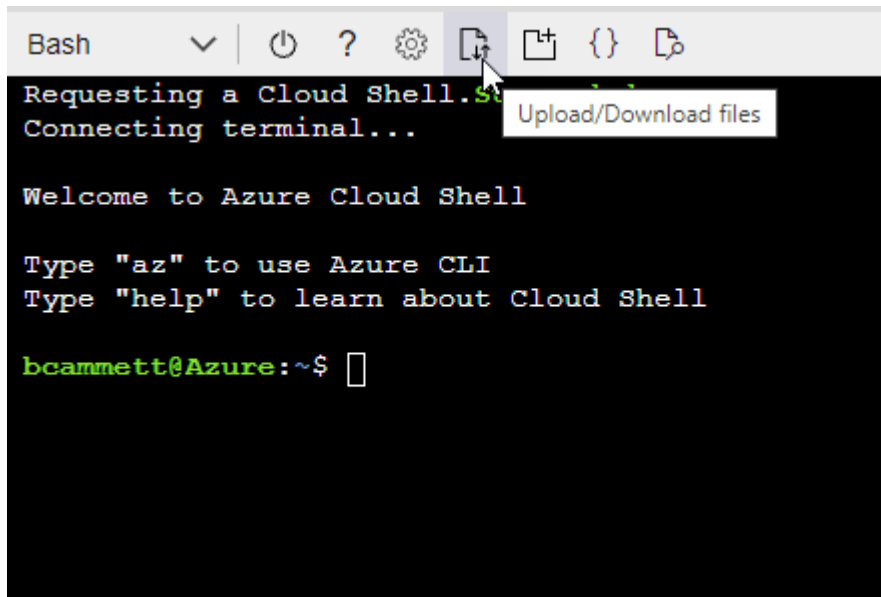
## Example

```
"AssignableScopes": [  
  "/subscriptions/d333af45-0d07-4154-943d-c25fbzzzzzzz",  
  "/subscriptions/54b91999-b3e6-4599-908e-416e0zzzzzzz",  
  "/subscriptions/398e471c-3b42-4ae7-9b59-ce5bbzzzzzzz"
```

- c. Use the JSON file to create a custom role in Azure.

The following steps describe how to create the role by using Bash in Azure Cloud Shell.

- Start [Azure Cloud Shell](#) and choose the Bash environment.
- Upload the JSON file.



- Use the Azure CLI to create the custom role:

```
az role definition create --role-definition Connector_Policy.json
```

You should now have a custom role called BlueXP Operator that you can assign to the Connector virtual machine.

2. Assign the role to the Connector virtual machine for one or more subscriptions:

- a. Open the **Subscriptions** service and then select the subscription in which you want to deploy Cloud Volumes ONTAP systems.
- b. Click **Access control (IAM) > Add > Add role assignment**.
- c. In the **Role** tab, select the **BlueXP Operator** role and click **Next**.



BlueXP Operator is the default name provided in the BlueXP policy. If you chose a different name for the role, then select that name instead.

- d. In the **Members** tab, complete the following steps:

- Assign access to a **Managed identity**.
- Click **Select members**, select the subscription in which the Connector virtual machine was created, choose **Virtual machine**, and then select the Connector virtual machine.
- Click **Select**.
- Click **Next**.

- e. Click **Review + assign**.



- f. If you want to deploy Cloud Volumes ONTAP from additional subscriptions, switch to that subscription and then repeat these steps.

## Result

The Connector now has the permissions that it needs to manage resources and processes within your public cloud environment. BlueXP will automatically use this Connector when you create new working environments. But if you have more than one Connector, you'll need to [switch between them](#).

If you have Azure Blob storage in the same Azure account where you created the Connector, you'll see an Azure Blob working environment appear on the Canvas automatically. [Learn more about what you can do with this working environment](#).

## Open port 3128 for AutoSupport messages

If you plan to deploy Cloud Volumes ONTAP systems in a subnet where an outbound internet connection won't be available, then BlueXP automatically configures Cloud Volumes ONTAP to use the Connector as a proxy server.

The only requirement is to ensure that the Connector's security group allows *inbound* connections over port 3128. You'll need to open this port after you deploy the Connector.

If you use the default security group for Cloud Volumes ONTAP, then no changes are needed to its security group. But if you plan to define strict outbound rules for Cloud Volumes ONTAP, then you'll also need to ensure that the Cloud Volumes ONTAP security group allows *outbound* connections over port 3128.

## Install the Connector on an existing Linux host that has internet access

The most common way to create a Connector is directly from BlueXP or from a cloud provider's marketplace. But you have the option to download and install the Connector software on an existing Linux host in your network or in the cloud. These steps are specific to hosts that have internet access.

[Learn about other ways to deploy a Connector](#).



If you want to create a Cloud Volumes ONTAP system in Google Cloud, then you must have a Connector that's running in Google Cloud as well. You can't use a Connector that's running in AWS, Azure, or on-prem.

## Verify host requirements

The Connector software must run on a host that meets specific operating system requirements, RAM requirements, port requirements, and so on.

### A dedicated host is required

The Connector is not supported on a host that is shared with other applications. The host must be a dedicated host.

### CPU

4 cores or 4 vCPUs

### RAM

14 GB

### **AWS EC2 instance type**

An instance type that meets the CPU and RAM requirements above. We recommend t3.xlarge.

### **Azure VM size**

An instance type that meets the CPU and RAM requirements above. We recommend DS3 v2.

### **GCP machine type**

An instance type that meets the CPU and RAM requirements above. We recommend n2-standard-4.

The Connector is supported in Google Cloud on a VM instance with an OS that supports [Shielded VM features](#)

### **Supported operating systems**

- CentOS 7.6
- CentOS 7.7
- CentOS 7.8
- CentOS 7.9
- Red Hat Enterprise Linux 7.6
- Red Hat Enterprise Linux 7.7
- Red Hat Enterprise Linux 7.8
- Red Hat Enterprise Linux 7.9
- Red Hat Enterprise Linux 8.6

The Red Hat Enterprise Linux system must be registered with Red Hat Subscription Management. If it is not registered, the system cannot access repositories to update required 3rd party software during Connector installation.

The Connector is supported on English-language versions of these operating systems.

### **Hypervisor**

A bare metal or hosted hypervisor that is certified to run CentOS or Red Hat Enterprise Linux [Red Hat Solution: Which hypervisors are certified to run Red Hat Enterprise Linux?](#)

### **Disk space in /opt**

100 GiB of space must be available

### **Disk space in /var**

20 GiB of space must be available

### **Docker Engine**

Docker Engine version 19.3.1 or later is required on the host before you install the Connector. [View installation instructions](#)

### **Outbound internet access**

The installer for the Connector must access the following URLs during the installation process:

- <https://support.netapp.com>
- <https://mysupport.netapp.com>

- <https://cloudmanager.cloud.netapp.com/tenancy>
- <https://stream.cloudmanager.cloud.netapp.com>
- <https://cloudmanagerinfraprod.azurecr.io>
- <https://production-artifacts.cloudmanager.cloud.netapp.com>
- [https://\\*.blob.core.windows.net](https://*.blob.core.windows.net)

The host might try to update operating system packages during installation. The host can contact different mirroring sites for these OS packages.

## Install the Connector

After you verify that you have a supported Linux host, you can obtain the Connector software and then install it.

### What you'll need

- Root privileges to install the Connector.
- Details about a proxy server, if a proxy is required for internet access from the Connector. HTTP and HTTPS are supported.

You have the option to configure a proxy server after installation but doing so requires restarting the Connector.

- A CA-signed certificate, if the proxy server uses HTTPS.

### About this task

- The installation installs the AWS command line tools (awscli) to enable recovery procedures from NetApp support.

If you receive a message that installing the awscli failed, you can safely ignore the message. The Connector can operate successfully without the tools.

- The installer that is available on the NetApp Support Site might be an earlier version. After installation, the Connector automatically updates itself if a new version is available.

### Steps

1. Verify that docker is enabled and running.

```
sudo systemctl enable docker && sudo systemctl start docker
```

2. If the `http_proxy` or `https_proxy` system variables are set on the host, remove them:

```
unset http_proxy
unset https_proxy
```

If you don't remove these system variables, the installation will fail.

3. Download the Connector software from the [NetApp Support Site](#), and then copy it to the Linux host.

You should download the Connector installer that's meant for use in your network or in the cloud.

#### 4. Assign permissions to run the script.

```
chmod +x OnCommandCloudManager-V3.9.23
```

#### 5. Run the installation script.

```
./OnCommandCloudManager-V3.9.23 --proxy <HTTP or HTTPS proxy server>  
--cacert <path and file name of a CA-signed certificate>
```

The `--proxy` and `--cacert` parameters are optional. If you have a proxy server, you will need to enter the parameter(s) as shown. The installer doesn't prompt you to provide information about a proxy.

Here's an example of the command using both optional parameters:

```
./OnCommandCloudManager-V3.9.23 --proxy  
https://user:password@10.0.0.30:8080/ --cacert  
/tmp/cacert/certificate.cer
```

`--proxy` configures the Connector to use an HTTP or HTTPS proxy server using one of the following formats:

- `http://address:port`
- `http://username:password@address:port`
- `https://address:port`
- `https://username:password@address:port`

`--cacert` specifies a CA-signed certificate to use for HTTPS access between the Connector and the proxy server. This parameter is required only if you specify an HTTPS proxy server.

### Result

The Connector is now installed. At the end of the installation, the Connector service (occm) restarts twice if you specified a proxy server.

### Set up the Connector

Sign up or log in and then set up the Connector to work with your account.

### Steps

1. Open a web browser and enter the following URL:

`https://ipaddress`

*ipaddress* can be localhost, a private IP address, or a public IP address, depending on the configuration of the host. For example, if the Connector is in the public cloud without a public IP address, you must enter a private IP address from a host that has a connection to the Connector host.

2. Sign up or log in.

3. If you installed the Connector in Google Cloud, set up a service account that has the permissions that BlueXP needs to create and manage Cloud Volumes ONTAP systems in projects.
  - a. [Create a role in GCP](#) that includes the permissions defined in the [Connector policy for GCP](#).
  - b. [Create a GCP service account and apply the custom role that you just created](#).
  - c. [Associate this service account with the Connector VM](#).
  - d. If you want to deploy Cloud Volumes ONTAP in other projects, [grant access by adding the service account with the BlueXP role to that project](#). You'll need to repeat this step for each project.
4. After you log in, set up BlueXP:
  - a. Specify the NetApp account to associate with the Connector.  
  
[Learn about NetApp accounts](#).
  - b. Enter a name for the system.

## Result

The Connector is now installed and set up with your NetApp account. BlueXP will automatically use this Connector when you create new working environments.

## After you finish

Set up permissions so BlueXP can manage resources and processes within your public cloud environment:

- AWS: [Set up an AWS account and then add it to BlueXP](#)
- Azure: [Set up an Azure account and then add it to BlueXP](#)
- Google Cloud: See step 3 above

## Install the Connector on-prem without internet access

You can install the Connector on an on-premises Linux host that doesn't have internet access. You can then discover on-prem ONTAP clusters, replicate data between them, back up volumes using Cloud Backup, and scan them with Cloud Data Sense.

These installation instructions are specifically for the use case described above. [Learn about other ways to deploy a Connector](#).

## Verify host requirements

The Connector software must run on a host that meets specific operating system requirements, RAM requirements, port requirements, and so on.

## A dedicated host is required

The Connector is not supported on a host that is shared with other applications. The host must be a dedicated host.

## CPU

4 cores or 4 vCPUs

## RAM

14 GB

## Supported operating systems

- CentOS 7.6
- CentOS 7.7
- CentOS 7.8
- CentOS 7.9
- Red Hat Enterprise Linux 7.6
- Red Hat Enterprise Linux 7.7
- Red Hat Enterprise Linux 7.8
- Red Hat Enterprise Linux 7.9
- Red Hat Enterprise Linux 8.6

The Red Hat Enterprise Linux system must be registered with Red Hat Subscription Management. If it is not registered, the system cannot access repositories to update required 3rd party software during Connector installation.

The Connector is supported on English-language versions of these operating systems.

## Hypervisor

A bare metal or hosted hypervisor that is certified to run CentOS or Red Hat Enterprise Linux  
[Red Hat Solution: Which hypervisors are certified to run Red Hat Enterprise Linux?](#)

## Disk type

An SSD is required

## Disk space in /opt

100 GiB of space must be available

## Disk space in /var

20 GiB of space must be available

## Docker Engine

Docker Engine version 19 or later is required on the host before you install the Connector. [View installation instructions](#)

## Install the Connector

After you verify that you have a supported Linux host, you can obtain the Connector software and then install it.

## Required privileges

Root privileges are required to install the Connector.

## Steps

1. Verify that docker is enabled and running.

```
sudo systemctl enable docker && sudo systemctl start docker
```

2. Download the Connector software from the [NetApp Support Site](#)

3. Copy the installer to the Linux host.
4. Assign permissions to run the script.

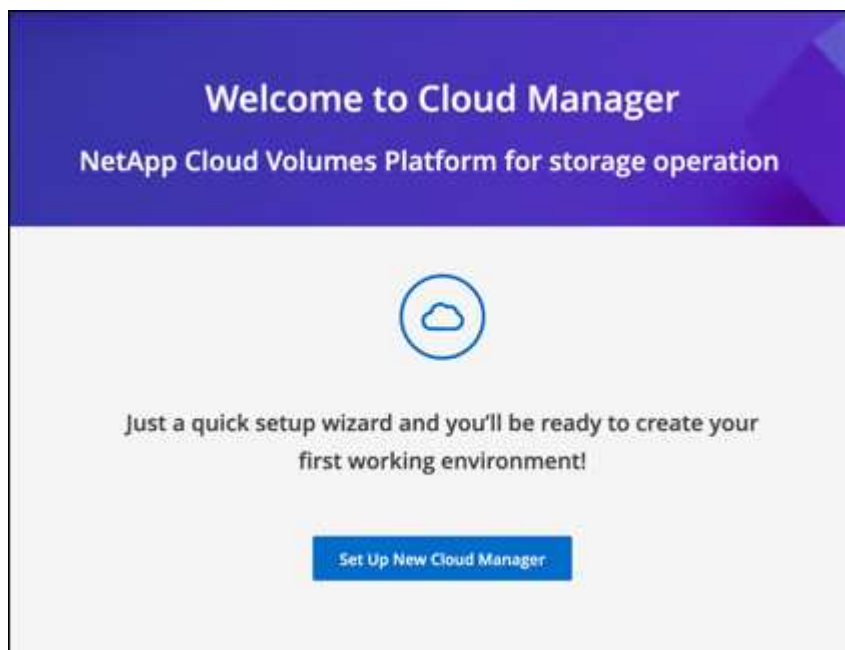
```
chmod +x /path/cloud-manager-connector-offline-v3.9.23
```

5. Run the installation script:

```
sudo /path/cloud-manager-connector-offline-v3.9.23
```

6. Open a web browser and enter `https://ipaddress` where *ipaddress* is the IP address of the Linux host.

You should see the following screen.



7. Click **Set Up New BlueXP** and follow the prompts to set up the system.
  - **System Details:** Enter a name for the Connector and your company name.

- **Create Admin User:** Create the admin user for the system.

This user account runs locally on the system. There's no connection to the auth0 service available through BlueXP.

- **Review:** Review the details, accept the license agreement, and then click **Set Up**.

8. Log in to BlueXP using the admin user that you just created.

## Result

The Connector is now installed and you can start using the BlueXP features that are available in a dark site deployment.

## What's next?

- [Discover on-prem ONTAP clusters](#)
- [Replicate data between on-prem ONTAP clusters](#)
- [Back up on-prem ONTAP volume data to StorageGRID using Cloud Backup](#)
- [Scan on-prem ONTAP volume data using Cloud Data Sense](#)

When new versions of the Connector software are available, they'll be posted to the NetApp Support Site. [Learn how to upgrade the Connector.](#)

## Finding the system ID for a Connector

To help you get started, your NetApp representative might ask you for the system ID for a Connector. The ID is typically used for licensing and troubleshooting purposes.

## Steps

1. In the upper right of the BlueXP console, click the Help icon.
2. Click **Support > Connector**.

The system ID appears at the top.

## Example





## Managing existing Connectors

After you create one or more Connectors, you can manage them by switching between Connectors, connecting to the local user interface running on a Connector, and more.

### Switch between Connectors

If you have multiple Connectors, you can switch between them to see the Working Environments that are associated with a specific Connector.

For example, let's say that you're working in a multi-cloud environment. You might have one Connector in AWS and another in Google Cloud. You'd need to switch between those Connectors to manage the Cloud Volumes ONTAP systems running in those clouds.

### Step

1. Click the **Connector** drop-down, select another Connector, and then click **Switch**.



BlueXP refreshes and shows the Working Environments associated with the selected Connector.

## Access the local UI

While you should perform almost all tasks from the SaaS user interface, a local user interface is still available on the Connector. If you're accessing BlueXP from a Government region or a site that doesn't have outbound internet access, then you need to use the local user interface running on the Connector.

### Steps

1. Open a web browser and enter the following URL:

`https://ipaddress`

*ipaddress* can be localhost, a private IP address, or a public IP address, depending on the configuration of the host. For example, if the Connector is in the public cloud without a public IP address, you must enter a private IP address from a host that has a connection to the Connector host.

2. Enter your user name and password to log in.

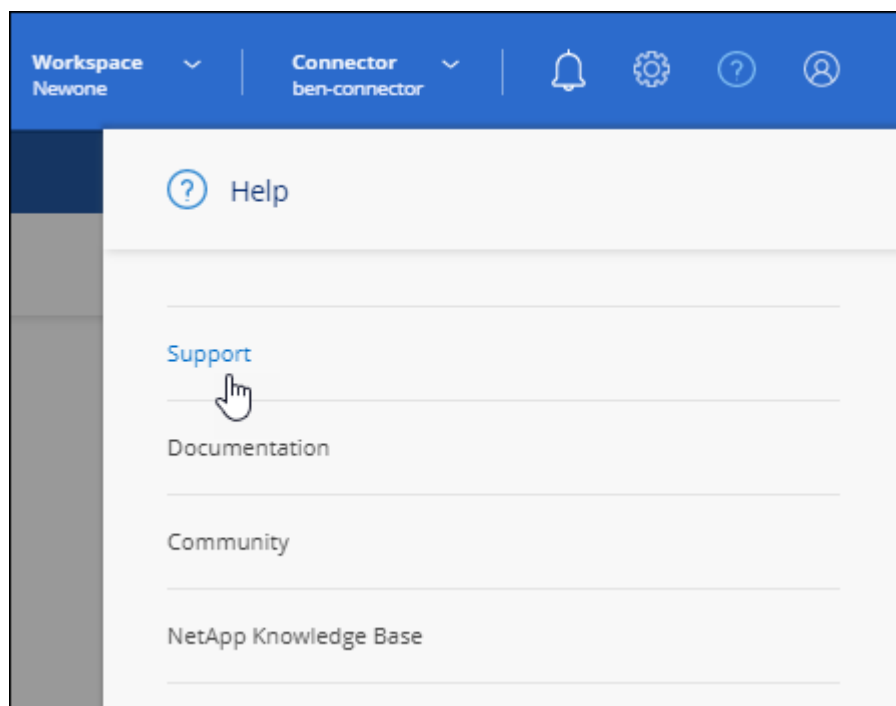
## Download or send an AutoSupport message

If you're having problems, NetApp personnel might ask you to send an AutoSupport message to NetApp support for troubleshooting purposes.

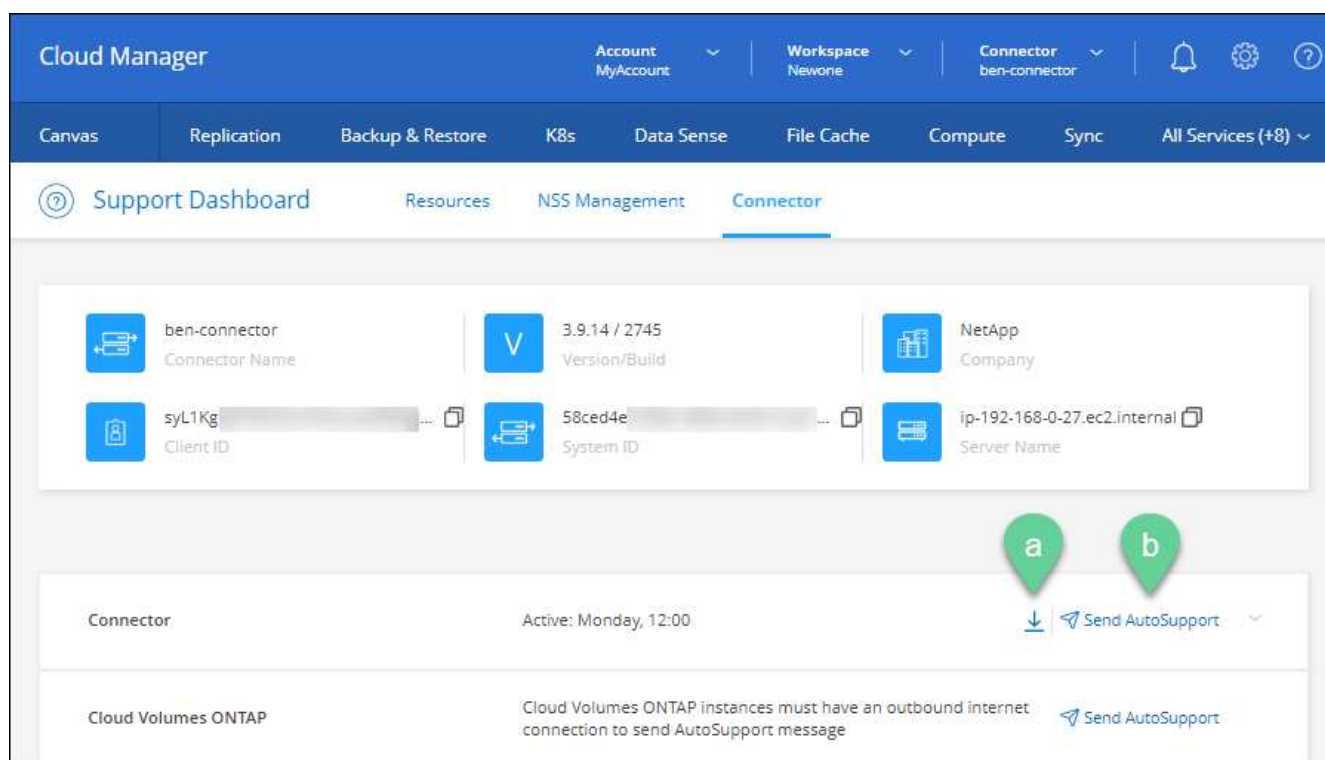
### Steps

1. Connect to the Connector local UI, as described in the section above.

2. In the upper right of the BlueXP console, click the Help icon, and select **Support**.



3. Click **Connector**.
4. Depending on how you need to send the information to NetApp support, choose one of the following options:
  - a. Select the option to download the AutoSupport message to your local machine. You can then send it to NetApp Support using a preferred method.
  - b. Click **Send AutoSupport** to directly send the message to NetApp Support.



## Connect to the Linux VM

If you need to connect to the Linux VM that the Connector runs on, you can do so by using the connectivity options available from your cloud provider.

### AWS

When you created the Connector instance in AWS, you provided an AWS access key and secret key. You can use this key pair to SSH to the instance.

[AWS Docs: Connect to your Linux instance](#)

### Azure

When you created the Connector VM in Azure, you chose to authenticate with a password or SSH public key. Use the authentication method that you chose to connect to the VM.

[Azure Docs: SSH into your VM](#)

### Google Cloud

You can't specify an authentication method when you create a Connector in Google Cloud. However, you can connect to the Linux VM instance using the Google Cloud Console or Google Cloud CLI (gcloud).

[Google Cloud Docs: Connect to Linux VMs](#)

## Apply security updates

Update the operating system on the Connector to ensure that it's patched with the latest security updates.

### Steps

1. Access the CLI shell on the Connector host.
2. Run the following commands with elevated privileges:

```
sudo -s
service netapp-service-manager stop
yum -y update --security
service netapp-service-manager start
```

## Change the IP address for a Connector

If it's required for your business, you can change the internal IP address and public IP address of the Connector instance that is automatically assigned by your cloud provider.

### Steps

1. Follow the instructions from your cloud provider to change the local IP address or public IP address (or both) for the Connector instance.
2. If you changed the public IP address and you need to connect to the local user interface running on the Connector, restart the Connector instance to register the new IP address with BlueXP.
3. If you changed the private IP address, update the backup location for Cloud Volumes ONTAP configuration files so that the backups are being sent to the new private IP address on the Connector.

- a. Run the following command from the Cloud Volumes ONTAP CLI to remove the current backup target:

```
system configuration backup settings modify -destination ""
```

- b. Go to BlueXP and open the working environment.
- c. Click the menu and select **Advanced > Configuration Backups**.
- d. Click **Set Backup Target**.

## Edit a Connector's URIs

Add and remove the URIs for a Connector.

### Steps

1. Click the **Connector** drop-down from the BlueXP header.
2. Click **Manage Connectors**.
3. Click the action menu for a Connector and click **Edit URIs**.
4. Add and remove URIs and then click **Apply**.

## Fix download failures when using a Google Cloud NAT gateway

The Connector automatically downloads software updates for Cloud Volumes ONTAP. The download can fail if your configuration uses a Google Cloud NAT gateway. You can correct this issue by limiting the number of parts that the software image is divided into. This step must be completed by using the BlueXP API.

### Step

1. Submit a PUT request to `/occm/config` with the following JSON as body:

```
{
  "maxDownloadSessions": 32
}
```

The value for *maxDownloadSessions* can be 1 or any integer greater than 1. If the value is 1, then the downloaded image will not be divided.

Note that 32 is an example value. The value that you should use depends on your NAT configuration and the number of sessions that you can have simultaneously.

[Learn more about the /occm/config API call.](#)

## Upgrade the Connector on-prem without internet access

If you [installed the Connector on an on-premises host that doesn't have internet access](#), you can upgrade the Connector when a newer version is available from the NetApp Support Site.

The Connector needs to restart during the upgrade process so the user interface will be unavailable during the upgrade.

### Steps

1. Download the Connector software from the [NetApp Support Site](#).
2. Copy the installer to the Linux host.
3. Assign permissions to run the script.

```
chmod +x /path/cloud-manager-connector-offline-v3.9.14
```

4. Run the installation script:

```
sudo /path/cloud-manager-connector-offline-v3.9.14
```

5. After the upgrade is complete, you can verify the Connector's version by going to **Help > Support > Connector**.

### What about software upgrades on hosts that have internet access?

The Connector automatically updates its software to the latest version, as long as it has outbound internet access to obtain the software update.

### Remove Connectors from BlueXP

If a Connector is inactive, you can remove it from the list of Connectors in BlueXP. You might do this if you deleted the Connector virtual machine or if you uninstalled the Connector software.

Note the following about removing a Connector:

- This action doesn't delete the virtual machine.
- This action can't be reverted—once you remove a Connector from BlueXP, you can't add it back

#### Steps

1. Click the **Connector** drop-down from the BlueXP header.
2. Click **Manage Connectors**.
3. Click the action menu for an inactive Connector and click **Remove Connector**.



4. Enter the name of the Connector to confirm and then click Remove.

## Result

BlueXP removes the Connector from its records.

## Uninstall the Connector software

Uninstall the Connector software to troubleshoot issues or to permanently remove the software from the host. The steps that you need to use depends on whether you installed the Connector on a host that has internet access or a host in a restricted network that doesn't have internet access.

### Uninstall from a host with internet access

The online Connector includes an uninstallation script that you can use to uninstall the software.

#### Step

1. From the Linux host, run the uninstallation script:

```
/opt/application/netapp/service-manager-2/uninstall.sh [silent]
```

*silent* runs the script without prompting you for confirmation.

### Uninstall from a host without internet access

Use these commands if you downloaded the Connector software from the NetApp Support Site and installed it in a restricted network that doesn't have internet access.

#### Step

1. From the Linux host, run the following commands:

```
docker-compose -f /opt/application/netapp/ds/docker-compose.yml down -v
rm -rf /opt/application/netapp/ds
```

## Managing an HTTPS certificate for secure access

By default, BlueXP uses a self-signed certificate for HTTPS access to the web console. You can install a certificate signed by a certificate authority (CA), which provides better security protection than a self-signed certificate.

### Before you get started

You need to create a Connector before you can change BlueXP settings. [Learn how.](#)

### Installing an HTTPS certificate

Install a certificate signed by a CA for secure access.

#### Steps

1. In the upper right of the BlueXP console, click the Settings icon, and select **HTTPS Setup**.



2. In the HTTPS Setup page, install a certificate by generating a certificate signing request (CSR) or by installing your own CA-signed certificate:

| Option                                 | Description   |
|--|---|
| Generate a CSR                         | <ol style="list-style-type: none"><li>a. Enter the host name or DNS of the Connector host (its Common Name), and then click <b>Generate CSR</b>.<br/><br/>BlueXP displays a certificate signing request.</li><li>b. Use the CSR to submit an SSL certificate request to a CA.<br/><br/>The certificate must use the Privacy Enhanced Mail (PEM) Base-64 encoded X.509 format.</li><li>c. Upload the certificate file and then click <b>Install</b>.</li></ol> |
| Install your own CA-signed certificate | <ol style="list-style-type: none"><li>a. Select <b>Install CA-signed certificate</b>.</li><li>b. Load both the certificate file and the private key and then click <b>Install</b>.<br/><br/>The certificate must use the Privacy Enhanced Mail (PEM) Base-64 encoded X.509 format.</li></ol>  |

#### Result

BlueXP now uses the CA-signed certificate to provide secure HTTPS access. The following image shows a BlueXP account that is configured for secure access:





## Renewing the BlueXP HTTPS certificate

You should renew the BlueXP HTTPS certificate before it expires to ensure secure access to the BlueXP console. If you don't renew the certificate before it expires, a warning appears when users access the web console using HTTPS.

### Steps

1. In the upper right of the BlueXP console, click the Settings icon, and select **HTTPS Setup**.

Details about the BlueXP certificate displays, including the expiration date.

2. Click **Change Certificate** and follow the steps to generate a CSR or install your own CA-signed certificate.

### Result

BlueXP uses the new CA-signed certificate to provide secure HTTPS access.

## Configure a Connector to use a proxy server

If your corporate policies require you to use a proxy server for all communication to the internet, then you need to configure your Connectors to use that proxy server. If you didn't configure a Connector to use a proxy server during installation, then you can configure the Connector to use that proxy server at any time.

BlueXP supports HTTP and HTTPS. The proxy server can be in the cloud or in your network.

Configuring the Connector to use a proxy server provides outbound internet access if a public IP address or a NAT gateway isn't available. This proxy server provides only the Connector with an outbound connection. It doesn't provide any connectivity for Cloud Volumes ONTAP systems.

If Cloud Volumes ONTAP systems don't have an outbound internet connection to send AutoSupport messages, BlueXP automatically configures those Cloud Volumes ONTAP systems to use a proxy server that's included

with the Connector. The only requirement is to ensure that the Connector's security group allows inbound connections over port 3128. You'll need to open this port after you deploy the Connector.

### Enable a proxy on a Connector

When you configure a Connector to use a proxy server, that Connector and the Cloud Volumes ONTAP systems that it manages (including any HA mediators), all use the proxy server.

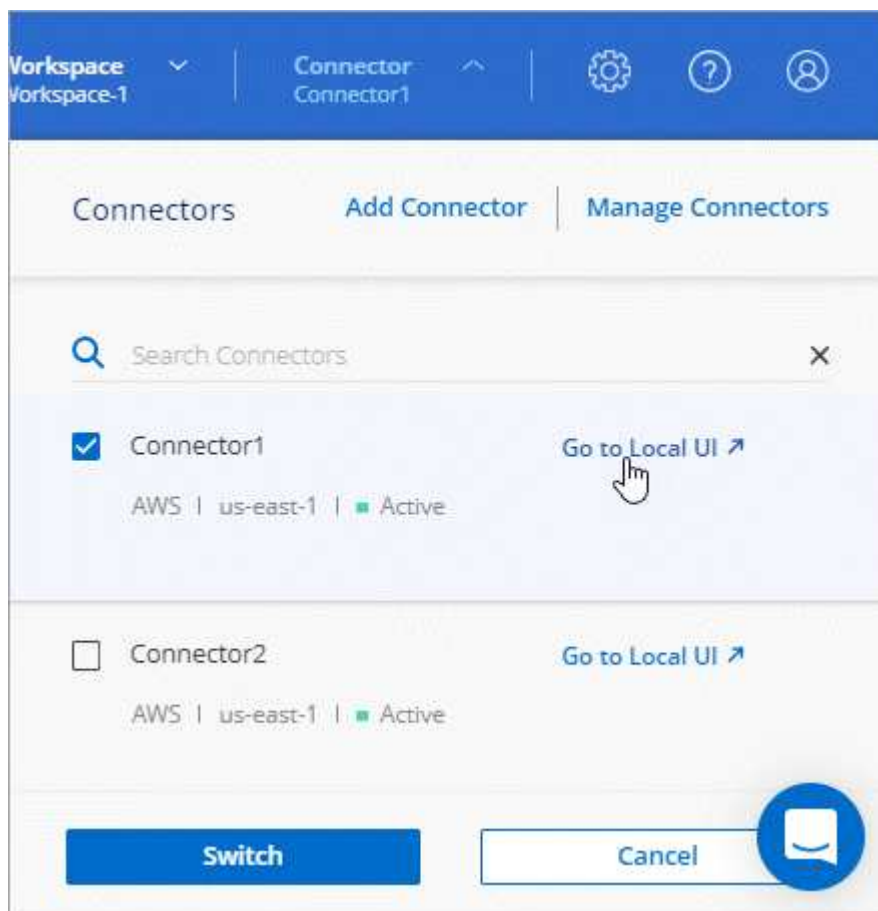
Note that this operation restarts the Connector. Ensure that the Connector isn't performing any operations before you proceed.

#### Steps

1. [Log in to the BlueXP SaaS interface](#) from a machine that has a network connection to the Connector instance.

If the Connector doesn't have a public IP address, you'll need a VPN connection or you'll need to connect from a jump host that's in the same network as the Connector.

2. Click the **Connector** drop-down and then click **Go to local UI** for a specific Connector.



The BlueXP interface running on the Connector loads in a new browser tab.

3. In the upper right of the BlueXP console, click the Settings icon, and select **Connector Settings**.



4. Under **General**, click **HTTP Proxy Configuration**.
5. Set up the proxy:
  - a. Click **Enable Proxy**.
  - b. Specify the server using the syntax `http://address:port` or `https://address:port`
  - c. Specify a user name and password if basic authentication is required for the server
  - d. Click **Save**.



BlueXP doesn't support passwords that include the @ character.

### Enable direct API traffic

If you configured a proxy server, you can send API calls directly to BlueXP without going through the proxy. This option is supported with Connectors that are running in AWS, in Azure, or in Google Cloud.

#### Steps

1. In the upper right of the BlueXP console, click the Settings icon, and select **Connector Settings**.



2. Under **General**, click **Support Direct API Traffic**.
3. Click the checkbox to enable the option and then click **Save**.

### Default configuration for the Connector

You might want to learn more about the Connector before you deploy it, or if you need to troubleshoot any issues.

#### Default configuration with internet access

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

##### AWS details

If you deployed the Connector from BlueXP or from the cloud provider's marketplace, note the following:

- The EC2 instance type is t3.xlarge.
- The operating system for the image is Red Hat Enterprise Linux 7.6 (HVM).

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

- The user name for the EC2 Linux instance is ec2-user.
- The default system disk is a 100 GiB gp2 disk.

#### **Azure details**

If you deployed the Connector from BlueXP or from the cloud provider's marketplace, note the following:

- The VM type is DS3 v2.
- The operating system for the image is CentOS 7.6.

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

- The default system disk is a 100 GiB premium SSD disk.

#### **Google Cloud details**

If you deployed the Connector from BlueXP or from the cloud provider's marketplace, note the following:

- The VM instance is n2-standard-4.
- The operating system for the image is Red Hat Enterprise Linux 8.6.

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

- The default system disk is a 100 GiB SSD persistent disk.

#### **Installation folder**

The Connector installation folder resides 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 Connector and docker images.

- /opt/application/netapp/cloudmanager/docker\_occm/data/log

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

#### **Connector service**

- The BlueXP 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 Connector 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 Connector on an on-premises Linux host that doesn't have internet access. [Learn more about this installation option.](#)

- The Connector installation folder resides 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 Connector and docker images.

- All services are running inside docker containers

The services are dependent on the docker runtime service running

- The Connector uses the following ports on the Linux host:
  - 80 for HTTP access
  - 443 for HTTPS access

# Manage PAYGO subscriptions and contracts

When you subscribe to BlueXP from a cloud provider's marketplace, you're redirected to the BlueXP website where you need to save your subscription and associate it with specific accounts. After you've subscribed, each subscription is available to manage from the Digital Wallet.

## View your subscriptions

The Digital Wallet provides details about each PAYGO subscription and annual contract associated with your BlueXP account and with Astra (Astra uses BlueXP's charging service).


### Steps

1. From the BlueXP navigation menu, select **Governance > Digital wallet**.
2. Select **Subscriptions**.

You'll only see the subscriptions that are associated with the account that you're currently viewing.

3. As you view the information about your subscriptions, you can interact with the details in the table as follows:

- Expand a row to view more details.



kobi contract

Annual Contract


Cloud Manager

Apr 01, 2020

Sep 14, 2023

Subscribed

...



Cloud Manager - Deploy & Manage NetApp Cloud Data Services

Product Title

N/A

Term

No

Auto Renew

Cloud Volumes ONTAP (2 Packages)

| Contract Option      | Units | Details                                    |
|----------------------|-------|--|
| Essentials (Primary) | 2 TiB | Single Node                                |
| Professional         | 1 TiB | High Availability + Unlimited Cloud Backup |

- Click  to choose which columns appear in the table.

Note that the Term and Auto Renew columns don't appear by default. The Auto Renew column displays renewal information for Azure contracts only.

Note the following about what you see in the table:

### Start date

The start date is when you successfully associated the subscription with your account and charging started.

### N/A

If you see N/A in the table, the information isn't available from the cloud provider's API at this time.

### Contracts

- If you expand the details for a contract, the Digital Wallet shows what's available for your current plan: the contract options and units (capacity or number of nodes).
- The Digital Wallet will identify the end date and whether the contract will renew soon, end soon, or whether it has already ended.
- If you have an AWS contract and you changed any of the contract's options after the start date, be sure to validate your contract options from the AWS.







## Manage your subscriptions

You can manage your subscriptions from the Digital Wallet by renaming a subscription and choosing the accounts that are associated with the subscription.

For example, let's say that you have two accounts and each is billed through separate subscriptions. You might disassociate a subscription from one of the accounts so the users in that account don't accidentally choose the wrong subscription when creating a Cloud Volume ONTAP working environment.

### Steps

1. From the BlueXP navigation menu, select **Governance > Digital wallet**.
2. Select **Subscriptions**.
3. Click the action menu in the row that corresponds to the subscription that you want to manage.

| Provider  | Name                    | Type            | Service       | Start Date   | End Date     | Status     |   |
|---|-------------------------|-----------------|---------------|--------------|--------------|------------|---|
|  | aws-sub-a2              | PAYGO           | Cloud Manager | Apr 02, 2020 | N/A          | Subscribed |  |
|  | Aleksey_aws_marketplace | Annual Contract | Astra         | Oct 18, 2022 | Oct 18, 2023 |            |  |
|  | By Capacity By Node 3   | PAYGO           | Cloud Manager | Mar 31, 2020 | N/A          | Subscribed |  |

4. Choose to rename the subscription or to manage the NetApp accounts that are associated with the subscription.

## Discovered cloud storage

### Viewing your Amazon S3 buckets

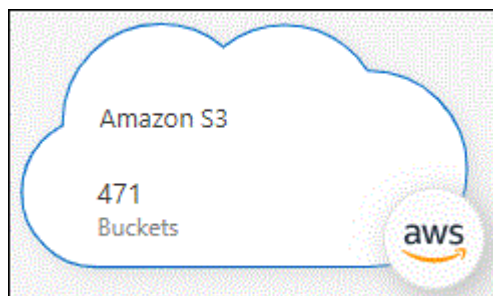
After you install a Connector in AWS, BlueXP can automatically discover information about the Amazon S3 buckets that reside in the AWS account where the Connector is installed. An Amazon S3 working environment is added to the Canvas so you can view this information.

You can see details about your S3 buckets, including the region, access policy, account, total and used capacity, and more. These buckets can be used as destinations for Cloud Backup, Cloud Tiering, or Cloud Sync operations. Additionally, you can use Cloud Data Sense to scan these buckets.

#### Steps

1. [Install a Connector](#) in the AWS account where you want to view your Amazon S3 buckets.
2. From the navigation menu, select **Storage > Canvas**.

You should automatically see an Amazon S3 working environment shortly after.



3. Click the working environment and select an action from the right pane.



4. Click **Sync data** to synchronize data to or from S3 buckets.

For more details, see [the overview for the Cloud Sync service](#).

5. Click **Enable** if you want Cloud Data Sense to scan the S3 buckets for personal and sensitive data.

For more details, see [Getting started with Cloud Data Sense for Amazon S3](#).

6. Click **Enter Working Environment** to view details about the S3 buckets in your AWS account.

Amazon S3

Overview

471

Total Buckets

6.94

TiB

Total Capacity

23

Total Regions

471 Buckets

| Bucket Name                    | AWS Account | Region                | Creation Date      | Encryption | Is Public                     | Size      | Total Objects |
|--------------------------------|-------------|-----------------------|--------------------|------------|-------------------------------|-----------|---------------|
| athena-query-results-us-east-1 | 4642620614  | US East (N. Virginia) | September 27, 2021 | Disabled   | Bucket and objects not public | 35.27 GiB | 3.01K         |
| catalog-sg                     | 4642620614  | US East (N. Virginia) | October 1, 2021    | Disabled   | Bucket and objects not public | 1.35 GiB  | 1.44K         |
| cbsqa                          | 4642620614  | US East (N. Virginia) | August 9, 2021     | Disabled   | Public                        | 33.95 GiB | 185           |
| template-19-ap-southeast-3     | 4642620614  | ap-southeast-3        | March 10, 2022     | Enabled ⓘ  | Objects can be public         | 21.38 KiB | 3             |
| template-7dxc-ca-central-1     | 4642620614  | Canada (Central)      | November 2, 2020   | Enabled ⓘ  | Objects can be public         | 24.01 KiB | 2             |



## Viewing your Azure Blob accounts

After you install a Connector in Azure, BlueXP can automatically discover information about the Azure storage accounts that reside in the Azure Subscriptions where the Connector is installed. An Azure Blob working environment is added to the Canvas so you can view this information.

You can see details about your Azure storage accounts, including the location, resource group, total and used capacity, and more. These accounts can be used as destinations for Cloud Backup, Cloud Tiering, or Cloud Sync operations.

### Steps

1. [Install a Connector](#) in the Azure account where you want to view your Azure storage accounts.
2. From the navigation menu, select **Storage > Canvas**.

You should automatically see an Azure Blob working environment shortly after.



3. Click the working environment and select an action from the right pane.


Azure Blob Storage
On

### INFORMATION

55
Storage Accounts

### SERVICES



Sync
On

20 MiB
Data Synced




Enter Working Environment


4. Click **Sync data** to synchronize data to or from Azure Blob storage.


For more details, see [the overview for the Cloud Sync service](#).


5. Click **Enter Working Environment** to view details about the Azure storage accounts in your Azure Blobs.


Azure blob

### Overview


637
Total Storage Accounts


1.5 TiB
Total Capacity


16
Total Locations

637 Storage Accounts

| Storage Account Name | Subscription | Location       | Creation Date     | Resource Group | Blob Capacity |
|----------------------|--------------|----------------|-------------------|----------------|---------------|
| ovu8llxvqdfypxn      | OCCM QA1     | West US        | June 24, 2021     | AdmAzureHa-rg  | 170 B         |
| rootsa9ktpjzcm       | OCCM QA1     | West US        | June 24, 2021     | AdmAzureHa-rg  | 950.22 GiB    |
| scvdwjcwehswli       | OCCM QA1     | West US        | June 24, 2021     | AdmAzureHa-rg  | 22.12 MiB     |
| 65qtx0smegmq2vt      | OCCM QA1     | West US        | June 24, 2021     | AdmAzureVsa-rg | 170 B         |
| bu9kixthymr1be       | OCCM QA1     | West US        | June 24, 2021     | AdmAzureVsa-rg | 1.01 MiB      |
| 8jzsvybvjiwieww8     | OCCM QA1     | Canada Central | December 12, 2019 | aff1-rg        | 170 B         |

## Viewing your Google Cloud Storage buckets

After you install a Connector in Google Cloud, BlueXP can automatically discover information about the Google Cloud Storage buckets that reside in the Google account where the Connector is installed. A Google Cloud Storage working environment is added to the Canvas so you can view this information.

You can see details about your Google Cloud Storage buckets, including the location, access status, storage class, total and used capacity, and more. These buckets can be used as destinations for Cloud Backup, Cloud Tiering, or Cloud Sync operations.

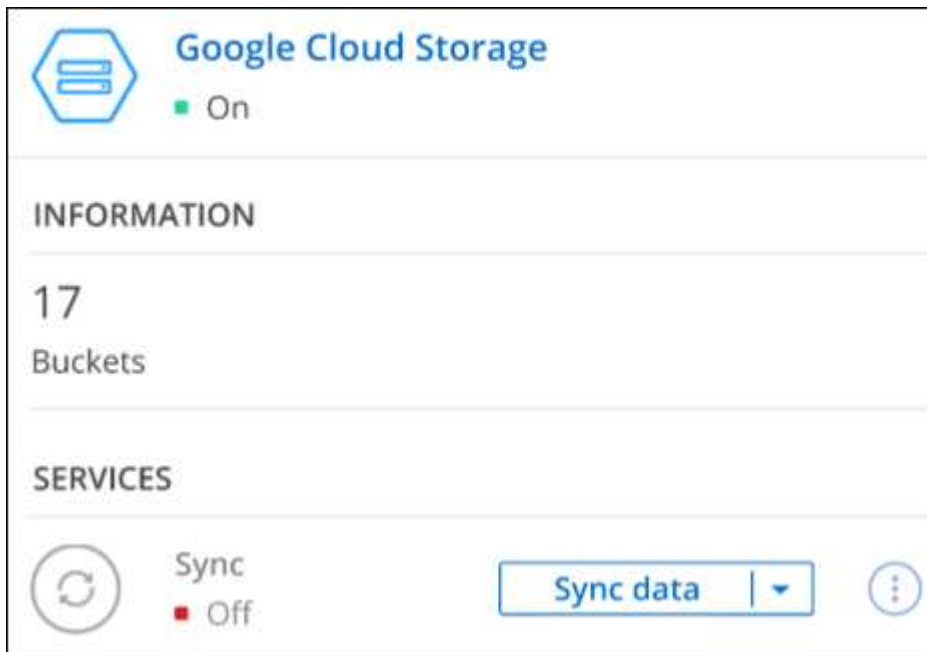
### Steps

1. [Install a Connector](#) in the Google account where you want to view your Google Cloud Storage buckets.
2. From the navigation menu, select **Storage > Canvas**.

You should automatically see a Google Cloud Storage working environment shortly after.



3. Click the working environment and select an action from the right pane.



4. Click **Sync data** to synchronize data to or from Google Cloud Storage buckets.

For more details, see [the overview for the Cloud Sync service](#).

5. Click **Enter Working Environment** to view details about the buckets in your Google account.

## AWS credentials

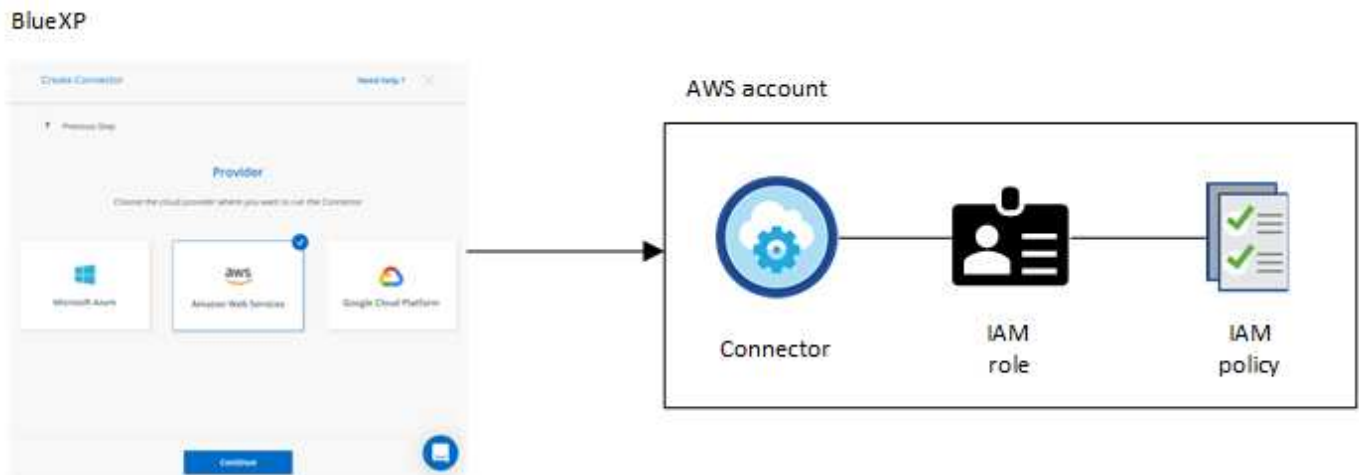
### AWS credentials and permissions

BlueXP enables you to choose the AWS credentials to use when deploying Cloud Volumes ONTAP. You can deploy all of your Cloud Volumes ONTAP systems using the initial AWS credentials, or you can add additional credentials.

#### Initial AWS credentials

When you deploy a Connector from BlueXP, you need to provide the ARN of an IAM role or access keys for an IAM user. The authentication method that you use must have the required permissions to deploy the Connector instance in AWS. The required permissions are listed in the [Connector deployment policy for AWS](#).

When BlueXP launches the Connector instance in AWS, it creates an IAM role and an instance profile for the instance. It also attaches a policy that provides the Connector with permissions to manage resources and processes within that AWS account. [Review how BlueXP uses the permissions](#).



BlueXP selects these AWS credentials by default when you create a new working environment for Cloud Volumes ONTAP:

| Details & Credentials |            |                          |                                  |
|-----------------------|------------|--------------------------|----------------------------------|
| Instance Profile      |            | QA Subscription          | <a href="#">Edit Credentials</a> |
| Credentials           | Account ID | Marketplace Subscription |                                  |

#### Additional AWS credentials

There are two ways to add additional AWS credentials.

## Add AWS credentials to an existing Connector

If you want to launch Cloud Volumes ONTAP in different AWS accounts, then you can either [provide AWS keys for an IAM user or the ARN of a role in a trusted account](#). The following image shows two additional accounts, one providing permissions through an IAM role in a trusted account and another through the AWS keys of an IAM user:



You would then [add the account credentials to BlueXP](#) by specifying the Amazon Resource Name (ARN) of the IAM role, or the AWS keys for the IAM user.

After you add another set of credentials, you can switch to them when creating a new working environment:

**Edit Credentials & Add Subscription**

Associate Subscription to Credentials ⓘ

Credentials

- keys | Account ID: [redacted]
- Instance Profile | Account ID: [redacted]
- casaba QA subscription

+ Add Subscription

Apply Cancel

## Add AWS credentials directly to BlueXP

Adding new AWS credentials to BlueXP provides the permissions needed to create and manage an FSx for ONTAP working environment or to create a Connector.

## What about Marketplace deployments and on-prem deployments?

The sections above describe the recommended deployment method for the Connector, which is from BlueXP. You can also deploy a Connector in AWS from the [AWS Marketplace](#) and you can [install the Connector on-premises](#).

If you use the Marketplace, permissions are provided in the same way. You just need to manually create and set up the IAM role, and then provide permissions for any additional accounts.

For on-premises deployments, you can't set up an IAM role for the BlueXP system, but you can provide permissions just like you would for additional AWS accounts.

### **How can I securely rotate my AWS credentials?**

As described above, BlueXP enables you to provide AWS credentials in a few ways: an IAM role associated with the Connector instance, by assuming an IAM role in a trusted account, or by providing AWS access keys.

With the first two options, BlueXP uses the AWS Security Token Service to obtain temporary credentials that rotate constantly. This process is the best practice—it's automatic and it's secure.

If you provide BlueXP with AWS access keys, you should rotate the keys by updating them in BlueXP at a regular interval. This is a completely manual process.

## **Manage AWS credentials and subscriptions for BlueXP**

Add and manage AWS credentials so that BlueXP has the permissions that it needs to deploy and manage cloud resources in your AWS accounts. If you manage multiple AWS subscriptions, you can assign each one of them to different AWS credentials from the Credentials page.

### **Overview**

You can add AWS credentials to an existing Connector or directly to BlueXP:

- Add additional AWS credentials to an existing Connector

Adding AWS credentials to an existing Connector provides the permissions needed to manage resources and processes within your public cloud environment. [Learn how to add AWS credentials to a Connector.](#)

- Add AWS credentials to BlueXP for creating a Connector

Adding new AWS credentials to BlueXP gives BlueXP the permissions needed to create a Connector. [Learn how to add AWS credentials to BlueXP.](#)

- Add AWS credentials to BlueXP for FSx for ONTAP

Adding new AWS credentials to BlueXP gives BlueXP the permissions needed to create and manage FSx for ONTAP. [Learn how to set up permissions for FSx for ONTAP](#)

### **How to rotate credentials**

BlueXP enables you to provide AWS credentials in a few ways: an IAM role associated with the Connector instance, by assuming an IAM role in a trusted account, or by providing AWS access keys. [Learn more about AWS credentials and permissions.](#)

With the first two options, BlueXP uses the AWS Security Token Service to obtain temporary credentials that rotate constantly. This process is the best practice because it's automatic and it's secure.

If you provide BlueXP with AWS access keys, you should rotate the keys by updating them in BlueXP at a

regular interval. This is a completely manual process.

## Add credentials to a Connector

Add AWS credentials to a Connector so that it has the permissions needed to manage resources and processes within your public cloud environment. You can either provide the ARN of an IAM role in another account or provide AWS access keys.

### Grant permissions

Before you add AWS credentials to a Connector, you need to provide the required permissions. The permissions enable BlueXP to manage resources and processes within that AWS account. How you provide the permissions depends on whether you want to provide BlueXP with the ARN of a role in a trusted account or AWS keys.



If you deployed a Connector from BlueXP, BlueXP automatically added AWS credentials for the account in which you deployed the Connector. This initial account is not added if you deployed the Connector from the AWS Marketplace or if you manually installed the Connector software on an existing system. [Learn about AWS credentials and permissions.](#)

### Choices

- [Grant permissions by assuming an IAM role in another account](#)
- [Grant permissions by providing AWS keys](#)

### Grant permissions by assuming an IAM role in another account

You can set up a trust relationship between the source AWS account in which you deployed the Connector instance and other AWS accounts by using IAM roles. You would then provide BlueXP with the ARN of the IAM roles from the trusted accounts.

If the Connector is installed on premises, you can't use this authentication method. You must use AWS keys.

### Steps

1. Go to the IAM console in the target account in which you want to provide the Connector with permissions.
2. Under Access Management, click **Roles > Create Role** and follow the steps to create the role.

Be sure to do the following:

- Under **Trusted entity type**, select **AWS account**.
  - Select **Another AWS account** and enter the ID of the account where the Connector instance resides.
  - Create the required policies by copying and pasting the contents of [the IAM policies for the Connector](#).
3. Copy the Role ARN of the IAM role so that you can paste it in BlueXP later on.

### Result

The account now has the required permissions. [You can now add the credentials to a Connector.](#)

### Grant permissions by providing AWS keys

If you want to provide BlueXP with AWS keys for an IAM user, then you need to grant the required permissions to that user. The BlueXP IAM policy defines the AWS actions and resources that BlueXP is allowed to use.

You must use this authentication method if the Connector is installed on premises. You can't use an IAM role.

## Steps

1. From the IAM console, create policies by copying and pasting the contents of [the IAM policies for the Connector](#).

[AWS Documentation: Creating IAM Policies](#)

2. Attach the policies to an IAM role or an IAM user.
  - [AWS Documentation: Creating IAM Roles](#)
  - [AWS Documentation: Adding and Removing IAM Policies](#)

## Result

The account now has the required permissions. [You can now add the credentials to a Connector](#).

## Add the credentials

After you provide an AWS account with the required permissions, you can add the credentials for that account to an existing Connector. This enables you to launch Cloud Volumes ONTAP systems in that account using the same Connector.

## Before you get started

If you just created these credentials in your cloud provider, it might take a few minutes until they are available for use. Wait a few minutes before you add the credentials to BlueXP.

## Steps

1. Ensure that the correct Connector is currently selected in BlueXP.
2. In the upper right of the BlueXP console, click the Settings icon, and select **Credentials**.



3. Click **Add Credentials** and follow the steps in the wizard.
  - a. **Credentials Location:** Select **Amazon Web Services > Connector**.
  - b. **Define Credentials:** Provide the ARN (Amazon Resource Name) of a trusted IAM role, or enter an AWS access key and secret key.
  - c. **Marketplace Subscription:** Associate a Marketplace subscription with these credentials by subscribing now or by selecting an existing subscription.

To pay for Cloud Volumes ONTAP at an hourly rate (PAYGO) or with an annual contract, AWS credentials must be associated with a subscription to Cloud Volumes ONTAP from the AWS Marketplace.

- d. **Review:** Confirm the details about the new credentials and click **Add**.

## Result

You can now switch to a different set of credentials from the Details and Credentials page when creating a new working environment:



## Edit Credentials & Add Subscription

---

### Associate Subscription to Credentials ?

Credentials

keys | Account ID:

Instance Profile | Account ID:

casaba QA subscription

+ Add Subscription

---

Apply

Cancel

### Add credentials to BlueXP for creating a Connector

Add AWS credentials to BlueXP by providing the ARN of an IAM role that gives BlueXP the permissions needed to create a Connector. You can choose these credentials when creating a new Connector.

#### Set up the IAM role

Set up an IAM role that enables the BlueXP SaaS to assume the role.

#### Steps

1. Go to the IAM console in the target account.
2. Under Access Management, click **Roles > Create Role** and follow the steps to create the role.

Be sure to do the following:

- Under **Trusted entity type**, select **AWS account**.
- Select **Another AWS account** and enter the ID of the BlueXP SaaS: 952013314444
- Create a policy that includes the permissions required to create a Connector.
  - [View the permissions needed for FSx for ONTAP](#)
  - [View the Connector deployment policy](#)

3. Copy the Role ARN of the IAM role so that you can paste it in BlueXP in the next step.

#### Result

The IAM role now has the required permissions. [You can now add it to BlueXP](#).

#### Add the credentials

After you provide the IAM role with the required permissions, add the role ARN to BlueXP.

## Before you get started

If you just created the IAM role, it might take a few minutes until they are available for use. Wait a few minutes before you add the credentials to BlueXP.

## Steps

1. In the upper right of the BlueXP console, click the Settings icon, and select **Credentials**.



2. Click **Add Credentials** and follow the steps in the wizard.
  - a. **Credentials Location:** Select **Amazon Web Services > BlueXP**.
  - b. **Define Credentials:** Provide the ARN (Amazon Resource Name) of the IAM role.
  - c. **Review:** Confirm the details about the new credentials and click **Add**.

## Result

You can now use the credentials when creating a new Connector.

## Associate an AWS subscription

After you add your AWS credentials to BlueXP, you can associate an AWS Marketplace subscription with those credentials. The subscription enables you to pay for Cloud Volumes ONTAP at an hourly rate (PAYGO) or using an annual contract, and to use other NetApp cloud services.

There are two scenarios in which you might associate an AWS Marketplace subscription after you've already added the credentials to BlueXP:

- You didn't associate a subscription when you initially added the credentials to BlueXP.
- You want to replace an existing AWS Marketplace subscription with a new subscription.

## What you'll need

You need to create a Connector before you can change BlueXP settings. [Learn how to create a Connector](#).

## Steps

1. In the upper right of the BlueXP console, click the Settings icon, and select **Credentials**.
2. Click the action menu for a set of credentials and then select **Associate Subscription**.



3. To associate the credentials with an existing subscription, select the subscription from the down-down list and click **Associate**.
4. To associate the credentials with a new subscription, click **Add Subscription > Continue** and follow the steps in the AWS Marketplace:
  - a. Click **View purchase options**.
  - b. Click **Subscribe**.
  - c. Click **Set up your account**.

You'll be redirected to the BlueXP website.

- d. From the **Subscription Assignment** page:
  - Select the NetApp accounts that you'd like to associate this subscription with.
  - In the **Replace existing subscription** field, choose whether you'd like to automatically replace the existing subscription for one account with this new subscription.

BlueXP replaces the existing subscription for all credentials in the account with this new subscription. If a set of credentials wasn't ever associated with a subscription, then this new subscription won't be associated with those credentials.

For all other accounts, you'll need to manually associate the subscription by repeating these steps.

- Click **Save**.

The following video shows the steps to subscribe from the Google Cloud Marketplace:

► [https://docs.netapp.com/us-en/cloud-manager-setup-admin//media/video\\_subscribing\\_aws.mp4](https://docs.netapp.com/us-en/cloud-manager-setup-admin//media/video_subscribing_aws.mp4)

(video)

## Edit credentials

Edit your AWS credentials in BlueXP by changing the account type (AWS keys or assume role), by editing the name, or by updating the credentials themselves (the keys or the role ARN).



You can't edit the credentials for an instance profile that is associated with a Connector instance.

### Steps

1. In the upper right of the BlueXP console, click the Settings icon, and select **Credentials**.
2. Click the action menu for a set of credentials and then select **Edit Credentials**.
3. Make the required changes and then click **Apply**.

## Deleting credentials

If you no longer need a set of credentials, you can delete them from BlueXP. You can only delete credentials that aren't associated with a working environment.



You can't delete the credentials for an instance profile that is associated with a Connector instance.

### Steps

1. In the upper right of the BlueXP console, click the Settings icon, and select **Credentials**.
2. Click the action menu for a set of credentials and then select **Delete Credentials**.
3. Click **Delete** to confirm.

# Azure credentials

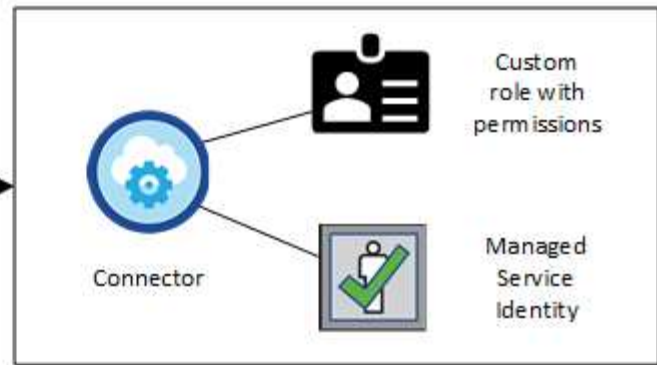
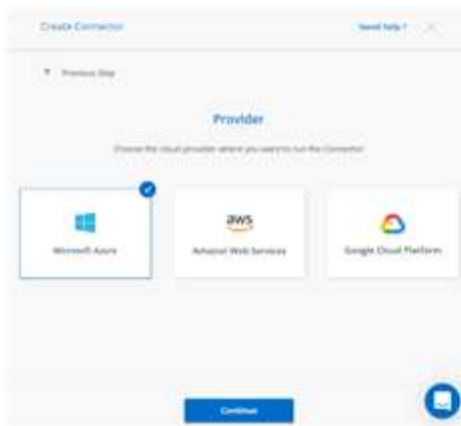
## Azure credentials and permissions

BlueXP enables you to choose the Azure credentials to use when deploying Cloud Volumes ONTAP. You can deploy all of your Cloud Volumes ONTAP systems using the initial Azure credentials, or you can add additional credentials.

### Initial Azure credentials

When you deploy a Connector from BlueXP, you need to use an Azure account or service principal that has permissions to deploy the Connector virtual machine. The required permissions are listed in the [Connector deployment policy for Azure](#).

When BlueXP deploys the Connector virtual machine in Azure, it enables a [system-assigned managed identity](#) on virtual machine, creates a custom role, and assigns it to the virtual machine. The role provides BlueXP with the permissions required to manage resources and processes within that Azure subscription. [Review how BlueXP uses the permissions](#).



BlueXP selects these Azure credentials by default when you create a new working environment for Cloud Volumes ONTAP:

| Details & Credentials  |                    |   |                                  |
|------------------------|--------------------|---|----------------------------------|
| Managed Service Ide... | OCCM QA1           | <span style="color: orange;">ⓘ No subscription is associated</span> | <a href="#">Edit Credentials</a> |
| Credential Name        | Azure Subscription | Marketplace Subscription  |                                  |

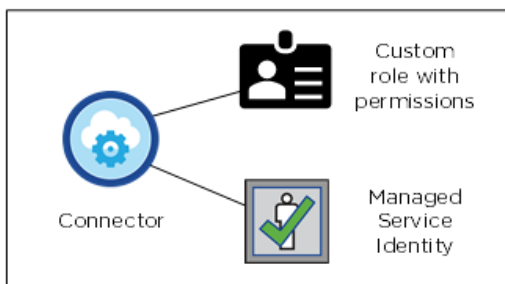
### Additional Azure subscriptions for a managed identity

The managed identity is associated with the subscription in which you launched the Connector. If you want to select a different Azure subscription, then you need to [associate the managed identity with those subscriptions](#).

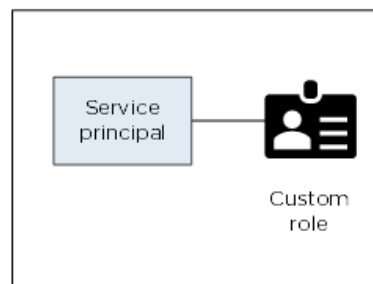
### Additional Azure credentials

If you want to deploy Cloud Volumes ONTAP using different Azure credentials, then you must grant the required permissions by [creating and setting up a service principal in Azure Active Directory](#) for each Azure account. The following image shows two additional accounts, each set up with a service principal and custom role that provides permissions:

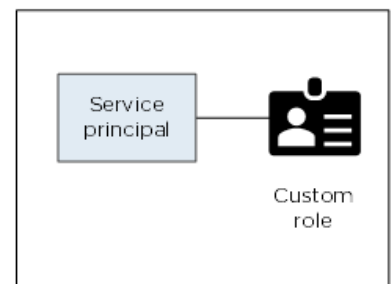
Initial Azure account



Second account



Third account

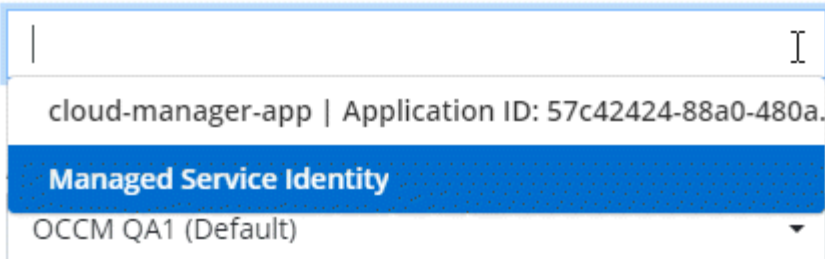


You would then [add the account credentials to BlueXP](#) by providing details about the AD service principal.

After you add another set of credentials, you can switch to them when creating a new working environment:

## Edit Account & Add Subscription

### Credentials



cloud-manager-app | Application ID: 57c42424-88a0-480a.

**Managed Service Identity**

OCCM QA1 (Default)

### What about Marketplace deployments and on-prem deployments?

The sections above describe the recommended deployment method for the Connector, which is from BlueXP. You can also deploy a Connector in Azure from the [Azure Marketplace](#), and you can [install the Connector on-premises](#).

If you use the Marketplace, permissions are provided in the same way. You just need to manually create and set up the managed identity for the Connector, and then provide permissions for any additional accounts.

For on-premises deployments, you can't set up a managed identity for the Connector, but you can provide permissions just like you would for additional accounts by using a service principal.

## Managing Azure credentials and subscriptions for BlueXP

When you create a Cloud Volumes ONTAP system, you need to select the Azure credentials to use with that system. You also need to choose a Marketplace subscription, if you're using pay-as-you-go licensing. Follow the steps on this page if you need to use multiple Azure credentials or multiple Azure Marketplace subscriptions for Cloud Volumes ONTAP.

There are two ways to add additional Azure subscriptions and credentials in BlueXP.

1. Associate additional Azure subscriptions with the Azure managed identity.
2. If you want to deploy Cloud Volumes ONTAP using different Azure credentials, grant Azure permissions using a service principal and add its credentials to BlueXP.

### Associating additional Azure subscriptions with a managed identity

BlueXP enables you to choose the Azure credentials and Azure subscription in which you want to deploy Cloud Volumes ONTAP. You can't select a different Azure subscription for the managed identity profile unless you associate the [managed identity](#) with those subscriptions.

## About this task

A managed identity is [the initial Azure account](#) when you deploy a Connector from BlueXP. When you deployed the Connector, BlueXP created the BlueXP Operator role and assigned it to the Connector virtual machine.

## Steps

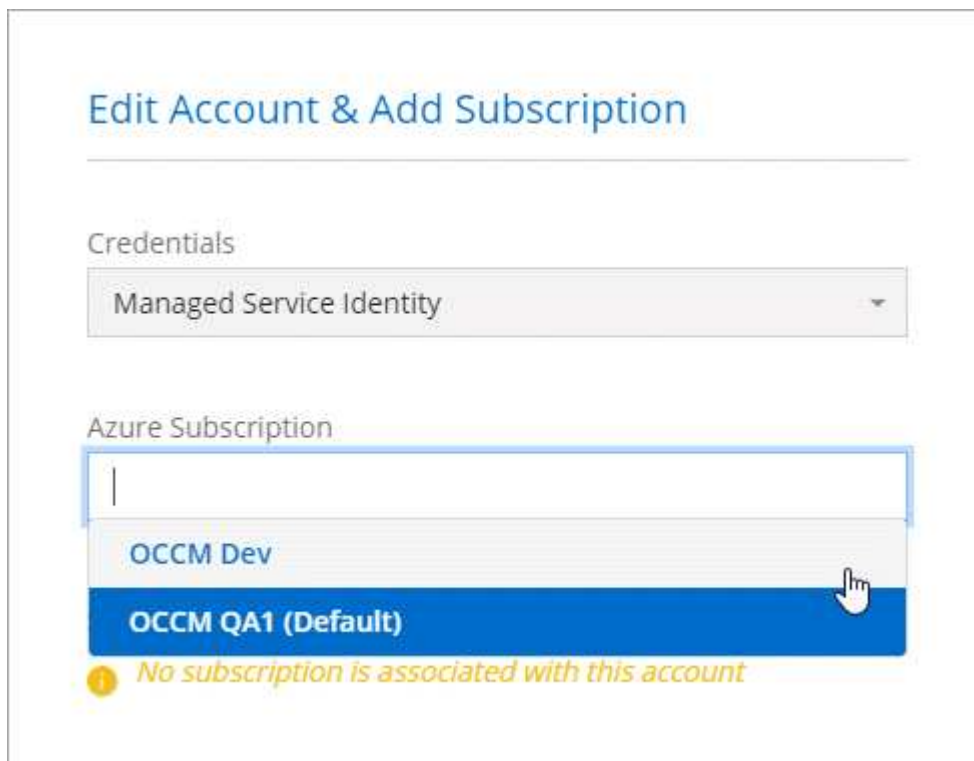
1. Log in to the Azure portal.
2. Open the **Subscriptions** service and then select the subscription in which you want to deploy Cloud Volumes ONTAP.
3. Click **Access control (IAM)**.
  - a. Click **Add > Add role assignment** and then add the permissions:
    - Select the **BlueXP Operator** role.
  - Assign access to a **Virtual Machine**.
  - Select the subscription in which the Connector virtual machine was created.
  - Select the Connector virtual machine.
  - Click **Save**.
4. Repeat these steps for additional subscriptions.



BlueXP Operator is the default name provided in the Connector policy. If you chose a different name for the role, then select that name instead.

## Result

When you create a new working environment, you should now have the ability to select from multiple Azure subscriptions for the managed identity profile.



## Adding additional Azure credentials to BlueXP

When you deploy a Connector from BlueXP, BlueXP enables a system-assigned managed identity on the virtual machine that has the required permissions. BlueXP selects these Azure credentials by default when you create a new working environment for Cloud Volumes ONTAP.



An initial set of credentials isn't added if you manually installed the Connector software on an existing system. [Learn about Azure credentials and permissions.](#)

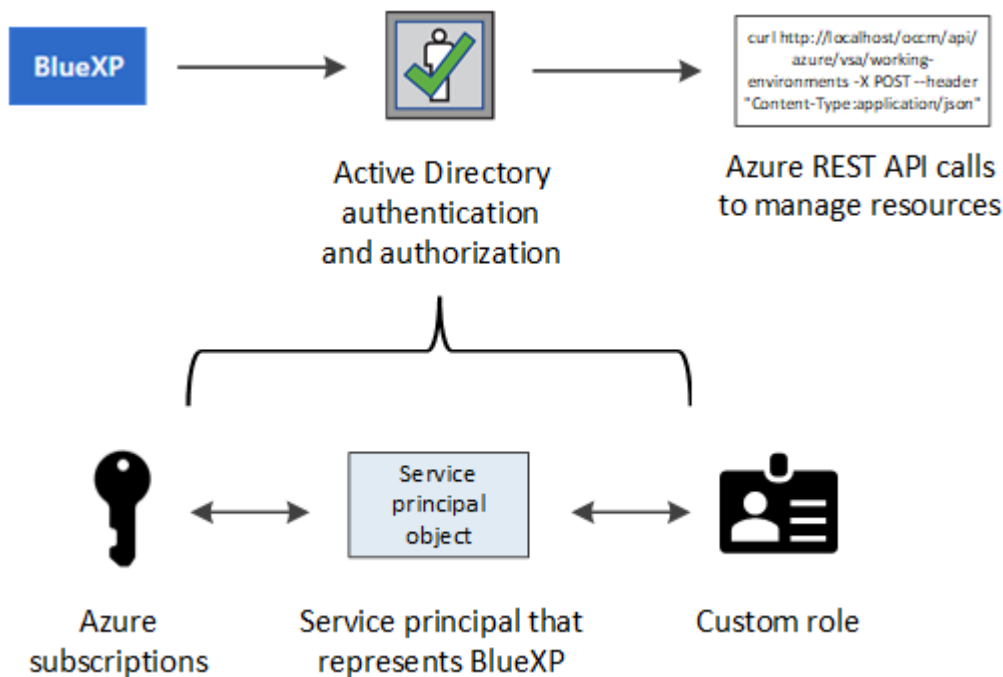
If you want to deploy Cloud Volumes ONTAP using *different* Azure credentials, then you must grant the required permissions by creating and setting up a service principal in Azure Active Directory for each Azure account. You can then add the new credentials to BlueXP.

### Granting Azure permissions using a service principal

BlueXP needs permissions to perform actions in Azure. You can grant the required permissions to an Azure account by creating and setting up a service principal in Azure Active Directory and by obtaining the Azure credentials that BlueXP needs.

### About this task

The following image depicts how BlueXP obtains permissions to perform operations in Azure. A service principal object, which is tied to one or more Azure subscriptions, represents BlueXP in Azure Active Directory and is assigned to a custom role that allows the required permissions.



### Steps

1. [Create an Azure Active Directory application.](#)
2. [Assign the application to a role.](#)
3. [Add Windows Azure Service Management API permissions.](#)
4. [Get the application ID and directory ID.](#)
5. [Create a client secret.](#)



## Creating an Azure Active Directory application

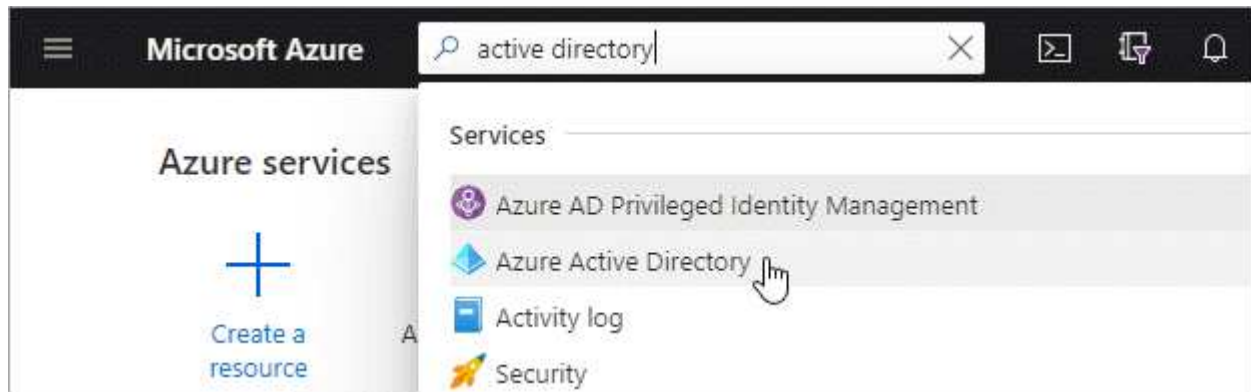
Create an Azure Active Directory (AD) application and service principal that BlueXP can use for role-based access control.

### Before you begin

You must have the right permissions in Azure to create an Active Directory application and to assign the application to a role. For details, refer to [Microsoft Azure Documentation: Required permissions](#).

### Steps

1. From the Azure portal, open the **Azure Active Directory** service.



2. In the menu, click **App registrations**.
3. Click **New registration**.
4. Specify details about the application:
  - **Name**: Enter a name for the application.
  - **Account type**: Select an account type (any will work with BlueXP).
  - **Redirect URI**: You can leave this field blank.
5. Click **Register**.

### Result

You've created the AD application and service principal.

## Assigning the application to a role

You must bind the service principal to one or more Azure subscriptions and assign it the custom "BlueXP Operator" role so BlueXP has permissions in Azure.

### Steps

1. Create a custom role:
  - a. Copy the contents of the [custom role permissions for the Connector](#) and save them in a JSON file.
  - b. Modify the JSON file by adding Azure subscription IDs to the assignable scope.

You should add the ID for each Azure subscription from which users will create Cloud Volumes ONTAP systems.

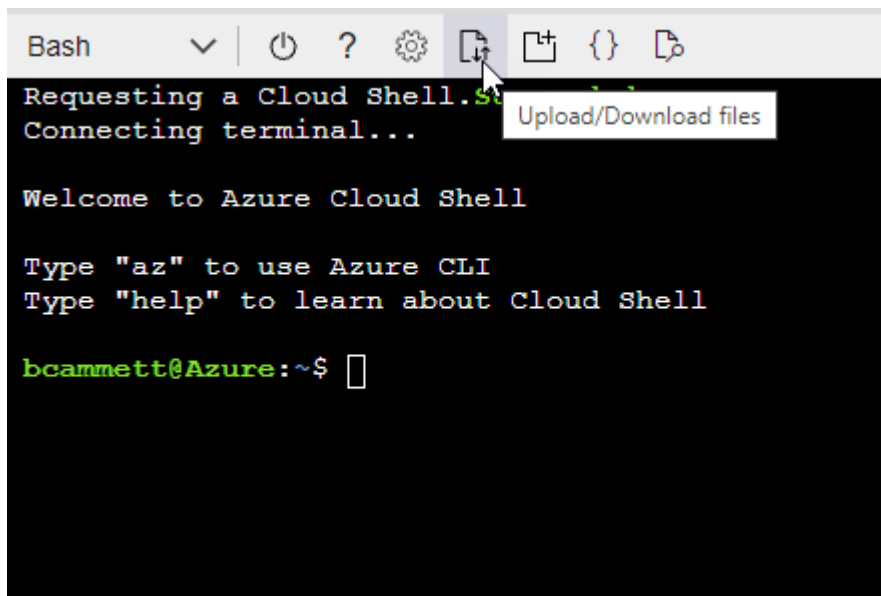
### Example

```
"AssignableScopes": [  
  "/subscriptions/d333af45-0d07-4154-943d-c25fbzzzzzzz",  
  "/subscriptions/54b91999-b3e6-4599-908e-416e0zzzzzzz",  
  "/subscriptions/398e471c-3b42-4ae7-9b59-ce5bbzzzzzzz"
```

- c. Use the JSON file to create a custom role in Azure.

The following steps describe how to create the role by using Bash in Azure Cloud Shell.

- Start [Azure Cloud Shell](#) and choose the Bash environment.
- Upload the JSON file.



- Use the Azure CLI to create the custom role:

```
az role definition create --role-definition Connector_Policy.json
```

You should now have a custom role called BlueXP Operator that you can assign to the Connector virtual machine.

2. Assign the application to the role:

- a. From the Azure portal, open the **Subscriptions** service.
- b. Select the subscription.
- c. Click **Access control (IAM) > Add > Add role assignment**.
- d. In the **Role** tab, select the **BlueXP Operator** role and click **Next**.
- e. In the **Members** tab, complete the following steps:
  - Keep **User, group, or service principal** selected.
  - Click **Select members**.

**Add role assignment** ...

[Got feedback?](#)

**Role**   **Members**   **Review + assign**

**Selected role**   Cloud Manager Operator 3.9.12\_B

**Assign access to**   ☒ User, group, or service principal  
☐ Managed identity

**Members**   [+ Select members](#)

- Search for the name of the application.

Here's an example:

**Select members** ×

Select ⓘ

test-service-principal

test-service-principal

- Select the application and click **Select**.
- Click **Next**.

f. Click **Review + assign**.

The service principal now has the required Azure permissions to deploy the Connector.

If you want to deploy Cloud Volumes ONTAP from multiple Azure subscriptions, then you must bind the service principal to each of those subscriptions. BlueXP enables you to select the subscription that you want to use when deploying Cloud Volumes ONTAP.

## Adding Windows Azure Service Management API permissions

The service principal must have "Windows Azure Service Management API" permissions.

### Steps

1. In the **Azure Active Directory** service, click **App registrations** and select the application.
2. Click **API permissions > Add a permission**.
3. Under **Microsoft APIs**, select **Azure Service Management**.

## Request API permissions

### Select an API

Microsoft APIs APIs my organization uses My APIs

#### Commonly used Microsoft APIs

**Microsoft Graph**  
Take advantage of the tremendous amount of data in Office 365, Enterprise Mobility + Security, and Windows 10. Access Azure AD, Excel, Intune, Outlook/Exchange, OneDrive, OneNote, SharePoint, Planner, and more through a single endpoint.



**Azure Batch**  
Schedule large-scale parallel and HPC applications in the cloud

**Azure Data Catalog**  
Programmatic access to Data Catalog resources to register, annotate and search data assets

**Azure Data Explorer**  
Perform ad-hoc queries on terabytes of data to build near real-time and complex analytics solutions

**Azure Data Lake**  
Access to storage and compute for big data analytic scenarios

**Azure DevOps**  
Integrate with Azure DevOps and Azure DevOps server

**Azure Import/Export**  
Programmatic control of import/export jobs

**Azure Key Vault**  
Manage your key vaults as well as the keys, secrets, and certificates within your Key Vaults

**Azure Rights Management Services**  
Allow validated users to read and write protected content

**Azure Service Management**  
Programmatic access to much of the functionality available through the Azure portal

**Azure Storage**  
Secure, massively scalable object and data lake storage for unstructured and semi-structured data

**Customer Insights**  
Create profile and interaction models for your products

**Data Export Service for Microsoft Dynamics 365**  
Export data from Microsoft Dynamics CRM organization to an external destination

4. Click **Access Azure Service Management as organization users** and then click **Add permissions**.

## Request API permissions

[← All APIs](#)



Azure Service Management

<https://management.azure.com/> [Docs](#)

What type of permissions does your application require?

### Delegated permissions

Your application needs to access the API as the signed-in user.

### Application permissions

Your application runs as a background service or daemon without a signed-in user.

Select permissions

[expand all](#)

| Type to search   |                        |
|--|------------------------|
| PERMISSION   | ADMIN CONSENT REQUIRED |
| <input checked="" type="checkbox"/> <b>user_impersonation</b><br>Access Azure Service Management as organization users (preview) | -                      |

## Getting the application ID and directory ID

When you add the Azure account to BlueXP, you need to provide the application (client) ID and the directory (tenant) ID for the application. BlueXP uses the IDs to programmatically sign in.

### Steps

1. In the **Azure Active Directory** service, click **App registrations** and select the application.
2. Copy the **Application (client) ID** and the **Directory (tenant) ID**.



## Creating a client secret

You need to create a client secret and then provide BlueXP with the value of the secret so BlueXP can use it to authenticate with Azure AD.

### Steps

1. Open the **Azure Active Directory** service.
2. Click **App registrations** and select your application.
3. Click **Certificates & secrets > New client secret**.

4. Provide a description of the secret and a duration.
5. Click **Add**.
6. Copy the value of the client secret.

#### Client secrets

A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.

| + New client secret |           |                                  |
|---------------------|-----------|----------------------------------|
| DESCRIPTION         | EXPIRES   | VALUE                            |
| test secret         | 8/16/2020 | *sZ1jSe2By:D*-ZR0V4NLfdAcY7:+0vA |

Copy to clipboard

### Result

Your service principal is now setup and you should have copied the application (client) ID, the directory (tenant) ID, and the value of the client secret. You need to enter this information in BlueXP when you add an Azure account.

### Adding the credentials to BlueXP

After you provide an Azure account with the required permissions, you can add the credentials for that account to BlueXP. Completing this step enables you to launch Cloud Volumes ONTAP using different Azure credentials.

### Before you get started

If you just created these credentials in your cloud provider, it might take a few minutes until they are available for use. Wait a few minutes before you add the credentials to BlueXP.

### What you'll need

You need to create a Connector before you can change BlueXP settings. [Learn how](#).

### Steps

1. In the upper right of the BlueXP console, click the Settings icon, and select **Credentials**.



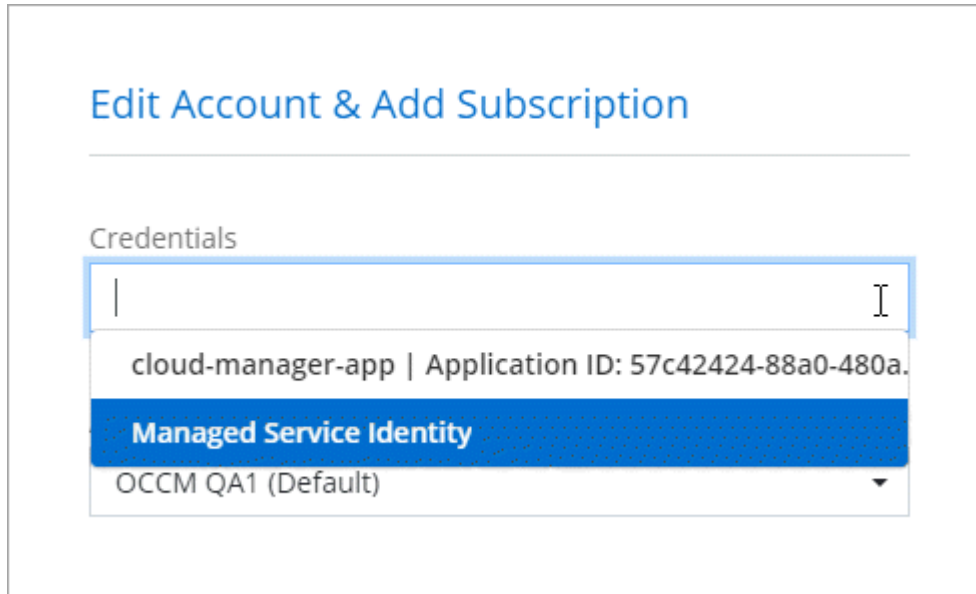
2. Click **Add Credentials** and follow the steps in the wizard.
  - a. **Credentials Location:** Select **Microsoft Azure > Connector**.
  - b. **Define Credentials:** Enter information about the Azure Active Directory service principal that grants the required permissions:
    - Application (client) ID: See [\[Getting the application ID and directory ID\]](#).
    - Directory (tenant) ID: See [\[Getting the application ID and directory ID\]](#).
    - Client Secret: See [Creating a client secret](#).
  - c. **Marketplace Subscription:** Associate a Marketplace subscription with these credentials by subscribing now or by selecting an existing subscription.

To pay for Cloud Volumes ONTAP at an hourly rate (PAYGO), these Azure credentials must be associated with a subscription from the Azure Marketplace.

- d. **Review:** Confirm the details about the new credentials and click **Add**.

## Result

You can now switch to different set of credentials from the Details and Credentials page [when creating a new working environment](#)



## Manage existing credentials

Manage the Azure credentials that you've already added to BlueXP by associating a Marketplace subscription, editing credentials, and deleting them.

### Associating an Azure Marketplace subscription to credentials

After you add your Azure credentials to BlueXP, you can associate an Azure Marketplace subscription to those credentials. The subscription enables you to create a pay-as-you-go Cloud Volumes ONTAP system, and to use other NetApp cloud services.

There are two scenarios in which you might associate an Azure Marketplace subscription after you've already added the credentials to BlueXP:

- You didn't associate a subscription when you initially added the credentials to BlueXP.
- You want to replace an existing Azure Marketplace subscription with a new subscription.

## What you'll need

You need to create a Connector before you can change BlueXP settings. [Learn how](#).

## Steps

1. In the upper right of the BlueXP console, click the Settings icon, and select **Credentials**.
2. Click the action menu for a set of credentials and then select **Associate Subscription**.



3. To associate the credentials with an existing subscription, select the subscription from the down-down list and click **Associate**.
4. To associate the credentials with a new subscription, click **Add Subscription > Continue** and follow the steps in the Azure Marketplace:
  - a. If prompted, log in to your Azure account.
  - b. Click **Subscribe**.
  - c. Fill out the form and click **Subscribe**.
  - d. After the subscription process is complete, click **Configure account now**.

You'll be redirected to the BlueXP website.

- e. From the **Subscription Assignment** page:
  - Select the NetApp accounts that you'd like to associate this subscription with.
  - In the **Replace existing subscription** field, choose whether you'd like to automatically replace the existing subscription for one account with this new subscription.

BlueXP replaces the existing subscription for all credentials in the account with this new subscription. If a set of credentials wasn't ever associated with a subscription, then this new subscription won't be associated with those credentials.

For all other accounts, you'll need to manually associate the subscription by repeating these steps.

- Click **Save**.

The following video shows the steps to subscribe from the Azure Marketplace:

► <https://docs.netapp.com/us-en/cloud-manager-setup->



## Editing credentials

Edit your Azure credentials in BlueXP by modifying the details about your Azure service credentials. For example, you might need to update the client secret if a new secret was created for the service principal application.

### Steps

1. In the upper right of the BlueXP console, click the Settings icon, and select **Credentials**.
2. Click the action menu for a set of credentials and then select **Edit Credentials**.
3. Make the required changes and then click **Apply**.

## Deleting credentials

If you no longer need a set of credentials, you can delete them from BlueXP. You can only delete credentials that aren't associated with a working environment.

### Steps

1. In the upper right of the BlueXP console, click the Settings icon, and select **Credentials**.
2. Click the action menu for a set of credentials and then select **Delete Credentials**.
3. Click **Delete** to confirm.

# Google Cloud credentials

## Google Cloud projects, permissions, and accounts

A service account provides BlueXP with permissions to deploy and manage Cloud Volumes ONTAP systems that are in the same project as the Connector, or in different projects.

### Project and permissions for BlueXP

Before you can deploy Cloud Volumes ONTAP in Google Cloud, you must first deploy a Connector in a Google Cloud project. The Connector can't be running on your premises, or in a different cloud provider.

Two sets of permissions must be in place before you deploy a Connector directly from BlueXP:

1. You need to deploy a Connector using a Google account that has permissions to launch the Connector VM instance from BlueXP.
2. When deploying the Connector, you are prompted to select a [service account](#) for the VM instance. BlueXP gets permissions from the service account to create and manage Cloud Volumes ONTAP systems on your behalf. Permissions are provided by attaching a custom role to the service account.

We have set up two YAML files that include the required permissions for the user and the service account.

[Learn how to use the YAML files to set up permissions.](#)

The following image depicts the permission requirements described in numbers 1 and 2 above:



## Project for Cloud Volumes ONTAP

Cloud Volumes ONTAP can reside in the same project as the Connector, or in a different project. To deploy Cloud Volumes ONTAP in a different project, you need to first add the Connector service account and role to that project.

- [Learn how to set up service account](#)
- [Learn how to deploy Cloud Volumes ONTAP in GCP and select a project](#)

## Managing Google Cloud credentials and subscriptions for BlueXP

You can manage the credentials that are associated with the Connector VM instance.

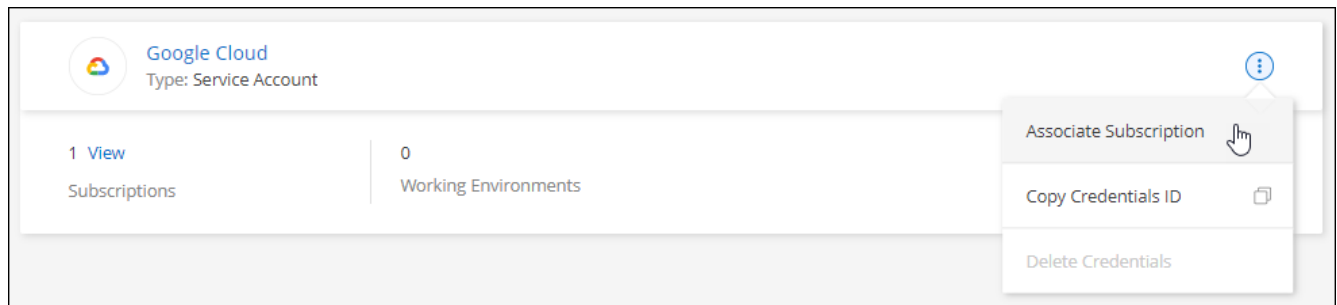
### Associating a Marketplace subscription with Google Cloud credentials

When you deploy a Connector in Google Cloud, BlueXP creates a default set of credentials that are associated with the Connector VM instance. These are the credentials that BlueXP uses to deploy Cloud Volumes ONTAP.

At any time, you can change the Marketplace subscription that's associated with these credentials. The subscription enables you to create a pay-as-you-go Cloud Volumes ONTAP system, and to use other NetApp cloud services.

### Steps

1. In the upper right of the BlueXP console, click the Settings icon, and select **Credentials**.
2. Click the action menu for a set of credentials and then select **Associate Subscription**.



3. To associate the credentials with an existing subscription, select a Google Cloud project and subscription from the down-down list, and then click **Associate**.

 A screenshot of the 'Associate Subscription' form in the Google Cloud console. It features two dropdown menus. The first is labeled 'Google Cloud Project' and has 'OCCM-Dev' selected. The second is labeled 'Subscription' and has 'GCP subscription for staging' selected, which is preceded by a green dot icon. Below these dropdowns is a horizontal line, and at the bottom left is a blue button with a plus icon and the text 'Add Subscription'.

4. If you don't already have a subscription, click **Add Subscription > Continue** and follow the steps in the Google Cloud Marketplace.



Before you complete the following steps, ensure that you have both Billing Admin privileges in your Google Cloud account as well as a BlueXP login.

- a. After you're redirected to the [NetApp BlueXP page on the Google Cloud Marketplace](#), ensure that the correct project is selected at the top navigation menu.

The screenshot shows the 'Product details' page for NetApp BlueXP on the Google Cloud platform. At the top, there's a navigation bar with the Google Cloud logo and a dropdown menu showing 'netapp.com'. Below this, a back arrow and the text 'Product details' are visible. The main content area features the NetApp logo, the product name 'NetApp BlueXP', and a link to 'NetApp, Inc.'. A description states: 'BlueXP lets you build, protect, and govern your hybrid multicloud data estate.' A prominent blue 'SUBSCRIBE' button is centered. Below the button is a horizontal menu with four tabs: 'OVERVIEW' (which is selected and underlined), 'PRICING', 'DOCUMENTATION', and 'SUPPORT'. The 'Overview' section contains two paragraphs of text describing BlueXP's capabilities. To the right of the overview text is a section titled 'Additional details' which lists the product type as 'SaaS & APIs', the last updated date as '12/19/22', and the category as 'Analytics, Developer tools, Storage'.

Google Cloud netapp.com

← Product details

**NetApp** [NetApp, Inc.](#)

BlueXP lets you build, protect, and govern your hybrid multicloud data estate.

**SUBSCRIBE**

OVERVIEW PRICING DOCUMENTATION SUPPORT

**Overview**

BlueXP is NetApp's hybrid multicloud storage and data services experience that helps organizations build and operate a centrally controlled data foundation across on-premises, edge, and cloud environments.

BlueXP abstracts the complexity of architecting the underlying Google Cloud infrastructure resources making it easier to deploy and operate NetApp's storage, mobility, protection, and analysis services within your Google Cloud environment.

**Additional details**

Type: [SaaS & APIs](#)

Last updated: 12/19/22

Category: [Analytics](#), [Developer tools](#), [Storage](#)

- b. Click **Subscribe**.
- c. Select the appropriate billing account and agree to the terms and conditions.
- d. Click **Subscribe**.

This step sends your transfer request to NetApp.

- e. On the pop-up dialog box, click **Register with NetApp, Inc.**

This step must be completed to link the Google Cloud subscription to your NetApp account. The process of linking a subscription isn't complete until you are redirected from this page and then sign in to BlueXP.



f. Complete the steps on the **Subscription Assignment** page:



If someone from your organization has already subscribed to the NetApp BlueXP subscription from your billing account, then you will be redirected to [the Cloud Volumes ONTAP page on the BlueXP website](#) instead. If this is unexpected, contact your NetApp sales team. Google enables only one subscription per Google billing account.

- Select the NetApp accounts that you'd like to associate this subscription with.
- In the **Replace existing subscription** field, choose whether you'd like to automatically replace the existing subscription for one account with this new subscription.

BlueXP replaces the existing subscription for all credentials in the account with this new subscription. If a set of credentials wasn't ever associated with a subscription, then this new subscription won't be associated with those credentials.

For all other accounts, you'll need to manually associate the subscription by repeating these steps.

- Click **Save**.

The following video shows the steps to subscribe from the Google Cloud Marketplace:

► <https://docs.netapp.com/us-en/cloud-manager-setup-admin//media/video-subscribing-google->


[cloud.mp4](#) (video)

- g. Once this process is complete, navigate back to the Credentials page in BlueXP and select this new subscription.


Google Cloud Project

OCCM-Dev

Subscription



GCP subscription for staging

 Add Subscription

### Troubleshooting the Marketplace subscription process

Sometimes subscribing to Cloud Volumes ONTAP through the Google Cloud Marketplace can become fragmented due to incorrect permissions or accidentally not following the redirection to the BlueXP website. If this happens, use the following steps to complete the subscription process.

#### Steps

1. Navigate to the [NetApp BlueXP page on the Google Cloud Marketplace](#) to check on the state of the order. If the page states **Manage on Provider**, scroll down and click **Manage Orders**.




#### Pricing



The product was purchased on 12/9/20.

[MANAGE ORDERS](#)

- If the order shows a green check mark and this is unexpected, somebody else from the organization using the same billing account might already be subscribed. If this is unexpected or you require the details of this subscription, contact your NetApp sales team.

| Filter Enter property name or value   |   |               |          |              |               |          |                  |            |           |   |
|---|---|---------------|----------|--------------|---------------|----------|------------------|------------|-----------|---|
| Status  | Order number  | Plan          | Discount | Start date ↓ | Plan duration | End date | Payment Schedule | Auto-renew | Next plan |   |
|  | 2eebbc...  | Cloud Manager | -        | 10/21/21     | 1 month       | -        | Postpay          | N/A        | N/A       |  |

- If the order shows a clock and **Pending** status, go back to the marketplace page and choose **Manage on Provider** to complete the process as documented above.

| Filter Enter property name or value |              |               |          |              |               |          |                  |            |           |   |
|-------------------------------------|--------------|---------------|----------|--------------|---------------|----------|------------------|------------|-----------|---|
| Status                              | Order number | Plan          | Discount | Start date ↓ | Plan duration | End date | Payment Schedule | Auto-renew | Next plan |   |
| 🕒                                   | d56c66... 📄  | Cloud Manager | -        | Pending      | 1 month       | Pending  | Postpay          | N/A        | N/A       | ⋮ |

## Add and manage NetApp Support Site accounts in BlueXP

Provide the credentials for your NetApp Support Site (NSS) accounts to register for support, enable key workflows for Cloud Volumes ONTAP, and more.

### Overview

Adding your NetApp Support Site account to BlueXP is required to enable the following tasks:

- To register for support
- To deploy Cloud Volumes ONTAP when you bring your own license (BYOL)

Providing your NSS account is required so that BlueXP can upload your license key and to enable the subscription for the term that you purchased. This includes automatic updates for term renewals.

- To register pay-as-you-go Cloud Volumes ONTAP systems

Providing your NSS account is required to activate support for your system and to gain access to NetApp technical support resources.

- To upgrade Cloud Volumes ONTAP software to the latest release

You'll also need to enter your NSS credentials to use Digital Advisor (formerly Active IQ) from within BlueXP. These credentials are associated directly with your user account and are for use with Digital Advisor only. Review more details in the section that follows.

### Manage an NSS account associated with Digital Advisor

When you access Digital Advisor in BlueXP, you're prompted to log in to Digital Advisor by entering your NSS credentials. After you enter your NSS credentials, you'll see this NSS account listed at the top of the NSS Management page. You can then manage those credentials as needed.

Note the following about this NSS account:

- The account is managed at the user level, which means it isn't viewable by other users who log in.
- The account can't be used with any other BlueXP feature: not with Cloud Volumes ONTAP creation, licensing, or support.
- There can be only one NSS account associated with Digital Advisor, per user.

### Steps

1. In the upper right of the BlueXP console, click the Help icon, and select **Support**.



2. Click **NSS Management**.
3. Under **Your NSS Credentials**, click **Action** and choose any of the following options:
  - **Associate NSS user**: Add credentials for a NetApp Support Site account so that you can access Digital Advisor in BlueXP.
  - **Update existing credentials**: Update the credentials for your NetApp Support Site account.
  - **Delete**: Remove the account associated with Digital Advisor.

### Result

BlueXP updates the NSS account associated with Digital Advisor.

## Add an NSS account

The Support Dashboard enables you to add and manage your NetApp Support Site accounts for use with BlueXP at the NetApp account level.

- If you have a customer-level account, you can add one or more NSS accounts.
- If you have a partner or reseller account, you can add one or more NSS accounts, but they can't be added alongside customer-level accounts.

### Steps

1. In the upper right of the BlueXP console, click the Help icon, and select **Support**.





2. Click **NSS Management > Add NSS Account**.
3. When you're prompted, click **Continue** to be redirected to a Microsoft login page.

NetApp uses Microsoft Azure Active Directory as the identity provider for authentication services specific to support and licensing.

4. At the login page, provide your NetApp Support Site registered email address and password to perform the authentication process.

These actions enable BlueXP to use your NSS account for things like license downloads, software upgrade verification, and future support registrations.

Note the following:

- The account must be a customer-level account (not a guest or temp account).
- Upon successful login, NetApp will store the NSS user name. This is a system generated ID that maps to your email. On the **NSS Management** page, you can display your email from the **...** menu.
- If you ever need to refresh your login credential tokens, there is also an **Update Credentials** option in the **...** menu. Using this option prompts you to log in again.

### What's next?

Users can now select the account when creating new Cloud Volumes ONTAP systems, when registering existing Cloud Volumes ONTAP systems, and when registering for support.

- [Launching Cloud Volumes ONTAP in AWS](#)
- [Launching Cloud Volumes ONTAP in Azure](#)
- [Launching Cloud Volumes ONTAP in GCP](#)
- [Registering pay-as-you-go systems](#)

## Update an NSS account for the new authentication method

Starting in November 2021, NetApp now uses Microsoft Azure Active Directory as the identity provider for authentication services specific to support and licensing. As a result of this update, BlueXP will prompt you to update the credentials for any existing accounts that you previously added.

## Steps

1. If you haven't already done so, [create a Microsoft Azure Active Directory B2C account that will be linked to your current NetApp account](#).
2. In the upper right of the BlueXP console, click the Help icon, and select **Support**.
3. Click **NSS Management**.
4. For the NSS account that you want to update, click **Update Account**.



5. When you're prompted, click **Continue** to be redirected to a Microsoft login page.

NetApp uses Microsoft Azure Active Directory as the identity provider for authentication services specific to support and licensing.

6. At the login page, provide your NetApp Support Site registered email address and password to perform the authentication process.

After the process is complete, the account that you updated should now be listed as a *new* account in the table. The *older* version of the account is still listed in the table, along with any existing working environment associations.

7. If existing Cloud Volumes ONTAP working environments are attached to the older version of the account, follow the steps below to [attach those working environments to a different NSS account](#).
8. Go to the older version of the NSS account, click **...** and then select **Delete**.

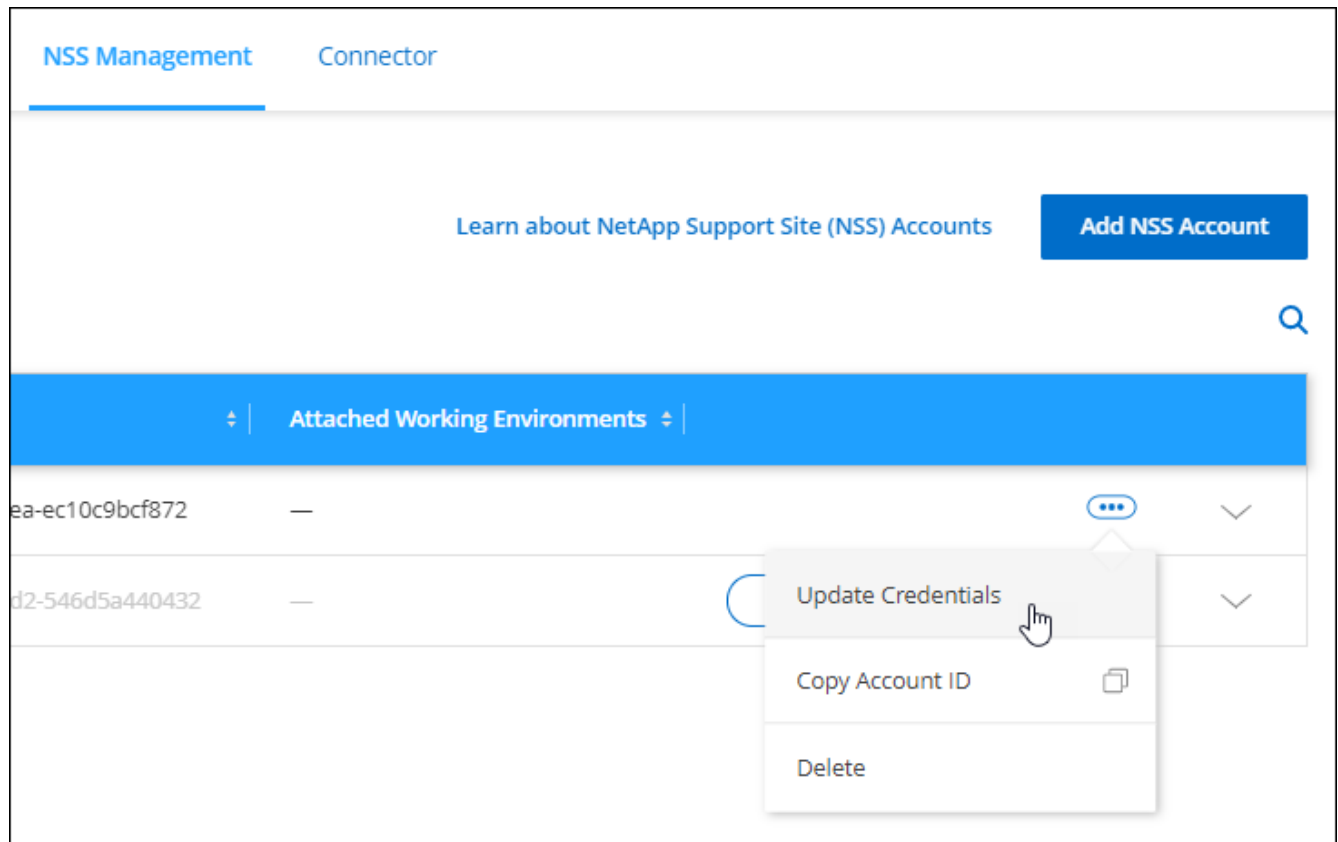
## Update NSS credentials

You'll need to update the credentials for your NSS accounts in BlueXP when either of the following happens:

- You change the credentials for the account
- The refresh token associated with your account expires after 3 months

## Steps

1. In the upper right of the BlueXP console, click the Help icon, and select **Support**.
2. Click **NSS Management**.
3. For the NSS account that you want to update, click **...** and then select **Update Credentials**.



4. When you're prompted, click **Continue** to be redirected to a Microsoft login page.

NetApp uses Microsoft Azure Active Directory as the identity provider for authentication services specific to support and licensing.

5. At the login page, provide your NetApp Support Site registered email address and password to perform the authentication process.

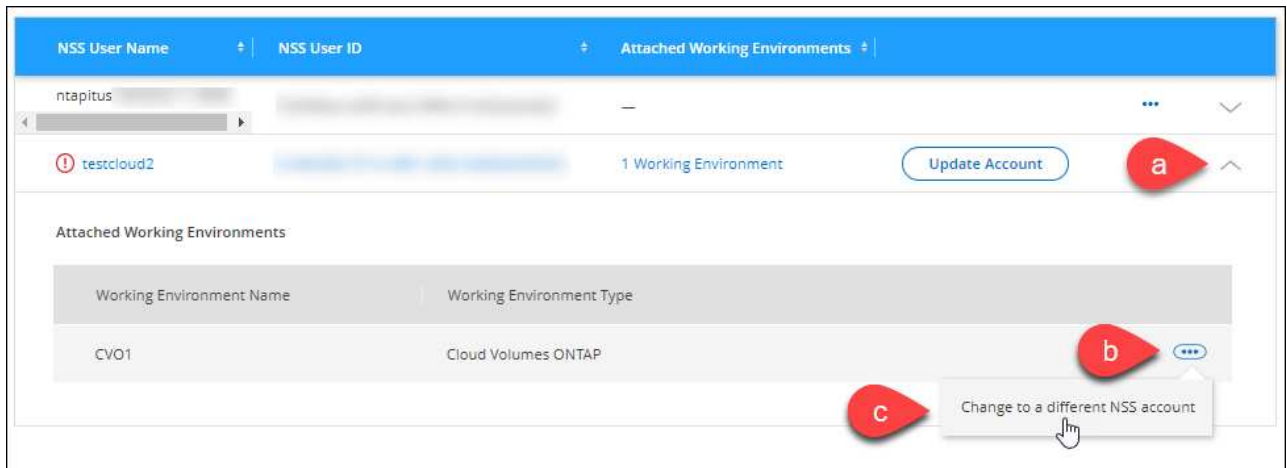
## Attach a working environment to a different NSS account

If your organization has multiple NetApp Support Site accounts, you can change which account is associated with a Cloud Volumes ONTAP system.

This feature is only supported with NSS accounts that are configured to use Microsoft Azure AD adopted by NetApp for identity management. Before you can use this feature, you need click **Add NSS Account** or **Update Account**.

### Steps

1. In the upper right of the BlueXP console, click the Help icon, and select **Support**.
2. Click **NSS Management**.
3. Complete the following steps to change the NSS account:
  - a. Expand the row for the NetApp Support Site account that the working environment is currently associated with.
  - b. For the working environment that you want to change the association for, click **...**
  - c. Select **Change to a different NSS account**.



d. Select the account and then click **Save**.

## Display the email address for an NSS account

Now that NetApp Support Site accounts use Microsoft Azure Active Directory for authentication services, the NSS user name that displays in BlueXP is typically an identifier generated by Azure AD. As a result, you might not immediately know the email address associated with that account. But BlueXP has an option to show you the associated email address.



When you go to the NSS Management page, BlueXP generates a token for each account in the table. That token includes information about the associated email address. The token is then removed when you leave the page. The information is never cached, which helps protect your privacy.

### Steps

1. In the upper right of the BlueXP console, click the Help icon, and select **Support**.
2. Click **NSS Management**.
3. For the NSS account that you want to update, click **...** and then select **Display Email Address**.



## Result

BlueXP displays the NetApp Support Site user name and the associated email address. You can use the copy button to copy the email address.

## Remove an NSS account

Delete any of the NSS accounts that you no longer want to use with BlueXP.

Note that you can't delete an account that is currently associated with a Cloud Volumes ONTAP working environment. You first need to [attach those working environments to a different NSS account](#).

## Steps

1. In the upper right of the BlueXP console, click the Help icon, and select **Support**.
2. Click **NSS Management**.
3. For the NSS account that you want to delete, click **...** and then select **Delete**.



4. Click **Delete** to confirm.

## My Opportunities

On the Canvas, the **My Opportunities** tab provides a centralized location to discover existing resources that you can add to BlueXP for consistent data services and operations across your hybrid multicloud.

Currently, My Opportunities enables you to discover existing FSx for ONTAP file systems in your AWS account.

[Learn how to discover FSx for ONTAP using My Opportunities](#)

# Reference

## Permissions

### Permissions summary for BlueXP

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

#### AWS permissions

| Purpose                       | Description   | Link   |
|-------------------------------|---|--|
| Connector deployment          | The user who creates a Connector from BlueXP needs specific permissions to deploy the instance in AWS.  | <a href="#">Create a Connector in AWS from BlueXP</a>      |
| Connector operation           | <p>When BlueXP launches the Connector, it attaches a policy to the instance that provides the permissions required to manage resources and processes in your AWS account.</p> <p>You need to set up the policy yourself if you <a href="#">launch a Connector from the marketplace</a> or if you <a href="#">add more AWS credentials to a Connector</a>.</p> <p>You also need to ensure that the policy is up to date as new permissions are added in subsequent releases.</p> | <a href="#">AWS permissions for the Connector</a>          |
| Cloud Volumes ONTAP operation | An IAM role must be attached to each Cloud Volumes ONTAP node in AWS. The same is true for the HA mediator. The default option is to let BlueXP create the IAM roles for you, but you can use your own.   | <a href="#">Learn how to set up the IAM roles yourself</a> |

#### Azure permissions

| Purpose              | Description  | Link  |
|----------------------|--|---|
| Connector deployment | When you deploy a Connector from BlueXP, you need to use an Azure account or service principal that has permissions to deploy the Connector VM in Azure. | <a href="#">Create a Connector in Azure from BlueXP</a> |

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

## Google Cloud permissions

| Purpose              | Description   | Link   |
|----------------------|---|--|
| Connector deployment | The Google Cloud user who deploys a Connector from BlueXP needs specific permissions to deploy the Connector in Google Cloud.   | <a href="#">Set up permissions to deploy the Connector</a> |
| Connector operation  | <p>The service account for the Connector VM instance must have specific permissions for day-to-day operations. You need to associate the service account with the Connector when you deploy it from BlueXP.</p> <p>You also need to ensure that the policy is up to date as new permissions are added in subsequent releases.</p> | <a href="#">Set up a service account for the Connector</a> |

## AWS permissions for the Connector

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

### IAM policies

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

If you create a Connector in a standard AWS region directly from BlueXP, BlueXP automatically applies policies to the Connector. You don't need to do anything in this case.

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

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



Select your region to view the required policies:

## Standard regions

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

The first policy provides permissions for the following services:

- Cloud Backup
- Cloud Data Sense
- Cloud Tiering
- Cloud Volumes ONTAP
- FSx for ONTAP
- S3 bucket discovery

The second policy provides permissions for the following services:

- AppTemplate tagging
- Global File Cache
- Kubernetes

## Policy #1

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

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

```

        "kms:ReEncrypt*",
        "kms:Describe*",
        "kms:CreateGrant",
        "ce:GetReservationUtilization",
        "ce:GetDimensionValues",
        "ce:GetCostAndUsage",
        "ce:GetTags",
        "fsx:Describe*",
        "fsx:List*"
    ],
    "Resource": "*",
    "Effect": "Allow",
    "Sid": "cvoServicePolicy"
},
{
    "Action": [
        "ec2:StartInstances",
        "ec2:StopInstances",
        "ec2:DescribeInstances",
        "ec2:DescribeInstanceState",
        "ec2:RunInstances",
        "ec2:TerminateInstances",
        "ec2:DescribeInstanceAttribute",
        "ec2:DescribeImages",
        "ec2:CreateTags",
        "ec2:CreateVolume",
        "ec2:CreateSecurityGroup",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:DescribeRegions",
        "cloudformation:CreateStack",
        "cloudformation>DeleteStack",
        "cloudformation:DescribeStacks",
        "kms:List*",
        "kms:Describe*",
        "ec2:DescribeVpcEndpoints",
        "kms:ListAliases",
        "athena:StartQueryExecution",
        "athena:GetQueryResults",
        "athena:GetQueryExecution",
        "glue:GetDatabase",
        "glue:GetTable",
        "glue:CreateTable",
        "glue:CreateDatabase",
        "glue:GetPartitions",
        "glue:BatchCreatePartition",
    ]
}

```

```

        "glue:BatchDeletePartition"
    ],
    "Resource": "*",
    "Effect": "Allow",
    "Sid": "backupPolicy"
},
{
    "Action": [
        "s3:GetBucketLocation",
        "s3:ListAllMyBuckets",
        "s3:ListBucket",
        "s3:CreateBucket",
        "s3:GetLifecycleConfiguration",
        "s3:PutLifecycleConfiguration",
        "s3:PutBucketTagging",
        "s3:ListBucketVersions",
        "s3:GetBucketAcl",
        "s3:PutBucketPublicAccessBlock",
        "s3:GetObject",
        "s3:PutEncryptionConfiguration",
        "s3:DeleteObject",
        "s3:DeleteObjectVersion",
        "s3:ListBucketMultipartUploads",
        "s3:PutObject",
        "s3:PutBucketAcl",
        "s3:AbortMultipartUpload",
        "s3:ListMultipartUploadParts",
        "s3:DeleteBucket",
        "s3:GetObjectVersionTagging",
        "s3:GetObjectVersionAcl",
        "s3:GetObjectRetention",
        "s3:GetObjectTagging",
        "s3:GetObjectVersion",
        "s3:PutObjectVersionTagging",
        "s3:PutObjectRetention",
        "s3:DeleteObjectTagging",
        "s3:DeleteObjectVersionTagging",
        "s3:GetBucketObjectLockConfiguration",
        "s3:GetBucketVersioning",
        "s3:PutBucketObjectLockConfiguration",
        "s3:PutBucketVersioning",
        "s3:BypassGovernanceRetention",
        "s3:PutBucketPolicy",
        "s3:PutBucketOwnershipControls"
    ],
    "Resource": [

```

```

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

```

```

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

```



```
]
}
```

## Policy #2

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

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

```

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

```

```

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

```

```

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

```

```

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

```

```

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

```

```

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

```



```

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

```

## How the AWS permissions are used

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

### AppTemplate tags

The Connector makes the following API requests to manage tags on AWS resources when you use the AppTemplate Tagging service:

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

## Cloud Backup

The Connector makes the following API requests to deploy the restore instance for Cloud Backup:

- 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

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

- s3:GetBucketLocation
- s3:ListAllMyBuckets
- s3:ListBucket
- s3:CreateBucket
- s3:GetLifecycleConfiguration
- s3:PutLifecycleConfiguration
- s3:PutBucketTagging
- s3:ListBucketVersions
- s3:GetBucketAcl
- s3:PutBucketPublicAccessBlock
- kms:List\*
- kms:Describe\*
- s3:GetObject
- ec2:DescribeVpcEndpoints
- kms:ListAliases
- s3:PutEncryptionConfiguration

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

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

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

- s3:GetObjectVersionTagging
- s3:GetBucketObjectLockConfiguration
- s3:GetObjectVersionAcl
- s3:PutObjectTagging
- s3>DeleteObject
- s3>DeleteObjectTagging
- s3:GetObjectRetention
- s3>DeleteObjectVersionTagging
- s3:PutObject
- s3:GetObject
- s3:PutBucketObjectLockConfiguration
- s3:GetLifecycleConfiguration
- s3:ListBucketByTags

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

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

- s3:PutBucketPolicy
- s3:PutBucketOwnershipControls

#### **Cloud Data Sense**

The Connector makes the following API requests to deploy the Cloud Data Sense instance:

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

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

The Connector makes the following API requests to scan S3 buckets when you use Cloud Data Sense:

- 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 Tiering

The Connector makes the following API requests to tier data to Amazon S3 when you use Cloud Tiering.

| Action                       | Used for set up? | Used for daily operations? |
|------------------------------|------------------|----------------------------|
| s3:CreateBucket              | Yes              | No                         |
| s3:PutLifecycleConfiguration | Yes              | No                         |
| s3:GetLifecycleConfiguration | Yes              | Yes                        |
| ec2:DescribeRegions          | Yes              | No                         |
| ec2:DescribeVpcEndpoints     | Yes              | No                         |

## Cloud Volumes ONTAP

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

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

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

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



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

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

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

### Global File Cache

The Connector makes the following API requests to deploy Global File Cache instances during deployment:

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

### FSx for ONTAP

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

- ec2:DescribeInstances
- ec2:DescribeInstanceStatus
- ec2:DescribeInstanceAttribute
- ec2:DescribeRouteTables
- ec2:DescribeImages
- ec2:CreateTags
- ec2:DescribeVolumes
- ec2:DescribeSecurityGroups
- ec2:DescribeNetworkInterfaces
- ec2:DescribeSubnets
- ec2:DescribeVpcs
- ec2:DescribeDhcpOptions
- ec2:DescribeSnapshots
- ec2:DescribeKeyPairs
- ec2:DescribeRegions

- ec2:DescribeTags
- ec2:DescribeIamInstanceProfileAssociations
- ec2:DescribeReservedInstancesOfferings
- ec2:DescribeVpcEndpoints
- ec2:DescribeVpcs
- ec2:DescribeVolumesModifications
- ec2:DescribePlacementGroups
- kms:List\*
- kms:Describe\*
- kms:CreateGrant
- kms:ListAliases
- fsx:Describe\*
- fsx:List\*

### **Kubernetes**

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

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

### **S3 bucket discovery**

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

s3:GetEncryptionConfiguration

### **Change log**

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

#### **14 February, 2023**

The following permission is now required for Cloud Tiering:

ec2:DescribeVpcEndpoints

### **Azure permissions for the Connector**

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

## Custom role permissions

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

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

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

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

```
{
  "Name": "BlueXP Operator",
  "Actions": [
    "Microsoft.Compute/disks/delete",
    "Microsoft.Compute/disks/read",
    "Microsoft.Compute/disks/write",
    "Microsoft.Compute/locations/operations/read",
    "Microsoft.Compute/locations/vmSizes/read",
    "Microsoft.Resources/subscriptions/locations/read",
    "Microsoft.Compute/operations/read",
    "Microsoft.Compute/virtualMachines/instanceView/read",
    "Microsoft.Compute/virtualMachines/powerOff/action",
    "Microsoft.Compute/virtualMachines/read",
    "Microsoft.Compute/virtualMachines/restart/action",
    "Microsoft.Compute/virtualMachines/deallocate/action",
    "Microsoft.Compute/virtualMachines/start/action",
    "Microsoft.Compute/virtualMachines/vmSizes/read",
    "Microsoft.Compute/virtualMachines/write",
    "Microsoft.Compute/images/read",
    "Microsoft.Network/locations/operationResults/read",
    "Microsoft.Network/locations/operations/read",
    "Microsoft.Network/networkInterfaces/read",
    "Microsoft.Network/networkInterfaces/write",
    "Microsoft.Network/networkInterfaces/join/action",
    "Microsoft.Network/networkSecurityGroups/read",
    "Microsoft.Network/networkSecurityGroups/write",
    "Microsoft.Network/networkSecurityGroups/join/action",
    "Microsoft.Network/virtualNetworks/read",

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

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

```

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

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

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

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

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

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

"Microsoft.Resources/subscriptions/resourceGroups/write",
    "Microsoft.Storage/checknameavailability/read",
    "Microsoft.Storage/operations/read",
    "Microsoft.Storage/storageAccounts/listkeys/action",
    "Microsoft.Storage/storageAccounts/read",
    "Microsoft.Storage/storageAccounts/delete",
    "Microsoft.Storage/storageAccounts/write",

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

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

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

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

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

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

```

```

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

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

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

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

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

"Microsoft.Storage/storageAccounts/PrivateEndpointConnectionsApproval/action",

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

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

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

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

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

"Microsoft.Resources/deployments/operationStatuses/read",
    "Microsoft.Insights/Metrics/Read",
    "Microsoft.Compute/virtualMachines/extensions/write",
    "Microsoft.Compute/virtualMachines/extensions/delete",
    "Microsoft.Compute/virtualMachines/extensions/read",
    "Microsoft.Compute/virtualMachines/delete",
    "Microsoft.Network/networkInterfaces/delete",
    "Microsoft.Network/networkSecurityGroups/delete",
    "Microsoft.Resources/deployments/delete",
    "Microsoft.Compute/diskEncryptionSets/read",

```

```

        "Microsoft.Compute/snapshots/delete",
        "Microsoft.Network/privateEndpoints/delete",
        "Microsoft.Compute/availabilitySets/delete",
        "Microsoft.KeyVault/vaults/read",
        "Microsoft.KeyVault/vaults/accessPolicies/write",
        "Microsoft.Compute/diskEncryptionSets/write",
        "Microsoft.KeyVault/vaults/deploy/action",
        "Microsoft.Compute/diskEncryptionSets/delete",
        "Microsoft.Resources/tags/read",
        "Microsoft.Resources/tags/write",
        "Microsoft.Resources/tags/delete",
        "Microsoft.Network/applicationSecurityGroups/write",
        "Microsoft.Network/applicationSecurityGroups/read",

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

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

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

"Microsoft.ContainerService/managedClusters/listClusterUserCredential/action",

        "Microsoft.ContainerService/managedClusters/read",
        "Microsoft.Synapse/workspaces/write",
        "Microsoft.Synapse/workspaces/read",
        "Microsoft.Synapse/workspaces/delete",
        "Microsoft.Synapse/register/action",
        "Microsoft.Synapse/checkNameAvailability/action",
        "Microsoft.Synapse/workspaces/operationStatuses/read",
        "Microsoft.Synapse/workspaces/firewallRules/read",

"Microsoft.Synapse/workspaces/replaceAllIpFirewallRules/action",
        "Microsoft.Synapse/workspaces/operationResults/read",
        "Microsoft.Network/publicIPAddresses/delete",

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

"Microsoft.ManagedIdentity/userAssignedIdentities/assign/action"
    ],
    "NotActions": [],
    "AssignableScopes": [],
    "Description": "BlueXP Permissions",
    "IsCustom": "true"
}

```



## How Azure permissions are used

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

### AppTemplate tags

The Connector makes the following API requests to manage tags on Azure resources when you use the AppTemplate Tagging service:

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

### Azure NetApp Files

The Connector makes the following API requests to manage Azure NetApp Files working environments:

- Microsoft.NetApp/netAppAccounts/read
- Microsoft.NetApp/netAppAccounts/capacityPools/read
- Microsoft.NetApp/netAppAccounts/capacityPools/volumes/write
- Microsoft.NetApp/netAppAccounts/capacityPools/volumes/read
- Microsoft.NetApp/netAppAccounts/capacityPools/volumes/delete

### Cloud Backup

The Connector makes the following API requests for backup and restore operations:

- Microsoft.Compute/virtualMachines/read
- Microsoft.Compute/virtualMachines/start/action
- Microsoft.Compute/virtualMachines/deallocate/action
- Microsoft.Storage/storageAccounts/listkeys/action
- Microsoft.Storage/storageAccounts/read
- Microsoft.Storage/storageAccounts/write
- Microsoft.Storage/storageAccounts/blobServices/containers/read
- Microsoft.Storage/storageAccounts/listAccountSas/action
- Microsoft.KeyVault/vaults/read
- Microsoft.KeyVault/vaults/accessPolicies/write
- Microsoft.Network/networkInterfaces/read
- Microsoft.Resources/subscriptions/locations/read
- Microsoft.Network/virtualNetworks/read
- Microsoft.Network/virtualNetworks/subnets/read

- Microsoft.Resources/subscriptions/resourceGroups/read
- Microsoft.Resources/subscriptions/resourcegroups/resources/read
- Microsoft.Resources/subscriptions/resourceGroups/write
- Microsoft.Authorization/locks/\*
- Microsoft.Network/privateEndpoints/write
- Microsoft.Network/privateEndpoints/read
- Microsoft.Network/privateDnsZones/virtualNetworkLinks/write
- Microsoft.Network/virtualNetworks/join/action
- Microsoft.Network/privateDnsZones/A/write
- Microsoft.Network/privateDnsZones/read
- Microsoft.Network/privateDnsZones/virtualNetworkLinks/read
- Microsoft.Compute/virtualMachines/extensions/delete
- Microsoft.Compute/virtualMachines/delete
- Microsoft.Network/networkInterfaces/delete
- Microsoft.Network/networkSecurityGroups/delete
- Microsoft.Resources/deployments/delete
- Microsoft.Network/publicIPAddresses/delete
- Microsoft.Storage/storageAccounts/blobServices/containers/write
- Microsoft.ManagedIdentity/userAssignedIdentities/assign/action

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

- Microsoft.Synapse/workspaces/write
- Microsoft.Synapse/workspaces/read
- Microsoft.Synapse/workspaces/delete
- Microsoft.Synapse/register/action
- Microsoft.Synapse/checkNameAvailability/action
- Microsoft.Synapse/workspaces/operationStatuses/read
- Microsoft.Synapse/workspaces/firewallRules/read
- Microsoft.Synapse/workspaces/replaceAllIpFirewallRules/action
- Microsoft.Synapse/workspaces/operationResults/read
- Microsoft.Synapse/workspaces/privateEndpointConnectionsApproval/action

#### Cloud Data Sense

The Connector makes the following API requests when you use Cloud Data Sense.

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

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

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

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

### Cloud Tiering

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

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

The Connector makes the following API requests for daily operations.

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

### Cloud Volumes ONTAP

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

| Purpose  | Action  | Used for deployment? | Used for daily operations? | Used for deletion? |
|--|---|----------------------|----------------------------|--------------------|
| Create VMs, stop, start, delete, and obtain the status of the system | 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                 |
| Enable deployment from a VHD   | Microsoft.Compute/images/read                       | 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                 |
| Create predefined 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                 |
| Get network information about regions, the target VNet and subnet, and add the VMs to VNets | Microsoft.Network/locations/operationResults/read                 | Yes                  | Yes                        | No                 |
|   | Microsoft.Network/locations/operations/read                       | Yes                  | Yes                        | No                 |
|   | Microsoft.Network/virtualNetworks/read                            | Yes                  | No                         | No                 |
|   | Microsoft.Network/virtualNetworks/checkIpAddressAvailability/read | Yes                  | No                         | No                 |
|   | Microsoft.Network/virtualNetworks/subnets/read                    | Yes                  | Yes                        | No                 |
|   | Microsoft.Network/virtualNetworks/subnets/virtualMachines/read    | Yes                  | Yes                        | No                 |
|   | Microsoft.Network/virtualNetworks/virtualMachines/read            | Yes                  | Yes                        | No                 |
|   | Microsoft.Network/virtualNetworks/subnets/join/action             | Yes                  | Yes                        | No                 |

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



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

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

| Purpose                                   | Action  | Used for deployment? | Used for daily operations? | Used for deletion? |
|---|---|----------------------|----------------------------|--------------------|
| Manage a load balancer for HA pairs       | Microsoft.Network/loadBalancers/read                            | Yes                  | Yes                        | No                 |
|   | Microsoft.Network/loadBalancers/write                           | Yes                  | No                         | No                 |
|   | Microsoft.Network/loadBalancers/delete                          | No                   | Yes                        | Yes                |
|   | Microsoft.Network/loadBalancers/backendAddressPools/read        | Yes                  | Yes                        | No                 |
|   | Microsoft.Network/loadBalancers/backendAddressPools/join/action | Yes                  | No                         | No                 |
|   | Microsoft.Network/loadBalancers/loadBalancingRules/read         | Yes                  | No                         | No                 |
|   | Microsoft.Network/loadBalancers/probes/read                     | Yes                  | No                         | No                 |
|   | Microsoft.Network/loadBalancers/probes/join/action              | Yes                  | No                         | No                 |
|   | Microsoft.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 by Azure 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                        | Yes                |
|  | Microsoft.Network/applicationSecurityGroups/joinIpConfiguration/action | No                   | Yes                        | No                 |
|  | Microsoft.Network/networkSecurityGroups/securityRules/write            | Yes                  | Yes                        | No                 |
|  | Microsoft.Network/applicationSecurityGroups/delete                     | No                   | Yes                        | No                 |
|  | 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                 |

## Global File Cache

The Connector makes the following API requests when you use Global File Cache:

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

## Kubernetes

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

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

## Change log

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

### 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 Cloud Backup.

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

This permission is required for Cloud Volumes ONTAP deployment.

### 1 December, 2022

The following permissions were added to the JSON policy:

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

This permission is required for Cloud Backup and Cloud Tiering.

- Microsoft.Network/publicIPAddresses/delete

This permissions is required for Cloud Backup.

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

- Microsoft.Compute/images/write
- Microsoft.Network/loadBalancers/frontendIPConfigurations/read
- Microsoft.Storage/storageAccounts/regeneratekey/action

## Google Cloud permissions for the Connector

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

### Service account permissions

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

You'll need to apply this custom role to a service account that gets attached to the Connector VM. [View step-by-step instructions](#).

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

```
title: NetApp BlueXP
description: Permissions for the service account associated with the
Connector instance.
stage: GA
includedPermissions:
- iam.serviceAccounts.actAs
- compute.regionBackendServices.create
- compute.regionBackendServices.get
- compute.regionBackendServices.list
- compute.networks.updatePolicy
- compute.backendServices.create
- compute.addresses.list
- compute.disks.create
- compute.disks.createSnapshot
- compute.disks.delete
- compute.disks.get
- compute.disks.list
- compute.disks.setLabels
- compute.disks.use
- compute.firewalls.create
```

- `compute.firewalls.delete`
- `compute.firewalls.get`
- `compute.firewalls.list`
- `compute.globalOperations.get`
- `compute.images.get`
- `compute.images.getFromFamily`
- `compute.images.list`
- `compute.images.useReadOnly`
- `compute.instances.addAccessConfig`
- `compute.instances.attachDisk`
- `compute.instances.create`
- `compute.instances.delete`
- `compute.instances.detachDisk`
- `compute.instances.get`
- `compute.instances.getSerialPortOutput`
- `compute.instances.list`
- `compute.instances.setDeletionProtection`
- `compute.instances.setLabels`
- `compute.instances.setMachineType`
- `compute.instances.setMetadata`
- `compute.instances.setTags`
- `compute.instances.start`
- `compute.instances.stop`
- `compute.instances.updateDisplayDevice`
- `compute.instanceGroups.get`
- `compute.addresses.get`
- `compute.instances.updateNetworkInterface`
- `compute.machineTypes.get`
- `compute.networks.get`
- `compute.networks.list`
- `compute.projects.get`
- `compute.regions.get`
- `compute.regions.list`
- `compute.snapshots.create`
- `compute.snapshots.delete`
- `compute.snapshots.get`
- `compute.snapshots.list`
- `compute.snapshots.setLabels`
- `compute.subnetworks.get`
- `compute.subnetworks.list`
- `compute.subnetworks.use`
- `compute.subnetworks.useExternalIp`
- `compute.zoneOperations.get`
- `compute.zones.get`
- `compute.zones.list`
- `compute.instances.setServiceAccount`



- deploymentmanager.compositeTypes.get
- deploymentmanager.compositeTypes.list
- deploymentmanager.deployments.create
- deploymentmanager.deployments.delete
- deploymentmanager.deployments.get
- deploymentmanager.deployments.list
- deploymentmanager.manifests.get
- deploymentmanager.manifests.list
- deploymentmanager.operations.get
- deploymentmanager.operations.list
- deploymentmanager.resources.get
- deploymentmanager.resources.list
- deploymentmanager.typeProviders.get
- deploymentmanager.typeProviders.list
- deploymentmanager.types.get
- deploymentmanager.types.list
- logging.logEntries.list
- logging.privateLogEntries.list
- resourcemanager.projects.get
- storage.buckets.create
- storage.buckets.delete
- storage.buckets.get
- storage.buckets.list
- cloudkms.cryptoKeyVersions.useToEncrypt
- cloudkms.cryptoKeys.get
- cloudkms.cryptoKeys.list
- cloudkms.keyRings.list
- storage.buckets.update
- iam.serviceAccounts.getIamPolicy
- iam.serviceAccounts.list
- storage.objects.get
- storage.objects.list
- monitoring.timeSeries.list
- storage.buckets.getIamPolicy
- cloudkms.cryptoKeys.getIamPolicy
- cloudkms.cryptoKeys.setIamPolicy
- cloudkms.keyRings.get
- cloudkms.keyRings.getIamPolicy
- cloudkms.keyRings.setIamPolicy

## How Google Cloud permissions are used

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

| Actions   | Purpose  |
|---|--|
| <ul style="list-style-type: none"> <li>- compute.networks.get</li> <li>- compute.networks.list</li> <li>- compute.regions.get</li> <li>- compute.regions.list</li> <li>- compute.subnetworks.get</li> <li>- compute.subnetworks.list</li> <li>- compute.zoneOperations.get</li> <li>- compute.zones.get</li> <li>- compute.zones.list</li> </ul>  | To get the networking information needed to create a new Cloud Volumes ONTAP virtual machine instance.   |
| <ul style="list-style-type: none"> <li>- deploymentmanager.compositeTypes.get</li> <li>- deploymentmanager.compositeTypes.list</li> <li>- deploymentmanager.deployments.create</li> <li>- deploymentmanager.deployments.delete</li> <li>- deploymentmanager.deployments.get</li> <li>- deploymentmanager.deployments.list</li> <li>- deploymentmanager.manifests.get</li> <li>- deploymentmanager.manifests.list</li> <li>- deploymentmanager.operations.get</li> <li>- deploymentmanager.operations.list</li> <li>- deploymentmanager.resources.get</li> <li>- deploymentmanager.resources.list</li> <li>- deploymentmanager.typeProviders.get</li> <li>- deploymentmanager.typeProviders.list</li> <li>- deploymentmanager.types.get</li> <li>- deploymentmanager.types.list</li> </ul> | To deploy the Cloud Volumes ONTAP virtual machine instance using Google Cloud Deployment Manager.  |
| <ul style="list-style-type: none"> <li>- logging.logEntries.list</li> <li>- logging.privateLogEntries.list</li> </ul>   | To get stack log drives.   |
| <ul style="list-style-type: none"> <li>- resourcemanager.projects.get</li> </ul>  | To support multi-projects.   |
| <ul style="list-style-type: none"> <li>- storage.buckets.create</li> <li>- storage.buckets.delete</li> <li>- storage.buckets.get</li> <li>- storage.buckets.list</li> <li>- storage.buckets.update</li> </ul>   | To create and manage a Google Cloud Storage bucket for data tiering.   |
| <ul style="list-style-type: none"> <li>- cloudkms.cryptoKeyVersions.useToEncrypt</li> <li>- cloudkms.cryptoKeys.get</li> <li>- cloudkms.cryptoKeys.list</li> <li>- cloudkms.keyRings.list</li> </ul>  | To use customer-managed encryption keys from the Cloud Key Management Service with Cloud Volumes ONTAP.  |
| <ul style="list-style-type: none"> <li>- compute.instances.setServiceAccount</li> <li>- iam.serviceAccounts.actAs</li> <li>- iam.serviceAccounts.getIamPolicy</li> <li>- iam.serviceAccounts.list</li> <li>- storage.objects.get</li> <li>- storage.objects.list</li> </ul>   | To set a service account on the Cloud Volumes ONTAP instance. This service account provides permissions for data tiering to a Google Cloud Storage bucket. |
| <ul style="list-style-type: none"> <li>- compute.addresses.list</li> </ul>  | To retrieve the addresses in a region when deploying an HA pair.   |

| Actions  | Purpose   |
|--|---|
| <ul style="list-style-type: none"> <li>- compute.backendServices.create</li> <li>- compute.regionBackendServices.create</li> <li>- compute.regionBackendServices.get</li> <li>- compute.regionBackendServices.list</li> </ul>  | To configure a backend service for distributing traffic in an HA pair.  |
| <ul style="list-style-type: none"> <li>- compute.networks.updatePolicy</li> </ul>  | To apply firewall rules on the VPCs and subnets for an HA pair.   |
| <ul style="list-style-type: none"> <li>- compute.subnetworks.use</li> <li>- compute.subnetworks.useExternallp</li> <li>- compute.instances.addAccessConfig</li> </ul>  | To enable Cloud Data Sense.   |
| <ul style="list-style-type: none"> <li>- container.clusters.get</li> <li>- container.clusters.list</li> </ul>  | To discover Kubernetes clusters running in Google Kubernetes Engine.  |
| <ul style="list-style-type: none"> <li>- compute.instanceGroups.get</li> <li>- compute.addresses.get</li> <li>- compute.instances.updateNetworkInterface</li> </ul>  | To create and manage storage VMs on Cloud Volumes ONTAP HA pairs.   |
| <ul style="list-style-type: none"> <li>- monitoring.timeSeries.list</li> <li>- storage.buckets.getIamPolicy</li> </ul>   | To discover information about Google Cloud Storage buckets.   |
| <ul style="list-style-type: none"> <li>- cloudkms.cryptoKeys.get</li> <li>- cloudkms.cryptoKeys.getIamPolicy</li> <li>- cloudkms.cryptoKeys.list</li> <li>- cloudkms.cryptoKeys.setIamPolicy</li> <li>- cloudkms.keyRings.get</li> <li>- cloudkms.keyRings.getIamPolicy</li> <li>- cloudkms.keyRings.list</li> <li>- cloudkms.keyRings.setIamPolicy</li> </ul> | To select your own customer-managed keys in the Cloud Backup activation wizard instead of using the default Google-managed encryption keys. |

## Change log

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

### 6 February, 2023

The following permission was added to this policy:

- compute.instances.updateNetworkInterface

This permission is required for Cloud Volumes ONTAP.

### 27 January, 2023

The following permissions were added to the policy:

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

These permissions are required for Cloud Backup.

## Ports

### Security group rules in AWS

The AWS security group for the Connector requires both inbound and outbound rules.

#### Inbound rules

| Protocol | Port       | Purpose   |
|----------|------------|---|
| SSH      | 22         | Provides SSH access to the Connector host   |
| HTTP     | 80         | Provides HTTP access from client web browsers to the local user interface   |
| HTTPS    | 443        | Provides HTTPS access from client web browsers to the local user interface, and connections from the Cloud Data Sense 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. <a href="#">Learn more about the Connector's proxy server.</a> |
| TCP      | 9060, 9061 | Provides the ability to enable and use Cloud Data Sense and Cloud Backup in Government Cloud deployments. These ports are also required for Cloud Backup if you disable the SaaS interface in your BlueXP account.  |

#### Outbound rules

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

#### Basic outbound rules

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

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

#### Advanced outbound rules

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



The source IP address is the Connector host.

| Service                   | Protocol | Port | Destination  | Purpose  |
|---------------------------|----------|------|--|--|
| API calls and AutoSupport | HTTPS    | 443  | Outbound internet and ONTAP cluster management LIF | API calls to AWS and ONTAP, to Cloud Data Sense, to the Ransomware service, and sending AutoSupport messages to NetApp |

| Service   | Protocol | Port | Destination       | Purpose                                  |
|-----------|----------|------|-------------------|--|
| API calls | TCP      | 3000 | ONTAP HA mediator | Communication with the ONTAP HA mediator |
|           | TCP      | 8088 | Backup to S3      | API calls to Backup to S3                |
| DNS       | UDP      | 53   | DNS               | Used for DNS resolve by BlueXP           |

## Security group rules in Azure

The Azure security group for the Connector requires both inbound and outbound rules.

### Inbound rules

| Protocol | Port       | Purpose   |
|----------|------------|---|
| SSH      | 22         | Provides SSH access to the Connector host   |
| HTTP     | 80         | Provides HTTP access from client web browsers to the local user interface   |
| HTTPS    | 443        | Provides HTTPS access from client web browsers to the local user interface, and connections from the Cloud Data Sense 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. <a href="#">Learn more about the Connector's proxy server.</a> |
| TCP      | 9060, 9061 | Provides the ability to enable and use Cloud Data Sense and Cloud Backup in Government Cloud deployments. These ports are also required for Cloud Backup if you disable the SaaS interface in your BlueXP account.  |

### Outbound rules

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

#### Basic outbound rules

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

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

#### Advanced outbound rules

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



The source IP address is the Connector host.

| Service                   | Protocol | Port | Destination  | Purpose  |
|---------------------------|----------|------|--|--|
| API calls and AutoSupport | HTTP     | 443  | Outbound internet and ONTAP cluster management LIF | API calls to Azure and ONTAP, to Cloud Data Sense, to the Ransomware service, and sending AutoSupport messages to NetApp |
| DNS                       | UDP      | 53   | DNS  | Used for DNS resolve by BlueXP   |

## Firewall rules in Google Cloud

The Google Cloud firewall rules for the Connector requires both inbound and outbound rules.

### Inbound rules

| Protocol | Port | Purpose   |
|----------|------|---|
| SSH      | 22   | Provides SSH access to the Connector host   |
| HTTP     | 80   | Provides HTTP access from client web browsers to the local user interface   |
| HTTPS    | 443  | Provides HTTPS access from client web browsers to the local user interface  |
| TCP      | 3128 | Provides Cloud Volumes ONTAP with internet access to send AutoSupport messages to NetApp Support. You must manually open this port after deployment. <a href="#">Learn more about the Connector's proxy server.</a> |

### Outbound rules

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

#### Basic outbound rules

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

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

#### Advanced outbound rules

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



The source IP address is the Connector host.

| Service                   | Protocol | Port | Destination  | Purpose  |
|---------------------------|----------|------|--|--|
| API calls and AutoSupport | HTTPS    | 443  | Outbound internet and ONTAP cluster management LIF | API calls to GCP and ONTAP, to Cloud Data Sense, to the Ransomware service, and sending AutoSupport messages to NetApp |
| DNS                       | UDP      | 53   | DNS  | Used for DNS resolve by BlueXP   |

## Ports for the on-prem Connector

The Connector uses the following *inbound* ports when installed manually on an on-premises Linux host.

These inbound rules apply to both deployment models for the on-prem Connector: installed with internet access or without internet access.

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



# Knowledge and support

## Register for support

Before you can open a support case with NetApp technical support, you need to add a NetApp Support Site (NSS) account to BlueXP and then register for support.

### Support for cloud provider solutions

For technical support on the following cloud provider solutions you've integrated into BlueXP, refer to "Getting help" in the BlueXP documentation for that product.

- [Amazon FSx for ONTAP](#)
- [Azure NetApp Files](#)
- [Cloud Volumes Service for Google Cloud](#)

### Support registration overview

There are two forms of registration to activate support entitlement:

- Registering your BlueXP account ID support subscription (your 20 digit 960xxxxxxx serial number located on the Support Resources page in BlueXP).

This serves as your single support subscription ID for any service within BlueXP. Each BlueXP account-level support subscription must be registered.

- Registering the Cloud Volumes ONTAP serial numbers associated with a subscription in your cloud provider's marketplace (these are 20 digit 909201xxxxxxx serial numbers).

These serial numbers are commonly referred to as *PAYGO serial numbers* and get generated by BlueXP at the time of Cloud Volumes ONTAP deployment.

Registering both types of serial numbers enables capabilities like opening support tickets and automatic case generation.

How you register depends on whether you're a new or existing customer or partner.

- Existing customer or partner

As an existing NetApp customer or partner, you can use your NetApp Support Site (NSS) SSO account to perform these registrations above. In the Support Dashboard, BlueXP provides an **NSS Management** page where you can add your NSS account. Once you add your NSS account, BlueXP automatically registers these serial numbers for you.

[Learn how to add your NSS account.](#)

- New to NetApp

If you're brand new to NetApp, you must complete a one-time registration of your BlueXP account ID serial number on NetApp's support registration site. Once you complete this registration and create a new NSS account, you can use this account in BlueXP to auto register going forward.

## Add an NSS account to BlueXP

The Support Dashboard enables you to add and manage your NetApp Support Site accounts for use with BlueXP.

- If you have a customer-level account, you can add one or more NSS accounts.
- If you have a partner or reseller account, you can add one or more NSS accounts, but they can't be added alongside customer-level accounts.

### Steps

1. In the upper right of the BlueXP console, click the Help icon, and select **Support**.



2. Click **NSS Management > Add NSS Account**.
3. When you're prompted, click **Continue** to be redirected to a Microsoft login page.

NetApp uses Microsoft Azure Active Directory as the identity provider for authentication services specific to support and licensing.

4. At the login page, provide your NetApp Support Site registered email address and password to perform the authentication process.

These actions enable BlueXP to use your NSS account for things like license downloads, software upgrade verification, and future support registrations.

Note the following:

- The account must be a customer-level account (not a guest or temp account).
- Upon successful login, NetApp will store the NSS user name. This is a system generated ID that maps to your email. On the **NSS Management** page, you can display your email from the **...** menu.
- If you ever need to refresh your login credential tokens, there is also an **Update Credentials** option in the **...** menu. Using this option prompts you to log in again.

## Register with NetApp

How you register for NetApp support depends on whether you already have a NetApp Support Site (NSS) account.

### Existing customer with an NSS account

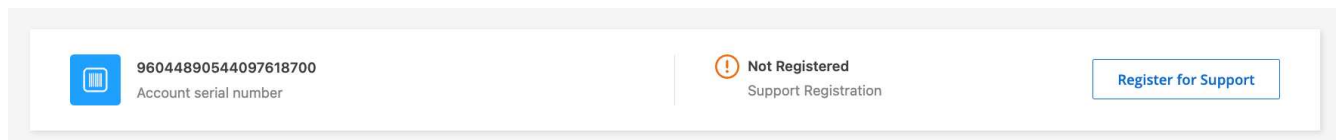
If you're a NetApp customer with an NSS account, you simply need to register for support through BlueXP.

#### Steps

1. In the upper right of the BlueXP console, click the Help icon, and select **Support**.



2. If you haven't already done so, add your NSS account to BlueXP.
3. On the **Resources** page, click **Register for Support**.



### Existing customer but no NSS account

If you're an existing NetApp customer with existing licenses and serial numbers but *no* NSS account, you just need to create an NSS account.

#### Steps

1. Create a NetApp Support Site account by completing the [NetApp Support Site User Registration form](#)
  - a. Be sure to select the appropriate User Level, which is typically **NetApp Customer/End User**.
  - b. Be sure to copy the BlueXP account serial number (960xxxx) used above for the serial number field. This will speed up the account processing.

### Brand new to NetApp

If you are brand new to NetApp and you don't have an NSS account, follow each step below.

## Steps

1. In the upper right of the BlueXP console, click the Help icon, and select **Support**.



2. Locate your account ID serial number from the Support Registration page.



3. Navigate to [NetApp's support registration site](#) and select **I am not a registered NetApp Customer**.
4. Fill out the mandatory fields (those with red asterisks).
5. In the **Product Line** field, select **Cloud Manager** and then select your applicable billing provider.
6. Copy your account serial number from step 2 above, complete the security check, and then confirm that you read NetApp's Global Data Privacy Policy.

An email is immediately sent to the mailbox provided to finalize this secure transaction. Be sure to check your spam folders if the validation email doesn't arrive in few minutes.

7. Confirm the action from within the email.

Confirming submits your request to NetApp and recommends that you create a NetApp Support Site account.

8. Create a NetApp Support Site account by completing the [NetApp Support Site User Registration form](#)
  - a. Be sure to select the appropriate User Level, which is typically **NetApp Customer/End User**.
  - b. Be sure to copy the account serial number (960xxxx) used above for the serial number field. This will speed up the account processing.

## After you finish

NetApp should reach out to you during this process. This is a one-time onboarding exercise for new users.

Once you have your NetApp Support Site account, you can navigate to BlueXP to add this NSS account for future registrations.

# Get help

NetApp provides support for BlueXP and its cloud services in a variety of ways. Extensive free self-support options are available 24x7, such as knowledgebase (KB) articles and a community forum. Your support registration includes remote technical support via web ticketing.

## Self support

These options are available for free, 24 hours a day, 7 days a week:

- [Knowledge base](#)

Search through the BlueXP knowledge base to find helpful articles to troubleshoot issues.

- [Communities](#)

Join the BlueXP community to follow ongoing discussions or create new ones.

- [Documentation](#)

The BlueXP documentation that you're currently viewing.

- [Feedback email](#)

We value your input. Submit feedback to help us improve BlueXP.

## NetApp support

In addition to the self-support options above, you can work with a NetApp Support specialist to resolve any issues after you activate support.

### Before you get started

To use the **Create a Case** capability, you must first perform a one-time registration of your BlueXP Account ID serial number (ie. 960xxxx) with NetApp. [Learn how to register for support.](#)

### Steps

1. In BlueXP, click **Help > Support**.
2. Choose one of the available options under Technical Support:
  - a. Click **Call Us** if you'd like to speak with someone on the phone. You'll be directed to a page on netapp.com that lists the phone numbers that you can call.
  - b. Click **Create a Case** to open a ticket with a NetApp Support specialists:
    - **NetApp Support Site Account:** Select the applicable NSS account associated with the person opening the support case. This person will be the primary contact for NetApp to reach out to, in addition to the additional emails provided below.

If you don't see your NSS account, you can navigate to the **NSS Management** tab within Support section of BlueXP to add it there.
    - **Service:** Select the service that the issue is associated with. For example, BlueXP when specific to a technical support issue with workflows or functionality within the service.
    - **Working Environment:** If applicable to storage, select **Cloud Volumes ONTAP** or **On-Prem** and

then the associated working environment.


The list of working environments are within scope of the BlueXP account, workspace, and Connector you have selected in the top banner of the service.

- **Case Priority:** Choose the priority for the case, which can be Low, Medium, High, or Critical.

To learn more details about these priorities, hover your mouse over the information icon next to the field name.

- **Issue Description:** Provide a detailed description of your problem, including any applicable error messages or troubleshooting steps that you performed.
- **Additional Email Addresses:** Enter additional email addresses if you'd like to make someone else aware of this issue.

### Create a Case

TESTCLOUD2NTAP 

NetApp Support Site Account


---

Service

Working Environment

Cloud Manager


Select...

Case Priority 


Low - General Guidance

Issue Description

Provide a detailed description of your problem, including any applicable error messages or troubleshooting steps that you performed.

Additional Email Addresses (Optional) 

Attachment (Optional) Coming Soon

No files selected 

### After you finish

A pop-up will appear with your support case number. A NetApp Support specialist will review your case and get back to you soon.

For a history of your support cases, you can click **Settings > Timeline** and look for actions named "create support case." A button to the far right lets you expand the action to see details.

It's possible that you might encounter the following error message when trying to create a case:

"You are not authorized to Create a Case against the selected service"

This error could mean that the NSS account and the company of record it's associated with is not the same company of record for the BlueXP account serial number (ie. 960xxxx) or the working environment serial number. You can check your list of NSS accounts at the top of the **Create a Case** form to find the right match, or you can seek assistance using one of the following options:

- Use the in-product chat
- Submit a non-technical case at <https://mysupport.netapp.com/site/help>

# Legal notices

Legal notices provide access to copyright statements, trademarks, patents, and more.

## Copyright

<http://www.netapp.com/us/legal/copyright.aspx>

## Trademarks

NETAPP, the NETAPP logo, and the marks listed on the NetApp Trademarks page are trademarks of NetApp, Inc. Other company and product names may be trademarks of their respective owners.

<http://www.netapp.com/us/legal/netapptmlist.aspx>

## Patents

A current list of NetApp owned patents can be found at:

<https://www.netapp.com/us/media/patents-page.pdf>

## Privacy policy

<https://www.netapp.com/us/legal/privacypolicy/index.aspx>

## Open source

Notice files provide information about third-party copyright and licenses used in NetApp software.

- [Notice for BlueXP](#)



## Copyright information

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

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

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

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

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

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

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

## Trademark information

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