



BlueXP setup and administration documentation

Setup and administration

NetApp
April 25, 2023

This PDF was generated from <https://docs.netapp.com/us-en/cloud-manager-setup-admin/index.html> on April 25, 2023. Always check docs.netapp.com for the latest.

Table of Contents

- BlueXP setup and administration documentation. 1
- Release notes 2
 - What’s new 2
 - Known limitations 17
- Get started 19
 - Learn the basics 19
 - Get started with standard mode 39
 - Get started with restricted mode 127
 - Get started with private mode 158
- Administer BlueXP 177
 - Using identity federation with BlueXP 177
 - BlueXP accounts 181
 - Connectors 195
 - Credentials 207
 - Discovered cloud storage 244
- Reference 248
 - Permissions 248
 - Ports 303
- Knowledge and support 308
 - Register for support 308
 - Get help 312
- Legal notices 318
 - Copyright 318
 - Trademarks 318
 - Patents 318
 - Privacy policy 318
 - Open source 318

BlueXP setup and administration documentation

Release notes

What's new

Learn what's new with BlueXP administration features: BlueXP accounts, Connectors, cloud provider credentials, and more.

4 April 2023

Deployment modes

BlueXP *deployment modes* enable you to use BlueXP in a way that meets your business and security requirements. You can choose from three modes:

- Standard mode
- Restricted mode
- Private mode

[Learn more about these deployment modes.](#)



The introduction of restricted mode replaces the option to enable or disable the SaaS platform. You can enable restricted mode at the time of account creation. It can't be enabled or disabled later.

3 April 2023

Connector 3.9.28

- Email notifications are now supported with the BlueXP digital wallet.

If you configure your notification settings, you can receive email notifications when your BYOL licenses are about to expire (a "Warning" notification) or if they have already expired (an "Error" notification).

[Learn how to set up email notifications.](#)

- The Connector is now supported in the Google Cloud Turin region.

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

- You can now discover VMware vCenter Servers in BlueXP.

After you discover a VMware vCenter Server that's running in AWS or on your premises, you can open the working environment to view details about the datastores and virtual machines that are associated with the server.

The only requirement is a Connector that has a connection to a VMware vCenter Server that is running version 7.0 or later.

To get started, select **Add Working Environment**, select **Amazon Web Services** or **On-Premises**, and then select **VMware vCenter Server**. Enter the domain name or IP address for the server, and then enter the user name and password for the admin user.

- You can now manage the user credentials that are associated with your BlueXP login: ONTAP credentials and NetApp Support Site (NSS) credentials.

When you go to **Settings > Credentials**, you can view the credentials, update the credentials, and delete them. For example, if you change the password for these credentials, then you'll need to update the password in BlueXP.

[Learn how to manage user credentials.](#)

- You can now upload attachments when you create a support case or when you update the case notes for an existing support case.

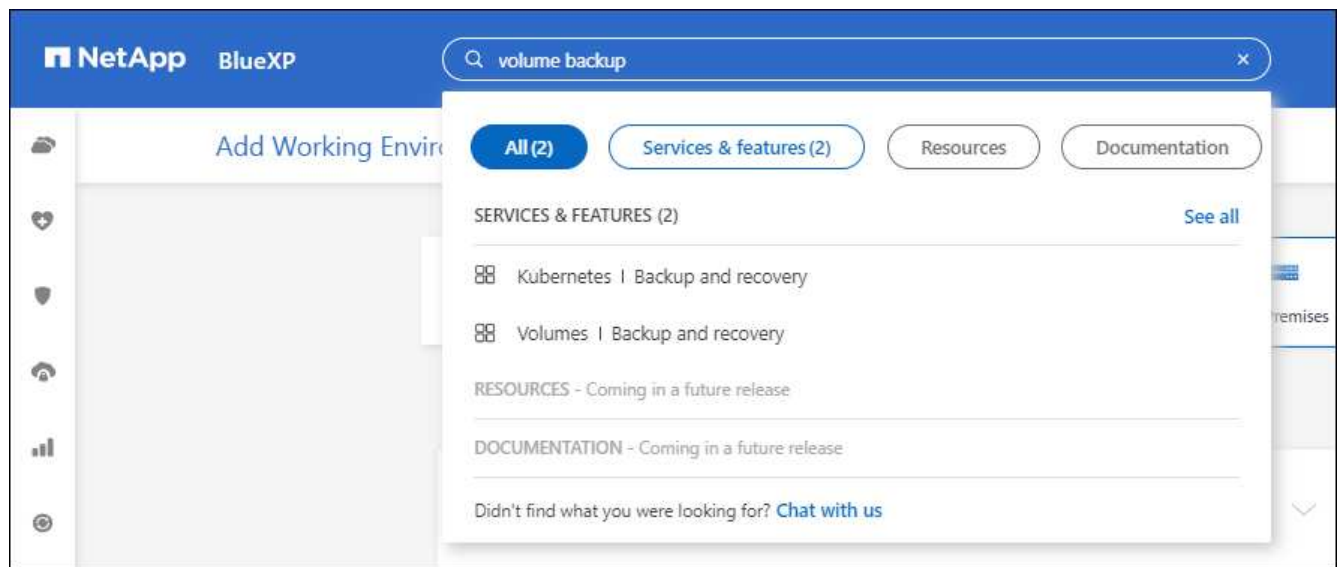
[Learn how to create and manage support cases.](#)

- 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](#)

5 March 2023

Connector 3.9.27

- Search is now available in the BlueXP console. At this time, you can use the search to find BlueXP services and features.



- You can view and manage active and resolved support cases directly from BlueXP. You can manage the cases associated with your NSS account and with your company.

[Learn how to manage your support cases.](#)

- The Connector is now supported on a host that's running Red Hat Enterprise Linux 8.7.

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

- The Connector is now supported in any cloud environment that has complete isolation from the internet.

You can then use the BlueXP console that's running on the Connector to deploy Cloud Volumes ONTAP in the same location and to discover on-premises ONTAP clusters (if you have a connection from your cloud environment to on your on-premises environment). You can also use BlueXP backup and recovery to back up Cloud Volumes ONTAP volumes in AWS and Azure commercial regions. No other BlueXP services are supported in this type of deployment, except for the BlueXP digital wallet.

The cloud region can be a region for secure US agencies like AWS C2S/SC2S, Azure IL6, or any commercial region.

To get started, manually install the Connector software, log in to the BlueXP console that's running on the Connector, add your BYOL license to the BlueXP digital wallet, and then deploy Cloud Volumes ONTAP.

- [Install the Connector in a location without internet access](#)
- [Access the BlueXP console on the Connector](#)
- [Add an unassigned license](#)
- [Get started with Cloud Volumes ONTAP](#)
- The Connector now enables you to add and manage Amazon S3 buckets from BlueXP.

[See how to add new Amazon S3 buckets in your AWS account from BlueXP.](#)

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

[Learn about Cloud Volumes ONTAP enhancements](#)

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



Log in to NetApp BlueXP

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:

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 |
| 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

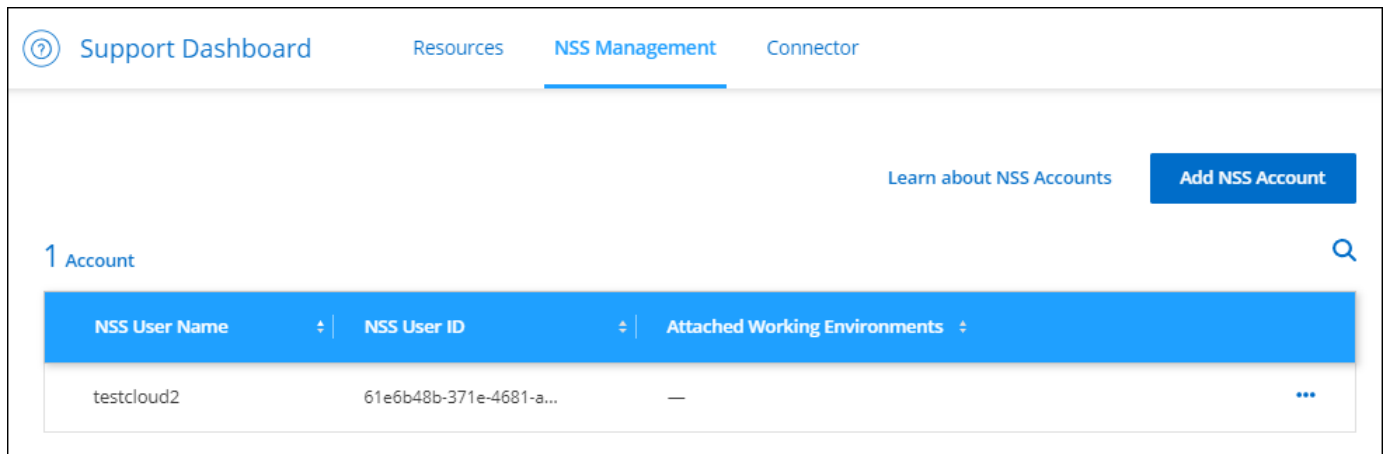
tags, specify a role (for AWS or Azure), upload a root certificate for a proxy server, view code for Terraform automation, view progress details, and more.

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

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.](#)



The screenshot shows the 'Support Dashboard' with tabs for 'Resources', 'NSS Management' (selected), and 'Connector'. In the 'NSS Management' section, there is a link 'Learn about NSS Accounts' and a blue button 'Add NSS Account'. Below this, it says '1 Account' with a search icon. A table displays the account details:

| 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

Default EC2 instance settings should not be changed

When you deploy the Connector in AWS, the following EC2 instance settings are configured by default:

- IMDSv2 is set to optional
- HttpTokens is set to optional

These settings should not be changed to required. Changing these settings to required impacts the Connector and Cloud Volumes ONTAP availability.

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 web-based console that's running on a Connector, the interface 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.

Get started

Learn the basics

Learn about BlueXP

NetApp BlueXP provides your organization with a single control plane that helps you build, protect, and govern data across your on-premises and cloud environments. The BlueXP SaaS platform includes storage and data services that provide storage management, data mobility, data protection, and data analysis and control. Management capabilities are provided through a web-based console and APIs.

Features

The BlueXP platform provides four main pillars of data management: storage, mobility, protection, and analysis and control.

Storage

Discover, deploy, and manage storage, whether it's in AWS, Azure, Google Cloud, or on premises.

- 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
- Orchestrate and protect [Kubernetes persistent data](#)

Mobility

Move data where it's needed by syncing, copying, tiering, and caching data.

- [Copy and sync](#)
- [Edge caching](#)
- [Tiering](#)

Protection

Use automated protection mechanisms to protect data against data loss, unplanned outages, ransomware, and other cyber threats.

- [Backup and recovery](#)
- [Replication](#)

Analysis and control

Use tools to monitor, map, and optimize your data storage and infrastructure.

- [Classification](#)
- [Digital advisor](#)
- [Ransomware protection](#)

[Learn more about how you can use BlueXP to help your organization](#)

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 web-based console that's provided through the SaaS layer, accounts that provide multi-tenancy, and Connectors that manage Cloud Volumes ONTAP and other cloud services.

Software-as-a-service

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

BlueXP account

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

[Learn more about accounts.](#)

Connectors

You don't need a Connector to get started with BlueXP, but you'll need to create a Connector to unlock all BlueXP features and services. A Connector enables the management of resources and processes across your on-premises and cloud environments. It's required to use Cloud Volumes ONTAP and other data services.

[Learn more about Connectors.](#)

Restricted mode and private mode

BlueXP is also supported in environments that have security and connectivity restrictions. You can use *restricted mode* or *private mode* to limit outbound connectivity to the BlueXP SaaS layer.

[Learn more about BlueXP deployment modes.](#)

SOC 2 Type 2 certification

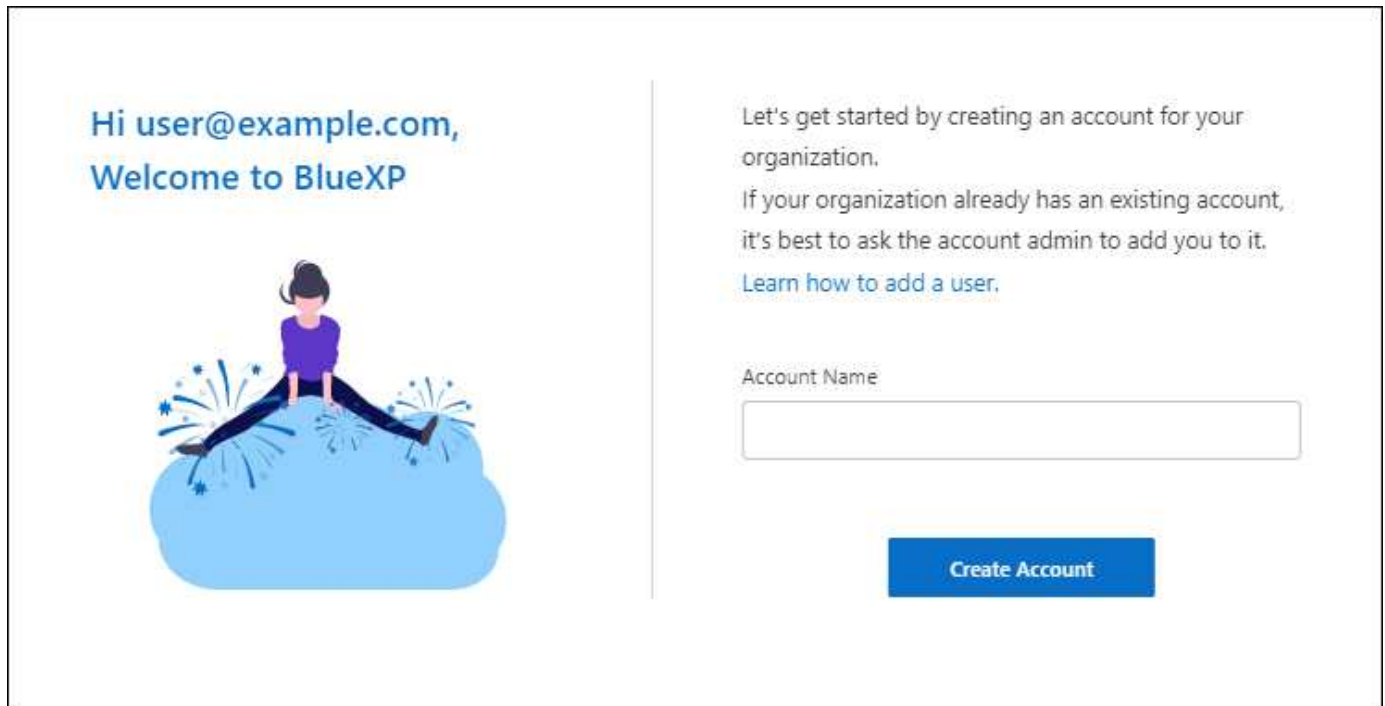
An independent certified public accountant firm and services auditor examined BlueXP and affirmed that it achieved SOC 2 Type 2 reports based on the applicable Trust Services criteria.

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

Learn about BlueXP accounts

A *BlueXP account* provides multi-tenancy for your organization, which enables you to organize users and resources in isolated *workspaces*. For example, a group of users can deploy and manage Cloud Volumes ONTAP systems in a workspace that isn't visible to other users.

When you first access BlueXP, you're prompted to select or create an account. For example, you'll see the following screen if you don't have an account yet:

The image shows a screenshot of the BlueXP account creation interface. On the left side, there is a welcome message: "Hi user@example.com, Welcome to BlueXP" in blue text. Below the text is an illustration of a person in a purple shirt and black pants sitting on a large blue cloud, with small blue starburst effects around them. On the right side, there is a vertical line separating the welcome message from the account creation form. The form contains the following elements: a paragraph of text stating "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.](#)", a text input field labeled "Account Name", and a blue button labeled "Create Account".

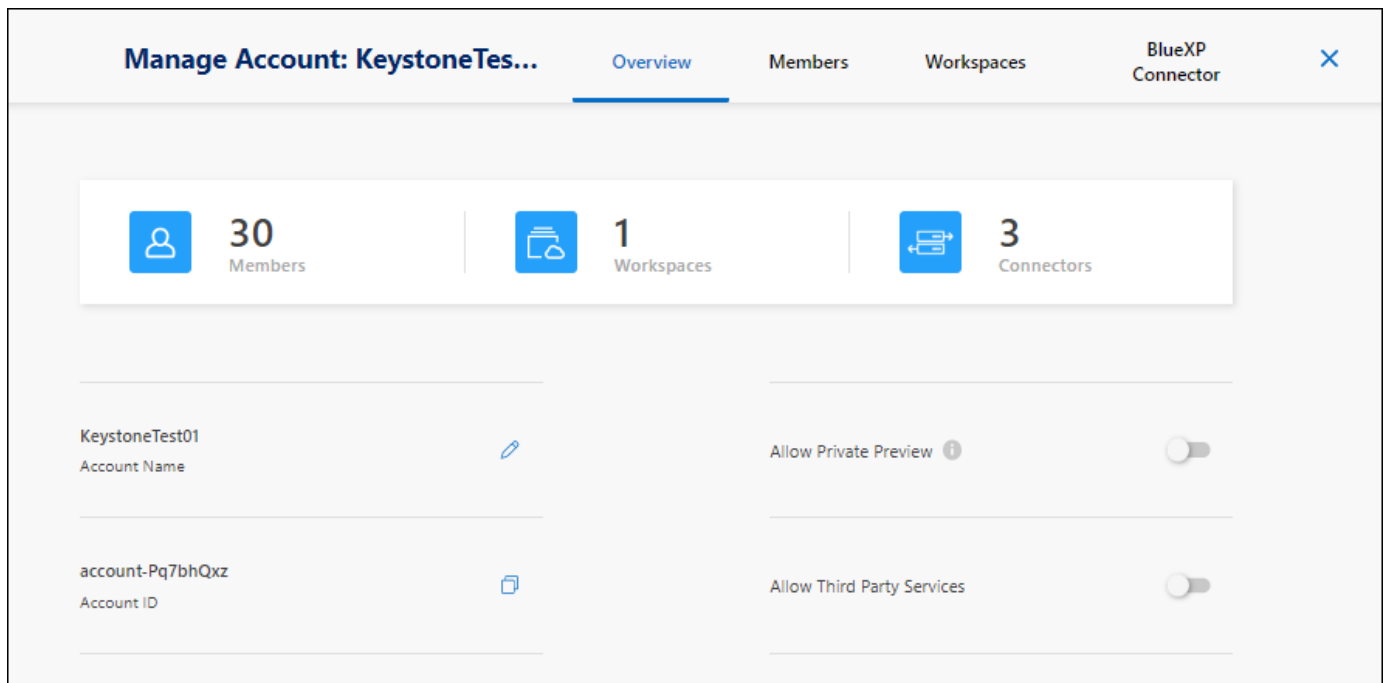
Hi user@example.com,
Welcome to BlueXP

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:



[Learn how to manage your BlueXP account.](#)

Deployment modes

BlueXP offers the following deployment modes for your account: standard mode, restricted mode, and private mode. These modes support environments that have varying levels of security and connectivity restrictions.

[Learn more about BlueXP deployment modes.](#)

Members

Members are BlueXP users that you associate with your BlueXP 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 compliance information for BlueXP classification and generate reports for workspaces that they have permission to access.

[Learn more about these roles.](#)

Workspaces

In BlueXP, a workspace isolates any number of *working environments* from other users in the account. 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 executes the actions that BlueXP needs to perform in order to manage your data infrastructure. The Connector runs on a virtual machine instance that you deploy in your cloud provider or on an on-premises host that you configured.

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

[Learn more about Connectors.](#)

Examples

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

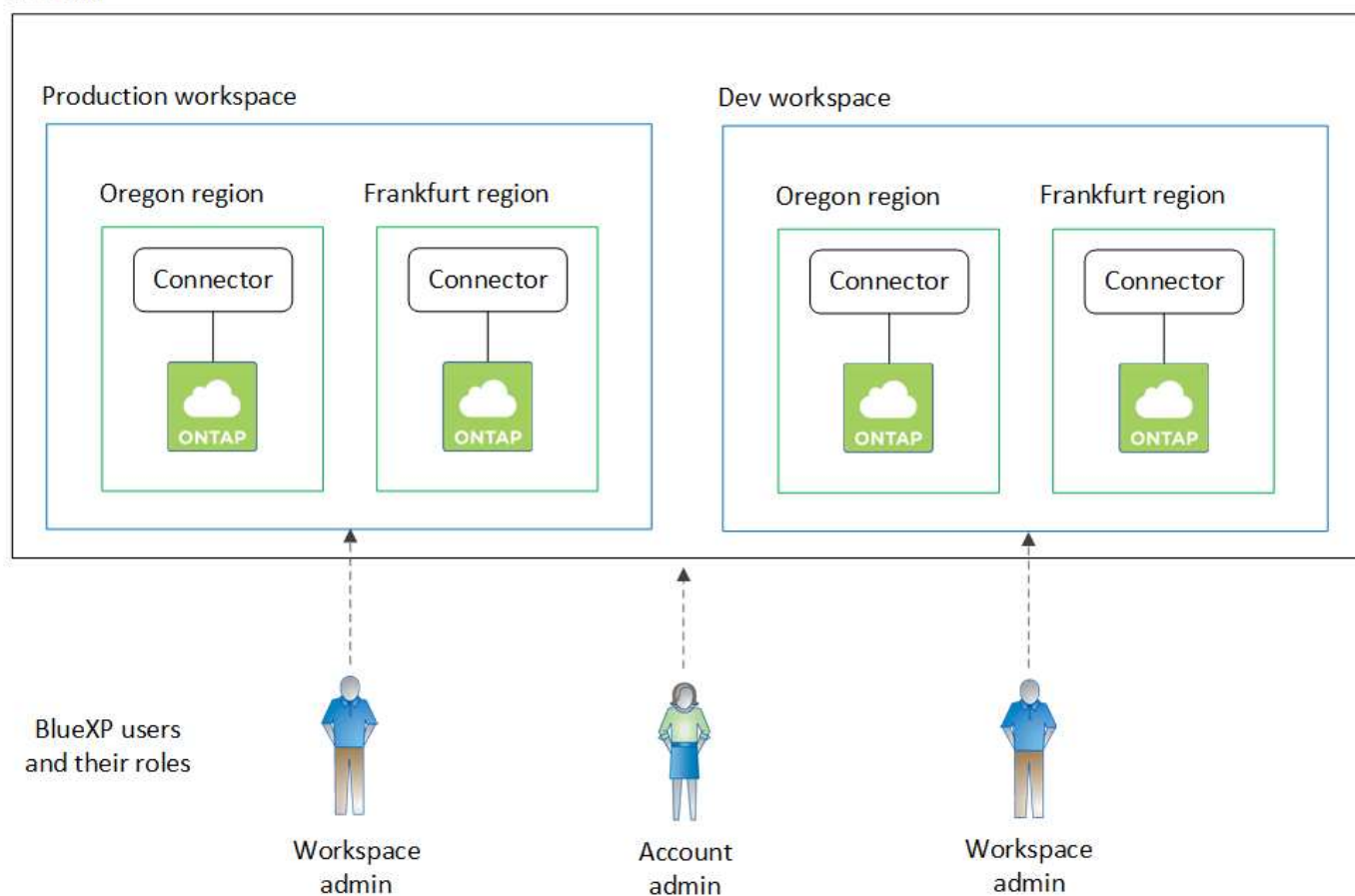


In both example images that follow, the Connector and the Cloud Volumes ONTAP systems don't actually reside *in* the BlueXP account—they're running in a cloud provider. This is a conceptual representation of the relationship between each component.

Multiple workspaces

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



Multiple accounts

Here's another example that shows the highest level of multi-tenancy by using two separate BlueXP 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.



Learn about Connectors

A *Connector* is NetApp software running in your cloud network or on-premises network. It executes the actions that BlueXP needs to perform in order to manage your data infrastructure. The Connector constantly polls the BlueXP SaaS layer for any actions that it needs to take. You don't need a Connector to get started with BlueXP, but you'll need to create a Connector to unlock all BlueXP features and services.

What you can do without a Connector

A Connector isn't required to get started with BlueXP. You can use several features and services within BlueXP without ever creating a Connector.

You can use the following BlueXP features and services without a Connector:

- Amazon FSx for NetApp 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 services such as BlueXP classification and BlueXP copy and 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 BlueXP classification to scan Azure NetApp Files data.

- Cloud Volumes Service for Google Cloud
- Copy and sync

- Digital advisor
- Digital wallet

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.

- 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](#)

When a Connector is required

When you use BlueXP in standard mode, a Connector is required for the following features and services in BlueXP:

- Amazon FSx for ONTAP management features
- Amazon S3 discovery
- Azure Blob discovery
- Backup and recovery
- Classification
- Cloud Volumes ONTAP
- E-Series systems
- Economic efficiency ¹
- Edge caching
- Google Cloud Storage discovery
- Kubernetes clusters
- On-premises ONTAP cluster integration with BlueXP data services
- Operational resiliency ¹
- StorageGRID systems
- Tiering

¹ While you can access these services without a Connector, a Connector is required to initiate actions from the services.

Connectors must be operational at all times

Connectors are a fundamental part of the BlueXP service architecture. It's your responsibility to ensure that relevant Connectors are up, operational, and accessible at all times. While the service is designed to overcome short outages of Connector availability, you must take immediate action when required to remedy infrastructure failures.

This documentation is governed by the EULA. If the product is not operated in accordance with the documentation, the functionality and operation of the product, as well as your rights under the EULA, may be adversely impacted.

Impact on Cloud Volumes ONTAP

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.

Supported locations

A Connector is supported in the following locations:

- Amazon Web Services
- Microsoft Azure

A Connector in Azure 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](#)

- Google Cloud

If you want to use BlueXP services with Google Cloud, then you must use a Connector that's running in Google Cloud.

- On your premises

Restricted mode and private mode

To use BlueXP in restricted mode or private mode, you get started with BlueXP by installing the Connector and then accessing the user interface that's running locally on the Connector.

[Learn about BlueXP deployment modes.](#)

How to create a Connector

A BlueXP Account Admin can create a Connector directly from BlueXP, from your cloud provider's marketplace, or by manually installing the software on your own Linux host. How you get started depends on whether you're using BlueXP in standard mode, restricted mode, or private mode.

- [Learn about BlueXP deployment modes](#)
- [Quick start for BlueXP in standard mode](#)
- [Quick start for BlueXP in restricted mode](#)
- [Quick start for BlueXP in private mode](#)

Permissions

Specific permissions are needed to create the Connector directly from BlueXP and another set of permissions are needed for the Connector instance itself. If you create the Connector in AWS or Azure directly from BlueXP, then BlueXP creates the Connector with the permissions that it needs.

To learn how to set up permissions, refer to the following pages:

- Standard mode
 - [Set up AWS permissions](#)
 - [Set up Azure permissions](#)
 - [Set up Google Cloud permissions](#)
 - [Set up cloud permissions for on-prem deployments](#)
- [Set up cloud permissions for restricted mode](#)
- [Set up cloud permissions for private mode](#)

To view the exact permissions that the Connector needs, refer to the following pages:

- [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. If you're using BlueXP in private mode, then you'll need to manually upgrade the Connector.

[Learn how to manually upgrade the Connector software.](#)

Operating system and VM maintenance

Maintaining the operating system on the Connector host is your responsibility. For example, you should apply security updates to the operating system on the Connector host by following your company's standard procedures for operating system distribution.

Note that you don't need to stop any services on the Connector host when running an OS update.

If you need to stop and then start the Connector VM, you should do so from your cloud provider's console or by using the standard procedures for on-premises management.

[Be aware that the Connector must be operational at all times.](#)

Multiple working environments

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.

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 have a multi-cloud environment (for example, AWS and Azure) and you prefer to 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 BlueXP 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.

When to switch

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.](#)

Disaster recovery

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.

Learn about BlueXP deployment modes

BlueXP offers multiple *deployment modes* that enable you to use BlueXP in a way that meets your business and security requirements. *Standard mode* leverages the BlueXP SaaS layer to provide full functionality, while *restricted mode* and *private mode* are available for organizations that have connectivity restrictions.

While BlueXP inhibits the flow of traffic, communication, and data when using restricted mode or private mode, it's your responsibility to ensure that your environment (on premises and in the cloud) is in compliance with the required regulations.

Overview

BlueXP offers the following deployment modes for your account. Each mode differs in terms of outbound connectivity requirements, deployment location, installation process, authentication method, available data and storage services, and charging methods.

Standard mode

BlueXP is accessible to users as a cloud service from the web-based console. Depending on the BlueXP services that you're planning to use, a BlueXP admin creates one or more Connectors to manage data within your hybrid cloud environment.

This mode uses encrypted data transmission over the public internet.

Restricted mode

A BlueXP Connector is installed in the cloud (in a government region, sovereign cloud region, or commercial region) and has limited outbound connectivity to the BlueXP SaaS layer. Users access BlueXP locally from the web-based console that's available from the Connector, not from the SaaS layer.

This mode is typically used by state and local governments and regulated companies.

[Learn more about outbound connectivity to the SaaS layer.](#)

Private mode

A BlueXP Connector is installed on premises or in the cloud (in a secure region, sovereign cloud region, or commercial region) and has *no* connectivity to the BlueXP SaaS layer. Users access BlueXP locally from the web-based console that's available from the Connector, not from the SaaS layer.

A secure region includes [AWS C2S and SC2S](#) and [Azure IL6](#)

The following table provides a comparison of these modes.

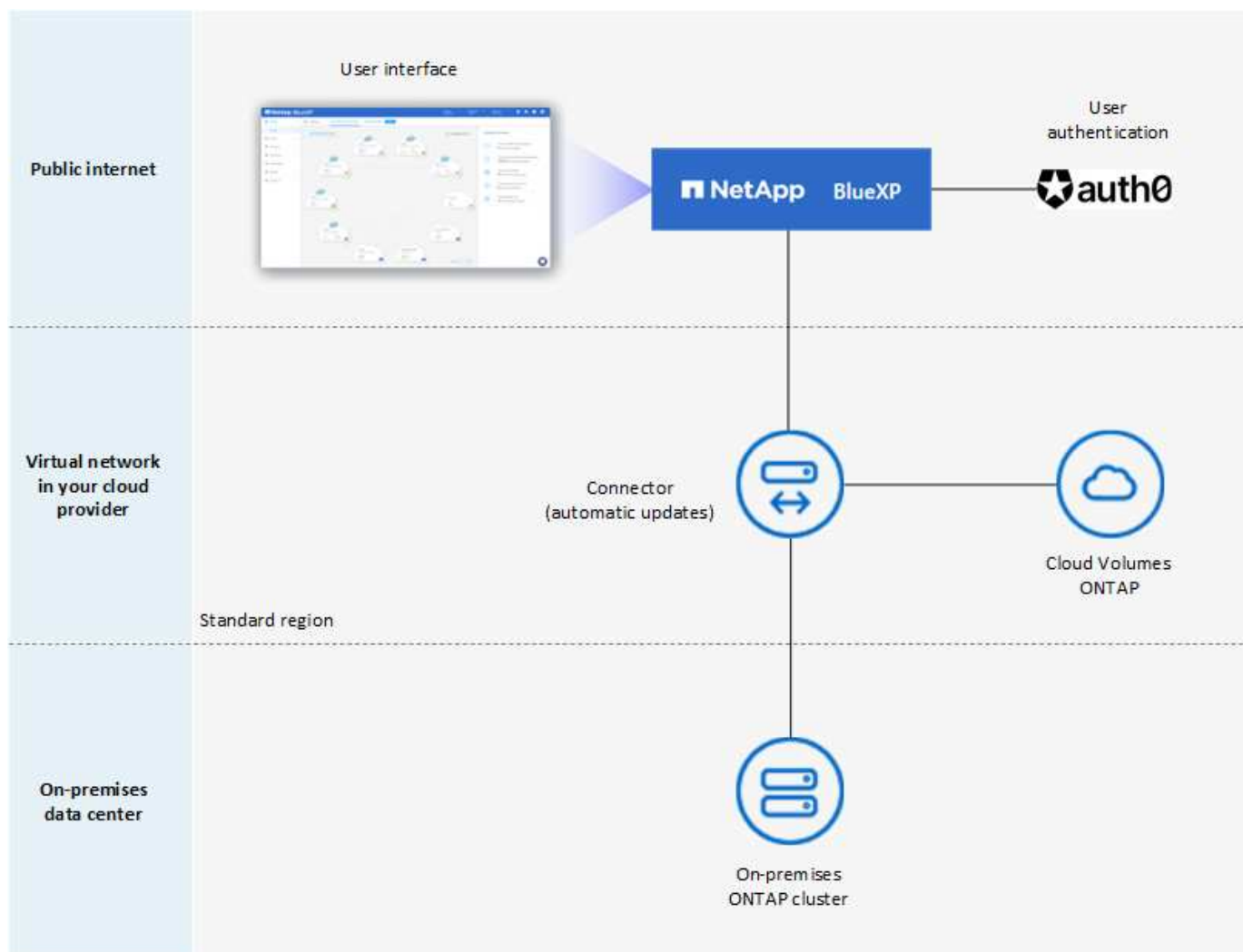
| | Standard mode | Restricted mode | Private mode |
|--|---|---|---|
| Connection required to BlueXP SaaS layer? | Yes | Outbound only | No |
| Connection required to your cloud provider? | Yes | Yes, within the region | Yes, within the region (if using Cloud Volumes ONTAP) |
| Connector installation | From BlueXP, cloud marketplace, or manual install | Cloud marketplace or manual install | Manual install |
| Connector upgrades | Automatic upgrades of NetApp Connector software | Automatic upgrades of NetApp Connector software | Manual upgrade required |
| UI access | From the BlueXP SaaS layer | Locally from the Connector VM | Locally from the Connector VM |

| | Standard mode | Restricted mode | Private mode |
|----------------------------------|---|---|---------------------------|
| API endpoint | The BlueXP SaaS layer | The BlueXP SaaS layer | The Connector |
| Authentication | Through SaaS using auth0, NSS login, or identity federation | Through SaaS using auth0 or identity federation | Local user authentication |
| Storage and data services | All are supported | Many are supported | Several are supported |
| Licensing options | Marketplace subscriptions and BYOL | Marketplace subscriptions and BYOL | BYOL |

Read through the following sections to learn more about these modes, including which BlueXP features and services are supported.

Standard mode

The following image is an example of a standard mode deployment.



BlueXP works as follows in standard mode:

Outbound communication

Connectivity is required from the Connector to the BlueXP SaaS layer, to your cloud provider's publicly available resources, and to other essential components for day-to-day operations.

- [Endpoints that the Connector contacts in AWS](#)
- [Endpoints that the Connector contacts in Azure](#)
- [Endpoints that the Connector contacts in Google Cloud](#)

Supported location for the Connector

In standard mode, the Connector is supported in the cloud or on your premises.

Connector installation

Connector installation is possible from a setup wizard in BlueXP, from the AWS or Azure Marketplace, or using an installer to manually install the Connector on your own Linux host in your data center or in the cloud.

Connector upgrades

Automated upgrades of the Connector software are available from BlueXP with monthly updates.

User interface access

The user interface is accessible from the web-based console that's provided through the SaaS layer.

API endpoint

API calls are made to the following endpoint:
<https://cloudmanager.cloud.netapp.com>

Authentication

Authentication is provided through BlueXP's cloud service using auth0 or through NetApp Support Site (NSS) logins. Identity federation is available.

Supported BlueXP services

All BlueXP services are available to users.

Supported licensing options

Marketplace subscriptions and BYOL are supported with standard mode; however, the supported licensing options depends on which BlueXP service you are using. Review the documentation for each service to learn more about the available licensing options.

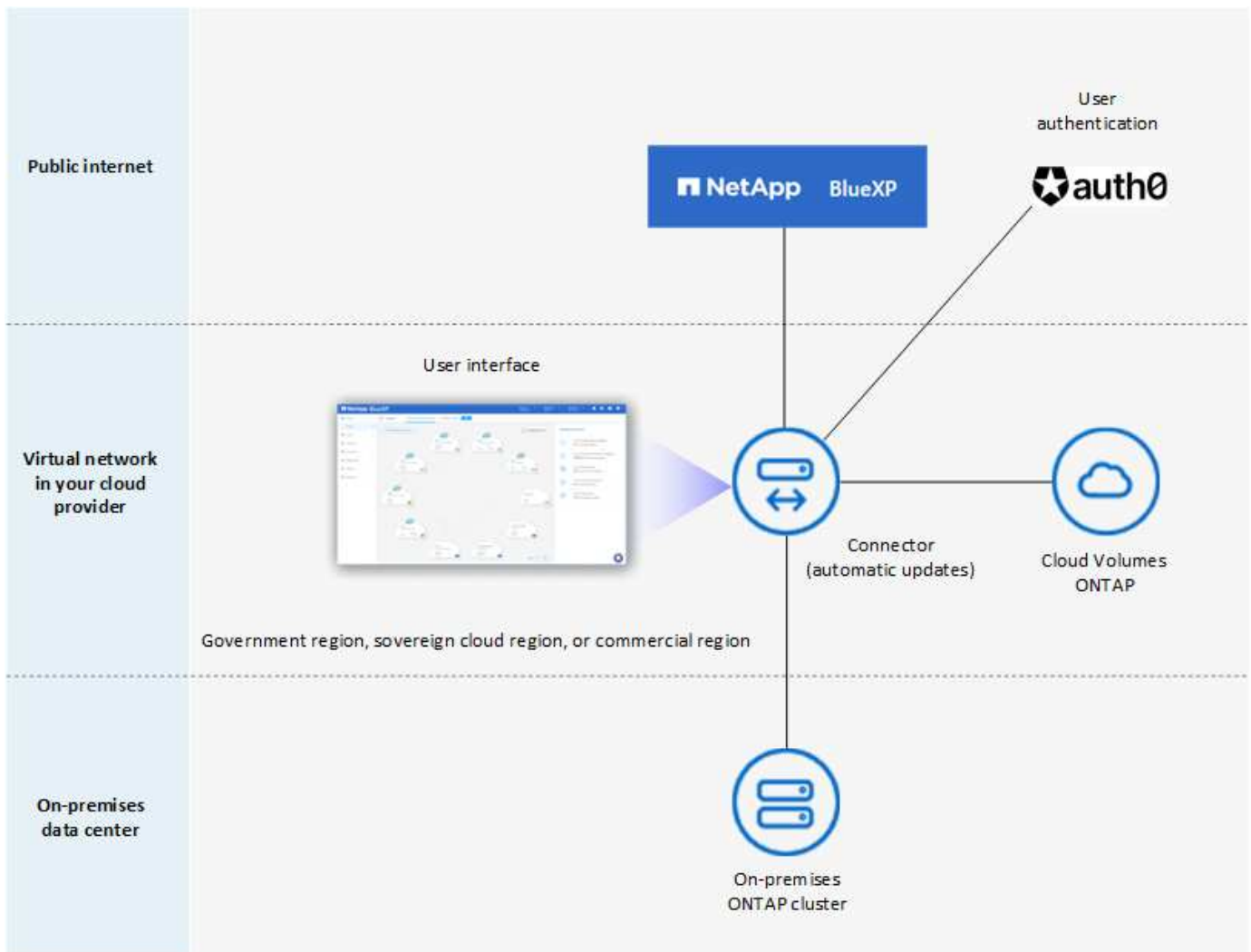
How to get started with standard mode

Go to the [BlueXP web-based console](#) and sign up.

[Learn how to get started with standard mode.](#)

Restricted mode

The following image is an example of a restricted mode deployment.



BlueXP works as follows in restricted mode:

Outbound communication

Outbound connectivity is required from the Connector to the BlueXP SaaS layer to use BlueXP data services, to enable automatic software upgrades of the Connector, to use auth0-based authentication, and to send metadata for charging purposes (storage VM name, allocated capacity, and volume UUID, type, and IOPS).

The BlueXP SaaS layer does not initiate communication to the Connector. All communication is initiated by the Connector, which can pull or push data from or to the SaaS layer as required.

A connection is also required to cloud provider resources from within the region.

Supported location for the Connector

In restricted mode, the Connector is supported in the cloud: in a government region, sovereign region, or commercial region.

Connector installation

Connector installation is possible from the AWS or Azure Marketplace or a manual installation on your own Linux host.

Connector upgrades

Automated upgrades of the Connector software are available from BlueXP with monthly updates.

User interface access

The user interface is accessible from the Connector that's deployed in your cloud region.

API endpoint

API calls are made to the following endpoint:

<https://cloudmanager.cloud.netapp.com>

Authentication

Authentication is provided through BlueXP's cloud service using auth0. Identity federation is also available.

Supported BlueXP services

BlueXP supports the following storage and data services with restricted mode:

| Supported services | Notes |
|----------------------------|---|
| Amazon FSx for ONTAP | Full support |
| Azure NetApp Files | Full support |
| Backup and recovery | Supported in Government regions and commercial regions with restricted mode. Not supported in sovereign regions with restricted mode. The following features are not supported: Applications, Virtual Machines, and Kubernetes. |
| Classification | Supported in Government regions with restricted mode. Not supported in commercial regions or in sovereign regions with restricted mode. The following limitations apply: <ul style="list-style-type: none">• OneDrive accounts, SharePoint accounts, and Google Drive accounts can't be scanned.• Microsoft Azure Information Protection (AIP) label functionality can't be integrated. |
| Cloud Volumes ONTAP | Full support |
| Digital wallet | You can use the digital wallet with the supported licensing options listed below for restricted mode. |
| On-premises ONTAP clusters | Discovery with a Connector and discovery without a Connector (direct discovery) are both supported. When you discover an on-prem cluster with a Connector, the Advanced view (System Manager) is not supported. |
| Replication | Supported in Government regions with restricted mode. Not supported in commercial regions or in sovereign regions with restricted mode. |

Supported licensing options

The following licensing options are supported with restricted mode:

- Marketplace subscriptions (hourly and annual contracts)

Note the following:

- For Cloud Volumes ONTAP, only capacity-based licensing is supported.
- In Azure, annual contracts are not supported with government regions.
- BYOL

For Cloud Volumes ONTAP, both capacity-based licensing and node-based licensing are supported with BYOL.

How to get started with restricted mode

You need to enable restricted mode when you create your BlueXP account.

If you don't have an account yet, you'll be prompted to create your account and enable restricted mode when you log in to BlueXP for the first time from a Connector that you manually installed or that you created from your cloud provider's marketplace.

If you already have an account and you want to create another one, then you need to use the Tenancy API.

Note that you can't change the restricted mode setting after BlueXP creates the account. You can't enable restricted mode later and you can't disable it later. It must be set at time of account creation.

- [Learn how to get started with restricted mode.](#)
- [Learn how to create an additional BlueXP account.](#)

Private mode

In private mode, you can install a Connector either on premises or in the cloud and then use BlueXP to manage data across your hybrid cloud. There is no connectivity to the BlueXP SaaS layer.

The following image shows an example of a private mode deployment where the Connector is installed in the cloud and manages both Cloud Volumes ONTAP and an on-premises ONTAP cluster.



Meanwhile, the second image shows an example of a private mode deployment where the Connector is installed on premises, manages an on-premises ONTAP cluster, and provides access to supported BlueXP data services.



BlueXP works as follows in private mode:

Outbound communication

No outbound connectivity is required. All packages, dependencies, and essential components are packaged with the Connector and served from the local machine. Connectivity to your cloud provider's publicly available resources is required only if you are deploying Cloud Volumes ONTAP.

Supported location for the Connector

In private mode, the Connector is supported in the cloud or on premises.

Connector installation

Manual installations of the Connector are supported on your own Linux host in the cloud or on premises.

Connector upgrades

You need to upgrade the Connector software manually. The Connector software is published to the NetApp Support Site at undefined intervals.

User interface access

The user interface is accessible from the Connector that's deployed in your cloud region or on premises.

API endpoint

API calls are made to the Connector virtual machine.

Authentication

Authentication is provided through local user management and access. Authentication is not provided through BlueXP's cloud service.

Supported BlueXP services in cloud deployments

BlueXP supports the following storage and data services with private mode when the Connector is installed in the cloud:

| Supported services | Notes |
|----------------------------|---|
| Backup and recovery | Supported in AWS and Azure commercial regions. Not supported in Google Cloud or in AWS C2S/SC2S or Azure IL6 |
| Cloud Volumes ONTAP | Because there's no internet access, the following features aren't available: automated software upgrades, AutoSupport, and AWS cost information. |
| Digital wallet | You can use the digital wallet with the supported licensing options listed below for private mode. |
| On-premises ONTAP clusters | Requires connectivity from the cloud (where the Connector is installed) to the on-premises environment. Discovery without a Connector (direct discovery) is not supported. |

Supported BlueXP services in on-prem deployments

BlueXP supports the following storage and data services with private mode when the Connector is installed on your premises:

| Supported services | Notes |
|----------------------------|---|
| Backup and recovery | <p>Only back up and restore of on-prem ONTAP volumes to StorageGRID systems is supported.</p> <p>Learn how to back up on-prem ONTAP data to StorageGRID</p> |
| Classification | <ul style="list-style-type: none"> The only supported data sources are the ones that you can discover locally. <p>View the sources that you can discover locally</p> <ul style="list-style-type: none"> Features that require outbound internet access are not supported. <p>View the feature limitations</p> |
| Digital wallet | You can use the digital wallet with the supported licensing options listed below for private mode. |
| On-premises ONTAP clusters | Discovery without a Connector (direct discovery) is not supported. |
| Replication | Full support |

Supported licensing options

Only BYOL is supported with private mode.

For Cloud Volumes ONTAP BYOL, only node-based licensing is supported. Capacity-based licensing is not supported. Because an outbound internet connection isn't available, you will need to manually upload your Cloud Volumes ONTAP licensing file in the BlueXP digital wallet.

[Learn how to add licenses to the BlueXP digital wallet](#)

How to get started with private mode

Private mode is available by downloading the "offline" installer from the NetApp Support Site.

[Learn how to get started with private mode.](#)

Service and feature comparison

The following table can help you quickly identify which BlueXP services and features are supported with restricted mode and private mode.

Note that some services might be supported with limitations. For more details about how these services are supported with restricted mode and private mode, refer to the sections above.

| Product area | BlueXP service or feature | Restricted mode | Private mode |
|-----------------------------|--|-----------------|--------------|
| Working environments | Amazon FSx for ONTAP | Yes | No |
| | Amazon S3 | No | No |
| | Azure Blob | No | No |
| | Azure NetApp Files | Yes | No |
| | Cloud Volumes ONTAP | Yes | Yes |
| | Cloud Volumes Service for Google Cloud | No | No |
| | Google Cloud Storage | No | No |
| | Kubernetes clusters | No | No |
| | On-prem ONTAP clusters | Yes | Yes |
| | E-Series | No | No |
| | StorageGRID | No | No |
| Services | Backup and recovery | Yes | Yes |
| | Classification | Yes | Yes |
| | Cloud ops | No | No |
| | Copy and sync | No | No |
| | Digital advisor | No | No |
| | Digital wallet | Yes | Yes |
| | Economic efficiency | No | No |
| | Edge caching | No | No |
| | Operational resiliency | No | No |
| | Ransomware protection | No | No |
| | Remediation | No | No |
| | Replication | Yes | Yes |
| | Tiering | No | No |
| Features | Credentials | Yes | Yes |
| | NSS accounts | Yes | No |
| | Notifications | Yes | No |
| | Timeline | Yes | Yes |

Get started with standard mode

Quick start for BlueXP in standard mode

Get started with BlueXP in standard mode by signing up from the BlueXP console,

optionally creating a Connector, and subscribing to BlueXP.

1

Sign up and create an account

Go to the [BlueXP console](#) and 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.

At this point, you're logged in and can start using several BlueXP services like Digital Advisor, Amazon FSx for ONTAP, Azure NetApp Files, and more. [Learn what you can do without a Connector](#).

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

2

Create a Connector

You don't need a Connector to get started with BlueXP, but you can create a Connector to unlock all BlueXP features and services. The Connector is NetApp software that enables BlueXP to manage resources and processes within your hybrid cloud environment.

A BlueXP Account Admin can create a Connector in your cloud or on-premises network.

- [Learn more about when Connectors are required and how they work](#)
- [Learn how to create a Connector in AWS](#)
- [Learn how to create a Connector in Azure](#)
- [Learn how to create a Connector in Google Cloud](#)
- [Learn how to create a Connector on premises](#)

Note that if you want to use BlueXP services to manage storage and data in Google Cloud, then the Connector must be running in Google Cloud.

3

Subscribe to BlueXP

Subscribe to BlueXP from your cloud provider's marketplace to pay for BlueXP services at an hourly rate (PAYGO) or through an annual contract.

[Learn how to subscribe to BlueXP](#).

Prepare networking for user access to the BlueXP console

As you use the BlueXP web-based console that's provided through the SaaS layer, it contacts several endpoints to complete data management tasks. The machine running the web browser must have connections to these endpoints.

| Endpoints | Purpose |
|--|---|
| https://console.bluelxp.netapp.com https://*.console.bluelxp.netapp.com | Your web browser contacts these URLs when you use the BlueXP web-based console. |

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

Related links

- [Prepare networking for user access to BlueXP console \(restricted mode\)](#)
- [Endpoints that the Connector contacts in AWS \(standard mode\)](#)
- [Endpoints that the Connector contacts in Azure \(standard mode\)](#)
- [Endpoints that the Connector contacts in Google Cloud \(standard mode\)](#)
- [Endpoints contacted during manual installation of the Connector \(standard mode\)](#)

Sign up to BlueXP

BlueXP is accessible from a web-based console. When you get started with BlueXP, your first step is to sign up using your existing NetApp Support Site credentials or by creating a NetApp cloud login.

Sign up options

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). You can set up a federation connection after you sign up. [Learn how to use identity federation with BlueXP.](#)

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 close out of BlueXP 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 (standard mode)

After you sign up to BlueXP, you can log in from the web-based console to start managing your data and storage infrastructure.

Log in options

You can log in to the BlueXP web-based console 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).
[Learn how to use identity federation with BlueXP.](#)

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.

Create a Connector

AWS

Quick start to create a Connector in AWS

Create a Connector in AWS by choosing an installation option, setting up networking, preparing permissions, and more.

1

Understand your installation options

The standard way to create a Connector in AWS is directly from BlueXP, but you can also create it from the AWS Marketplace, or you can manually install the software on a pre-existing Linux host.

[Learn more about your installation options.](#)

2

Set up networking

Prepare the following for the Connector:

- A VPC and subnet
- A network connection to the networks where you're planning to create and manage working environments
- Outbound internet access to specific endpoints for day-to-day operations
- The IP address, credentials, and HTTPS certificate of a proxy server, if a proxy server is required for outbound internet

[Learn more about networking requirements.](#)

3

Review host requirements

The Connector software must run on a host that meets specific requirements. If you plan to manually install the Connector software on your own Linux host, then you should ensure that your host meets these requirements. If you're creating the Connector from BlueXP or from the AWS Marketplace, then these requirements are taken care of for you because the software is deployed from an image.

The key requirements are as follows:

- A dedicated host running CentOS or Red Hat Enterprise Linux
- 4 CPUs
- 14 GB of RAM
- Docker Engine

[Learn more about these host requirements.](#)

4

Set up AWS permissions

Set up AWS permissions based on the installation option that you're planning to use:

- **Install from BlueXP:** Create an IAM policy and attach it to an IAM role that BlueXP can assume or to an IAM user that you can provide access keys for. BlueXP authenticates with AWS and uses these permissions to create the Connector instance on your behalf.
- **Install from the AWS Marketplace:** Create an IAM policy and attach it to an IAM role. You'll associate this role with the Connector instance during installation.
- **Manual install:** Create an IAM policy and attach it to an IAM role or to an IAM user. You'll either associate the role with the Connector instance or provide BlueXP with an access key for the IAM user.

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

5

Create the Connector

Create the Connector using one of the available installation options:

- **From BlueXP:** Click the Connector drop-down, select **Add Connector** and follow the prompts.
- **From the AWS Marketplace:** Go to the [BlueXP page on the AWS Marketplace](#) and follow the prompts to launch through EC2 so that you can attach an IAM role.
- **Manual install:** Download the Connector software from the [NetApp Support Site](#) and run the installation script.

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

6

Provide BlueXP with permissions

If you manually installed the Connector software on your own Linux host, you need to provide BlueXP with the permissions that you previously set up.

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

Connector installation options in AWS

There are a few different ways to create a Connector in AWS. Directly from BlueXP is the most common way. The installation option that you choose determines how you prepare for deployment.

The following installation options are available:

- Create the Connector directly from BlueXP (this is the standard option)

This action launches an EC2 instance running Linux and the Connector software in a VPC of your choice.
- Create a Connector from the AWS Marketplace

This action also launches an EC2 instance running Linux and the Connector software.
- Download and manually install the software on your own Linux host

The installation option that you choose impacts how you prepare for installation. This includes how you provide BlueXP with the required permissions that it needs to authenticate and manage resources in AWS.

[Learn how to install the Connector in AWS.](#)

Set up AWS networking

Set up your networking so the Connector can manage resources and processes within your hybrid cloud environment. For example, you need to ensure that connections are available to target networks and that outbound internet access is available.

VPC and subnet

When you create the Connector, you need to specify the VPC and subnet where the Connector should reside.

Connections to target networks

A Connector requires a network connection to the location where you're planning to create and manage working environments.

Outbound internet access

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

Endpoints contacted during manual installation


If you plan to manually install the Connector on your own Linux host, the installer for the Connector requires access to 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://cloudmanagerinfraproduct.azurecr.io>
- <https://production-artifacts.cloudmanager.cloud.netapp.com>
- 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.

Endpoints contacted for day-to-day operations

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 |
|--|--|
| AWS services (amazonaws.com): <ul style="list-style-type: none"> • CloudFormation • Elastic Compute Cloud (EC2) • Identity and Access Management (IAM) • Key Management Service (KMS) • Security Token Service (STS) • Simple Storage Service (S3) | To manage resources in AWS. The exact endpoint depends on the region in which you deploy the Connector. Refer to AWS documentation for details |
| https://support.netapp.com | To obtain licensing information and to send AutoSupport messages to NetApp support. |
| https://*.api.bluexp.netapp.com https://api.bluexp.netapp.com https://*.cloudmanager.cloud.netapp.com https://cloudmanager.cloud.netapp.com | <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 https://*.blob.core.windows.net | To upgrade the Connector and its Docker components. |

Related link

[Prepare networking for user access to the BlueXP console](#)

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

Ports

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 (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.
- 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. 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.

IP address limitation

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

Review Connector host requirements for AWS installs

The Connector software must run on a host that meets specific operating system requirements, RAM requirements, port requirements, and so on. If you plan to manually install the Connector, you should ensure that your host meets these requirements.

When you deploy the Connector from BlueXP or from the AWS Marketplace, the image includes the required OS and software components.

Dedicated host

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

Supported operating systems

- CentOS 7.6, 7.7, 7.8, and 7.9
- Red Hat Enterprise Linux 7.6, 7.7, 7.8, 7.9, 8.6, and 8.7

The host must be registered with Red Hat Subscription Management. If it's not registered, the host can't 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 is required. [Red Hat Solution: Which hypervisors are certified to run Red Hat Enterprise Linux?](#)

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.

Key pair

When you create the Connector from BlueXP or from the AWS Marketplace, you'll need to select an EC2 key pair to use with the instance.

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](#)

Set up AWS permissions

Set up permissions in AWS so that you can deploy the Connector with the permissions that it needs to manage your data and storage infrastructure. How you set up and provide the permissions depends on the installation option that you're planning to use.

You can choose from the following installation options:

- **Install from BlueXP:** Set up permissions that enable BlueXP to authenticate with AWS and deploy the instance. BlueXP automatically sets up permissions for the Connector instance during deployment.

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

- **Install from the AWS Marketplace:** Set up an IAM role that you can associate with the Connector instance.

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

- **Manual install:** Create IAM policies and attach them to an IAM role or to an IAM user.

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

Set up permissions to create the Connector from BlueXP

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, the first step is to create an IAM policy. This policy contains only the permissions needed to launch the Connector instance in AWS from BlueXP.

If needed, you can restrict the IAM policy by using the IAM `Condition` element. [AWS documentation: Condition element](#)



When BlueXP creates the Connector, it applies a new set of permissions to the Connector instance that enables the Connector to AWS resources.

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**.
8. Either attach the policy to an IAM role that BlueXP can assume or to an IAM user so that you can provide BlueXP with access keys:
 - (Option 1) Set up an IAM role that BlueXP can assume:
 - a. Go to the AWS IAM console in the target account.
 - b. Under Access Management, click **Roles > Create Role** and follow the steps to create the role.
 - c. Under **Trusted entity type**, select **AWS account**.
 - d. Select **Another AWS account** and enter the ID of the BlueXP SaaS account: 952013314444
 - e. Select the policy that you created in the previous section.
 - f. After you create the role, copy the Role ARN so that you can paste it in BlueXP when you create the Connector.
 - (Option 2) Set up permissions for an IAM user so that you can provide BlueXP with access keys:
 - a. From the AWS IAM console, click **Users** and then select the user name.
 - b. Click **Add permissions > Attach existing policies directly**.
 - c. Select the policy that you created.
 - d. Click **Next** and then click **Add permissions**.
 - e. Ensure that you have the access key and secret key for the IAM user.

Result

You should now have an IAM role that has the required permissions or an IAM user that has the required permissions. When you create the Connector from BlueXP, you can provide information about the role or access keys.

Set up permissions for the Connector when deploying from the AWS Marketplace

Create IAM policies in AWS and attach them to an IAM role. When you create the Connector from the AWS Marketplace, you'll be prompted to select that IAM role.

Steps

1. From the IAM console, create a policy:
 - a. Click **Policies > Create policy**.
 - b. Select **JSON** and copy and paste the contents of the [IAM policies for the Connector](#).
 - c. Finish the remaining steps to create the policy.

Depending on the BlueXP services that you're planning to use, you might need to create a second policy.

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.

2. Back in the IAM console, create an IAM role:
 - a. Click **Roles > Create role**.
 - b. Select **AWS service > EC2**.
 - c. Add permissions by attaching the policies that you created in the previous step.
 - d. Finish the remaining steps to create the role.

Result

You now have an IAM role that you can associate with the EC2 instance during deployment from the AWS Marketplace.

Set up permissions to assign after manual installation

If you manually install the Connector software on your own Linux host in AWS, you can provide permissions in the following ways:

- Option 1: Create IAM policies and attach the policies to an IAM role that you can associate with the EC2 instance.
- Option 2: Provide BlueXP with AWS access keys for an IAM user who has the required permissions.

IAM role

Steps

1. From the IAM console, create a policy:
 - a. Click **Policies > Create policy**.
 - b. Select **JSON** and copy and paste the contents of the [IAM policy for the Connector](#).
 - c. Finish the remaining steps to create the policy.

Depending on the BlueXP services that you're planning to use, you might need to create a second policy.

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. [Learn more about IAM policies for the Connector](#).

2. Back in the IAM console, create an IAM role:
 - a. Click **Roles > Create role**.
 - b. Select **AWS service > EC2**.
 - c. Add permissions by attaching the policies that you created in the previous step.
 - d. Finish the remaining steps to create the role.

Result

You now have an IAM role that you can associate with the EC2 instance after you install the Connector. [Learn how to provide these permissions to BlueXP](#).

AWS access key

Steps

1. From the IAM console, create a policy:
 - a. Click **Policies > Create policy**.
 - b. Select **JSON** and copy and paste the contents of the [IAM policy for the Connector](#).
 - c. Finish the remaining steps to create the policy.

Depending on the BlueXP services that you're planning to use, you might need to create a second policy.

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. [Learn more about IAM policies for the Connector](#).

2. Attach the policies to an IAM user.
 - [AWS Documentation: Creating IAM Roles](#)
 - [AWS Documentation: Adding and Removing IAM Policies](#)
3. Ensure that the user has an access key that you can add to BlueXP after you install the Connector.

Result

You now have an IAM user that has the required permissions and an access key that you can provide to BlueXP. [Learn how to provide these permissions to BlueXP](#).

Create a Connector in AWS

Create a Connector directly from the BlueXP web-based console, from the AWS Marketplace, or by installing the software on your own Linux host.

BlueXP

What you'll need

- An AWS authentication method: either an IAM role or access keys for an IAM user with the required permissions.

[Learn how to set up AWS permissions](#)

- A VPC and subnet that meets networking requirements.

[Learn about networking requirements](#)

- A key pair for the EC2 instance.
- Details about a proxy server, if a proxy is required for internet access from the Connector.

Steps

1. 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.

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 the required inbound and outbound rules.

[View security group rules for AWS.](#)

- **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.

Result

After the process is complete, the Connector is available for use from BlueXP.

AWS Marketplace

What you'll need

- A VPC and subnet that meets networking requirements.

[Learn about networking requirements.](#)

- An IAM role with an attached policy that includes the required permissions for the Connector.

[Learn how to set up AWS permissions.](#)

- Permissions to subscribe and unsubscribe from the AWS Marketplace for your IAM user.
- A key pair for the EC2 instance.

Steps

1. Go to the [BlueXP page on the AWS Marketplace](#)
2. On the Marketplace page, click **Continue to Subscribe** and then click **Continue to Configuration**.



3. Change any of the default options and click **Continue to Launch**.

4. 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.

5. 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.

A few more rule are required for specific configurations.

[View security group rules for AWS.](#)

- **Configure storage:** Keep the default storage options.
- **Advanced details:** Under **IAM instance profile**, choose the IAM role that includes the required permissions for the Connector.

[Learn how to set up AWS permissions.](#)

- **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.

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

`https://ipaddress`

7. After you log in, set up the Connector:
 - a. Specify the BlueXP account to associate with the Connector.
 - b. Enter a name for the system.
 - c. Under **Are you running in a secured environment?** keep restricted mode disabled.

You should keep restricted mode disabled because these steps describe how to use BlueXP in standard mode. You should enable restricted mode only if you have a secure environment and want to disconnect this account from BlueXP backend services. If that's the case, [follow steps to get started with BlueXP in restricted mode](#).

- d. Click **Let's start**.

Result

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

Open a web browser and go to the [BlueXP console](#) to start using the Connector with BlueXP.

Manual install

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.

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 or if the proxy is an intercepting proxy.

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 "online" Connector installer that's meant for use in your network or in the cloud. A separate "offline" installer is available for the Connector, but it's only supported with private mode deployments.

4. Assign permissions to run the script.

```
chmod +x OnCommandCloudManager-<version>
```

Where `<version>` is the version of the Connector that you downloaded.

5. Run the installation script.

```
./OnCommandCloudManager-<version> --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-V3.9.26 --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 or if the proxy is an intercepting proxy.

6. Wait for the installation to complete.

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

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

`https://ipaddress`

8. After you log in, set up the Connector:
 - a. Specify the BlueXP account to associate with the Connector.
 - b. Enter a name for the system.
 - c. Under **Are you running in a secured environment?** keep restricted mode disabled.

You should keep restricted mode disabled because these steps describe how to use BlueXP in standard mode. You should enable restricted mode only if you have a secure environment and want to disconnect this account from BlueXP backend services. If that's the case, [follow steps to get started with BlueXP in restricted mode](#).

- d. Click **Let's start**.

Result

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

What's next?

[Provide BlueXP with the permissions that you previously setup.](#)

Provide AWS permissions to BlueXP

If you manually installed the Connector software on your own Linux host, you need to provide BlueXP with the permissions that you previously set up. Providing the permissions enables BlueXP to manage your data and storage infrastructure in AWS.

[Learn how to set up these permissions.](#)

These steps don't apply if you deployed the Connector directly from BlueXP or from the AWS Marketplace because the required permissions were provided during deployment.

IAM role

Attach the IAM role that you previously created to the Connector EC2 instance.

Steps

1. Go to the Amazon EC2 console.
2. Select **Instances**.
3. Select the Connector instance.
4. Select **Actions > Security > Modify IAM role**.
5. Select the IAM role and click **Update IAM role**.

Result

BlueXP now has the permissions that it needs to perform actions in AWS on your behalf. Go to the [BlueXP console](#) to start using the Connector with BlueXP.

AWS access key

Provide BlueXP with the AWS access key for an IAM user that has the required permissions.

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:** 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.
 - d. **Review:** Confirm the details about the new credentials and click **Add**.

Result

BlueXP now has the permissions that it needs to perform actions in AWS on your behalf. Go to the [BlueXP console](#) to start using the Connector with BlueXP.

Azure

Quick start to create a Connector in Azure

Create a Connector in Azure by choosing an installation option, setting up networking, preparing permissions, and more.

1

Understand your installation options

The standard way to create a Connector in Azure is directly from BlueXP, but you can also create it from the Azure Marketplace, or you can manually install the software on a pre-existing Linux host.

[Learn more about your installation options.](#)

2

Set up networking

Prepare the following for the Connector:

- A VNet and subnet
- A network connection to the networks where you're planning to create and manage working environments
- Outbound internet access to specific endpoints for day-to-day operations
- The IP address, credentials, and HTTPS certificate of a proxy server, if a proxy server is required for outbound internet

[Learn more about networking requirements.](#)

3

Review host requirements

The Connector software must run on a host that meets specific requirements. If you plan to manually install the Connector software on your own Linux host, then you should ensure that your host meets these requirements. If you're creating the Connector from BlueXP or from the Azure Marketplace, then these requirements are taken care of for you because the software is deployed from an image.

The key requirements are as follows:

- A dedicated host running CentOS or Red Hat Enterprise Linux
- 4 CPUs
- 14 GB of RAM
- Docker Engine

[Learn more about these host requirements.](#)

4

Set up Azure permissions

Set up Azure permissions for the installation option that you're planning to use:

- **Install from BlueXP:** Create a custom role and then apply it to your Azure account or an Azure AD service principal. BlueXP authenticates with Azure and uses these permissions to create the Connector instance on your behalf.
- **Install from the Azure Marketplace:** Create a custom role that you can associate with the Connector VM instance or with an Azure AD service principal.
- **Manual install:** Create a custom role that you can associate with the Connector VM instance or with an Azure AD service principal.

[Follow step-by-step instructions for each of these options.](#)

5

Create the Connector

Create the Connector using one of the available installation options:

- **From BlueXP:** Click the Connector drop-down, select **Add Connector** and follow the prompts.
- **From the Azure Marketplace:** Go to the [NetApp Connector VM page in the Azure Marketplace](#) and follow the prompts to create the Connector VM.
- **Manual install:** Download the Connector software from the [NetApp Support Site](#) and run the installation script.

[Follow step-by-step instructions for each of these options.](#)

6

Provide BlueXP with permissions

If you created the Connector from the Azure Marketplace or manually installed the software, you need to provide BlueXP with the permissions that you previously set up.

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

Connector installation options in Azure

There are a few different ways to create a Connector in Azure. Directly from BlueXP is the most common way. The installation option that you choose determines how you prepare for deployment.

The following installation options are available:

- Create the Connector directly from BlueXP (this is the standard option)

This action launches a VM running Linux and the Connector software in a VNet of your choice.

- Create a Connector from the Azure Marketplace

This action also launches a VM running Linux and the Connector software.

- Download and manually install the software on your own Linux host

The installation option that you choose impacts how you prepare for installation. This includes how you provide BlueXP with the required permissions that it needs to authenticate and manage resources in Azure.

[Learn how to install the Connector in Azure.](#)

Set up Azure networking

Set up your networking so the Connector can manage resources and processes within your hybrid cloud environment. For example, you need to ensure that connections are available to target networks and that outbound internet access is available.

VNet and subnet

When you create the Connector, you need to specify the VNet and subnet where the Connector should reside.

Azure region

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](#)

Connections to target networks

A Connector requires a network connection to the location where you're planning to create and manage working environments.

Outbound internet access

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

Endpoints contacted during manual installation

If you plan to manually install the Connector on your own Linux host, the installer for the Connector requires access to 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

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

Endpoints contacted for day-to-day operations

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://management.azure.com https://login.microsoftonline.com https://blob.core.windows.net https://core.windows.net | To manage resources in Azure public regions. |
| https://management.chinacloudapi.cn https://login.chinacloudapi.cn https://blob.core.chinacloudapi.cn https://core.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. |

| Endpoints | Purpose |
|--|--|
| https://*.api.bluexp.netapp.com https://api.bluexp.netapp.com https://*.cloudmanager.cloud.netapp.com https://cloudmanager.cloud.netapp.com | To provide SaaS features and services within BlueXP. <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 https://*.blob.core.windows.net | To upgrade the Connector and its Docker components. |

Related link

[Prepare networking for user access to the BlueXP console](#)

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

Ports

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 (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.
- 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. 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.

IP address limitation

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

Review Connector host requirements for Azure installs

The Connector software must run on a host that meets specific operating system requirements, RAM requirements, port requirements, and so on. If you plan to manually install the Connector, you should ensure that your host meets these requirements.

When you deploy the Connector from BlueXP or from the Azure Marketplace, the image includes the required

OS and software components.

Dedicated host

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

Supported operating systems

- CentOS 7.6, 7.7, 7.8, and 7.9
- Red Hat Enterprise Linux 7.6, 7.7, 7.8, 7.9, 8.6, and 8.7

The host must be registered with Red Hat Subscription Management. If it's not registered, the host can't 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 is required. [Red Hat Solution: Which hypervisors are certified to run Red Hat Enterprise Linux?](#)

CPU

4 cores or 4 vCPUs

RAM

14 GB

Azure VM size

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

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](#)

Set up Azure permissions

Set up permissions in Azure so that you can deploy the Connector with the permissions that it needs to manage your data and storage infrastructure. How you set up permissions depends on the installation option that you're planning to use.

You can choose from the following installation options:

- **Install from BlueXP:** Set up permissions that enable BlueXP to authenticate with Azure and deploy the VM. BlueXP automatically sets up permissions for the Connector VM during deployment.

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

- **Install from the Azure Marketplace:** Set up an Azure custom role to associate with the Connector VM or

with an Azure AD service principal.

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

- **Manual install:** Set up an Azure custom role to associate with the Connector VM or with an Azure AD service principal.

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

Set up permissions to create the Connector from BlueXP

To create a Connector from BlueXP, 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.
2. Provide details about an Azure AD service principal. This service principal also requires specific permissions.

With both options, the first step is create a custom role.

Create a custom role

Create a custom role that you can assign to your Azure account or to a service principal.

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/read",

```

```

ents/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*. You can now apply this custom role to your user account or to a service principal.

Set up an authentication method

To deploy the BlueXP Connector, BlueXP needs to authenticate with Azure. You can choose between two Azure authentication methods.

Azure user account

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

Steps

1. In the Azure portal, open the **Subscriptions** service and select the user's subscription.
2. Click **Access control (IAM)**.
3. Click **Add > Add role assignment** and then add the permissions:
 - a. 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.

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

Result

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

Service principal

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

Create and set up a service principal in Azure Active Directory and obtain the Azure credentials that BlueXP needs.

Create an Azure Active Directory application for role-based access control

1. Ensure that you have 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](#).

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



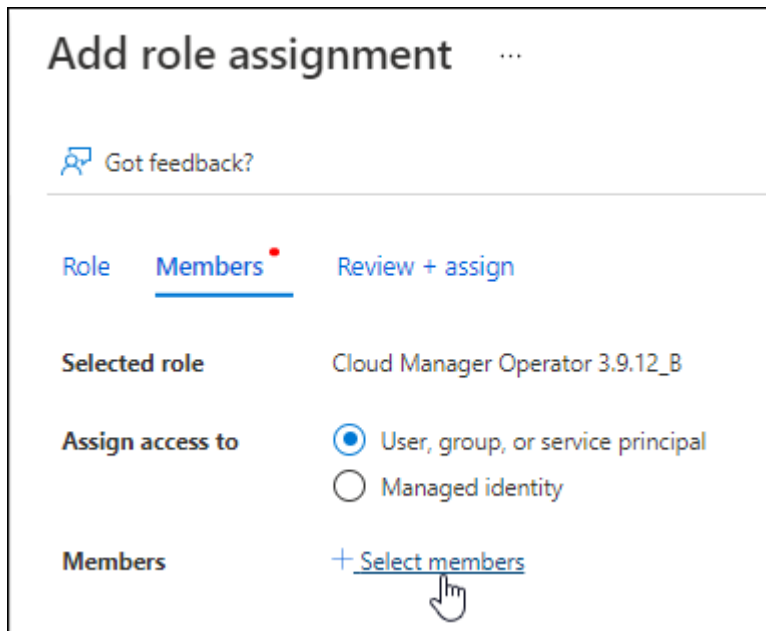
3. In the menu, click **App registrations**.

4. Click **New registration**.
5. 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.
6. Click **Register**.

You've created the AD application and service principal.

Assign the custom role to the application

1. From the Azure portal, open the **Subscriptions** service.
2. Select the subscription.
3. Click **Access control (IAM) > Add > Add role assignment**.
4. In the **Role** tab, select the **BlueXP Operator** role and click **Next**.
5. In the **Members** tab, complete the following steps:
 - a. Keep **User, group, or service principal** selected.
 - b. Click **Select members**.



- c. Search for the name of the application.

Here's an example:



- d. Select the application and click **Select**.
 - e. Click **Next**.
6. 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.

Add Windows Azure Service Management API permissions

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



user_impersonation

Access Azure Service Management as organization users (preview) ⓘ

Get the application ID and directory ID for the application

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**.



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.


Create a client secret

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 |  |

You now have a client secret that BlueXP can use it to authenticate with Azure AD.

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.

Set up permissions to assign after Azure Marketplace deployment or manual installation

If you deploy the Connector from the Azure Marketplace or if you manually install the Connector software on your own Linux host, you can provide permissions in the following ways:

- Option 1: Assign a custom role to the Azure VM using a system-assigned managed identity.
- Option 2: Provide BlueXP with the credentials for an Azure service principal that has the required permissions.

Custom role

Steps

1. If you're planning to manually install the software on your own host, enable a system-assigned managed identity on the VM so that you can provide the required Azure permissions through a custom role.

[Microsoft Azure documentation: Configure managed identities for Azure resources on a VM using the Azure portal](#)

2. Copy the contents of the [custom role permissions for the Connector](#) and save them in a JSON file.
3. 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"
```

4. 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. Use the Azure CLI to create the custom role:

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

Result

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

[Learn how to provide these permissions to BlueXP.](#)

Service principal

Create and set up a service principal in Azure Active Directory and obtain the Azure credentials that BlueXP needs.

Create an Azure Active Directory application for role-based access control

1. Ensure that you have 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](#).

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



3. In the menu, click **App registrations**.
4. Click **New registration**.
5. 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.
6. Click **Register**.

You've created the AD application and service principal.

Assign the custom role to the application

1. From the Azure portal, open the **Subscriptions** service.
2. Select the subscription.
3. Click **Access control (IAM) > Add > Add role assignment**.

4. In the **Role** tab, select the **BlueXP Operator** role and click **Next**.
5. In the **Members** tab, complete the following steps:
 - a. Keep **User, group, or service principal** selected.
 - b. Click **Select members**.



- c. Search for the name of the application.

Here's an example:



- d. Select the application and click **Select**.
 - e. Click **Next**.
6. 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.

Add Windows Azure Service Management API permissions

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



user_impersonation

Access Azure Service Management as organization users (preview) ⓘ

Get the application ID and directory ID for the application

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**.



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.


Create a client secret

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*-ZRoV4NLfdAcY7:+0vA |  |

Copy to clipboard

You now have a client secret that BlueXP can use it to authenticate with Azure AD.

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.

[Learn how to provide these permissions to BlueXP.](#)

Create a Connector in Azure

Create a Connector directly from the BlueXP web-based console, from the Azure Marketplace, or by installing the software on your own Linux host.

BlueXP

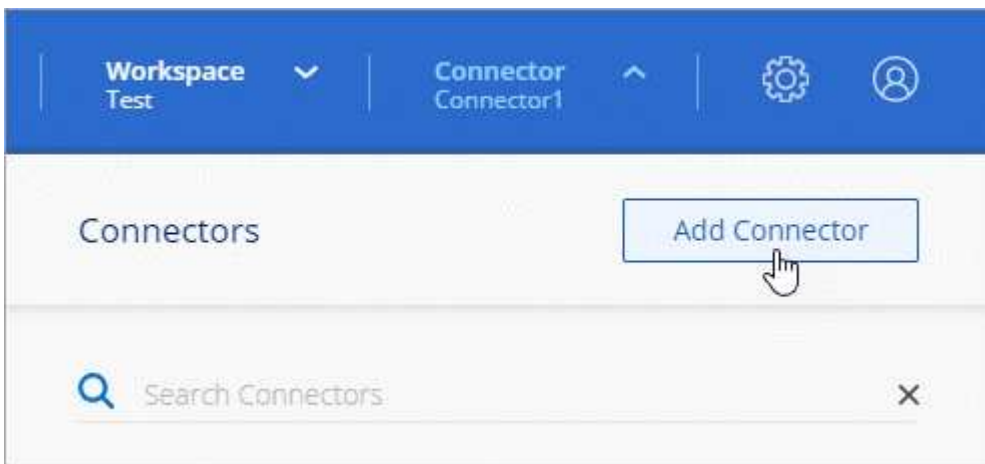
What you'll need

- 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**, select the authentication option that matches how you set up Azure permissions:

- Select **Azure user account** to log in to your Microsoft account, which should have the required permissions.

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.

- Select **Active Directory service principal** to enter information about the Azure Active Directory service principal that grants the required permissions:

- Application (client) ID
- Directory (tenant) ID
- Client Secret

[Learn how to obtain these values for a service principal.](#)

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 the required inbound and outbound rules.

[View security group rules for Azure.](#)

- **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.

Result

After the process is complete, the Connector is available for use from BlueXP.

Azure Marketplace

Steps

1. Go to the NetApp Connector VM page in the Azure Marketplace.

[Azure Marketplace page for commercial 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. A few more rule are required for specific configurations.

[View security group rules for Azure.](#)

- Under **Management**, enable **System assigned managed identity** for the Connector VM 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. After you're done, you'll need to assign the custom role that you created to [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 BlueXP account to associate with the Connector.
 - b. Enter a name for the system.
 - c. Under **Are you running in a secured environment?** keep restricted mode disabled.

You should keep restricted mode disabled because these steps describe how to use BlueXP in standard mode. You should enable restricted mode only if you have a secure environment and want to disconnect this account from BlueXP backend services. If that's the case, [follow steps to get started with BlueXP in restricted mode](#).

- d. Click **Let's start**.

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

What's next?

[Provide BlueXP with the permissions that you previously setup.](#)

Manual install

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.

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 or if the proxy is an intercepting proxy.
- A managed identity enabled on the VM in Azure so that you can provide the required Azure permissions through a custom role.

[Microsoft Azure documentation: Configure managed identities for Azure resources on a VM using the Azure portal](#)

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 "online" Connector installer that's meant for use in your network or in the cloud. A separate "offline" installer is available for the Connector, but it's only supported with private mode deployments.

4. Assign permissions to run the script.

```
chmod +x OnCommandCloudManager-<version>
```

Where <version> is the version of the Connector that you downloaded.

5. Run the installation script.

```
./OnCommandCloudManager-<version> --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-V3.9.26 --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 or if the proxy is an intercepting proxy.

6. Wait for the installation to complete.

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

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

`https://ipaddress`

8. After you log in, set up the Connector:
 - a. Specify the BlueXP account to associate with the Connector.
 - b. Enter a name for the system.
 - c. Under **Are you running in a secured environment?** keep restricted mode disabled.

You should keep restricted mode disabled because these steps describe how to use BlueXP in standard mode. You should enable restricted mode only if you have a secure environment and want to disconnect this account from BlueXP backend services. If that's the case, [follow steps to get started with BlueXP in restricted mode](#).

- d. Click **Let's start**.

Result

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

What's next?

[Provide BlueXP with the permissions that you previously setup.](#)

Provide Azure permissions to BlueXP

If you created the Connector from the Azure Marketplace or manually installed the software, you need to provide BlueXP with the permissions that you previously set up. Providing the permissions enables BlueXP to manage your data and storage

infrastructure in Azure.

[Learn how to set up these permissions.](#)

These steps don't apply if you deployed the Connector directly from BlueXP because BlueXP assigns the required permissions during deployment.

Custom role

Go to the Azure portal and assign the Azure custom role to the Connector virtual machine for one or more subscriptions.

Steps

1. From the Azure Portal, open the **Subscriptions** service and select your subscription.
2. Click **Access control (IAM) > Add > Add role assignment**.
3. 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.

4. In the **Members** tab, complete the following steps:
 - a. Assign access to a **Managed identity**.
 - b. Click **Select members**, select the subscription in which the Connector virtual machine was created, choose **Virtual machine**, and then select the Connector virtual machine.
 - c. Click **Select**.
 - d. 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

BlueXP now has the permissions that it needs to perform actions in Azure on your behalf.

What's next?

Go to the [BlueXP console](#) to start using the Connector with BlueXP.

Service principal

Steps

1. Go to the [BlueXP console](#) and log in.
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 **Microsoft Azure > Connector**.
 - b. **Define Credentials:** Enter information about the Azure Active Directory service principal that grants the required permissions:
 - Application (client) ID
 - Directory (tenant) ID
 - Client Secret

- c. **Marketplace Subscription:** Associate a Marketplace subscription with these credentials by subscribing now or by selecting an existing subscription.
- d. **Review:** Confirm the details about the new credentials and click **Add**.

Result

BlueXP now has the permissions that it needs to perform actions in Azure on your behalf.

Google Cloud

Quick start to create a Connector in Google Cloud

Create a Connector in Google Cloud by choosing an installation option, setting up networking, preparing permissions, and more.

1

Understand your installation options

The standard way to create a Connector in Google Cloud is directly from BlueXP, but you can also create it using gcloud, or by manually installing the software on a pre-existing Linux host.

[Learn more about your installation options.](#)

2

Set up networking

Prepare the following for the Connector:

- A VPC and subnet
- A network connection to the networks where you're planning to create and manage working environments
- Outbound internet access to specific endpoints for day-to-day operations
- The IP address, credentials, and HTTPS certificate of a proxy server, if a proxy server is required for outbound internet

[Learn more about networking requirements.](#)

3

Review host requirements

The Connector software must run on a host that meets specific requirements. If you plan to manually install the Connector software on your own Linux host, then you should ensure that your host meets these requirements. If you're creating the Connector from BlueXP or by using gcloud, then these requirements are taken care of for you because the software is deployed from an image.

The key requirements are as follows:

- A dedicated host running CentOS or Red Hat Enterprise Linux
- 4 CPUs
- 14 GB of RAM
- Docker Engine

[Learn more about these host requirements.](#)

4

Set up Google Cloud permissions

Set up Google Cloud permissions for the installation option that you're planning to use:

- **Installation from BlueXP or gcloud:** Create a custom role and attach it to the user who will deploy the Connector. Create another custom role and assign it to a service account for the Connector VM instance.
- **Manual install:** Create a custom role and assign it to a service account for the Connector VM instance.

[Follow step-by-step instructions for each of these options.](#)

5

Enable Google Cloud APIs

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

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

6

Create the Connector

Create the Connector using one of the available installation options:

- **From BlueXP:** Click the Connector drop-down, select **Add Connector** and follow the prompts.
- **Using gcloud:** Use the `gcloud compute instances create` command.
- **Manual install:** Download the Connector software from the [NetApp Support Site](#) and run the installation script.

[Follow step-by-step instructions for each of these options.](#)

7

Provide BlueXP with permissions

If you manually installed the Connector software on your own Linux host, you need to provide BlueXP with the permissions that you previously set up.

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

Connector installation options in Google Cloud

There are a few different ways to create a Connector in Google Cloud. Directly from BlueXP is the most common way. The installation option that you choose determines how you prepare for deployment.

The following installation options are available:

- Create the Connector directly from BlueXP (this is the standard option)

This action launches a VM instance running Linux and the Connector software in a VPC of your choice.

- Create the Connector using gcloud

This action also launches a VM instance running Linux and the Connector software.

- Download and manually install the software on your own Linux host

The installation option that you choose impacts how you prepare for installation. This includes how you provide BlueXP with the required permissions that it needs to authenticate and manage resources in Google Cloud.

[Learn how to install the Connector in Google Cloud.](#)

Set up Google Cloud networking

Set up your networking so the Connector can manage resources and processes within your hybrid cloud environment. For example, you need to ensure that connections are available to target networks and that outbound internet access is available.

VPC and subnet

When you create the Connector, you need to specify the VPC and subnet where the Connector should reside.

Connections to target networks

A Connector requires a network connection to the location where you're planning to create and manage working environments.

Outbound internet access

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

Endpoints contacted during manual installation


If you plan to manually install the Connector on your own Linux host, the installer for the Connector requires access to 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://cloudmanagerinfraproduct.azurecr.io>
- <https://production-artifacts.cloudmanager.cloud.netapp.com>
- 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.

Endpoints contacted for day-to-day operations

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://www.googleapis.com/compute/v1/ https://compute.googleapis.com/compute/v1 https://cloudresourcemanager.googleapis.com/v1/projects https://www.googleapis.com/compute/beta https://storage.googleapis.com/storage/v1 https://www.googleapis.com/storage/v1 https://iam.googleapis.com/v1 https://cloudkms.googleapis.com/v1 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 https://api.bluexp.netapp.com https://*.cloudmanager.cloud.netapp.com 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 https://*.blob.core.windows.net | To upgrade the Connector and its Docker components. |

Related link

[Prepare networking for user access to the BlueXP console](#)

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

Ports

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 (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.
- 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. 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.

IP address limitation

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

Review Connector host requirements for Google Cloud installs

The Connector software must run on a host that meets specific operating system requirements, RAM requirements, port requirements, and so on. If you plan to manually install the Connector, you should ensure that your host meets these requirements.

When you deploy the Connector from BlueXP or by using glcloud, the image includes the required OS and software components.

Dedicated host

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

Supported operating systems

- CentOS 7.6, 7.7, 7.8, and 7.9
- Red Hat Enterprise Linux 7.6, 7.7, 7.8, 7.9, 8.6, and 8.7

The host must be registered with Red Hat Subscription Management. If it's not registered, the host can't 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 is required. [Red Hat Solution: Which hypervisors are certified to run Red Hat Enterprise Linux?](#)

CPU

4 cores or 4 vCPUs

RAM

14 GB

Google Cloud 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](#)

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](#)

Set up Google Cloud permissions

Set up permissions in Google Cloud so that you can deploy the Connector with the permissions that it needs to manage your data and storage infrastructure.

You need to set up Google Cloud permissions as follows:

- If you are planning to create the Connector from BlueXP or by using gcloud, then you need to set up permissions for the Google Cloud user who will deploy the Connector VM.
- Set up permissions for the Connector by creating a role and granting the role to a service account.

You'll associate this service account with the Connector VM so that BlueXP has the required permissions.

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 create the Connector from BlueXP or gcloud

Before you can deploy a Connector from BlueXP or by using gcloud, you need to ensure that your Google Cloud account has the correct permissions.

Steps

1. Create a custom role in Google Cloud:
 - a. Create a YAML file 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`

- From Google Cloud, activate cloud shell.
- Upload the YAML file that includes the required permissions.
- Create a custom role by using the `gcloud iam roles create` command.

The following example creates a role named "connectorDeployment" at the project level:

```
gcloud iam roles create connectorDeployment --project=myproject --file=connector-deployment.yaml
```

[Google Cloud docs: Creating and managing custom roles](#)

- Assign this custom role to the user who will deploy the Connector from BlueXP or by using `gcloud`.

[Google Cloud docs: Grant a single role](#)

Result

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

Set up permissions for the Connector

A service account is required to provide the Connector with the permissions that BlueXP needs to manage resources in Google Cloud. You need to associate this service account with the Connector VM.

Steps

- Create a custom role in Google Cloud:
 - Create a YAML file that includes the contents of the [service account permissions for the Connector](#).
 - From Google Cloud, activate cloud shell.
 - Upload the YAML file that includes the required permissions.
 - Create a custom role by using the `gcloud iam roles create` command.

The following example creates a role named "connector" at the project level:

```
gcloud iam roles create connector --project=myproject --file=connector.yaml
```

[Google Cloud docs: Creating and managing custom roles](#)

- Create a service account in Google Cloud:
 - From the IAM & Admin service, click **Service Accounts > Create Service Account**.
 - Enter service account details and click **Create and Continue**.
 - Select the role that you just created.
 - Finish the remaining steps to create the role.

[Google Cloud docs: Creating a service account](#)

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 you'll need to prepare your permissions.

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 to deploy the Connector | Custom | Service Project | Connector deployment policy | compute.networkUser | Deploying the Connector in the service project |
| Connector service account | Custom | Service project | Connector service account policy | <ul style="list-style-type: none">• compute.networkUser• deploymentmanager.editor | Deploying and maintaining Cloud Volumes ONTAP and services in the service project |
| Cloud Volumes ONTAP service account | Custom | Service project | <ul style="list-style-type: none">• storage.admin• member: BlueXP service account as serviceAccount.user | N/A | (Optional) For data tiering and BlueXP backup and recovery |

| Identity | Creator | Hosted in | Service project permissions | Host project permissions | Purpose |
|---|--------------|-----------------|-----------------------------|--------------------------|---|
| Google APIs service agent | Google Cloud | Service project | (Default) Editor | compute.networkUser | 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 | (Default) Editor | compute.networkUser | 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.

Enable Google Cloud APIs

Several Google Cloud APIs must be enabled before you can deploy the Connector and Cloud Volumes ONTAP in Google Cloud.

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

[Google Cloud documentation: Enabling APIs](#)

Create a Connector in Google Cloud

Create a Connector directly from the BlueXP web-based console, by using gcloud, or by installing the software on your own Linux host.

BlueXP

What you'll need

- The required Google Cloud permissions to create the Connector and a service account for the Connector VM.

[Learn how to set up Google Cloud permissions](#)

- A VPC and subnet that meets networking requirements.

[Learn about networking requirements](#)

- Details about a proxy server, if a proxy is required for internet access from the Connector.

Steps

1. 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 the required inbound and outbound rules.

[Firewall rules in Google Cloud](#)

- **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.

Result

After the process is complete, the Connector is available for use from BlueXP.

gcloud

What you'll need

- The required Google Cloud permissions to create the Connector and a service account for the Connector VM.

[Learn how to set up Google Cloud permissions](#)

- A VPC and subnet that meets networking requirements.

[Learn about networking requirements](#)

Steps

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 BlueXP account to associate with the Connector.

[Learn about BlueXP accounts](#).

- b. Enter a name for the system.

Result

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

Open a web browser and go to the [BlueXP console](#) to start using the Connector with BlueXP.

Manual install**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.

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 or if the proxy is an intercepting proxy.

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 "online" Connector installer that's meant for use in your network or in the cloud. A separate "offline" installer is available for the Connector, but it's only supported with private mode deployments.

4. Assign permissions to run the script.

```
chmod +x OnCommandCloudManager-<version>
```

Where `<version>` is the version of the Connector that you downloaded.

5. Run the installation script.

```
./OnCommandCloudManager-<version> --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-V3.9.26 --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 or if the proxy is an intercepting proxy.

6. Wait for the installation to complete.

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

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

`https://ipaddress`

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

- Specify the BlueXP account to associate with the Connector.
- Enter a name for the system.
- Under **Are you running in a secured environment?** keep restricted mode disabled.

You should keep restricted mode disabled because these steps describe how to use BlueXP in standard mode. You should enable restricted mode only if you have a secure environment and want to disconnect this account from BlueXP backend services. If that's the case, [follow steps to get started with BlueXP in restricted mode](#).

- Click **Let's start**.

Result

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

What's next?

[Provide BlueXP with the permissions that you previously setup.](#)

Provide Google Cloud permissions to BlueXP

If you manually installed the Connector software on your own Linux host, you need to provide BlueXP with the permissions that you previously set up. Providing the permissions enables BlueXP to manage your data and storage infrastructure in Google Cloud.

[Learn how to set up these permissions.](#)

These steps don't apply if you deployed the Connector directly from BlueXP or by using gcloud.

Steps

- Go to the Google Cloud portal and assign the service account to the Connector VM instance.

[Google Cloud documentation: Changing the service account and access scopes for an instance](#)

- 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

BlueXP now has the permissions that it needs to perform actions in Google Cloud on your behalf.

On premises

Quick start to create a Connector on premises

Create a Connector on your premises by setting up networking, preparing a host, preparing cloud permissions, and more.

1

Set up networking

Prepare the following for the Connector:

- A network location where you plan to install the Connector
- A network connection to the networks where you're planning to create and manage working environments
- Outbound internet access to specific endpoints for day-to-day operations
- The IP address, credentials, and HTTPS certificate of a proxy server, if a proxy server is required for outbound internet

[Learn more about networking requirements.](#)

2

Review host requirements

The Connector software must run on a host that meets specific requirements. The key requirements are as follows:

- A dedicated host running CentOS or Red Hat Enterprise Linux
- 4 CPUs
- 14 GB of RAM
- Docker Engine

[Learn more about these host requirements.](#)

3

Set up cloud permissions

Set up permissions for your cloud provider so that you can use BlueXP to manage storage in the cloud:

- **AWS:** Create an IAM policy and attach the policy to an IAM user. After installation, you need to provide BlueXP with access keys for that IAM user.
- **Azure:** Set up a service principal in Azure Active Directory that includes the required permissions. After installation, you need to provide BlueXP with the credentials for the service principal.

When the Connector is installed on your premises, it can't manage storage or data in Google Cloud. The Connector must be installed in Google Cloud to manage any storage or data that resides there.

[Follow step-by-step instructions for each of these options.](#)

4

Install the Connector software

Download the Connector software from the [NetApp Support Site](#) and run the installation script.

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

5

Provide BlueXP with permissions

After you install and set up the Connector, you need to add your cloud credentials so that BlueXP has the required permissions to perform actions in AWS or Azure.

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

Set up on-prem networking

Set up your networking so the Connector can manage resources and processes within your hybrid cloud environment. For example, you need to ensure that connections are available to target networks and that outbound internet access is available.

Connections 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 want to launch Cloud Volumes ONTAP in the cloud, then you must set up a VPN connection from your corporate network to the virtual network where you plan to launch Cloud Volumes ONTAP.

Outbound internet access

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

Endpoints contacted during manual installation


When you manually install the Connector on your own Linux host, the installer for the Connector requires access to 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://cloudmanagerinfraproduct.azurecr.io>
- <https://production-artifacts.cloudmanager.cloud.netapp.com>
- 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.

Endpoints contacted for day-to-day operations

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 |
|---|---|
| AWS services (amazonaws.com): <ul style="list-style-type: none">• CloudFormation• Elastic Compute Cloud (EC2)• Identity and Access Management (IAM)• Key Management Service (KMS)• Security Token Service (STS)• Simple Storage Service (S3) | To manage resources in AWS. The exact endpoint depends on the region in which you deploy the Connector. Refer to AWS documentation for details |
| https://management.azure.com https://login.microsoftonline.com | To manage resources in Azure public regions. |
| https://management.chinacloudapi.cn https://login.chinacloudapi.cn | To manage resources in Azure China regions. |
| https://www.googleapis.com/compute/v1/ https://compute.googleapis.com/compute/v1/ https://cloudresourcemanager.googleapis.com/v1/projects https://www.googleapis.com/compute/beta https://storage.googleapis.com/storage/v1 https://www.googleapis.com/storage/v1 https://iam.googleapis.com/v1 https://cloudkms.googleapis.com/v1 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.bluelxp.netapp.com https://api.bluelxp.netapp.com https://*.cloudmanager.cloud.netapp.com https://cloudmanager.cloud.netapp.com | <div>The Connector is currently contacting "cloudmanager.cloud.netapp.com" but it will start contacting "api.bluelxp.netapp.com" in an upcoming release.</div> |
| https://cloudmanagerinfraprod.azurecr.io https://*.blob.core.windows.net | To upgrade the Connector and its Docker components. |

Related link

[Prepare networking for user access to the BlueXP console](#)

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

Ports

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 (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.
- 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. 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.

IP address limitation

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

Review Connector host requirements for on-prem installs

The Connector software must run on a host that meets specific operating system requirements, RAM requirements, port requirements, and so on. Ensure that your host meets these requirements before you install the Connector.

Dedicated host

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

Supported operating systems

- CentOS 7.6, 7.7, 7.8, and 7.9
- Red Hat Enterprise Linux 7.6, 7.7, 7.8, 7.9, 8.6, and 8.7

The host must be registered with Red Hat Subscription Management. If it's not registered, the host can't 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 is required. [Red Hat Solution: Which hypervisors are certified to run Red Hat Enterprise Linux?](#)

CPU

4 cores or 4 vCPUs

RAM

14 GB

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](#)

Set up cloud permissions for on-prem deployments

If you want to use BlueXP services in AWS or Azure with an on-premises Connector, then you need to set up permissions in your cloud provider so that you can add the credentials to the Connector after you install it.



Why not Google Cloud? When the Connector is installed on your premises, it can't manage your resources in Google Cloud. The Connector must be installed in Google Cloud to manage any resources that resides there.

AWS

When the Connector is installed on premises, you need to provide BlueXP with AWS permissions by adding access keys for an IAM user who has the required permissions.

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 a policy:
 - a. Click **Policies > Create policy**.
 - b. Select **JSON** and copy and paste the contents of the [IAM policy for the Connector](#).
 - c. Finish the remaining steps to create the policy.

Depending on the BlueXP services that you're planning to use, you might need to create a second policy.

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. [Learn more about IAM policies for the Connector](#).

2. Attach the policies to an IAM user.
 - [AWS Documentation: Creating IAM Roles](#)
 - [AWS Documentation: Adding and Removing IAM Policies](#)
3. Ensure that the user has access keys that you can add to BlueXP after you install the Connector.

Result

You should now have access keys for an IAM user who has the required permissions. After you install the Connector, you'll need to associate these credentials with the Connector from BlueXP.

[Learn how to provide these permissions to BlueXP](#).

Azure

When the Connector is installed on premises, you need to provide BlueXP with Azure permissions by setting up a service principal in Azure Active Directory and obtaining the Azure credentials that BlueXP needs.

Create an Azure Active Directory application for role-based access control

1. Ensure that you have 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](#).

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



3. In the menu, click **App registrations**.
4. Click **New registration**.
5. 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.
6. Click **Register**.

You've created the AD application and service principal.

Assign the application to a role

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.

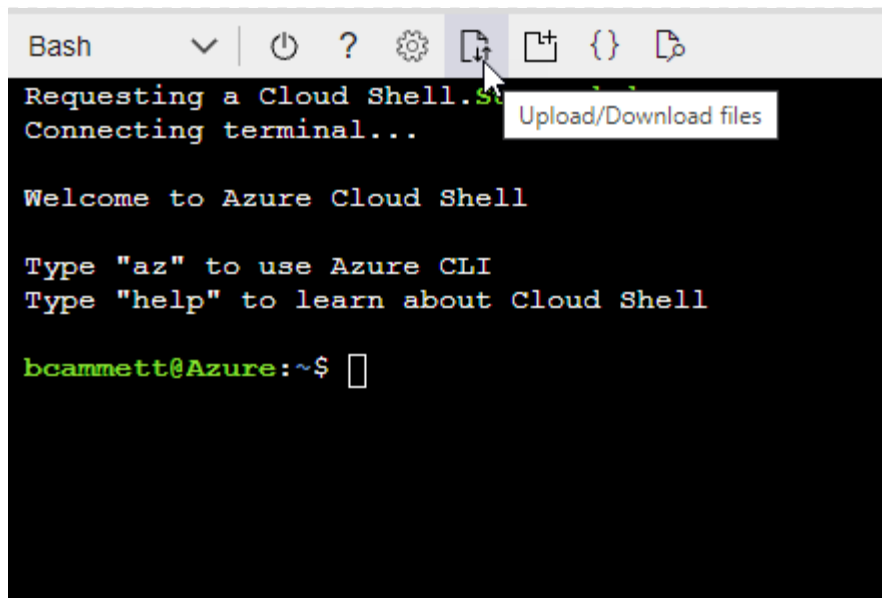
Example

```
"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.

Add Windows Azure Service Management API permissions

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



user_impersonation

Access Azure Service Management as organization users (preview) ⓘ

Get the application ID and directory ID for the application

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**.

Delete Endpoints

Welcome to the new and improved App registrations. Looking to learn

Display name : test-service-principal

Application (client) ID : 73de25f9-99be-4ae0-8b24-538ca787a6b3

Directory (tenant) ID : 4b0911a0-929b-4715-944b-c03745165b3a

Object ID : b37489a9-379f-49c2-b27c-e630514106a5

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.

Create a client secret

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 | |

You now have a client secret that BlueXP can use it to authenticate with Azure AD.

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. After you install the Connector, you'll need to associate these credentials with the Connector from BlueXP.

[Learn how to provide these permissions to BlueXP.](#)

Install and set up a Connector on premises

Install a Connector on premises and then log in and set it up to work with your BlueXP account.

Install the Connector

Download and install the Connector software on an existing Linux host on premises.

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.

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 or if the proxy is an intercepting proxy.

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 "online" Connector installer that's meant for use in your network or in the cloud. A separate "offline" installer is available for the Connector, but it's only supported with private mode deployments.

4. Assign permissions to run the script.

```
chmod +x OnCommandCloudManager-<version>
```

Where `<version>` is the version of the Connector that you downloaded.

5. Run the installation script.

```
./OnCommandCloudManager-<version> --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-V3.9.26 --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 or if the proxy is an intercepting proxy.

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. After you log in, set up BlueXP:
 - a. Specify the BlueXP account to associate with the Connector.
 - b. Enter a name for the system.
 - c. Under **Are you running in a secured environment?** keep restricted mode disabled.

You should keep restricted mode disabled because these steps describe how to use BlueXP in standard mode. (In addition, restricted mode isn't supported when the Connector is installed on premises.)

- d. Click **Let's start**.

Result

BlueXP is now set up with the Connector that you just installed.

What's next?

[Provide BlueXP with the permissions that you previously setup.](#)

Provide permissions to BlueXP for on-prem installs

After you install and set up the Connector, you need to add your cloud credentials so that BlueXP has the required permissions to perform actions in AWS or Azure.



Why not Google Cloud? When the Connector is installed on your premises, it can't manage your resources in Google Cloud. The Connector must be installed in Google Cloud to manage any resources that resides there.

AWS

Before you get started

If you just created these credentials in AWS, 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 > Connector**.
 - b. **Define Credentials:** 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.
 - d. **Review:** Confirm the details about the new credentials and click **Add**.

Result

BlueXP now has the permissions that it needs to perform actions in AWS on your behalf. You can now go to the [BlueXP console](#) to start using the Connector with BlueXP.

Azure

Before you get started

If you just created these credentials in Azure, 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 **Microsoft Azure > Connector**.
 - b. **Define Credentials:** Enter information about the Azure Active Directory service principal that grants the required permissions:
 - Application (client) ID
 - Directory (tenant) ID
 - Client Secret
 - c. **Marketplace Subscription:** Associate a Marketplace subscription with these credentials by subscribing now or by selecting an existing subscription.
 - d. **Review:** Confirm the details about the new credentials and click **Add**.

Result

BlueXP now has the permissions that it needs to perform actions in Azure on your behalf. You can now go to the [BlueXP console](#) to start using the Connector with BlueXP.

Subscribe to BlueXP (standard mode)

Subscribe to BlueXP from your cloud provider's marketplace to pay for BlueXP services at an hourly rate (PAYGO) or through an annual contract. If you purchased a license from NetApp (BYOL), you also need to subscribe to the PAYGO offering. Your license is always charged first, but you'll be charged at the hourly rate if you exceed your licensed capacity or if the license's term expires.

AWS

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 BlueXP 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**.

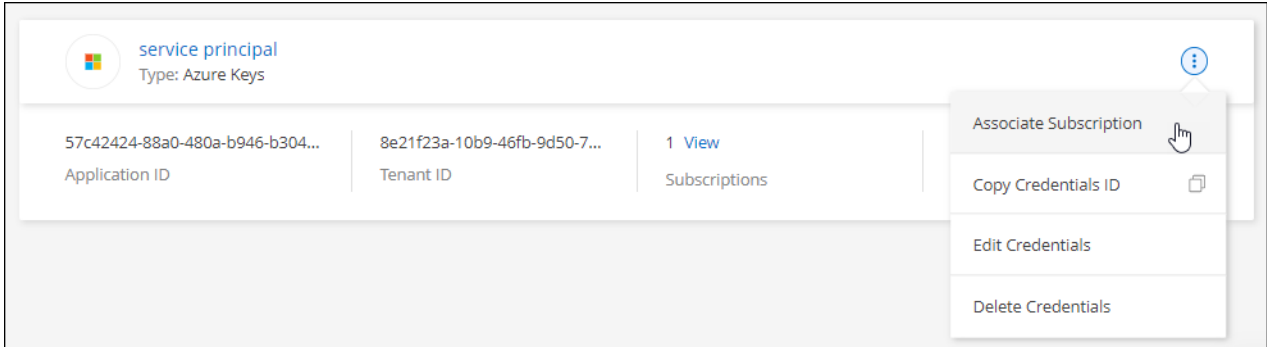
The following video shows the steps to subscribe from the AWS Marketplace:

► <https://docs.netapp.com/us-en/cloud-manager-setup->

Azure

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 BlueXP 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**.

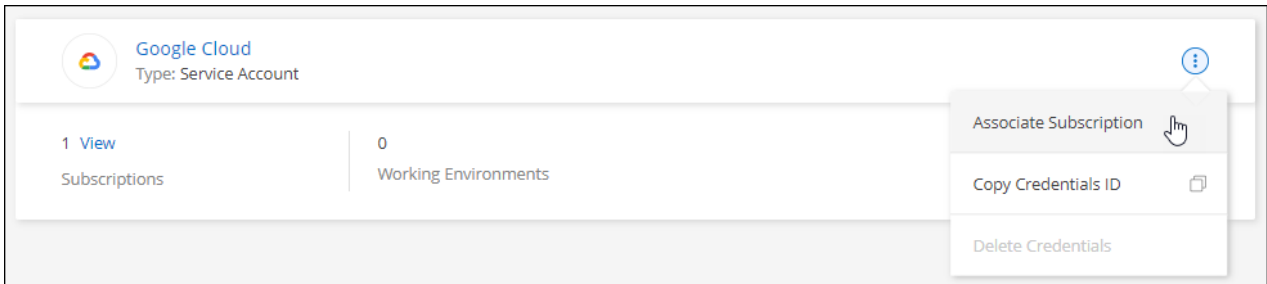
The following video shows the steps to subscribe from the Azure Marketplace:

► <https://docs.netapp.com/us-en/cloud-manager-setup->

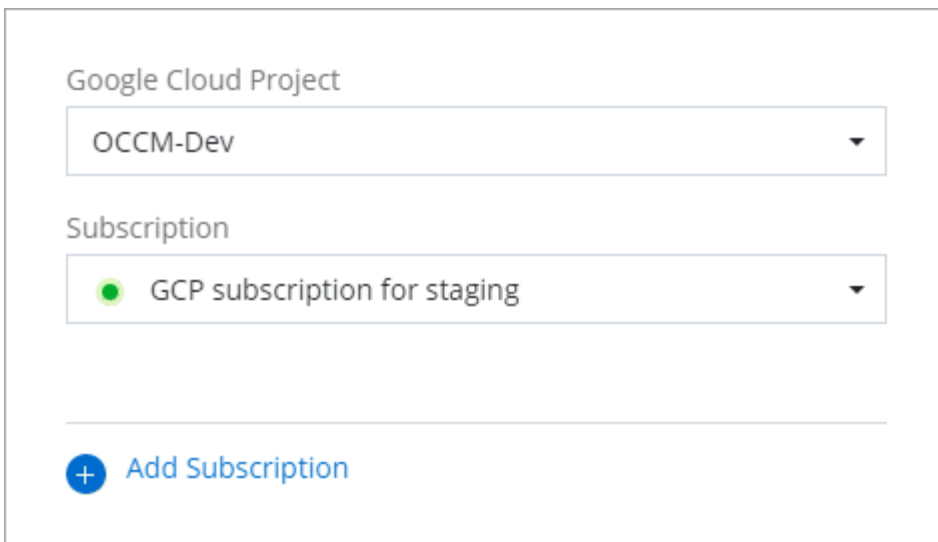
Google Cloud

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**.



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 Google Cloud console interface for the NetApp BlueXP product. At the top, the Google Cloud logo and the URL 'netapp.com' are visible. Below the navigation bar, the page title 'Product details' is shown. The main content area features the NetApp logo and the product name 'NetApp BlueXP'. A description states: 'BlueXP lets you build, protect, and govern your hybrid multicloud data estate.' A prominent blue 'SUBSCRIBE' button is centered. Below this, a navigation menu includes links for 'OVERVIEW', 'PRICING', 'DOCUMENTATION', and 'SUPPORT'. The 'OVERVIEW' section is active, displaying two paragraphs of text about BlueXP's capabilities. To the right, an 'Additional details' section provides metadata: 'Type: SaaS & APIs', 'Last updated: 12/19/22', and 'Category: 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 BlueXP account. The process of linking a subscription isn't complete until you are redirected from this page and then sign in to BlueXP.

Your order request has been sent to NetApp, Inc.



Your new subscription to the Cloud Manager 1 month plan for Cloud Manager for Cloud Volumes ONTAP requires your registration with NetApp, Inc.. After NetApp, Inc. approves your request, your subscription will be active and you will begin getting charged. This processing time will depend on the vendor, and you should reach out to NetApp, Inc. directly with any questions related to signup.

[VIEW ORDERS](#)

[REGISTER WITH NETAPP, INC.](#)

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 BlueXP 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.



The screenshot shows a form with two dropdown menus. The first dropdown is labeled 'Google Cloud Project' and has 'OCCM-Dev' selected. The second dropdown is labeled 'Subscription' and has 'GCP subscription for staging' selected, which is preceded by a green status indicator. Below the dropdowns is a blue button with a plus icon and the text 'Add Subscription'.

What you can do next (standard mode)

Now that you've logged in and set up BlueXP in standard mode, users can create and discover working environments and use BlueXP data services.

For help, go to the [home page for the BlueXP documentation](#) to view the docs for all BlueXP services.

Related link

[BlueXP deployment modes](#)

Get started with restricted mode

Quick start for BlueXP in restricted mode

Get started with BlueXP in restricted mode by preparing your environment, deploying the Connector, and subscribing to BlueXP.

1

Prepare for deployment

- Prepare a dedicated Linux host that meets requirements for CPU, RAM, disk space, Docker Engine, and more.
- Set up networking that provides access to the target networks, outbound internet access for manual installations, and outbound internet for day-to-day access.
- Set up permissions in your cloud provider so that you can associate those permissions with the Connector instance after you deploy it.

[Learn how to prepare for deployment.](#)

2

Deploy the Connector

- a. Install the Connector from your cloud provider's marketplace or by manually installing the software on your own Linux host.
- b. Set up BlueXP by opening a web browser and entering the Linux host's IP address.
- c. Provide BlueXP with the permissions that you previously set up.

[Learn how to deploy the Connector.](#)

3

Subscribe to BlueXP

Subscribe to BlueXP from your cloud provider's marketplace to pay for BlueXP services at an hourly rate (PAYGO) or through an annual contract.

[Learn how to subscribe to BlueXP.](#)

Prepare for deployment in restricted mode

Prepare your environment before you deploy BlueXP in restricted mode. For example, you need to review host requirements, prepare networking, set up permissions, and more.

Understand how restricted mode works

Before you get started, you should have an understanding of how BlueXP works in restricted mode.

For example, you should understand that you need to use the browser-based interface that is available locally from the BlueXP Connector that you need to install. You can't access BlueXP from the web-based console that's provided through the SaaS layer.

In addition, not all BlueXP services are available.

[Learn how restricted mode works.](#)

Review installation options

In restricted mode, you can only install the Connector in the cloud. The following installation options are available:

- From the AWS Marketplace
- From the Azure Marketplace
- Manually installing the Connector on your own Linux host that's running in AWS, Azure, or Google Cloud

Review host requirements

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

When you deploy the Connector from the AWS or Azure Marketplace, the image includes the required OS and software components. You simply need to choose an instance type that meets CPU and RAM requirements.

Dedicated host

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

Supported operating systems

- CentOS 7.6, 7.7, 7.8, and 7.9
- Red Hat Enterprise Linux 7.6, 7.7, 7.8, 7.9, 8.6, and 8.7

The host must be registered with Red Hat Subscription Management. If it's not registered, the host can't 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 is required. [Red Hat Solution: Which hypervisors are certified to run Red Hat Enterprise Linux?](#)

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.

Google Cloud 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](#)

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](#)

Prepare networking for the Connector

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.

Connections to target networks

The Connector must have a network connection to the location where you plan to manage storage. For example, the VPC or VNet where you plan to deploy Cloud Volumes ONTAP, or the data center where your on-premises ONTAP clusters reside.

Outbound internet access for manual installs

If you plan to manually install the Connector on your own Linux host, the installer for the Connector requires access to 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://cloudmanagerinfraproduct.azurecr.io>
- <https://production-artifacts.cloudmanager.cloud.netapp.com>
- 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.

Outbound internet access for day-to-day operations

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 |
|--|--|
| AWS services (amazonaws.com): <ul style="list-style-type: none">• CloudFormation• Elastic Compute Cloud (EC2)• Identity and Access Management (IAM)• Key Management Service (KMS)• Security Token Service (STS)• Simple Storage Service (S3) | To manage resources in AWS. The exact endpoint depends on the region in which you deploy the Connector. Refer to AWS documentation for details |
| https://management.azure.com https://login.microsoftonline.com https://blob.core.windows.net https://core.windows.net | To manage resources in Azure public regions. |
| https://management.usgovcloudapi.net https://login.microsoftonline.us https://blob.core.usgovcloudapi.net https://core.usgovcloudapi.net | To manage resources in Azure Government regions. |

| Endpoints | Purpose |
|---|--|
| https://management.chinacloudapi.cn https://login.chinacloudapi.cn https://blob.core.chinacloudapi.cn https://core.chinacloudapi.cn | To manage resources in Azure China regions. |
| https://www.googleapis.com/compute/v1/ https://compute.googleapis.com/compute/v1 https://cloudresourcemanager.googleapis.com/v1/projects https://www.googleapis.com/compute/beta https://storage.googleapis.com/storage/v1 https://www.googleapis.com/storage/v1 https://iam.googleapis.com/v1 https://cloudkms.googleapis.com/v1 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 https://api.bluexp.netapp.com https://*.cloudmanager.cloud.netapp.com 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 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

Public IP address in Azure

If you want to use a public IP address with the Connector VM in Azure, the IP address must use a Basic SKU to ensure that BlueXP uses this public IP address.

Create public IP address

Name *

newIP

SKU * ⓘ

☒ Basic
 ☐ Standard

Assignment

☐ Dynamic
 ☒ Static

If you use a Standard SKU IP address instead, then BlueXP uses the *private* IP address of the Connector, instead of the public IP. If the machine that you're using to access the BlueXP Console doesn't have access to that private IP address, then actions from the BlueXP Console will fail.

[Azure documentation: Public IP SKU](#)

Ports

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

HTTP (80) and HTTPS (443) provide access to the BlueXP console. SSH (22) is only needed if you need to connect to the host for troubleshooting.

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. 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.

Prepare networking for user access to BlueXP console

In restricted mode, the BlueXP user interface is accessible from the Connector. As you use the BlueXP user interface, it contacts a few endpoints to complete data management tasks. The machine running the web browser must have connections to the following endpoints.

| Endpoints | Purpose |
|--|---|
| https://signin.b2c.netapp.com | Required to update NetApp Support Site (NSS) credentials or to add new NSS credentials to BlueXP. |
| https://netapp-cloud-account.auth0.com | Your web browser connects to these endpoints for centralized user authentication through BlueXP. |
| https://cdn.auth0.com | |
| https://services.cloud.netapp.com | |
| https://widget.intercom.io | For in-product chat that enables you to talk to NetApp cloud experts. |

Prepare cloud permissions

BlueXP requires permissions from your cloud provider to deploy Cloud Volumes ONTAP in a virtual network and to use BlueXP data services. You need to set up permissions in your cloud provider and then associate those permissions with the Connector.

To view the required steps, select the authentication option that you'd like to use for your cloud provider.

AWS IAM role

Use an IAM role to provide the Connector with permissions.

If you're creating the Connector from the AWS Marketplace, you'll be prompted to select that IAM role when you launch the EC2 instance.

If you're manually installing the Connector on your own Linux host, you'll need to attach the role to the EC2 instance.

Steps

1. Log in to the AWS console and navigate to the IAM service.
2. Create a policy:
 - a. Click **Policies > Create policy**.
 - b. Select **JSON** and copy and paste the contents of the [IAM policy for the Connector](#).
 - c. Finish the remaining steps to create the policy.
3. Create an IAM role:
 - a. Click **Roles > Create role**.
 - b. Select **AWS service > EC2**.
 - c. Add permissions by attaching the policy that you just created.
 - d. Finish the remaining steps to create the role.

Result

You now have an IAM role for the Connector EC2 instance.

AWS access key

Set up permissions and an access key for an IAM user. You'll need to provide BlueXP with the AWS access key after you install the Connector and set up BlueXP.

Steps

1. From the IAM console, create a policy:
 - a. Click **Policies > Create policy**.
 - b. Select **JSON** and copy and paste the contents of the [IAM policy for the Connector](#).
 - c. Finish the remaining steps to create the policy.

Depending on the BlueXP services that you're planning to use, you might need to create a second policy.

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. [Learn more about IAM policies for the Connector](#).

2. Attach the policies to an IAM user.
 - [AWS Documentation: Creating IAM Roles](#)
 - [AWS Documentation: Adding and Removing IAM Policies](#)
3. Ensure that the user has access keys that you can add to BlueXP after you install the Connector.

Result

The account now has the required permissions.

Azure role

Create an Azure custom role with the required permissions. You'll assign this role to the Connector VM.

Steps

1. If you're planning to manually install the software on your own host, enable a system-assigned managed identity on the so that you can provide the required Azure permissions through a custom role.

[Microsoft Azure documentation: Configure managed identities for Azure resources on a VM using the Azure portal](#)

2. Copy the contents of the [custom role permissions for the Connector](#) and save them in a JSON file.
3. 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.

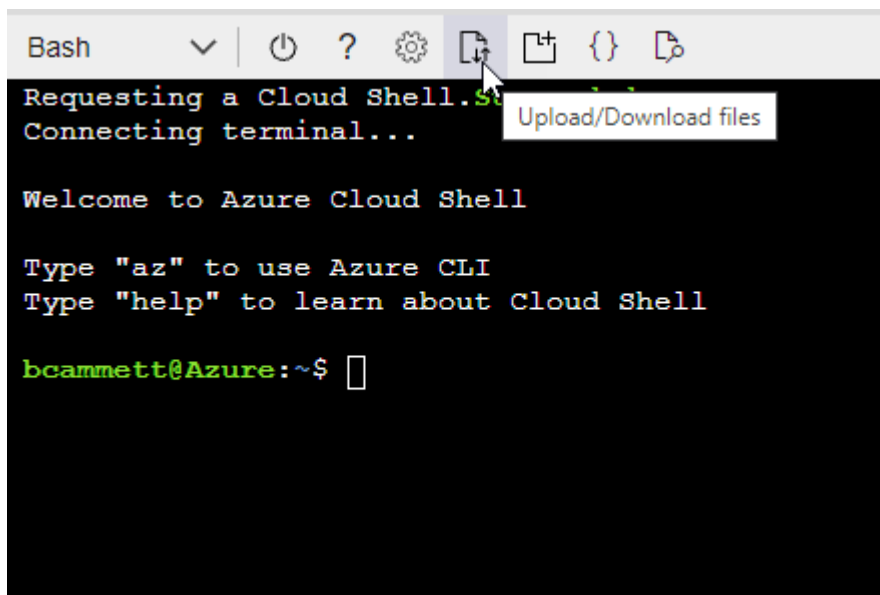
Example

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

4. 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. Use the Azure CLI to create the custom role:

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

Result

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

Azure service principal

Create and set up a service principal in Azure Active Directory and obtain the Azure credentials that BlueXP needs. You'll need to provide BlueXP with these credentials after you install the Connector and set up BlueXP.

Create an Azure Active Directory application for role-based access control

1. Ensure that you have 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](#).

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



3. In the menu, click **App registrations**.
4. Click **New registration**.
5. 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.
6. Click **Register**.

You've created the AD application and service principal.

Assign the custom role to the application

1. From the Azure portal, open the **Subscriptions** service.
2. Select the subscription.
3. Click **Access control (IAM) > Add > Add role assignment**.

4. In the **Role** tab, select the **BlueXP Operator** role and click **Next**.
5. In the **Members** tab, complete the following steps:
 - a. Keep **User, group, or service principal** selected.
 - b. Click **Select members**.



- c. Search for the name of the application.

Here's an example:



- d. Select the application and click **Select**.
 - e. Click **Next**.
6. 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.

Add Windows Azure Service Management API permissions

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



user_impersonation

Access Azure Service Management as organization users (preview) ⓘ

Get the application ID and directory ID for the application

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**.



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.

Create a client secret

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*-ZRoV4NLfdAcY7:+0vA |

Copy to clipboard

You now have a client secret that BlueXP can use it to authenticate with Azure AD.

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.

Google Cloud service account

Create a role and apply it to a service account that you'll use for the Connector VM instance.

Steps

1. Create a custom role in Google Cloud:
 - a. Create a YAML file that includes the permissions defined in the [Connector policy for Google Cloud](#).
 - b. From Google Cloud, activate cloud shell.
 - c. Upload the YAML file that includes the required permissions for the Connector.
 - d. Create a custom role by using the `gcloud iam roles create` command.

The following example creates a role named "connector" at the project level:

```
gcloud iam roles create connector --project=myproject
--file=connector.yaml
```

[Google Cloud docs: Creating and managing custom roles](#)

2. Create a service account in Google Cloud:
 - a. From the IAM & Admin service, click **Service Accounts > Create Service Account**.
 - b. Enter service account details and click **Create and Continue**.
 - c. Select the role that you just created.
 - d. Finish the remaining steps to create the role.

[Google Cloud docs: Creating a service account](#)

Result

You now have a service account that you can assign to the Connector VM instance.

Enable Google Cloud APIs

Several APIs are required to deploy Cloud Volumes ONTAP in Google Cloud.

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

Deploy the Connector in restricted mode

Deploy the Connector in restricted mode so that you can use BlueXP with limited outbound connectivity to the BlueXP SaaS layer. To get started, install the Connector, set up BlueXP by accessing the user interface that's running on the Connector, and then provide the cloud permissions that you previously set up.

Install the Connector

Install the Connector from your cloud provider's marketplace or by manually installing the software on your own Linux host.

AWS Commercial Marketplace

What you'll need

- A VPC and subnet that meets networking requirements.

[Learn about networking requirements](#)

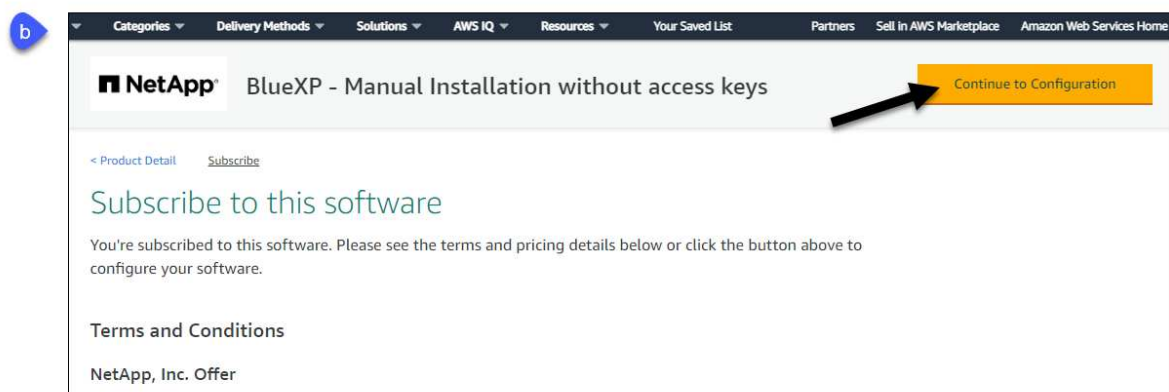
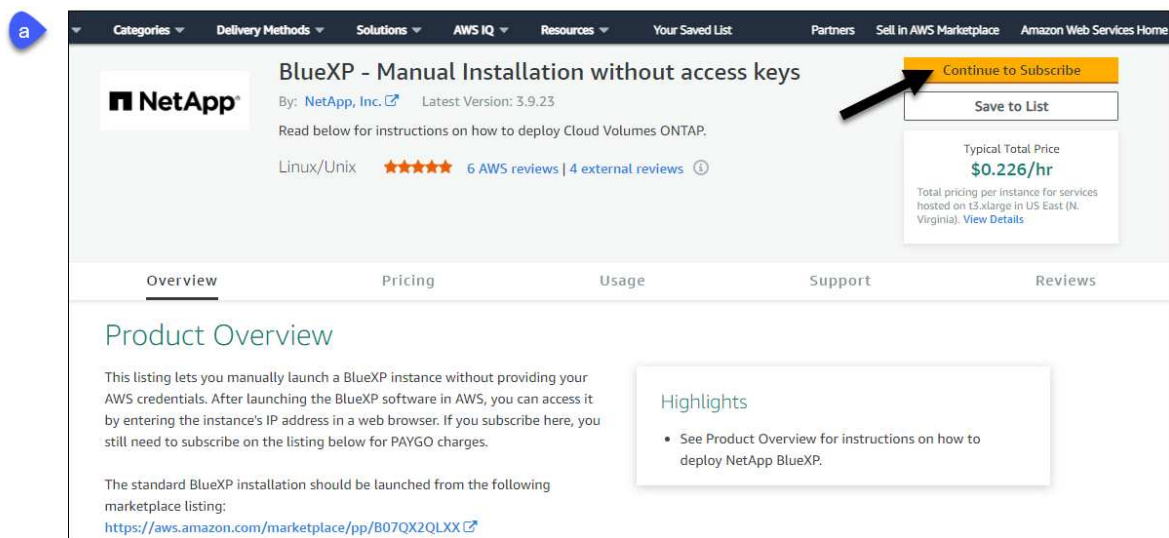
- An IAM role with an attached policy that includes the required permissions for the Connector.

[Learn how to set up AWS permissions](#)

- Permissions to subscribe and unsubscribe from the AWS Marketplace for your IAM user.
- A key pair for the EC2 instance.

Steps

1. Go to the [BlueXP page on the AWS Marketplace](#)
2. On the Marketplace page, click **Continue to Subscribe** and then click **Continue to Configuration**.



3. Change any of the default options and click **Continue to Launch**.
4. 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.

5. 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 includes the required permissions for the Connector.

[Learn how to set up AWS permissions.](#)

- **Summary:** Review the summary and click **Launch instance**.

Result

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

What's next?

Set up BlueXP.

AWS Gov Marketplace

What you'll need

- A VPC and subnet that meets networking requirements.

[Learn about networking requirements](#)

- An IAM role with an attached policy that includes the required permissions for the Connector.

[Learn how to set up AWS permissions](#)

- Permissions to subscribe and unsubscribe from the AWS Marketplace for your IAM user.
- A key pair for the EC2 instance.

Steps

1. Go to the BlueXP offering in the AWS Marketplace.
 - a. Open the EC2 service and select **Launch instance**.
 - b. Select **AWS Marketplace**.

c. Search for BlueXP and select the offering.

1. Choose AMI 2. Choose Instance Type 3. Configure Instance 4. Add Storage 5. Add Tags 6. Configure Security Group 7. Review

Cancel and Exit

Step 1: Choose an Amazon Machine Image (AMI)

An AMI is a template that contains the software configuration (operating system, application server, and applications) required to launch your instance. You can select an AMI provided by AWS, our user community, or the AWS Marketplace; or you can select one of your own AMIs.

Search by Systems Manager parameter

Quick Start

My AMIs

AWS Marketplace

Community AMIs

Categories

Search: bluexp

NetApp

BlueXP - Manual Installation without access keys

★★★★★ (6) | 3.9.23 | By NetApp, Inc.

Linux/Unix, Red Hat Enterprise Linux Red Hat Linux | 64-bit (x86) Amazon Machine Image (AMI) | Updated: 11/17/22

Read below for instructions on how to deploy Cloud Volumes ONTAP.

[More info](#)

Select

d. Click **Continue**.

2. 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 [Launch into Auto Scaling Group ⓘ](#)

Purchasing option ⓘ ☐ Request Spot instances

Network ⓘ vpc-a76d91c2 | VPC4QA (default) ⓘ [Create new VPC](#)

Subnet ⓘ subnet-39536c13 | QASubnet1 | us-east-1b ⓘ [Create new subnet](#)

155 IP Addresses available

Auto-assign Public IP ⓘ Enable ⓘ

Placement group ⓘ ☐ Add instance to placement group

Capacity Reservation ⓘ Open ⓘ [Create new Capacity Reservation](#)

IAM role ⓘ Cloud_Manager ⓘ [Create new IAM role](#)

CPU options ⓘ ☐ Specify CPU options

Shutdown behavior ⓘ Stop ⓘ

Enable termination protection ⓘ ☒ Protect against accidental termination

Monitoring ⓘ ☐ Enable CloudWatch detailed monitoring

[Additional charges apply.](#)

- **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**.

Result

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

What's next?

Set up BlueXP.

Azure Marketplace

What you'll need

- A VNet and subnet that meets networking requirements.

[Learn about networking requirements](#)

- An Azure custom role that includes the required permissions for the Connector.

[Learn how to set up Azure permissions](#)

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:

- **VM size:** Choose a VM size that meets CPU and RAM requirements. We recommend DS3 v2.
- **Disks:** The Connector can perform optimally with either HDD or SSD disks.
- **Public IP:** If you want to use a public IP address with the Connector VM, the IP address must use a Basic SKU to ensure that BlueXP uses this public IP address.

If you use a Standard SKU IP address instead, then BlueXP uses the *private* IP address of the

Connector, instead of the public IP. If the machine that you're using to access the BlueXP Console doesn't have access to that private IP address, then actions from the BlueXP Console will fail.

[Azure documentation: Public IP SKU](#)

- **Network security group:** The Connector requires inbound connections using SSH, HTTP, and HTTPS.

[Learn about networking requirements.](#)

- **Identity:** Under **Management**, select **Enable system assigned managed identity**.

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.

Result

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

What's next?

Set up BlueXP.

Manual install

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.

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 or if the proxy is an intercepting proxy.

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 "online" Connector installer that's meant for use in your network or in the cloud. A separate "offline" installer is available for the Connector, but it's only supported with private mode deployments.

4. Assign permissions to run the script.

```
chmod +x OnCommandCloudManager-<version>
```

Where <version> is the version of the Connector that you downloaded.

5. Run the installation script.

```
./OnCommandCloudManager-<version> --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-V3.9.26 --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. h

Result

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

What's next?

Set up BlueXP.

Set up BlueXP

When you access the BlueXP console for the first time, you'll be prompted to choose an account to associate the Connector with and you'll need to enable restricted mode.



If you already have an account and you want to create another one, then you need to use the Tenancy API. [Learn how to create an additional BlueXP account.](#)

Steps

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

`https://ipaddress`

2. Sign up or log in to BlueXP.
3. After you're logged in, set up BlueXP:
 - a. Enter a name for the Connector.
 - b. Enter a name for a new BlueXP account or select an existing account.

You can select an existing account if your log in is already associated with a BlueXP account.


- c. Select **Are you running in a secured environment?**
- d. Select **Enable restricted mode on this account.**

Note that you can't change this setting after BlueXP creates the account. You can't enable restricted mode later and you can't disable it later.

If you deployed the Connector in a Government region, the checkbox is already enabled and can't be changed. This is because restricted mode is the only mode supported in Government regions.

Hi Tami,

Welcome to NetApp 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 user](#)

Connector name

BlueXP1

Account name

MyCompany

Are you running in a secured environment?

Use restricted deployment mode to disconnect this account from the BlueXP backend services. Restricted deployments are often required in extremely secure or regulated environments. Note: Use this option only if you're sure you need it as some BlueXP functionality is not available in restricted deployments.

[Learn more about BlueXP deployment modes](#)

☒ Enable restricted mode on this account

Let's start

e. Click **Let's start**.

Result

The Connector is now installed and set up with your BlueXP account. All users need to access BlueXP using the IP address of the Connector instance.

What's next?

Provide BlueXP with the permissions that you previously set up.

Provide permissions to BlueXP

If you deployed the Connector from the Azure Marketplace or if you manually installed the Connector software, you need to provide the permissions that you previously set up so that you can use BlueXP services.

These steps don't apply if you deployed the Connector from the AWS Marketplace because you chose the required IAM role during deployment.

[Learn how to prepare cloud permissions.](#)

AWS IAM role

Attach the IAM role that you previously created to the EC2 instance where you installed the Connector.

These steps apply only if you manually installed the Connector in AWS. For AWS Marketplace deployments, you already associated the Connector instance with an IAM role that includes the required permissions.

Steps

1. Go to the Amazon EC2 console.
2. Select **Instances**.
3. Select the Connector instance.
4. Select **Actions > Security > Modify IAM role**.
5. Select the IAM role and click **Update IAM role**.

Result

BlueXP now has the permissions that it needs to perform actions in AWS on your behalf.

AWS access key

Provide BlueXP with the AWS access key for an IAM user that has the required permissions.

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:** 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.
 - d. **Review:** Confirm the details about the new credentials and click **Add**.

Result

BlueXP now has the permissions that it needs to perform actions in AWS on your behalf.

Azure role

Go to the Azure portal and assign the Azure custom role to the Connector virtual machine for one or more subscriptions.

Steps

1. From the Azure Portal, open the **Subscriptions** service and select your subscription.
2. Click **Access control (IAM) > Add > Add role assignment**.
3. 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.

4. In the **Members** tab, complete the following steps:
 - a. Assign access to a **Managed identity**.
 - b. Click **Select members**, select the subscription in which the Connector virtual machine was created, choose **Virtual machine**, and then select the Connector virtual machine.
 - c. Click **Select**.
 - d. 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

BlueXP now has the permissions that it needs to perform actions in Azure on your behalf.

Azure service principal

Provide BlueXP with the credentials for the Azure service principal that you previously setup.

Steps

1. Go to the [BlueXP console](#) and log in.
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 **Microsoft Azure > Connector**.
 - b. **Define Credentials**: Enter information about the Azure Active Directory service principal that grants the required permissions:
 - Application (client) ID
 - Directory (tenant) ID
 - Client Secret
 - c. **Marketplace Subscription**: Associate a Marketplace subscription with these credentials by subscribing now or by selecting an existing subscription.
 - d. **Review**: Confirm the details about the new credentials and click **Add**.

Result

BlueXP now has the permissions that it needs to perform actions in Azure on your behalf.

Google Cloud service account

Associate the service account with the Connector VM.

Steps

1. Go to the Google Cloud portal and assign the service account to the Connector VM instance.

[Google Cloud documentation: Changing the service account and access scopes for an instance](#)

2. 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

BlueXP now has the permissions that it needs to perform actions in Google Cloud on your behalf.

Log in to BlueXP (restricted mode)

When you use BlueXP in restricted mode, you need to log in to the BlueXP console from the user interface that runs locally on the Connector.

Log in options

BlueXP supports logging in with one of the following options when your account is set up in restricted mode:

- 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).

[Learn how to use identity federation with BlueXP.](#)

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 where you installed the Connector. For example, you might need to 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.

Result

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

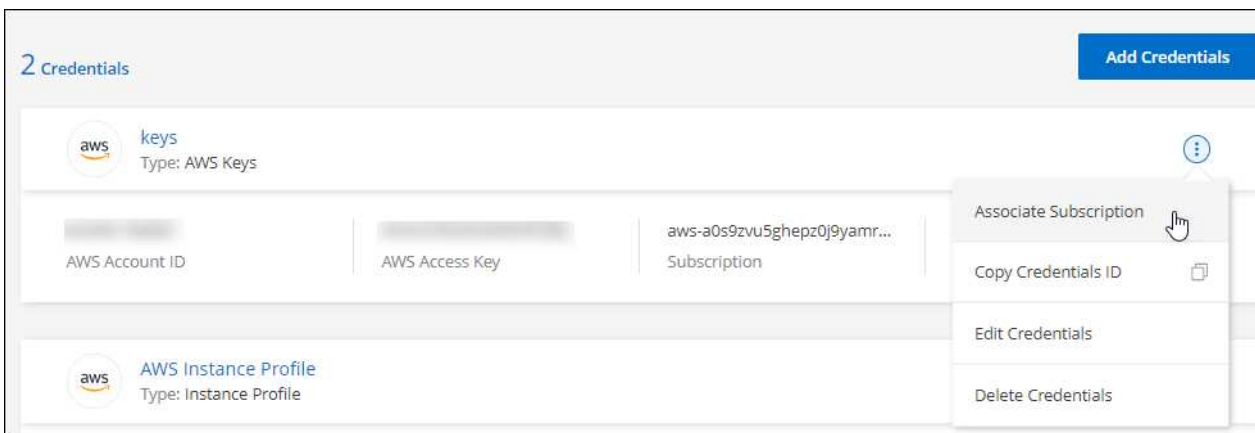
Subscribe to BlueXP (restricted mode)

Subscribe to BlueXP from your cloud provider's marketplace to pay for BlueXP services at an hourly rate or through an annual contract. If you purchased a license from NetApp, you also need to subscribe to the PAYGO offering. Your license is always charged first, but you'll be charged at the hourly rate if you exceed your licensed capacity or if the license's term expires.

AWS

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 BlueXP 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 AWS Marketplace:

► <https://docs.netapp.com/us-en/cloud-manager-setup->

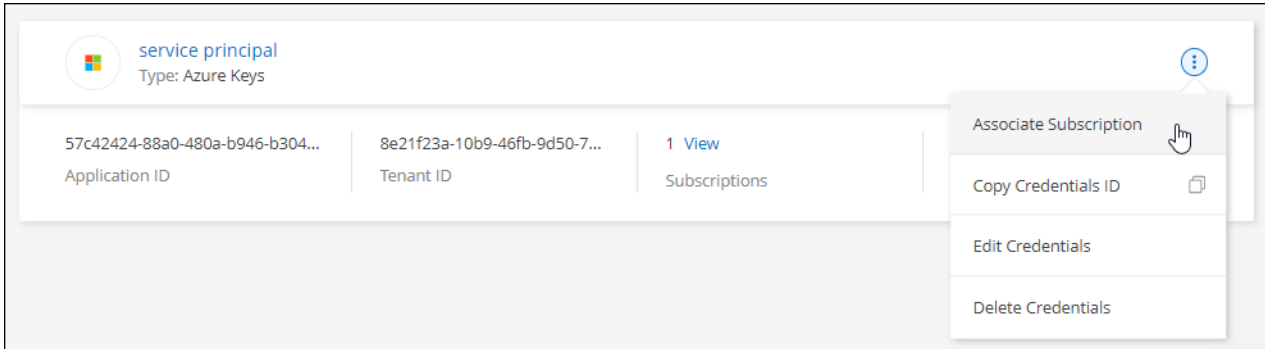
Azure



In Azure, annual contracts are not supported with government regions.

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 BlueXP 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->

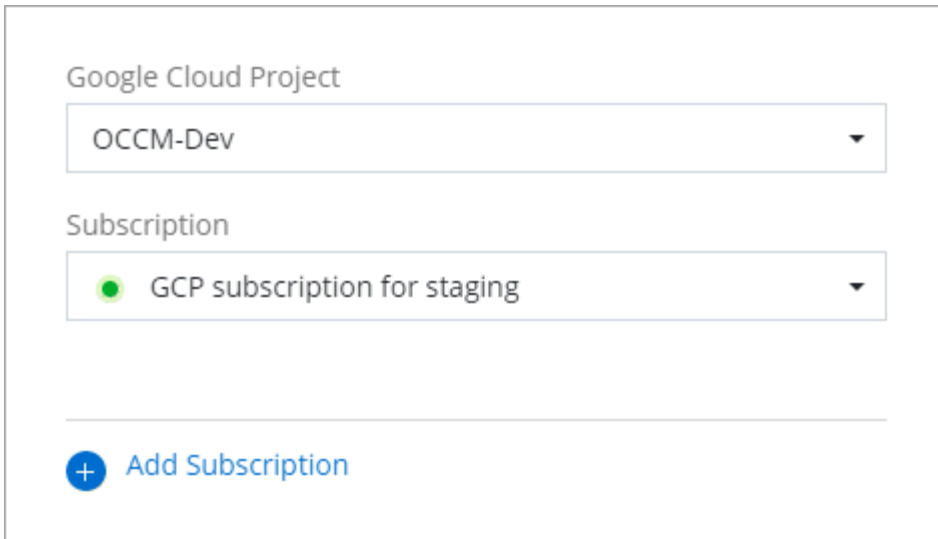
Google Cloud

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**.



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 Google Cloud console interface for the NetApp BlueXP product. At the top, the Google Cloud logo and the URL 'netapp.com' are visible. Below the navigation bar, the page title is 'Product details'. The main content area features the NetApp logo and the product name 'NetApp BlueXP'. A description states: 'BlueXP lets you build, protect, and govern your hybrid multicloud data estate.' A prominent blue 'SUBSCRIBE' button is centered. Below this, a navigation menu includes 'OVERVIEW' (which is selected), 'PRICING', 'DOCUMENTATION', and 'SUPPORT'. The 'Overview' section contains two paragraphs: '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.' and '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.' To the right of the overview, an 'Additional details' section lists: 'Type: [SaaS & APIs](#)', 'Last updated: 12/19/22', and '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 BlueXP account. The process of linking a subscription isn't complete until you are redirected from this page and then sign in to BlueXP.

Your order request has been sent to NetApp, Inc.



Your new subscription to the Cloud Manager 1 month plan for Cloud Manager for Cloud Volumes ONTAP requires your registration with NetApp, Inc.. After NetApp, Inc. approves your request, your subscription will be active and you will begin getting charged. This processing time will depend on the vendor, and you should reach out to NetApp, Inc. directly with any questions related to signup.

[VIEW ORDERS](#)

[REGISTER WITH NETAPP, INC.](#)

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 BlueXP 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.



The screenshot shows a form with two dropdown menus. The first dropdown is labeled 'Google Cloud Project' and has 'OCCM-Dev' selected. The second dropdown is labeled 'Subscription' and has 'GCP subscription for staging' selected, which is preceded by a green circular icon. Below these dropdowns is a horizontal line, and then a blue button with a plus sign and the text 'Add Subscription'.

What you can do next (restricted mode)

After you get up and running with BlueXP in restricted mode, you can start using the BlueXP services that are supported with restricted mode.

For help, refer to the documentation for these services:

- [Amazon FSx for ONTAP docs](#)
- [Azure NetApp Files docs](#)
- [Backup and recovery docs](#)
- [Classification docs](#)
- [Cloud Volumes ONTAP docs](#)
- [On-premises ONTAP cluster docs](#)
- [Replication docs](#)

Related link

[BlueXP deployment modes](#)

Get started with private mode

Quick start for BlueXP in private mode

Get started with BlueXP in private mode by preparing your environment and deploying the Connector.

1

Prepare for deployment

- a. Prepare a dedicated Linux host that meets requirements for CPU, RAM, disk space, Docker Engine, and more.
- b. Set up networking that provides access to the target networks.
- c. For cloud deployments, set up permissions in your cloud provider so that you can associate those permissions with the Connector after you install the software.

[Learn how to prepare for deployment.](#)

2

Deploy the Connector

- a. Install the Connector software on your own Linux host.
- b. Set up BlueXP by opening a web browser and entering the Linux host's IP address.
- c. For cloud deployments, provide BlueXP with the permissions that you previously set up.

[Learn how to deploy the Connector.](#)

Prepare for deployment in private mode

Prepare your environment before you deploy BlueXP in private mode. For example, you need to review host requirements, prepare networking, set up permissions, and more.



If you want to use BlueXP in the [AWS Commercial Cloud Services \(C2S\) environment](#) then you should follow separate instructions that describe how to prepare, install the Connector, and launch Cloud Volumes ONTAP. [Learn how to get started with Cloud Volumes ONTAP in the AWS C2S environment](#)

Understand how private mode works

Before you get started, you should have an understanding of how BlueXP works in private mode.

For example, you should understand that you need to use the browser-based interface that is available locally from the BlueXP Connector that you need to install. You can't access BlueXP from the web-based console that's provided through the SaaS layer.

In addition, not all BlueXP services are available.

[Learn how private mode works.](#)

Review installation options

In private mode, you can install the Connector on premises or in the cloud by manually installing the Connector on your own Linux host.

If you want to create a Cloud Volumes ONTAP system in Google Cloud, then the Connector must be running in Google Cloud—it can't be running on premises.

Review host requirements

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

Dedicated host

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

Supported operating systems

- CentOS 7.6, 7.7, 7.8, and 7.9
- Red Hat Enterprise Linux 7.6, 7.7, 7.8, 7.9, 8.6, and 8.7

The host must be registered with Red Hat Subscription Management. If it's not registered, the host can't 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 is required. [Red Hat Solution: Which hypervisors are certified to run Red Hat Enterprise Linux?](#)

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.

Google Cloud 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](#)

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](#)

Prepare networking for the Connector

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.

Connections to target networks

The Connector must have a network connection to the location where you plan to manage storage. For example, the VPC or VNet where you plan to deploy Cloud Volumes ONTAP, or the data center where your on-premises ONTAP clusters reside.

Endpoints for day-to-day operations

The Connector contacts the following endpoints to deploy and manage Cloud Volumes ONTAP in your public cloud environment.

| Endpoints | Purpose |
|--|--|
| AWS services (amazonaws.com): <ul style="list-style-type: none">• CloudFormation• Elastic Compute Cloud (EC2)• Identity and Access Management (IAM)• Key Management Service (KMS)• Security Token Service (STS)• Simple Storage Service (S3) | To manage resources in AWS. The exact endpoint depends on the region in which you deploy the Connector. Refer to AWS documentation for details |
| https://management.azure.com https://login.microsoftonline.com https://blob.core.windows.net https://core.windows.net | To manage resources in Azure public regions. |
| https://management.azure.microsoft.scloud https://login.microsoftonline.microsoft.scloud https://blob.core.microsoft.scloud https://core.microsoft.scloud | To manage resources in the Azure IL6 region. |
| https://management.chinacloudapi.cn https://login.chinacloudapi.cn https://blob.core.chinacloudapi.cn https://core.chinacloudapi.cn | To manage resources in Azure China regions. |

| Endpoints | Purpose |
|---|--------------------------------------|
| https://www.googleapis.com/compute/v1/ https://compute.googleapis.com/compute/v1 https://cloudresourcemanager.googleapis.com/v1/projects https://www.googleapis.com/compute/beta https://storage.googleapis.com/storage/v1 https://www.googleapis.com/storage/v1 https://iam.googleapis.com/v1 https://cloudkms.googleapis.com/v1 https://www.googleapis.com/deploymentmanager/v2/projects | To manage resources in Google Cloud. |

Proxy server

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

- IP address
- Credentials
- HTTPS certificate

With private mode, the only time that BlueXP sends outbound traffic is to your cloud provider in order to create a Cloud Volumes ONTAP system.

Public IP address in Azure

If you want to use a public IP address with the Connector VM in Azure, the IP address must use a Basic SKU to ensure that BlueXP uses this public IP address.

Create public IP address ✕

Name * ✓

SKU * ⓘ
☒ Basic ☐ Standard

Assignment
☐ Dynamic ☒ Static

If you use a Standard SKU IP address instead, then BlueXP uses the *private* IP address of the Connector, instead of the public IP. If the machine that you're using to access the BlueXP Console doesn't have access to that private IP address, then actions from the BlueXP Console will fail.

[Azure documentation: Public IP SKU](#)

Ports

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

HTTP (80) and HTTPS (443) provide access to the BlueXP console. SSH (22) is only needed if you need to connect to the host for troubleshooting.

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. 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.

Prepare cloud permissions

If you are planning to create Cloud Volumes ONTAP systems, then BlueXP requires permissions from your cloud provider. You need to set up permissions in your cloud provider and then associate those permission with the Connector instance after you install it.

To view the required steps, select the authentication option that you'd like to use for your cloud provider.

If you're going to install the Connector on premises, then you must provide permissions using AWS access keys or an Azure service principal. The other options are not supported.

AWS IAM role

Use an IAM role to provide the Connector with permissions. You'll need to manually attach the role to the EC2 instance for the Connector.

Steps

1. Log in to the AWS console and navigate to the IAM service.
2. Create a policy:
 - a. Click **Policies > Create policy**.
 - b. Select **JSON** and copy and paste the contents of the [IAM policy for the Connector](#).
 - c. Finish the remaining steps to create the policy.
3. Create an IAM role:
 - a. Click **Roles > Create role**.
 - b. Select **AWS service > EC2**.
 - c. Add permissions by attaching the policy that you just created.
 - d. Finish the remaining steps to create the role.

Result

You now have an IAM role for the Connector EC2 instance.

AWS access key

Set up permissions and an access key for an IAM user. You'll need to provide BlueXP with the AWS access key after you install the Connector and set up BlueXP.

Steps

1. From the IAM console, create a policy:
 - a. Click **Policies > Create policy**.
 - b. Select **JSON** and copy and paste the contents of the [IAM policy for the Connector](#).
 - c. Finish the remaining steps to create the policy.

Depending on the BlueXP services that you're planning to use, you might need to create a second policy.

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. [Learn more about IAM policies for the Connector](#).

2. Attach the policies to an IAM user.
 - [AWS Documentation: Creating IAM Roles](#)
 - [AWS Documentation: Adding and Removing IAM Policies](#)
3. Ensure that the user has access keys that you can add to BlueXP after you install the Connector.

Result

The account now has the required permissions.

Azure role

Create an Azure custom role with the required permissions. You'll assign this role to the Connector VM.

Steps

1. Enable a system-assigned managed identity on the VM where you plan to install the Connector so that you can provide the required Azure permissions through a custom role.

[Microsoft Azure documentation: Configure managed identities for Azure resources on a VM using the Azure portal](#)

2. Copy the contents of the [custom role permissions for the Connector](#) and save them in a JSON file.
3. 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.

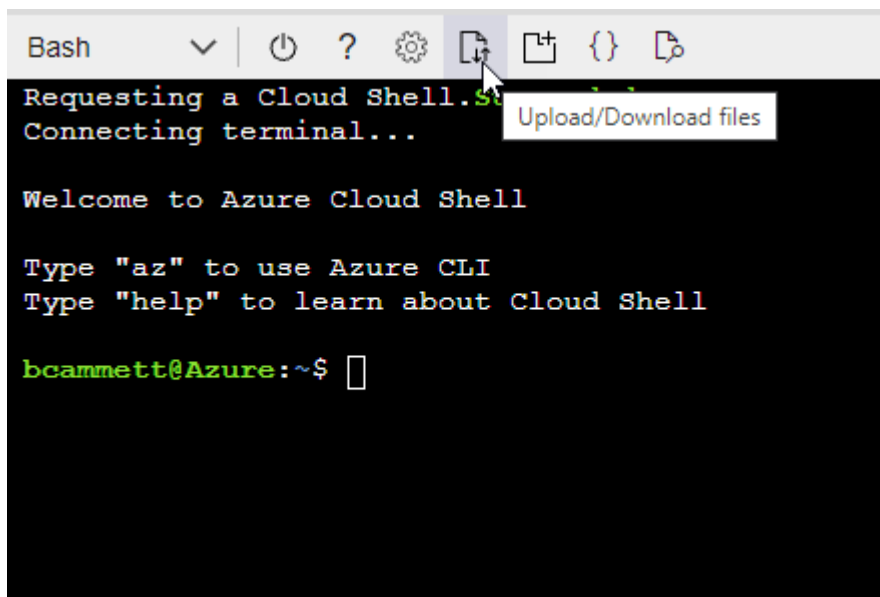
Example

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

4. 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. Use the Azure CLI to create the custom role:

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

Result

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

Azure service principal

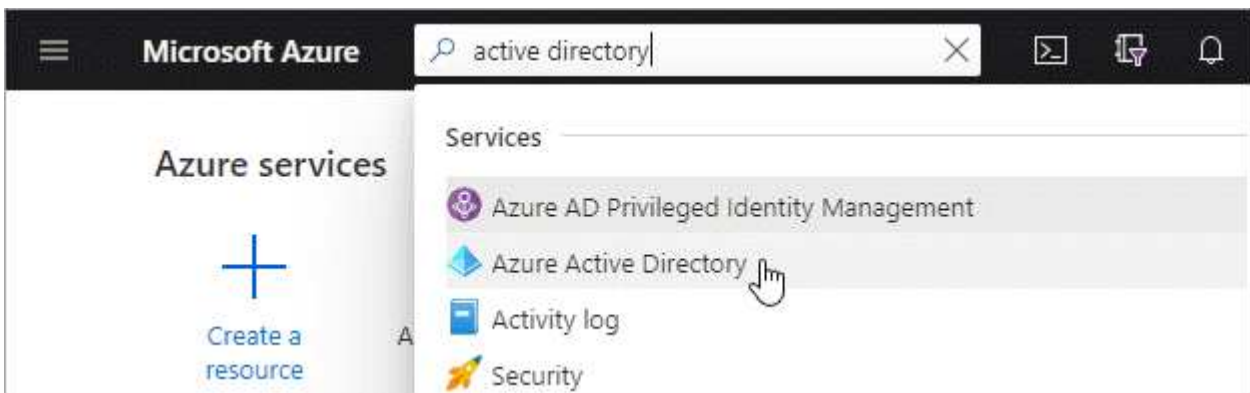
Create and set up a service principal in Azure Active Directory and obtain the Azure credentials that BlueXP needs. You'll need to provide BlueXP with these credentials after you install the Connector and set up BlueXP.

Create an Azure Active Directory application for role-based access control

1. Ensure that you have 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](#).

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



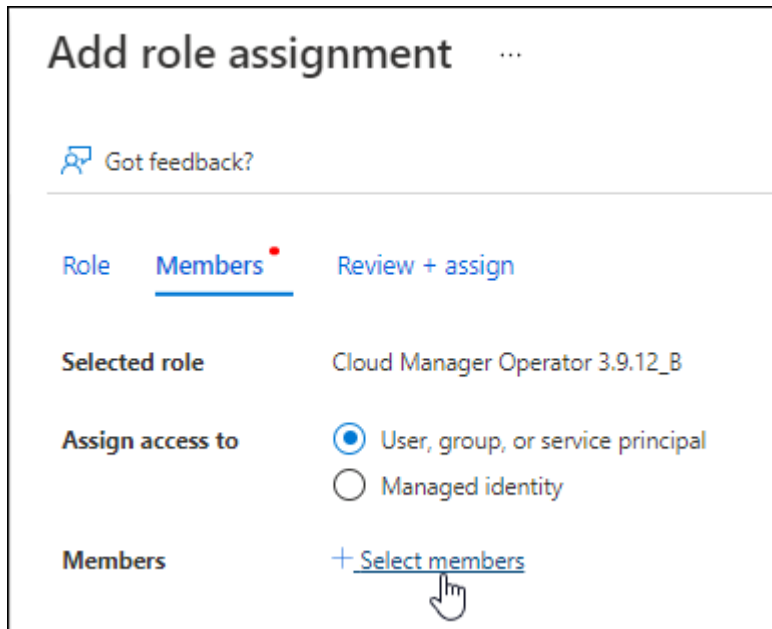
3. In the menu, click **App registrations**.
4. Click **New registration**.
5. Specify details about the application:
 - **Name**: Enter a name for the application.
 - **Account type**: Select an account type (any will work with BlueXP).
 - **Redirect URI**: You can leave this field blank.
6. Click **Register**.

You've created the AD application and service principal.

Assign the custom role to the application

1. From the Azure portal, open the **Subscriptions** service.
2. Select the subscription.
3. Click **Access control (IAM) > Add > Add role assignment**.
4. In the **Role** tab, select the **BlueXP Operator** role and click **Next**.

5. In the **Members** tab, complete the following steps:
 - a. Keep **User, group, or service principal** selected.
 - b. Click **Select members**.



- c. Search for the name of the application.

Here's an example:



- d. Select the application and click **Select**.
 - e. Click **Next**.
6. 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.

Add Windows Azure Service Management API permissions

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



user_impersonation

Access Azure Service Management as organization users (preview) ⓘ

Get the application ID and directory ID for the application

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**.

Delete Endpoints

Welcome to the new and improved App registrations. Looking to learn

Display name : test-service-principal

Application (client) ID : 73de25f9-99be-4ae0-8b24-538ca787a6b3

Directory (tenant) ID : 4b0911a0-929b-4715-944b-c03745165b3a

Object ID : b37489a9-379f-49c2-b27c-e630514106a5

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.

Create a client secret

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*-ZRoV4NLfdAcY7:+0vA |

Copy to clipboard

You now have a client secret that BlueXP can use it to authenticate with Azure AD.

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.

Google Cloud service account

Create a role and apply it to a service account that you'll use for the Connector VM instance.

Steps

1. Create a custom role in Google Cloud:
 - a. Create a YAML file that includes the permissions defined in the [Connector policy for Google Cloud](#).
 - b. From Google Cloud, activate cloud shell.
 - c. Upload the YAML file that includes the required permissions for the Connector.
 - d. Create a custom role by using the `gcloud iam roles create` command.

The following example creates a role named "connector" at the project level:

```
gcloud iam roles create connector --project=myproject
--file=connector.yaml
```

[Google Cloud docs: Creating and managing custom roles](#)

2. Create a service account in Google Cloud:
 - a. From the IAM & Admin service, click **Service Accounts > Create Service Account**.
 - b. Enter service account details and click **Create and Continue**.
 - c. Select the role that you just created.
 - d. Finish the remaining steps to create the role.

[Google Cloud docs: Creating a service account](#)

Result

You now have a service account that you can assign to the Connector VM instance.

Enable Google Cloud APIs

Several APIs are required to deploy Cloud Volumes ONTAP in Google Cloud.

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

Deploy the Connector in private mode

Deploy the Connector in private mode so that you can use BlueXP with no outbound connectivity to the BlueXP SaaS layer. To get started, install the Connector, set up BlueXP by accessing the user interface that's running on the Connector, and then provide the cloud permissions that you previously set up.

Install the Connector

Download the product installer from the [NetApp Support Site](#) and then manually install the Connector on your own Linux host.

If you want to use BlueXP in the [AWS Commercial Cloud Services \(C2S\) environment](#) then you should follow separate instructions to get started in that environment. [Learn how to get started with Cloud Volumes ONTAP in the AWS C2S environment](#)

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](#)

Be sure to download the installer for restricted networks without internet access.

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

```
chmod +x /path/cloud-manager-connector-offline-<version>
```

Where <version> is the version of the Connector that you downloaded.

5. Run the installation script:

```
sudo /path/cloud-manager-connector-offline-<version>
```

Where <version> is the version of the Connector that you downloaded.

Result

The Connector software is installed. You can now set up BlueXP.

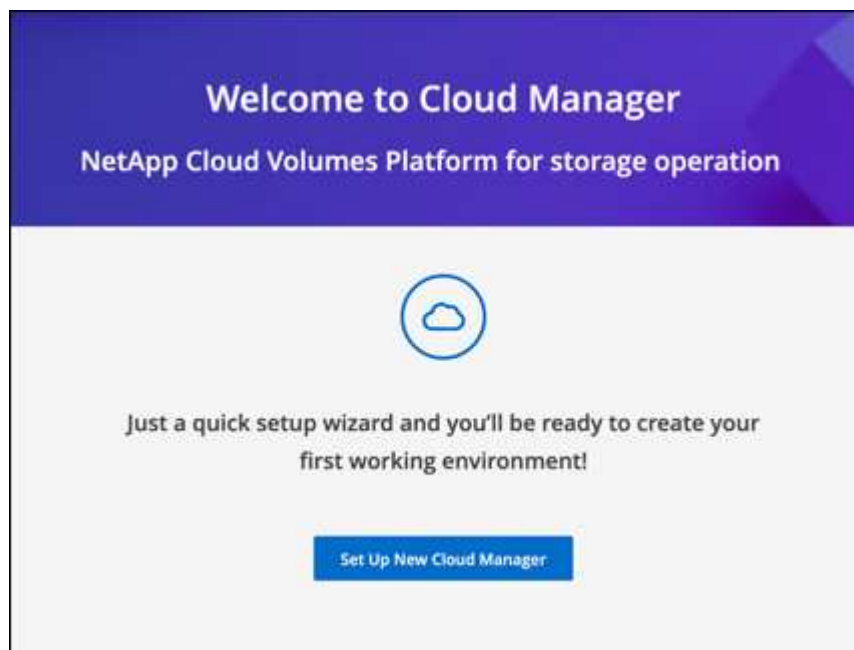
Set up BlueXP

When you access the BlueXP console for the first time, you'll be prompted to set up BlueXP.

Steps

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

You should see the following screen.



2. 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.

1 System Details 2 Create Admin User 3 Review

System Details

To help us provide better support, enter a name for Cloud Manager and your company name.

Cloud Manager Name

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**.

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

Result

The Connector is now installed and set up.

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

What's next?

Provide BlueXP with the permissions that you previously set up.

Provide permissions to BlueXP

If you want to create Cloud Volumes ONTAP working environments, you'll need to provide BlueXP with the cloud permissions that you previously set up.

[Learn how to prepare cloud permissions.](#)

AWS IAM role

Attach the IAM role that you previously created to the Connector EC2 instance.

Steps

1. Go to the Amazon EC2 console.
2. Select **Instances**.
3. Select the Connector instance.
4. Select **Actions > Security > Modify IAM role**.
5. Select the IAM role and click **Update IAM role**.

Result

BlueXP now has the permissions that it needs to perform actions in AWS on your behalf.

AWS access key

Provide BlueXP with the AWS access key for an IAM user that has the required permissions.

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 > Connector**.
 - b. **Define Credentials**: 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.
 - d. **Review**: Confirm the details about the new credentials and click **Add**.

Result

BlueXP now has the permissions that it needs to perform actions in AWS on your behalf.

Azure role

Go to the Azure portal and assign the Azure custom role to the Connector virtual machine for one or more subscriptions.

Steps

1. From the Azure Portal, open the **Subscriptions** service and select your subscription.
2. Click **Access control (IAM) > Add > Add role assignment**.
3. 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.

4. In the **Members** tab, complete the following steps:

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

BlueXP now has the permissions that it needs to perform actions in Azure on your behalf.

Azure service principal

Provide BlueXP with the credentials for the Azure service principal that you previously setup.

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
 - Directory (tenant) ID
 - Client Secret
 - c. **Marketplace Subscription**: Associate a Marketplace subscription with these credentials by subscribing now or by selecting an existing subscription.
 - d. **Review**: Confirm the details about the new credentials and click **Add**.

Result

BlueXP now has the permissions that it needs to perform actions in Azure on your behalf.

Google Cloud service account

Associate the service account with the Connector VM.

Steps

1. Go to the Google Cloud portal and assign the service account to the Connector VM instance.

[Google Cloud documentation: Changing the service account and access scopes for an instance](#)

2. 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

BlueXP now has the permissions that it needs to perform actions in Google Cloud on your behalf.

Log in to BlueXP (private mode)

When you use BlueXP in private mode, you need to log in to the BlueXP console from the user interface that runs locally on the Connector.

Log in options

Private mode supports local user management and access. Authentication is not provided through BlueXP's cloud service.

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 where you installed the Connector. For example, you might need to 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.

Result

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

What you can do next (private mode)

After you get up and running with BlueXP in private mode, you can start using the BlueXP services that are supported with private mode.

For help, refer to the following documentation:

- [Create Cloud Volumes ONTAP systems](#)
- [Discover on-premises ONTAP clusters](#)
- [Replicate data](#)
- [Scan on-prem ONTAP volume data using BlueXP classification](#)
- [Back up on-prem ONTAP volume data to StorageGRID using BlueXP backup and recovery](#)

Related link

[BlueXP deployment modes](#)

Administer BlueXP

Using identity federation with BlueXP

Identity federation enables single sign-on with BlueXP so that users can log in using credentials from your corporate identity. To get started, learn how identity federation works with BlueXP and then review an overview of the setup process.

Identity federation with NSS credentials

If you use your NetApp Support Site (NSS) credentials to log in to BlueXP, you should not follow the instructions on this page to set up identity federation. You should do the following instead:

- Download and complete the [NetApp Federation Request Form](#)
- Submit the form to the email address specified in the form

The NetApp Identity and Access Management team will review your request.

How identity federation works

Setting up identity federation creates a trust connection between BlueXP's authentication service provider (auth0) and your own identity management provider.

The following image depicts how identity federation works with BlueXP:



1. A user enters their email address on the BlueXP login page.
2. BlueXP identifies that the email domain is part of a federated connection and sends the authentication request to the identity provider using the trusted connection.

When you set up a federated connection, BlueXP always uses that federated connection for authentication.

3. The user authenticates by using credentials from your corporate directory.
4. Your identity provider authenticates the user's identity and the user is logged in to BlueXP.

Identity federation uses open standards, such as Security Assertion Markup Language 2.0 (SAML) and OpenID Connect (OIDC).

Supported identity providers

BlueXP supports the following identity providers:

- Security Assertion Markup Language (SAML) identity providers
- Microsoft Azure Active Directory (AD)
- Active Directory Federation Services (ADFS)
- PingFederate

BlueXP supports service provider initiated (SP-initiated) SSO only. Identity provider initiated (IdP-initiated) SSO is not supported.

Overview of the setup process

Before you set up a connection between BlueXP and your identity management provider, you should understand the steps that you'll need to take so that you can prepare accordingly.

These steps are specific to users who log in to BlueXP using a NetApp cloud login. If you use your NSS credentials to log in to BlueXP, [learn how to set up identity federation with NSS credentials](#).

SAML identity provider


At a high-level, setting up a federated connection between BlueXP and a SAML identity provider includes the following steps:

| Step | Completed by | Description |
|------|-----------------------------|---|
| 1 | Active Directory (AD) admin | <p>Configure your SAML identity provider to enable identity federation with BlueXP.</p> <p>View instructions for your SAML identity provider:</p> <ul style="list-style-type: none">• ADFS• Okta• OneLogin• PingFederate• SalesForce• SiteMinder• SSOCircle <p>If your identity provider doesn't appear in the list above, follow these generic instructions</p> <div> Do <i>not</i> complete the steps that describe how to create a connection in auth0. You'll create that connection in the next step.</div> |

| Step | Completed by | Description |
|------|--------------|--|
| 2 | BlueXP admin | <p>Go to the NetApp Federation Setup page and create the connection with BlueXP.</p> <p>To complete this step, you need to obtain the following from your AD admin about the identity provider:</p> <ul style="list-style-type: none"> • Sign in URL • An X509 signing certificate (PEM or CER format) • Sign out URL (optional) <p>After you create the connection using this information, the Federation Setup page lists the parameters that you can send to your AD admin to complete the configuration in the next step.</p> |
| 3 | AD admin | Complete the configuration on the identity provider using the parameters shown on the Federation Setup page after finishing step 2. |
| 4 | BlueXP admin | <p>Test and enable the connection from the NetApp Federation Setup page</p> <p>Note that the page refreshes between testing the connection and enabling the connection.</p> |

Microsoft Azure AD

At a high-level, setting up a federated connection between BlueXP and Azure AD includes the following steps:

| Step | Completed by | Description |
|------|--------------|--|
| 1 | AD admin | <p>Configure Azure Active Directory to enable identity federation with BlueXP.</p> <p>View instructions for registering the application with Azure AD</p> <div>  <p>Do <i>not</i> complete the steps that describe how to create a connection in auth0. You'll create that connection in the next step.</p> </div> |
| 2 | BlueXP admin | <p>Go to the NetApp Federation Setup page and create the connection with BlueXP.</p> <p>To complete this step, you need to obtain the following from your AD admin:</p> <ul style="list-style-type: none"> • Client ID • Client secret value • Microsoft Azure AD domain <p>After you create the connection using this information, the Federation Setup page lists the parameters that you can send to your AD admin to complete the configuration in the next step.</p> |
| 3 | AD admin | Complete the configuration in Azure AD using the parameters shown on the Federation Setup page after finishing step 2. |

| Step | Completed by | Description |
|------|--------------|---|
| 4 | BlueXP admin | <p>Test and enable the connection from the NetApp Federation Setup page</p> <p>Note that the page refreshes between testing the connection and enabling the connection.</p> |

ADFS

At a high-level, setting up a federated connection between BlueXP and ADFS includes the following steps:

| Step | Completed by | Description |
|------|--------------|---|
| 1 | AD admin | <p>Configure the ADFS server to enable identity federation with BlueXP.</p> <p>View instructions for configuring the ADFS server with auth0</p> |
| 2 | BlueXP admin | <p>Go to the NetApp Federation Setup page and create the connection with BlueXP.</p> <p>To complete this step, you need to obtain the following from your AD admin: the URL for the ADFS server or the federation metadata file.</p> <p>After you create the connection using this information, the Federation Setup page lists the parameters that you can send to your AD admin to complete the configuration in the next step.</p> |
| 3 | AD admin | <p>Complete the configuration on the ADFS server using the parameters shown on the Federation Setup page after finishing step 2.</p> |
| 4 | BlueXP admin | <p>Test and enable the connection from the NetApp Federation Setup page</p> <p>Note that the page refreshes between testing the connection and enabling the connection.</p> |

PingFederate

At a high-level, setting up a federated connection between BlueXP and a PingFederate server includes the following steps:

| Step | Completed by | Description |
|------|--------------|---|
| 1 | AD admin | <p>Configure your PingFederate server to enable identity federation with BlueXP.</p> <p>View instructions for creating a connection</p> <div>  <p>Do <i>not</i> complete the steps that describe how to create a connection in auth0. You'll create that connection in the next step.</p> </div> |

| Step | Completed by | Description |
|------|--------------|---|
| 2 | BlueXP admin | <p>Go to the NetApp Federation Setup page and create the connection with BlueXP.</p> <p>To complete this step, you need to obtain the following from your AD admin:</p> <ul style="list-style-type: none"> • The URL for the PingFederate server • An X509 signing certificate (PEM or CER format) <p>After you create the connection using this information, the Federation Setup page lists the parameters that you can send to your AD admin to complete the configuration in the next step.</p> |
| 3 | AD admin | Complete the configuration on the PingFederate server using the parameters shown on the Federation Setup page after finishing step 2. |
| 4 | BlueXP admin | <p>Test and enable the connection from the NetApp Federation Setup page</p> <p>Note that the page refreshes between testing the connection and enabling the connection.</p> |

Updating a federated connection

After the BlueXP admin enables a connection, the admin can update the connection at any time from the [NetApp Federation Setup page](#)

For example, you might need to update the connection by uploading a new certificate.

The BlueXP admin who created the connection is the only authorized user who can update the connection. If you'd like to add additional admins, contact NetApp Support.

BlueXP accounts

Manage your BlueXP account

When you create a BlueXP account, it only includes a single admin user and a workspace. You can manage the account to fit your organization's needs by adding users, creating service accounts for automation purposes, by adding workspaces, and more.

[Learn how BlueXP accounts work.](#)

Manage 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](#)

Create and manage users

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

Add users

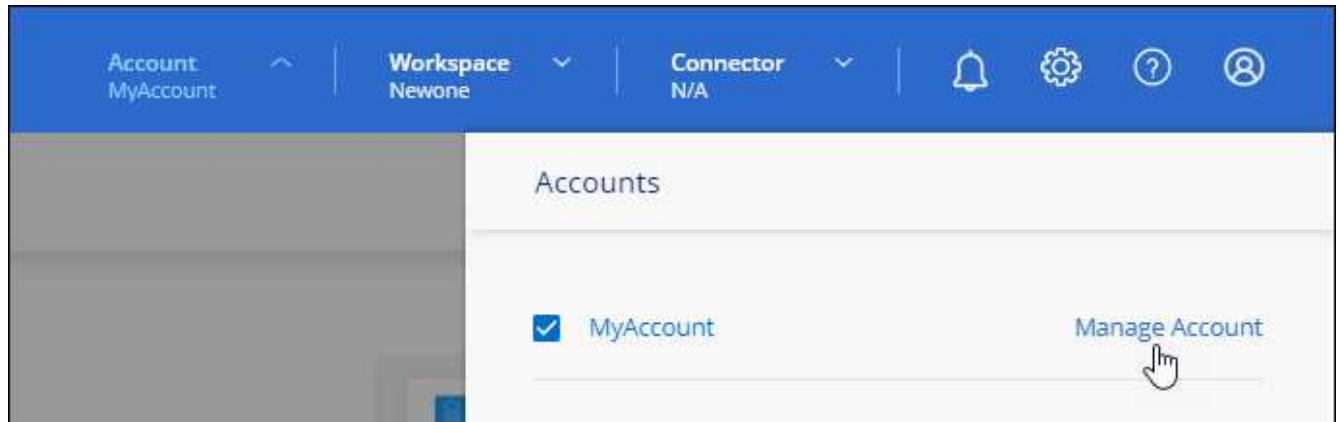
Associate users with your BlueXP account so those users can create and manage working environments in BlueXP.

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, select the **Account** drop-down.



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



4. From the Members tab, select **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 compliance information for BlueXP classification and generate reports for workspaces that they have permission to access.
6. If you selected Workspace Admin or Compliance Viewer, 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 instructions: "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." The form contains three fields: "User's Email" with the text "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 icon. At the bottom are two buttons: "Cancel" and "Associate 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

test@netapp.com

Role

Workspace Admin

Associate User to Workspaces

Workspace-1

Cancel Associate User

7. Select **Associate**.

Result

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

Remove users

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

Steps

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



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



3. Select **Disassociate User** and select **Disassociate** to confirm.

Result

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

Manage 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, select the **Account** drop-down and select **Manage Account**.



2. From the Members tab, select 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. Select **Manage Workspaces**.

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

Result

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

Create and manage 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.

Create 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, select the **Account** drop-down.



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



3. From the Members tab, select **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. Select **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. Select **Close**.

Obtain 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.

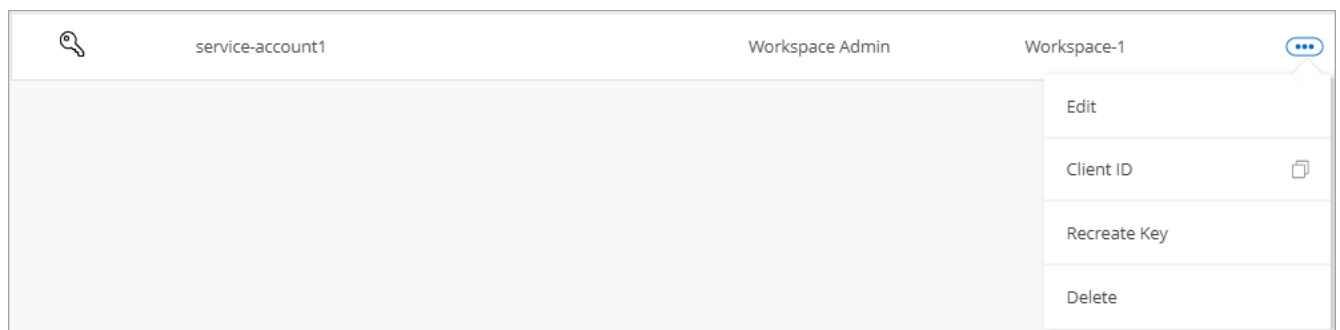
[Learn how to create a service account token](#)

Copy the client ID

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

Steps

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



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

Recreate 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, select the action menu in the row that corresponds to the service account.



2. Select **Recreate Key**.
3. Select **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. Select **Close**.

Delete a service account

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

Steps

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



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

Manage 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, select the **Account** drop-down and select **Manage Account**.
2. Select **Workspaces**.
3. Choose one of the following options:
 - Select **Add New Workspace** to create a new workspace.
 - Select **Rename** to rename the workspace.
 - Select **Delete** to delete the workspace.

Manage 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, select the **Account** drop-down and select **Manage Account**.
2. Select **Connector**.
3. Select **Manage Workspaces** for the Connector that you want to associate.
4. Select the workspaces to associate with the Connector and select **Apply**.

Change 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, select the **Account** drop-down and select **Manage Account**.
2. In the **Overview** tab, select the edit icon next to the account name.
3. Type a new account name and select **Save**.

Allow private previews

Allow private previews in your account to get access to new 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, select the **Account** drop-down and select **Manage Account**.
2. In the **Overview** tab, enable the **Allow Private Preview** setting.

Allow 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, select the **Account** drop-down and select **Manage Account**.
- 2. In the **Overview** tab, enable the **Allow Third Party Services** setting.

Monitor 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.

The following 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 |
| 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 |

Monitor 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 BlueXP 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. |

Filter 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".

| Filter Services (All) ▲ | Filter Type (All) ▲ |
|--|--|
| <input checked="" type="checkbox"/> Digital Wallet (3) | <input type="checkbox"/> Information (0) |
| <input checked="" type="checkbox"/> Active IQ (2) | <input type="checkbox"/> Success (1) |
| <input type="checkbox"/> AppTemplate (1) | <input checked="" type="checkbox"/> Warning (2) |
| <input type="button" value="Clear"/> | <input checked="" type="checkbox"/> Error (1) |
| <input type="button" value="Apply"/> | <input checked="" type="checkbox"/> Critical (0) |
| | <input type="checkbox"/> Recommendation (0) |
| | <input type="button" value="Clear"/> |
| | <input type="button" value="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.

Set 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 BlueXP 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, BlueXP copy and sync, BlueXP backup and recovery, BlueXP digital wallet, and BlueXP 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, select **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, select the menu in the Notifications column for that user, check the types of Notifications to be sent, and select **Apply**.
 - To make changes for multiple users, check the box for each user, select **Manage Email Notifications**, check the types of Notifications to be sent, and select **Apply**.



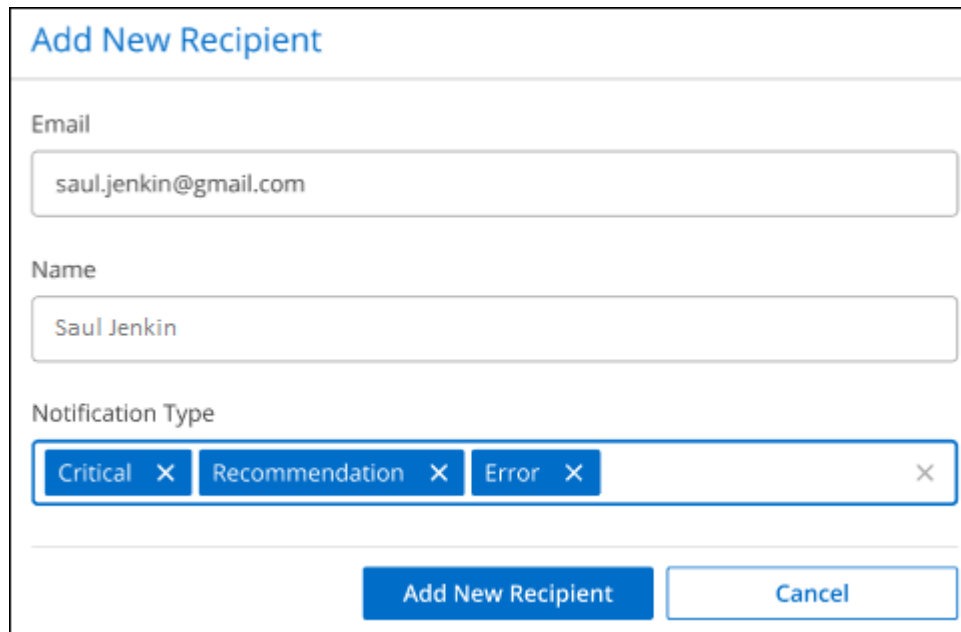
Add additional email recipients

The users who appear in the *Account Users* tab are populated automatically from the users in your BlueXP 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, select **Add New Recipients**.

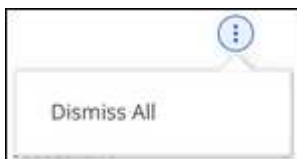
A form titled "Add New Recipient" with three input fields: "Email" containing "saul.jenkin@gmail.com", "Name" containing "Saul Jenkin", and "Notification Type" which is a multi-select dropdown showing "Critical", "Recommendation", and "Error". At the bottom are two buttons: "Add New Recipient" and "Cancel".

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

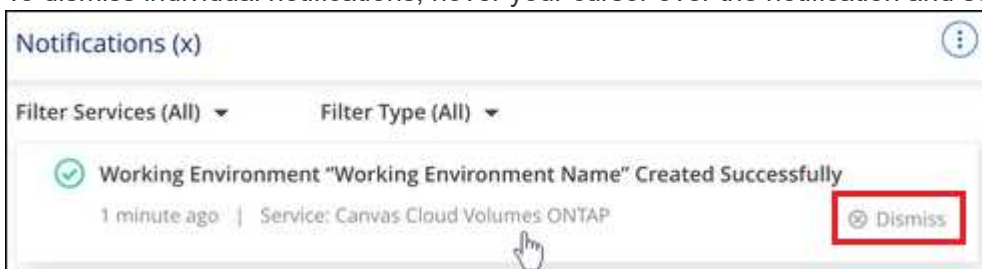
Dismiss notifications

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, select  and select **Dismiss All**.



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



Audit 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, select **Settings > Timeline**.
- 2. Under the Filters, select **Service**, enable **Tenancy**, and select **Apply**.

Result

The Timeline updates to show you account management actions.

Create another BlueXP account

When you sign up to BlueXP, you’re prompted to create an account for your organization. This account might be all that you need, but if your business requires multiple accounts, then you’ll need to create additional accounts by using the Tenancy API.

Use the following API call to create an additional BlueXP account:

POST /tenancy/account/{accountName}

If you want to enable restricted mode, you need to include the following in the request body:

```
{
  "isSaasDisabled": true
}
```



You can’t change the restricted mode setting after BlueXP creates the account. You can’t enable restricted mode later and you can’t disable it later. It must be set at time of account creation.

[Learn how to use this API call](#)

Related links

- [Learn about BlueXP accounts](#)
- [Learn about BlueXP deployment modes](#)

Roles

The Account Admin, Workspace Admin, Compliance Viewer, and SnapCenter Admin roles provide specific permissions to users. You can assign one of these roles when you associate a new user with your BlueXP account.

The Compliance Viewer role is for read-only BlueXP classification access.

| Task | Account Admin | Workspace Admin | Compliance Viewer | SnapCenter Admin |
|-----------------------------|---------------|-----------------|-------------------|------------------|
| Manage working environments | Yes | Yes | No | No |

| Task | Account Admin | Workspace Admin | Compliance Viewer | SnapCenter Admin |
|---|---------------|-----------------|-------------------|------------------|
| 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 |
| View BlueXP classification 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 BlueXP 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 |

Related links

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

Connectors

Find the system ID for a Connector

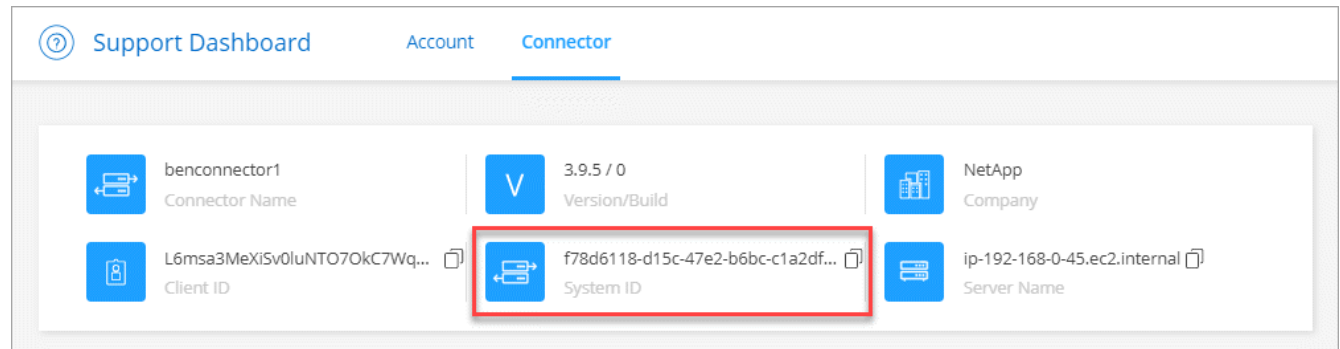
To help you get started, your NetApp representative might ask you for the system ID of your Connector. The ID is typically used for licensing and troubleshooting purposes.

Steps

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

The system ID appears at the top.

Example



Manage existing Connectors

After you create a Connector, you might need to manage it every now and then. For example, you might want to switch between Connectors if you have more than one. Or you might need to manually upgrade the Connector when using BlueXP in private mode.

[Learn how Connectors work.](#)

Operating system and VM maintenance

Maintaining the operating system on the Connector host is your responsibility. For example, you should apply security updates to the operating system on the Connector host by following your company's standard procedures for operating system distribution.

Note that you don't need to stop any services on the Connector host when running an OS update.

If you need to stop and then start the Connector VM, you should do so from your cloud provider's console or by using the standard procedures for on-premises management.

[Be aware that the Connector must be operational at all times.](#)

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. Select the **Connector** drop-down, select another Connector, and then select **Switch**.



Result

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

Download or send an AutoSupport message

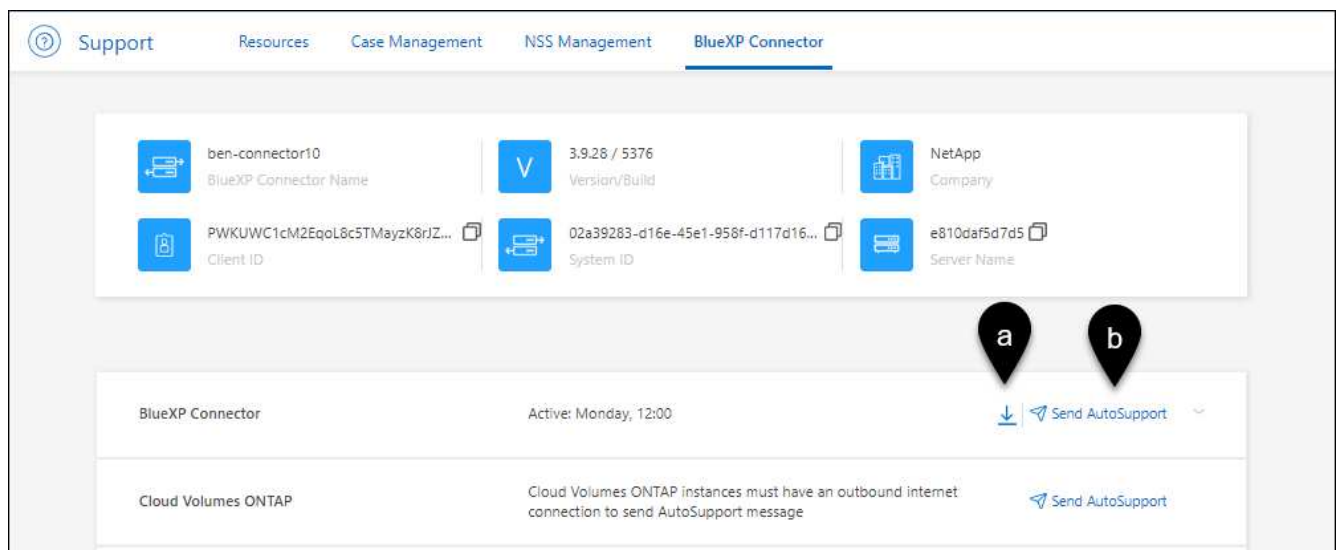
If you're having problems, NetApp personnel might ask you to send an AutoSupport message to NetApp support for troubleshooting purposes.

Steps

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



2. Select **BlueXP Connector**.
3. 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. Select **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](#)

Upgrade the Connector when using private mode

If you are using BlueXP in private mode, 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 web-based console will be unavailable during the upgrade.



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.

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-<version>
```

Where <version> is the version of the Connector that you downloaded.

4. Run the installation script:

```
sudo /path/cloud-manager-connector-offline-<version>
```

Where <version> is the version of the Connector that you downloaded.

5. After the upgrade is complete, you can verify the Connector's version by going to **Help > Support > Connector**.

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. Select the menu and select **Advanced > Configuration Backups**.
- d. Select **Set Backup Target**.

Edit a Connector's URIs

Add and remove the Uniform Resource Identifier (URI) for a Connector.

Steps

1. Select the **Connector** drop-down from the BlueXP header.
2. Select **Manage Connectors**.
3. Select the action menu for a Connector and select **Edit URIs**.
4. Add and remove URIs and then select **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](#)

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. Select the **Connector** drop-down from the BlueXP header.
2. Select **Manage Connectors**.
3. Select the action menu for an inactive Connector and select **Remove Connector**.



4. Enter the name of the Connector to confirm and then select **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
```

Install an HTTPS certificate for secure access

By default, BlueXP uses a self-signed certificate for HTTPS access to the web console. If required by your business, 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](#).

Install an HTTPS certificate

Install a certificate signed by a CA for secure access.

Steps

1. In the upper right of the BlueXP console, select the Settings icon, and select **HTTPS Setup**.

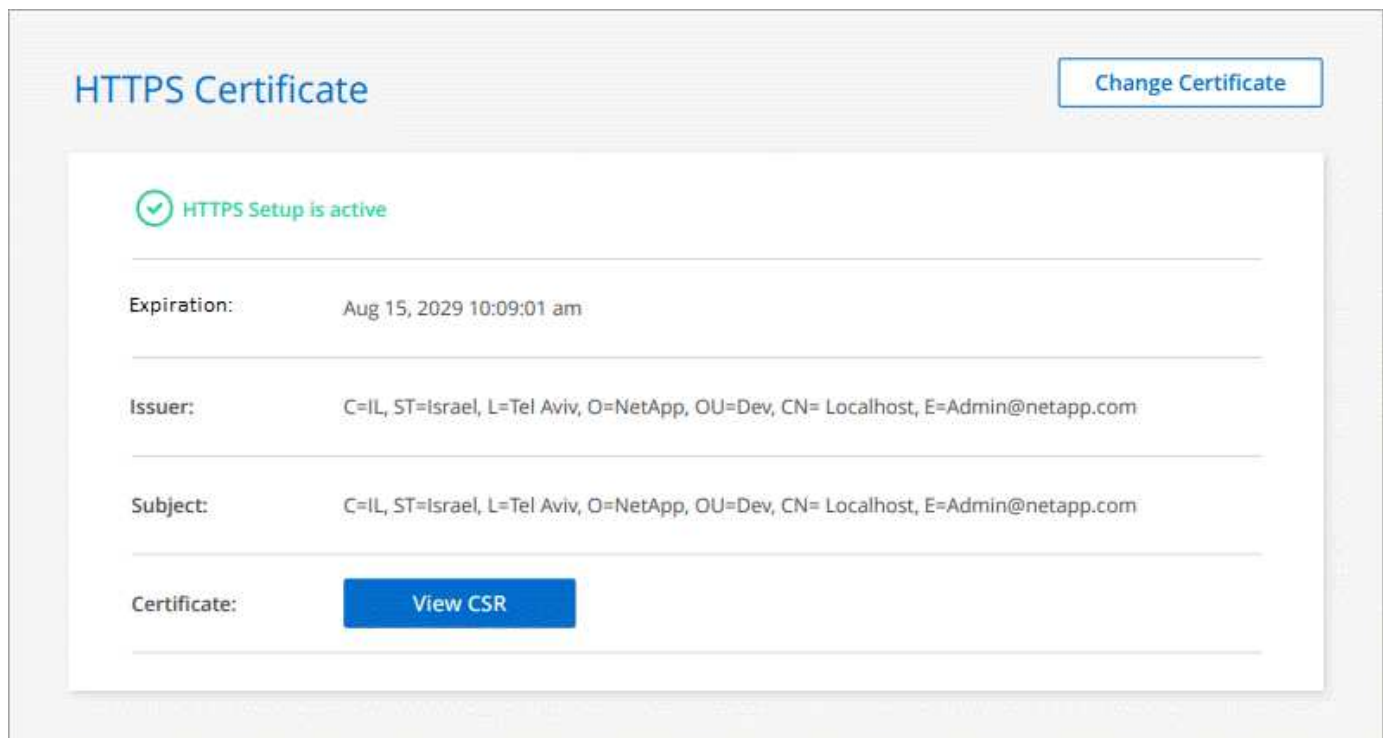


2. In the HTTPS Setup page, install a certificate by generating a certificate signing request (CSR) or by installing your own CA-signed certificate:

| Option | Description |
|--|--|
| Generate a CSR | <p>a. Enter the host name or DNS of the Connector host (its Common Name), and then select Generate CSR.</p> <p>BlueXP displays a certificate signing request.</p> <p>b. Use the CSR to submit an SSL certificate request to a CA.</p> <p>The certificate must use the Privacy Enhanced Mail (PEM) Base-64 encoded X.509 format.</p> <p>c. Upload the certificate file and then select Install.</p> |
| Install your own CA-signed certificate | <p>a. Select Install CA-signed certificate.</p> <p>b. Load both the certificate file and the private key and then select Install.</p> <p>The certificate must use the Privacy Enhanced Mail (PEM) Base-64 encoded X.509 format.</p> |

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:



Renew 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, select the Settings icon, and select **HTTPS Setup**.

Details about the BlueXP certificate displays, including the expiration date.

2. Select **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. In the upper right of the BlueXP console, select the Settings icon, and select **Connector Settings**.



2. Under **General**, select **HTTP Proxy Configuration**.
3. Set up the proxy:
 - a. Select **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. Select **Save**.



BlueXP doesn't support passwords that include the @ character.

Enable direct API traffic

If you configured a Connector to use a proxy server, you can enable direct API traffic on the Connector in order to send API calls directly to cloud provider services without going through the proxy. This option is supported with Connectors that are running in AWS, in Azure, or in Google Cloud.

If you disabled the use of Azure Private Links with Cloud Volumes ONTAP and are using service endpoints instead, then you must enable direct API traffic. Otherwise, the traffic won't be routed properly.

[Learn more about using an Azure Private Link or service endpoints with Cloud Volumes ONTAP](#)

Steps

1. In the upper right of the BlueXP console, select the Settings icon, and select **Connector Settings**.



2. Under **General**, select **Support Direct API Traffic**.
3. Select the checkbox to enable the option and then select **Save**.

Default configuration for the Connector

You might want to learn more about the Connector's configuration 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

Credentials

Manage AWS credentials

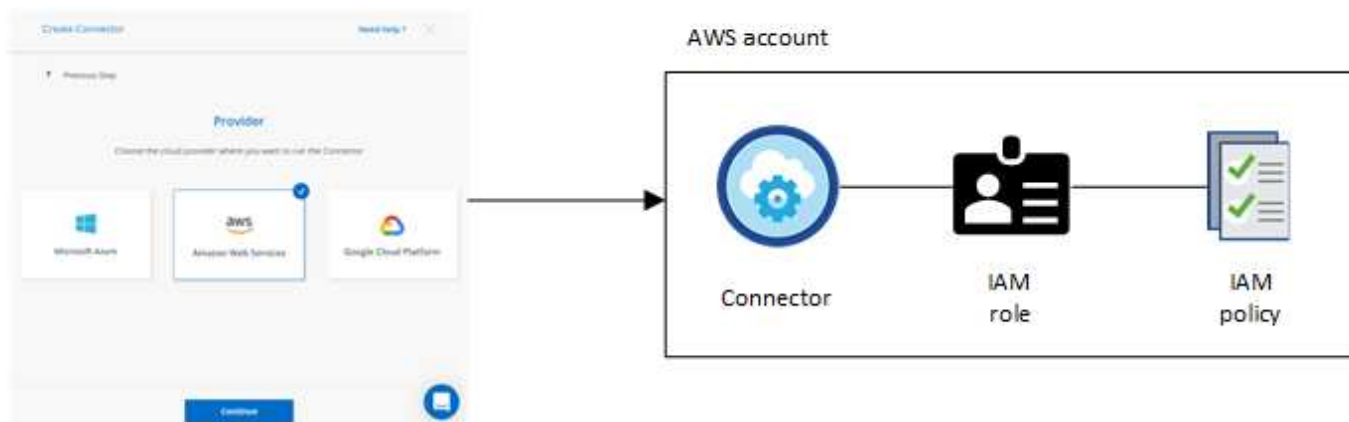
AWS credentials and permissions

Learn how BlueXP uses AWS credentials and permissions to perform actions on your behalf. Understanding these details can be helpful as you manage the credentials for one or more AWS accounts in BlueXP. For example, you might want to learn about when to add additional AWS credentials to BlueXP.

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 | Edit Credentials |
| Credentials | Account ID | Marketplace Subscription | |

You can deploy all of your Cloud Volumes ONTAP systems using the initial AWS credentials, or you can add additional credentials.

Additional AWS credentials

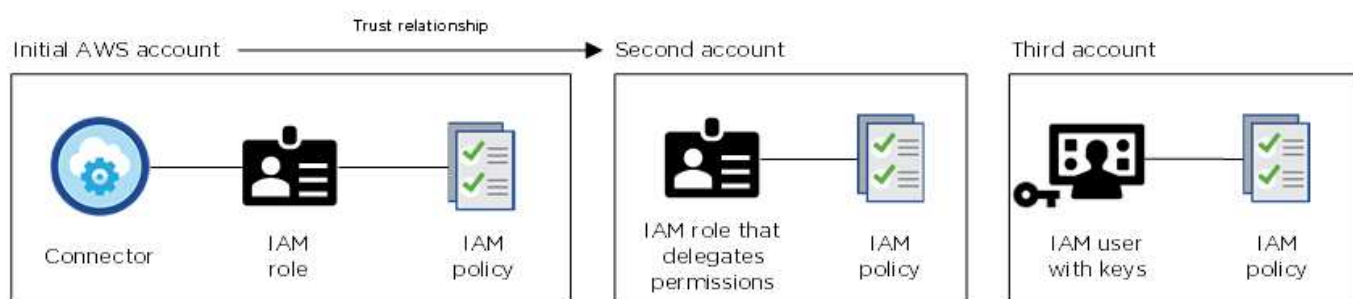
There are two ways to add additional AWS credentials:

- You can add AWS credentials to an existing Connector
- You can add AWS credentials directly to BlueXP

Review the sections below for more details.

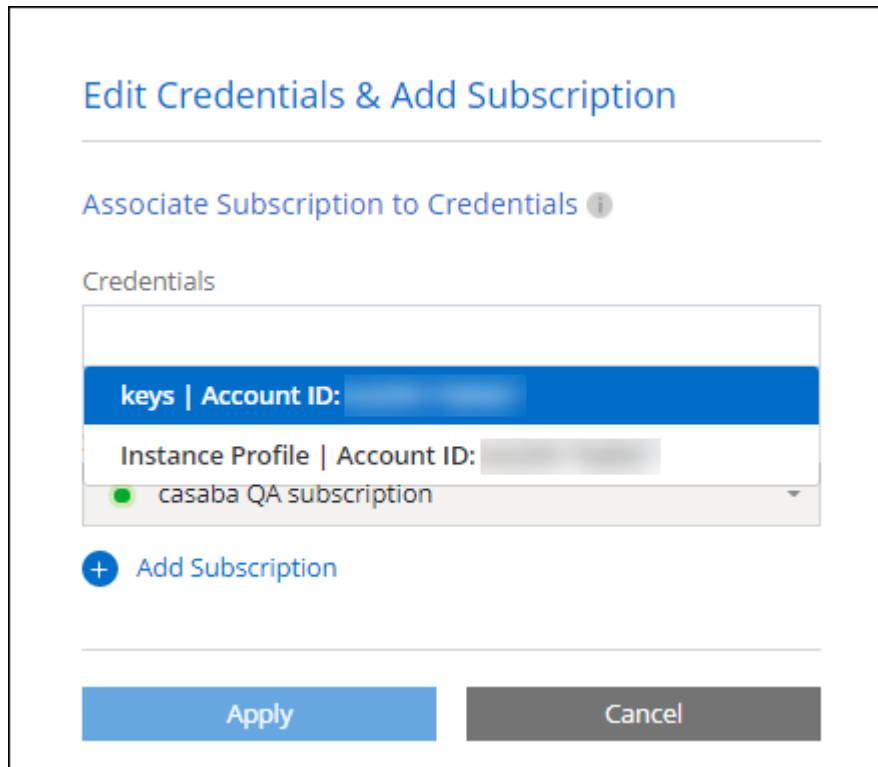
Add AWS credentials to an existing Connector

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:



[Learn how to add AWS credentials to an existing Connector.](#)

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.

- [Learn how to add AWS credentials to BlueXP for Amazon FSx for ONTAP](#)
- [Learn how to add AWS credentials to BlueXP for creating 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 manually install the Connector software on your own Linux host.

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 using AWS access keys.

To learn how to set up permissions, refer to the following pages:

- Standard mode

- [Set up AWS permissions](#)
- [Set up cloud permissions for on-prem deployments](#)
- [Set up cloud permissions for restricted mode](#)
- [Set up cloud permissions for private mode](#)

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 Marketplace 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 additional credentials to a Connector

Add additional 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.

If you're just getting started with BlueXP, [Learn how BlueXP uses AWS credentials and permissions](#).

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, select **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, select the Settings icon, and select **Credentials**.



3. On the **Account credentials** page, select **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 select **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: [redacted]
- Instance Profile | Account ID: [redacted]
- 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 layer to assume the role.

Steps

1. Go to the IAM console in the target account.
2. Under Access Management, select **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, select the Settings icon, and select **Credentials**.



2. On the **Account credentials** page, select **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 select **Add**.

Result

You can now use the credentials when creating a new Connector.

Add credentials to BlueXP for Amazon FSx for ONTAP

For details, refer to the [BlueXP documentation for Amazon FSx for ONTAP](#)

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 BlueXP 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, select the Settings icon, and select **Credentials**.
2. On the **Account credentials** page, select 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 select **Associate**.
4. To associate the credentials with a new subscription, select **Add Subscription > Continue** and follow the steps in the AWS Marketplace:
 - a. Select **View purchase options**.
 - b. Select **Subscribe**.
 - c. Select **Set up your account**.

You'll be redirected to the BlueXP website.

- d. From the **Subscription Assignment** page:
 - Select the BlueXP 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.

- Select **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

(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, select the Settings icon, and select **Credentials**.
2. On the **Account credentials** page, select the action menu for a set of credentials and then select **Edit Credentials**.
3. Make the required changes and then select **Apply**.

Delete 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, select the Settings icon, and select **Credentials**.
2. On the **Account credentials** page, select the action menu for a set of credentials and then select **Delete Credentials**.
3. Select **Delete** to confirm.

Manage Azure credentials

Azure credentials and permissions

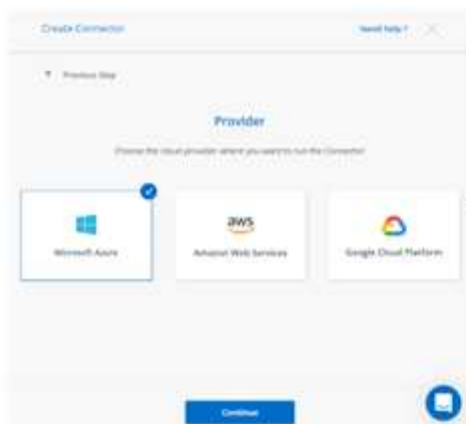
Learn how BlueXP uses Azure credentials and permissions to perform actions on your behalf. Understanding these details can be helpful as you manage the credentials for one or more Azure subscriptions. For example, you might want to learn when to add additional Azure credentials to BlueXP.

Initial Azure credentials

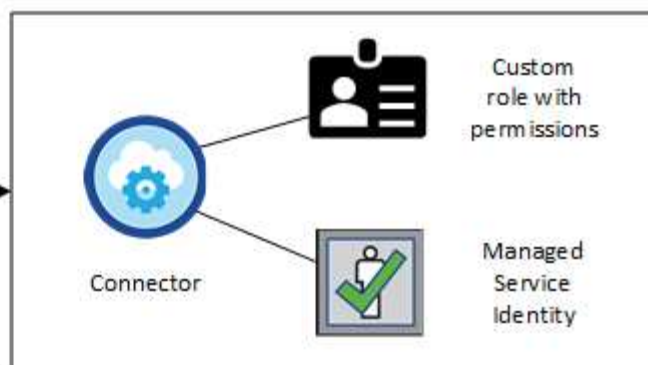
When you deploy a Connector from BlueXP, you need to use an Azure account or service principal that has permissions to deploy the Connector virtual machine. The required permissions are listed in the [Connector deployment policy for Azure](#).

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



Azure account



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 | ⓘ No subscription is associated | Edit Credentials |
| Credential Name | Azure Subscription | Marketplace Subscription | |

You can deploy all of your Cloud Volumes ONTAP systems using the initial Azure credentials, or you can add additional credentials.

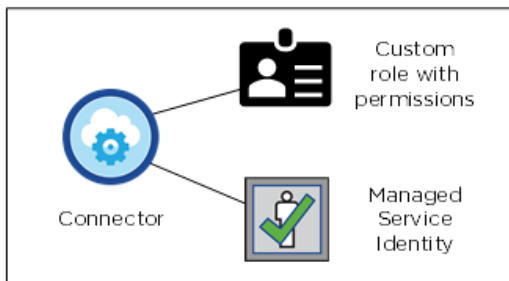
Additional Azure subscriptions for a managed identity

The system-assigned managed identity assigned to the Connector VM 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](#).

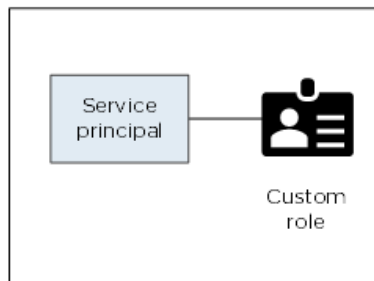
Additional Azure credentials

If you want to use different Azure credentials with BlueXP, 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:

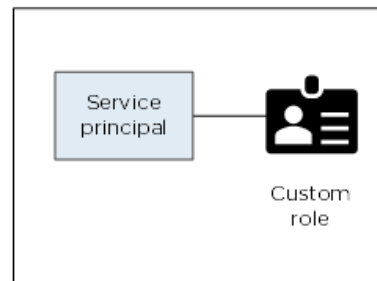
Initial Azure account



Second account



Third account



You would then [add the account credentials to BlueXP](#) by providing details about the AD service principal.

For example, you can switch between credentials when creating a new Cloud Volumes ONTAP working environment:



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 software on your own Linux host.

If you use the Marketplace, you can provide permissions by assigning a custom role to the Connector VM and to a system-assigned managed identity, or you can use Azure AD service principal.

For on-premises deployments, you can't set up a managed identity for the Connector, but you can provide permissions by using a service principal.

To learn how to set up permissions, refer to the following pages:

- Standard mode
 - [Set up Azure permissions](#)
 - [Set up cloud permissions for on-prem deployments](#)
- [Set up cloud permissions for restricted mode](#)
- [Set up cloud permissions for private mode](#)

Manage Azure credentials and subscriptions for BlueXP

Add and manage Azure credentials so that BlueXP has the permissions that it needs to deploy and manage cloud resources in your Azure subscriptions. If you manage multiple Azure Marketplace subscriptions, you can assign each one of them to different Azure credentials from the Credentials page.

Follow the steps on this page if you need to use multiple Azure credentials or multiple Azure Marketplace subscriptions for Cloud Volumes ONTAP.

Overview

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.

Associate 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. Select **Access control (IAM)**.
 - a. Select **Add > Add role assignment** and then add the permissions:

- Select the **BlueXP Operator** role.



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.

- Assign access to a **Virtual Machine**.
- Select the subscription in which the Connector virtual machine was created.
- Select the Connector virtual machine.
- Select **Save**.

4. Repeat these steps for additional subscriptions.

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.

Edit Account & Add Subscription

Credentials

Managed Service Identity

Azure Subscription

OCCM Dev

OCCM QA1 (Default)

No subscription is associated with this account

Add 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.

Grant 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.](#)

Create an Azure Active Directory application

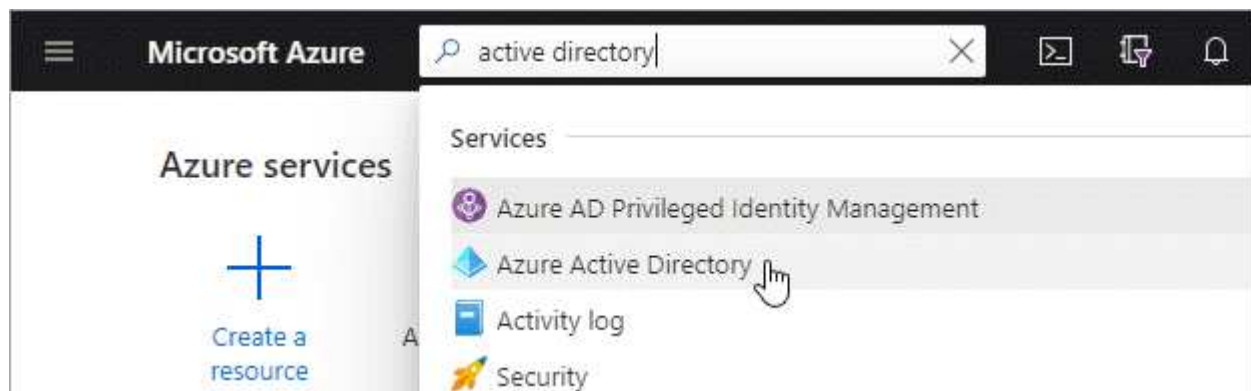
Create an Azure Active Directory (AD) application and service principal that BlueXP can use for role-based access control.

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, select **App registrations**.
3. Select **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. Select **Register**.

Result

You've created the AD application and service principal.

Assign 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:

- From the Azure portal, open the **Subscriptions** service.
- Select the subscription.
- Select **Access control (IAM) > Add > Add role assignment**.
- In the **Role** tab, select the **BlueXP Operator** role and select **Next**.
- In the **Members** tab, complete the following steps:
 - Keep **User, group, or service principal** selected.
 - Select **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 select **Select**.
 - Select **Next**.
- f. Select **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.

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, select **App registrations** and select the application.
2. Select **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. Select **Access Azure Service Management as organization users** and then select **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"/> user_impersonation Access Azure Service Management as organization users (preview) | - |

Get 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, select **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. Select **App registrations** and select your application.
3. Select **Certificates & secrets > New client secret**.

4. Provide a description of the secret and a duration.
5. Select **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*-ZRoV4NLfdAcY7:+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.

Add 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, select the Settings icon, and select **Credentials**.



2. On the **Account credentials** page, select **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 [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](#).
 - 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 select **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.

Associate 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 BlueXP 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, select the Settings icon, and select **Credentials**.
2. On the **Account credentials** page, select 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 select **Associate**.
4. To associate the credentials with a new subscription, select **Add Subscription > Continue** and follow the steps in the Azure Marketplace:
 - a. If prompted, log in to your Azure account.
 - b. Select **Subscribe**.
 - c. Fill out the form and select **Subscribe**.
 - d. After the subscription process is complete, select **Configure account now**.

You'll be redirected to the BlueXP website.

- e. From the **Subscription Assignment** page:
 - Select the BlueXP 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.

- Select **Save**.

The following video shows the steps to subscribe from the Azure Marketplace:

► <https://docs.netapp.com/us-en/cloud-manager-setup->

Edit 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, select the Settings icon, and select **Credentials**.
2. On the **Account credentials** page, select the action menu for a set of credentials and then select **Edit Credentials**.
3. Make the required changes and then select **Apply**.

Delete 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, select the Settings icon, and select **Credentials**.
2. On the **Account credentials** page, select the action menu for a set of credentials and then select **Delete Credentials**.
3. Select **Delete** to confirm.

Manage Google Cloud credentials

Google Cloud projects, permissions, and accounts

Learn how BlueXP uses Google Cloud credentials and permissions to perform actions on your behalf. Understanding these details can be helpful as you manage the credentials for one or more Google Cloud projects. For example, you might want to learn about the service account that's associated with the Connector VM.

Project and permissions for BlueXP

Before you can use BlueXP to manage resources in your Google Cloud project, you must first deploy a Connector. 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, and more. Permissions are provided by attaching a custom role to the service account.

The following image depicts the permission requirements described in numbers 1 and 2 above:



To learn how to set up permissions, refer to the following pages:

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

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 Google Cloud and select a project](#)

Manage Google Cloud credentials and subscriptions for BlueXP

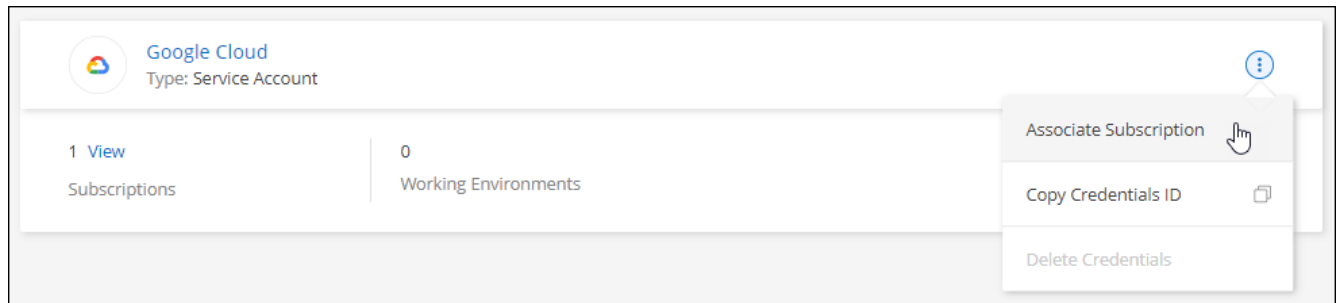
You can manage the Google Cloud credentials that are associated with the Connector VM instance by associating a marketplace subscription and by troubleshooting the subscription process. Both of these tasks ensure that you can use your marketplace subscription to pay for BlueXP services.

Associate 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. 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 BlueXP services.

Steps

1. In the upper right of the BlueXP console, select the Settings icon, and select **Credentials**.
2. On the **Account credentials** page, select 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 select **Associate**.

Google Cloud Project

OCCM-Dev

Subscription

GCP subscription for staging

Add Subscription

4. If you don't already have a subscription, select **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.

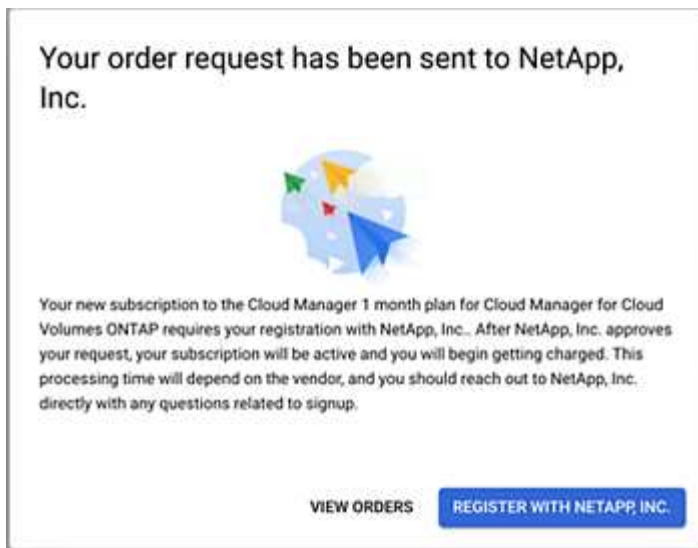
The screenshot shows the 'Product details' page for NetApp BlueXP on the Google Cloud platform. At the top, there's a navigation bar with the Google Cloud logo and a dropdown menu showing 'netapp.com'. Below this, a back arrow and the text 'Product details' are visible. The main content area features 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, there are four tabs: 'OVERVIEW' (which is selected and underlined), 'PRICING', 'DOCUMENTATION', and 'SUPPORT'. The 'Overview' section contains two paragraphs of text describing BlueXP as a hybrid multicloud storage and data services experience. To the right of the overview, under the heading 'Additional details', there is information about the product type ('SaaS & APIs'), the last update date ('12/19/22'), and categories ('Analytics', 'Developer tools', 'Storage').

- b. Select **Subscribe**.
- c. Select the appropriate billing account and agree to the terms and conditions.
- d. Select **Subscribe**.

This step sends your transfer request to NetApp.

- e. On the pop-up dialog box, select **Register with NetApp, Inc.**

This step must be completed to link the Google Cloud subscription to your BlueXP 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 BlueXP 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.

- Select **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

Troubleshoot the Marketplace subscription process

Sometimes subscribing to BlueXP 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 select **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 | ⋮ |

Manage NSS credentials associated with a BlueXP account

Provide BlueXP with the credentials for your NetApp Support Site (NSS) accounts to register for support, enable key workflows for Cloud Volumes ONTAP, and more. These NSS credentials are associated with the entire BlueXP account.



BlueXP also supports associating one NSS account per BlueXP user. [Learn how to manage user-level credentials.](#)

Overview

Associating NetApp Support Site credentials with your specific BlueXP account ID is required to enable the following tasks in BlueXP:

- Registering for support
- Creating support cases
- Deploying 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.

- Registering 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.

- Upgrading Cloud Volumes ONTAP software to the latest release

These credentials are associated with your specific BlueXP account ID. Users who belong to the BlueXP account can access these credentials from **Support > NSS Management**.

Add an NSS account

The Support Dashboard enables you to add and manage your NetApp Support Site accounts for use with BlueXP at the BlueXP 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, select the Help icon, and select **Support**.



2. Select **NSS Management > Add NSS Account**.
3. When you're prompted, select **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 NSS account must be a customer-level account (not a guest or temp account). You can have multiple customer-level NSS accounts.
- There can be only one NSS account if that account is a partner-level account. If you try to add customer-level NSS accounts and a partner-level account exists, you'll get the following error message:

"The NSS customer type is not allowed for this account as there are already NSS Users of different type."

The same is true if you have pre-existing customer-level NSS accounts and try to add a partner-level 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. Note that the token for these accounts expire after 90 days. A notification will be posted to alert you of this.

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 Google Cloud](#)
- [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 BlueXP account](#).
2. In the upper right of the BlueXP console, select the Help icon, and select **Support**.
3. Select **NSS Management**.
4. For the NSS account that you want to update, select **Update Account**.



5. When you're prompted, select **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, select ... 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, select the Help icon, and select **Support**.
2. Select **NSS Management**.
3. For the NSS account that you want to update, select **...** and then select **Update Credentials**.



4. When you're prompted, select **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 select **Add NSS Account** or **Update Account**.

Steps

1. In the upper right of the BlueXP console, select the Help icon, and select **Support**.
2. Select **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, select ...
 - c. Select **Change to a different NSS account**.



- d. Select the account and then select **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, select the Help icon, and select **Support**.
2. Select **NSS Management**.
3. For the NSS account that you want to update, select ... 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, select the Help icon, and select **Support**.
2. Select **NSS Management**.
3. For the NSS account that you want to delete, select **...** and then select **Delete**.



4. Select **Delete** to confirm.

Manage credentials associated with your BlueXP login

Depending on the actions that you've taken in BlueXP, you might have associated ONTAP credentials and NetApp Support Site (NSS) credentials with your BlueXP user login. You can view and manage those credentials in BlueXP after you've associated them. For example, if you change the password for these credentials, then you'll need to update the password in BlueXP.

ONTAP credentials

When you directly discover an on-premises ONTAP cluster without using a Connector, you're prompted to enter ONTAP credentials for the cluster. These credentials are managed at the user level, which means they aren't viewable by other users who log in.

NSS credentials

The NSS credentials associated with your BlueXP login enables access to Digital Advisor and case management capabilities.

- When you access Digital Advisor in BlueXP, you're prompted to log in to Digital Advisor by entering your NSS credentials.
- When you access **Support > Case Management**, you're prompted to enter your NSS credentials, if you haven't already done so. This page enables you to manage the support cases associated with your NSS account and with your company.

Note the following about the 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 case creation.
- There can be only one NSS account associated with Digital Advisor and case management, per user.

NetApp Support Site credentials are also associated with the BlueXP account that you are a member of. NSS account-level credentials enable you to register for support, deploy Cloud Volumes ONTAP when you bring your own license (BYOL), and more.

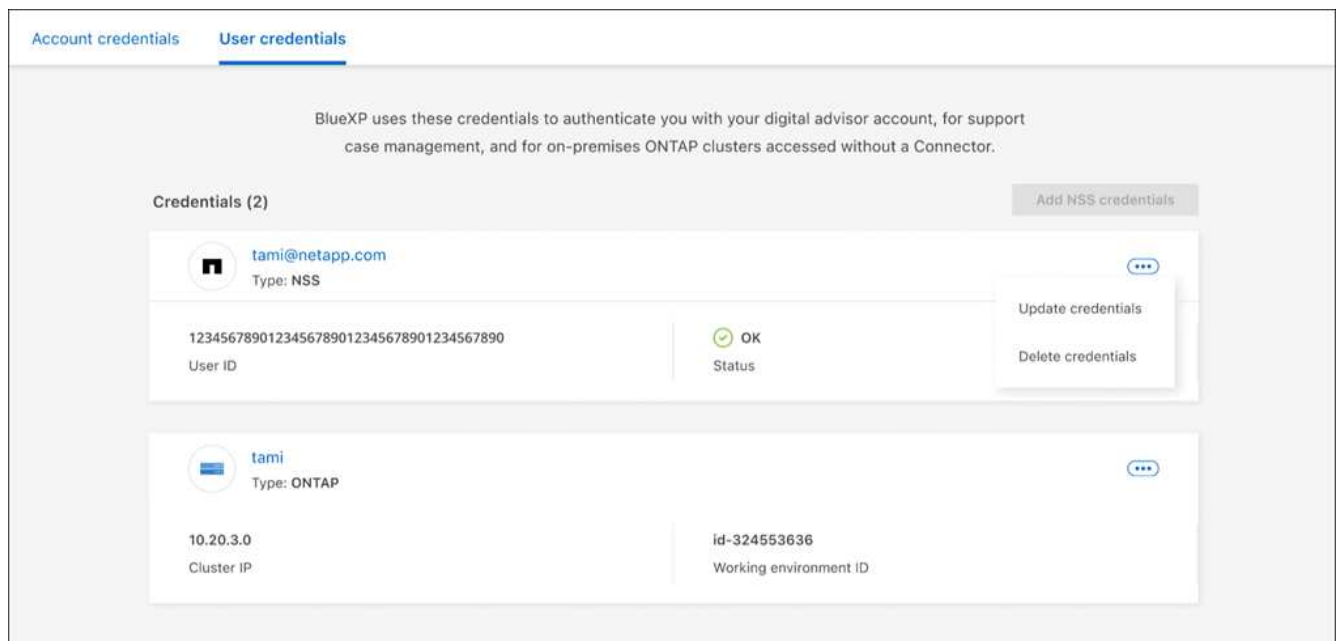
[Learn more about using NSS credentials with your BlueXP account.](#)

Manage your user credentials

Manage your user credentials by updating the user name and password or by deleting the credentials.

Steps

1. In the upper right of the BlueXP console, click the Settings icon, and select **Credentials**.
2. Click **User Credentials**.
3. If you don't have any user credentials yet, you can select **Add NSS credentials** to add your NetApp Support Site account.
4. Manage existing credentials by choosing the following options:
 - **Update credentials:** Update the user name and password for the account.
 - **Delete credentials:** Remove the account associated with your BlueXP user account.



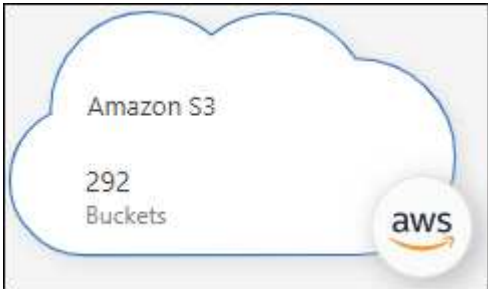
Result

BlueXP updates your credentials. The changes will be reflected when you access the ONTAP cluster, Digital Advisor, or the Case Management page.

Discovered cloud storage

Manage 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 view 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 BlueXP backup and recovery, BlueXP tiering, or BlueXP copy and sync operations. Additionally, you can use BlueXP classification to scan these buckets.

A newly added feature now enables you to create and edit S3 buckets. [Go here to see how you can view, create, and manage your S3 buckets using BlueXP](#)

View your Azure Blob accounts

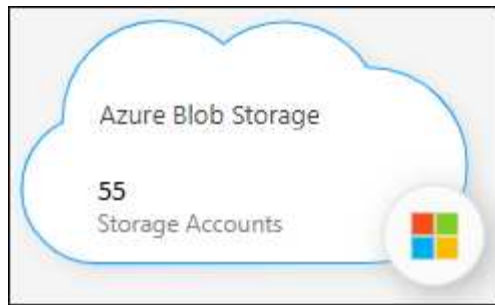
After you install a Connector in Azure, BlueXP can automatically discover information about the Azure storage accounts that reside in the Azure Subscriptions where the Connector is installed. An Azure Blob working environment is added to the Canvas so you can view this information.

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 BlueXP backup and recovery, BlueXP tiering, or BlueXP copy and sync operations.

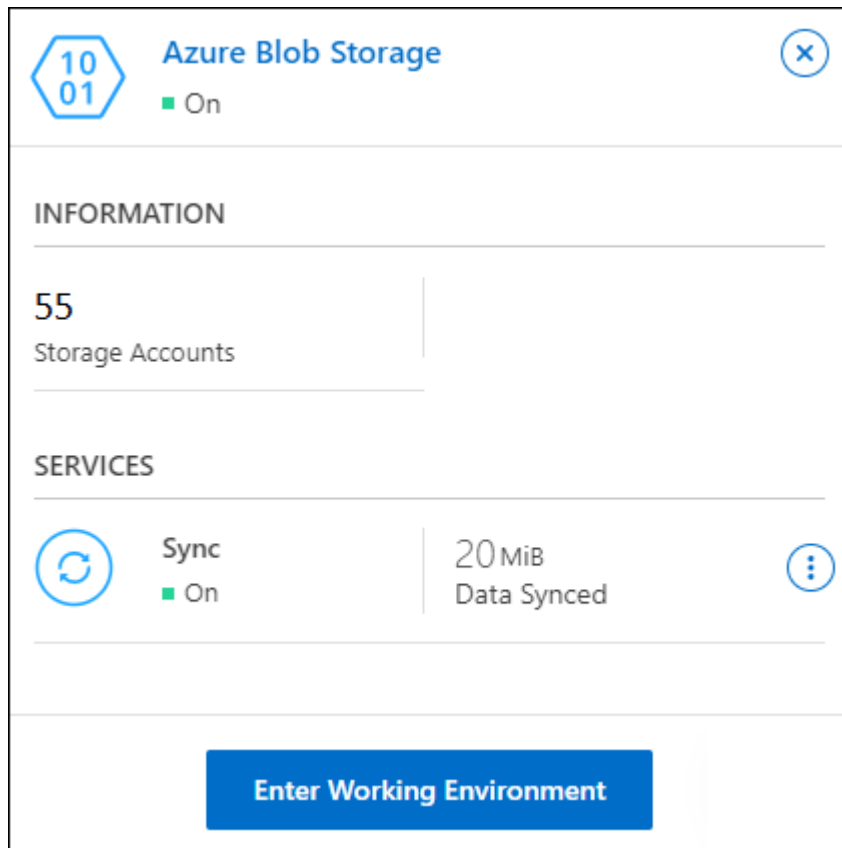
Steps

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. Select the working environment and select an action from the right pane.



4. Select **Sync data** to synchronize data to or from Azure Blob storage.

For more details, see [the overview for BlueXP copy and sync](#)

5. Select **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 |
| scvdwjcwefhswli | 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 |
| 8jzsvybviwieww8 | OCCM QA1 | Canada Central | December 12, 2019 | aff1-rg | 170 B |

View 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 BlueXP backup and recovery, BlueXP tiering, or BlueXP copy and sync operations.

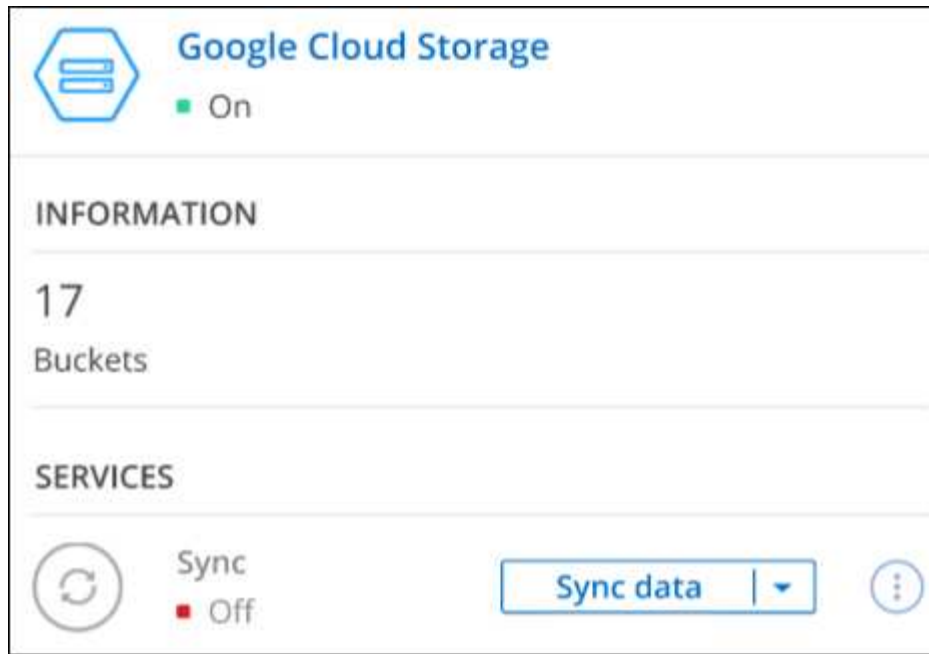
Steps

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. Select the working environment and select an action from the right pane.



4. Select **Sync data** to synchronize data to or from Google Cloud Storage buckets.

For more details, see [the overview for BlueXP copy and sync](#)

5. Select **Enter Working Environment** to view details about the buckets in your Google account.

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 from BlueXP | The user who creates a Connector from BlueXP needs specific permissions to deploy the instance in AWS. | Set up AWS permissions |
| Connector operation | <p>When BlueXP launches the Connector, it attaches a policy to the instance that provides the permissions required to manage resources and processes in your AWS account.</p> <p>You need to set up the policy yourself if you launch a Connector from the marketplace, manually install the Connector, or if you add more AWS credentials to a Connector.</p> <p>You also need to ensure that the policy is up to date as new permissions are added in subsequent releases.</p> | AWS permissions for the Connector |
| Cloud Volumes ONTAP operation | An IAM role must be attached to each Cloud Volumes ONTAP node in AWS. The same is true for the HA mediator. The default option is to let BlueXP create the IAM roles for you, but you can use your own. | Learn how to set up the IAM roles yourself |

Azure permissions

| Purpose | Description | Link |
|----------------------------------|--|--|
| Connector deployment from BlueXP | When you deploy a Connector from BlueXP, you need to use an Azure account or service principal that has permissions to deploy the Connector VM in Azure. | Set up Azure permissions |

| 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 launch a Connector from the marketplace, manually install the Connector, or if you add more Azure credentials to a Connector.</p> <p>You also need to ensure that the policy is up to date as new permissions are added in subsequent releases.</p> | Azure permissions for the Connector |

Google Cloud permissions

| Purpose | Description | Link |
|----------------------|---|--|
| Connector deployment | The Google Cloud user who deploys a Connector from BlueXP needs specific permissions to deploy the Connector in Google Cloud. | Set up permissions to deploy the Connector |
| Connector operation | <p>The service account for the Connector VM instance must have specific permissions for day-to-day operations. You need to associate the service account with the Connector when you deploy it from BlueXP.</p> <p>You also need to ensure that the policy is up to date as new permissions are added in subsequent releases.</p> | Google Cloud permissions for the Connector |

AWS permissions for the Connector

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

IAM policies

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

Note the following:

- If you create a Connector in a standard AWS region directly from BlueXP, BlueXP automatically applies policies to the Connector. You don't need to do anything in this case.
- You need to set up the policies yourself if you deploy the Connector from the AWS Marketplace, if you

manually install the Connector on a Linux host, or if you want to add additional AWS credentials to BlueXP.

- You also need to ensure that the policies are up to date as new permissions are added in subsequent releases.
- If needed, you can restrict the IAM policies by using the IAM `Condition` element. [AWS documentation: Condition element](#)
- To view step-by-step instructions for using these policies, refer to the following pages:
 - [Set up permissions for Connector installation in AWS \(standard mode\)](#)
 - [Set up permissions for Connector installation on premises \(standard mode\)](#)
 - [Set up permissions for restricted mode](#)
 - [Set up permissions for private mode](#)

Select your region to view the required policies:

Standard regions

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

The first policy provides permissions for the following services:

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

The second policy provides permissions for the following services:

- Edge caching
- Kubernetes
- Remediation

Policy #1

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

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

```

        "kms:List*",
        "kms:ReEncrypt*",
        "kms:Describe*",
        "kms:CreateGrant",
        "ce:GetReservationUtilization",
        "ce:GetDimensionValues",
        "ce:GetCostAndUsage",
        "ce:GetTags",
        "fsx:Describe*",
        "fsx:List*"
    ],
    "Resource": "*",
    "Effect": "Allow",
    "Sid": "cvoServicePolicy"
},
{
    "Action": [
        "ec2:StartInstances",
        "ec2:StopInstances",
        "ec2:DescribeInstances",
        "ec2:DescribeInstanceStatus",
        "ec2:RunInstances",
        "ec2:TerminateInstances",
        "ec2:DescribeInstanceAttribute",
        "ec2:DescribeImages",
        "ec2:CreateTags",
        "ec2:CreateVolume",
        "ec2:CreateSecurityGroup",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:DescribeRegions",
        "cloudformation:CreateStack",
        "cloudformation>DeleteStack",
        "cloudformation:DescribeStacks",
        "kms:List*",
        "kms:Describe*",
        "ec2:DescribeVpcEndpoints",
        "kms:ListAliases",
        "athena:StartQueryExecution",
        "athena:GetQueryResults",
        "athena:GetQueryExecution",
        "glue:GetDatabase",
        "glue:GetTable",
        "glue:CreateTable",
        "glue:CreateDatabase",
        "glue:GetPartitions",
    ]
}

```



```

        "glue:BatchCreatePartition",
        "glue:BatchDeletePartition"
    ],
    "Resource": "*",
    "Effect": "Allow",
    "Sid": "backupPolicy"
},
{
    "Action": [
        "s3:GetBucketLocation",
        "s3:ListAllMyBuckets",
        "s3:ListBucket",
        "s3:CreateBucket",
        "s3:GetLifecycleConfiguration",
        "s3:PutLifecycleConfiguration",
        "s3:PutBucketTagging",
        "s3:ListBucketVersions",
        "s3:GetBucketAcl",
        "s3:PutBucketPublicAccessBlock",
        "s3:GetObject",
        "s3:PutEncryptionConfiguration",
        "s3:DeleteObject",
        "s3:DeleteObjectVersion",
        "s3:ListBucketMultipartUploads",
        "s3:PutObject",
        "s3:PutBucketAcl",
        "s3:AbortMultipartUpload",
        "s3:ListMultipartUploadParts",
        "s3:DeleteBucket",
        "s3:GetObjectVersionTagging",
        "s3:GetObjectVersionAcl",
        "s3:GetObjectRetention",
        "s3:GetObjectTagging",
        "s3:GetObjectVersion",
        "s3:PutObjectVersionTagging",
        "s3:PutObjectRetention",
        "s3:DeleteObjectTagging",
        "s3:DeleteObjectVersionTagging",
        "s3:GetBucketObjectLockConfiguration",
        "s3:GetBucketVersioning",
        "s3:PutBucketObjectLockConfiguration",
        "s3:PutBucketVersioning",
        "s3:BypassGovernanceRetention",
        "s3:PutBucketPolicy",
        "s3:PutBucketOwnershipControls"
    ],

```

```

    "Resource": [
        "arn:aws:s3:::netapp-backup-*"
    ],
    "Effect": "Allow",
    "Sid": "backupS3Policy"
},
{
    "Action": [
        "s3:CreateBucket",
        "s3:GetLifecycleConfiguration",
        "s3:PutLifecycleConfiguration",
        "s3:PutBucketTagging",
        "s3:ListBucketVersions",
        "s3:GetBucketPolicyStatus",
        "s3:GetBucketPublicAccessBlock",
        "s3:GetBucketAcl",
        "s3:GetBucketPolicy",
        "s3:PutBucketPublicAccessBlock",
        "s3>DeleteBucket"
    ],
    "Resource": [
        "arn:aws:s3:::fabric-pool*"
    ],
    "Effect": "Allow",
    "Sid": "fabricPoolsS3Policy"
},
{
    "Action": [
        "ec2:DescribeRegions"
    ],
    "Resource": "*",
    "Effect": "Allow",
    "Sid": "fabricPoolPolicy"
},
{
    "Condition": {
        "StringLike": {
            "ec2:ResourceTag/netapp-adc-manager": "*"
        }
    },
    "Action": [
        "ec2:StartInstances",
        "ec2:StopInstances",
        "ec2:TerminateInstances"
    ],
    "Resource": [

```

```

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

```

```

    }
  ]
}

```

Policy #2

```

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

```

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

```

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

```

```

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

```

```

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

```



```

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

```

```

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

```

```

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

```

```

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

```

How the AWS permissions are used

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

Amazon FSx for ONTAP

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

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

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

Amazon S3 bucket discovery

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

s3:GetEncryptionConfiguration

Backup and recovery

The Connector makes the following API requests to deploy the restore instance for BlueXP backup and recovery:

- 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

Classification

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

- ec2:DescribeInstances
- ec2:DescribeInstanceStatus
- ec2:RunInstances
- ec2:TerminateInstances
- ec2:CreateTags
- ec2:CreateVolume
- ec2:AttachVolume
- ec2:CreateSecurityGroup
- ec2>DeleteSecurityGroup
- ec2:DescribeSecurityGroups
- ec2:CreateNetworkInterface
- ec2:DescribeNetworkInterfaces
- ec2>DeleteNetworkInterface
- ec2:DescribeSubnets
- ec2:DescribeVpcs
- ec2:CreateSnapshot
- ec2:DescribeRegions
- cloudformation:CreateStack
- cloudformation>DeleteStack
- cloudformation:DescribeStacks
- cloudformation:DescribeStackEvents
- iam:AddRoleToInstanceProfile
- ec2:AssociateIamInstanceProfile
- ec2:DescribeIamInstanceProfileAssociations

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

- iam:AddRoleToInstanceProfile
- ec2:AssociateIamInstanceProfile
- ec2:DescribeIamInstanceProfileAssociations
- s3:GetBucketTagging

- s3:GetBucketLocation
- s3:ListAllMyBuckets
- s3:ListBucket
- s3:GetBucketPolicyStatus
- s3:GetBucketPolicy
- s3:GetBucketAcl
- s3:GetObject
- iam:GetRole
- s3:DeleteObject
- s3:DeleteObjectVersion
- s3:PutObject
- sts:AssumeRole

Cloud Volumes ONTAP

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

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

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

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

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

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

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

Edge caching

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

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

Kubernetes

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

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

Remediation

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

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

- tag:UntagResources

Change log

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

14 February, 2023

The following permission is now required for BlueXP tiering:

ec2:DescribeVpcEndpoints

Azure permissions for the Connector

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

Custom role permissions

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

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

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

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

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

```
{
  "Name": "BlueXP Operator",
  "Actions": [
    "Microsoft.Compute/disks/delete",
    "Microsoft.Compute/disks/read",
    "Microsoft.Compute/disks/write",
    "Microsoft.Compute/locations/operations/read",
    "Microsoft.Compute/locations/vmSizes/read",
    "Microsoft.Resources/subscriptions/locations/read",
    "Microsoft.Compute/operations/read",
    "Microsoft.Compute/virtualMachines/instanceView/read",
    "Microsoft.Compute/virtualMachines/powerOff/action",
```



```

"Microsoft.Compute/virtualMachines/read",
"Microsoft.Compute/virtualMachines/restart/action",
"Microsoft.Compute/virtualMachines/deallocate/action",
"Microsoft.Compute/virtualMachines/start/action",
"Microsoft.Compute/virtualMachines/vmSizes/read",
"Microsoft.Compute/virtualMachines/write",
"Microsoft.Compute/images/read",
"Microsoft.Network/locations/operationResults/read",
"Microsoft.Network/locations/operations/read",
"Microsoft.Network/networkInterfaces/read",
"Microsoft.Network/networkInterfaces/write",
"Microsoft.Network/networkInterfaces/join/action",
"Microsoft.Network/networkSecurityGroups/read",
"Microsoft.Network/networkSecurityGroups/write",
"Microsoft.Network/networkSecurityGroups/join/action",
"Microsoft.Network/virtualNetworks/read",

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

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

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

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

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

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

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

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

"Microsoft.Resources/subscriptions/resourceGroups/write",
"Microsoft.Storage/checknameavailability/read",
"Microsoft.Storage/operations/read",
"Microsoft.Storage/storageAccounts/listkeys/action",
"Microsoft.Storage/storageAccounts/read",
"Microsoft.Storage/storageAccounts/delete",
"Microsoft.Storage/storageAccounts/write",

```

```

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

"Microsoft.Storage/storageAccounts/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 BlueXP service. This information can be helpful if your corporate policies dictate that permissions are only provided as needed.

Azure NetApp Files

The Connector makes the following API requests 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

Backup and recovery

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

- Microsoft.Compute/virtualMachines/read
- Microsoft.Compute/virtualMachines/start/action
- Microsoft.Compute/virtualMachines/deallocate/action
- Microsoft.Storage/storageAccounts/listkeys/action

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

Classification

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

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

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

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

Cloud Volumes ONTAP

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

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

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

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

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

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

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

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

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

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

Edge caching

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

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

Kubernetes

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

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

Remediation

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

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

Tiering

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

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

The Connector makes the following API requests for daily operations.

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

Change log

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

23 March, 2023

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

This permission is still required for Cloud Volumes ONTAP.

5 January, 2023

The following permissions were added to the JSON policy:

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

These permissions are required for BlueXP backup and recovery.

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

This permission is required for Cloud Volumes ONTAP deployment.

1 December, 2022

The following permissions were added to the JSON policy:

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

This permission is required for BlueXP backup and recovery and BlueXP tiering.

- Microsoft.Network/publicIPAddresses/delete

This permission is required for BlueXP backup and recovery.

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.

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

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

```
title: NetApp BlueXP
description: Permissions for the service account associated with the
Connector instance.
stage: GA
includedPermissions:
- iam.serviceAccounts.actAs
- compute.regionBackendServices.create
- compute.regionBackendServices.get
- compute.regionBackendServices.list
- compute.networks.updatePolicy
- compute.backendServices.create
- compute.addresses.list
- compute.disks.create
- compute.disks.createSnapshot
- compute.disks.delete
- compute.disks.get
- compute.disks.list
- compute.disks.setLabels
- compute.disks.use
- compute.firewalls.create
- compute.firewalls.delete
- compute.firewalls.get
- compute.firewalls.list
- compute.globalOperations.get
- compute.images.get
- compute.images.getFromFamily
- compute.images.list
- compute.images.useReadOnly
```

- `compute.instances.addAccessConfig`
- `compute.instances.attachDisk`
- `compute.instances.create`
- `compute.instances.delete`
- `compute.instances.detachDisk`
- `compute.instances.get`
- `compute.instances.getSerialPortOutput`
- `compute.instances.list`
- `compute.instances.setDeletionProtection`
- `compute.instances.setLabels`
- `compute.instances.setMachineType`
- `compute.instances.setMetadata`
- `compute.instances.setTags`
- `compute.instances.start`
- `compute.instances.stop`
- `compute.instances.updateDisplayDevice`
- `compute.instanceGroups.get`
- `compute.addresses.get`
- `compute.instances.updateNetworkInterface`
- `compute.machineTypes.get`
- `compute.networks.get`
- `compute.networks.list`
- `compute.projects.get`
- `compute.regions.get`
- `compute.regions.list`
- `compute.snapshots.create`
- `compute.snapshots.delete`
- `compute.snapshots.get`
- `compute.snapshots.list`
- `compute.snapshots.setLabels`
- `compute.subnetworks.get`
- `compute.subnetworks.list`
- `compute.subnetworks.use`
- `compute.subnetworks.useExternalIp`
- `compute.zoneOperations.get`
- `compute.zones.get`
- `compute.zones.list`
- `compute.instances.setServiceAccount`
- `deploymentmanager.compositeTypes.get`
- `deploymentmanager.compositeTypes.list`
- `deploymentmanager.deployments.create`
- `deploymentmanager.deployments.delete`
- `deploymentmanager.deployments.get`
- `deploymentmanager.deployments.list`
- `deploymentmanager.manifests.get`
- `deploymentmanager.manifests.list`

- deploymentmanager.operations.get
- deploymentmanager.operations.list
- deploymentmanager.resources.get
- deploymentmanager.resources.list
- deploymentmanager.typeProviders.get
- deploymentmanager.typeProviders.list
- deploymentmanager.types.get
- deploymentmanager.types.list
- logging.logEntries.list
- logging.privateLogEntries.list
- resourcemanager.projects.get
- storage.buckets.create
- storage.buckets.delete
- storage.buckets.get
- storage.buckets.list
- cloudkms.cryptoKeyVersions.useToEncrypt
- cloudkms.cryptoKeys.get
- cloudkms.cryptoKeys.list
- cloudkms.keyRings.list
- storage.buckets.update
- iam.serviceAccounts.getIamPolicy
- iam.serviceAccounts.list
- storage.objects.get
- storage.objects.list
- monitoring.timeSeries.list
- storage.buckets.getIamPolicy
- cloudkms.cryptoKeys.getIamPolicy
- cloudkms.cryptoKeys.setIamPolicy
- cloudkms.keyRings.get
- cloudkms.keyRings.getIamPolicy
- cloudkms.keyRings.setIamPolicy

How Google Cloud permissions are used

| Actions | Purpose |
|---|---|
| <ul style="list-style-type: none"> - compute.disks.create - compute.disks.createSnapshot - compute.disks.delete - compute.disks.get - compute.disks.list - compute.disks.setLabels - compute.disks.use | To create and manage disks for Cloud Volumes ONTAP. |
| <ul style="list-style-type: none"> - compute.firewalls.create - compute.firewalls.delete - compute.firewalls.get - compute.firewalls.list | To create firewall rules for Cloud Volumes ONTAP. |

| Actions | Purpose |
|--|--|
| - compute.globalOperations.get | To get the status of operations. |
| - compute.images.get - compute.images.getFromFamily - compute.images.list - compute.images.useReadOnly | To get images for VM instances. |
| - compute.instances.attachDisk - compute.instances.detachDisk | To attach and detach disks to Cloud Volumes ONTAP. |
| - compute.instances.create - compute.instances.delete | To create and delete Cloud Volumes ONTAP VM instances. |
| - compute.instances.get | To list VM instances. |
| - compute.instances.getSerialPortOutput | To get console logs. |
| - compute.instances.list | To retrieve the list of instances in a zone. |
| - compute.instances.setDeletionProtection | To set deletion protection on the instance. |
| - compute.instances.setLabels | To add labels. |
| - compute.instances.setMachineType - compute.instances.setMinCpuPlatform | To change the machine type for Cloud Volumes ONTAP. |
| - compute.instances.setMetadata | To add metadata. |
| - compute.instances.setTags | To add tags for firewall rules. |
| - compute.instances.start - compute.instances.stop - compute.instances.updateDisplayDevice | To start and stop Cloud Volumes ONTAP. |
| - compute.machineTypes.get | To get the numbers of cores to check quotas. |
| - compute.projects.get | To support multi-projects. |
| - compute.snapshots.create - compute.snapshots.delete - compute.snapshots.get - compute.snapshots.list - compute.snapshots.setLabels | To create and manage persistent disk snapshots. |
| - compute.networks.get - compute.networks.list - compute.regions.get - compute.regions.list - compute.subnetworks.get - compute.subnetworks.list - compute.zoneOperations.get - compute.zones.get - compute.zones.list | To get the networking information needed to create a new Cloud Volumes ONTAP virtual machine instance. |

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

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

Change log

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

6 February, 2023

The following permission was added to this policy:

- compute.instances.updateNetworkInterface

This permission is required for Cloud Volumes ONTAP.

27 January, 2023

The following permissions were added to the policy:

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

These permissions are required for BlueXP backup and recovery.

Ports

Security group rules in AWS

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

Inbound rules

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

Outbound rules

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

Basic outbound rules

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

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

Advanced outbound rules

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



The source IP address is the Connector host.

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

Security group rules in Azure

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

Inbound rules

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

Outbound rules

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

Basic outbound rules

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

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

Advanced outbound rules

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



The source IP address is the Connector host.

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

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

Firewall rules in Google Cloud

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

Inbound rules

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

Outbound rules

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

Basic outbound rules

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

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

Advanced outbound rules

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



The source IP address is the Connector host.

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

Ports for the on-prem Connector

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

These inbound rules apply to all BlueXP deployment models.

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

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.

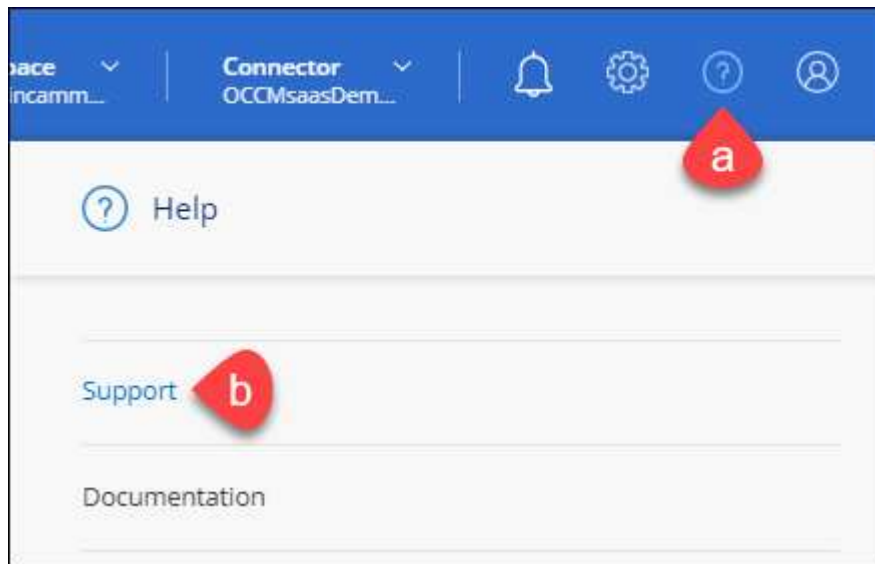
Add an NSS account to BlueXP

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 NSS account must be a customer-level account (not a guest or temp account). You can have multiple customer-level NSS accounts.
- There can be only one NSS account if that account is a partner-level account. If you try to add customer-level NSS accounts and a partner-level account exists, you'll get the following error message:

"The NSS customer type is not allowed for this account as there are already NSS Users of different type."

The same is true if you have pre-existing customer-level NSS accounts and try to add a partner-level 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. Note that the token for these accounts expire after 90 days. A notification will be posted to alert you of this.

Register with NetApp

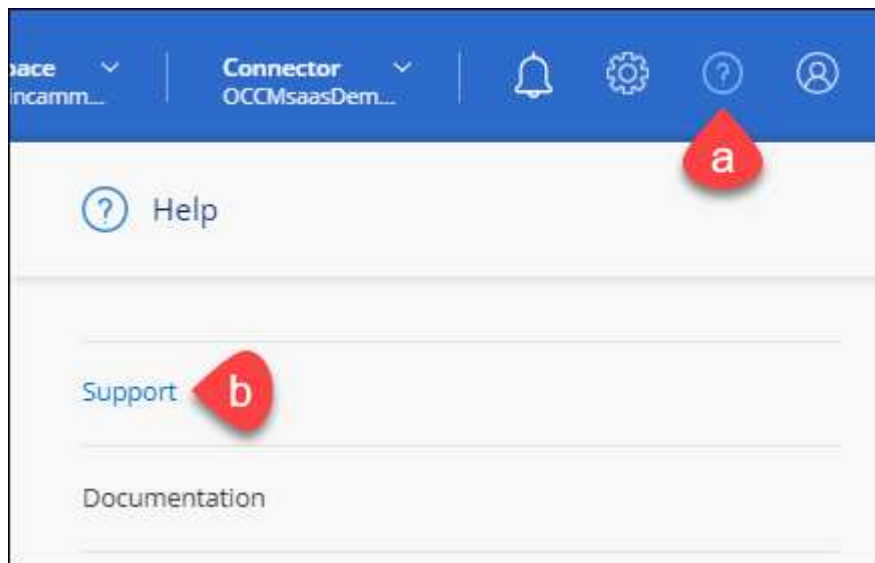
How you register for NetApp support depends on whether you already have a NetApp Support Site (NSS) account.

Existing customer with an NSS account

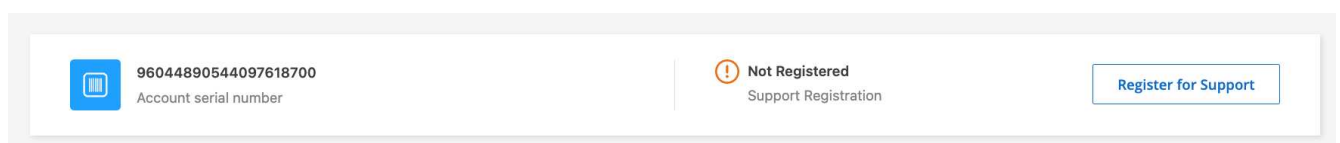
If you're a NetApp customer with an NSS account, you simply need to register for support through BlueXP.

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

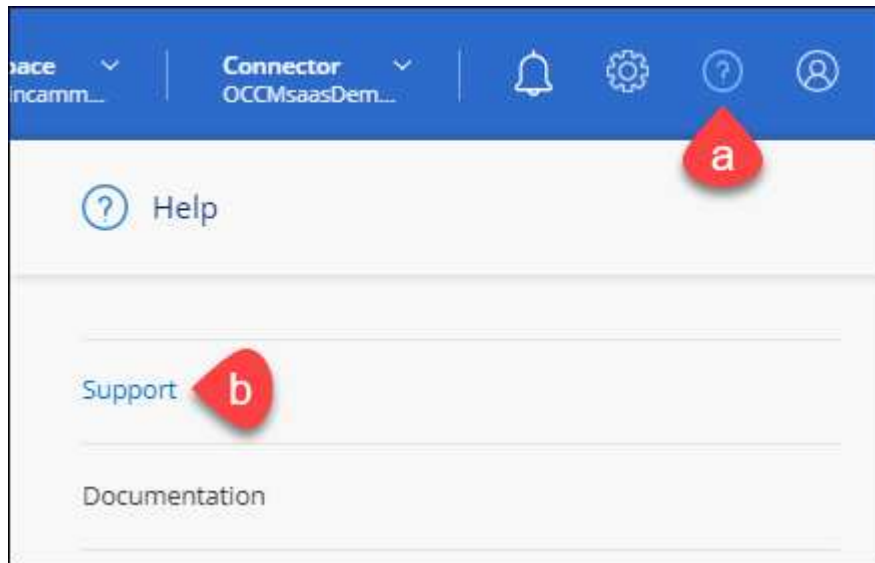
1. Create a NetApp Support Site account by completing the [NetApp Support Site User Registration form](#)
 - a. Be sure to select the appropriate User Level, which is typically **NetApp Customer/End User**.
 - b. Be sure to copy the BlueXP account serial number (960xxxx) used above for the serial number 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.

Use self-support options

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.

Create a case with 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. On the **Resources** page, 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 specialist:

- **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.
- **Attachment (Optional):** Upload up to five attachments, one at a time.

Attachments are limited to 25 MB per file. The following file extensions are supported: txt, log, pdf, jpg/jpeg, rtf, doc/docx, xls/xlsx, and csv.

ntapitdemo
NetApp Support Site Account

Service

Select

Working Enviroment

Select

Case Priority

Low - General guidance

Issue Description

Provide detailed description of problem, applicable error messages and troubleshooting steps taken.

Additional Email Addresses (Optional)

Type here

Attachment (Optional)

No files selected

Upload

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>

Manage your support cases (Preview)

You can view and manage active and resolved support cases directly from BlueXP. You can manage the cases associated with your NSS account and with your company.

Case management is available as a Preview. We plan to refine this experience and add enhancements in upcoming releases. Please send us feedback by using the in-product chat.

Note the following:

- The case management dashboard at the top of the page offers two views:
 - The view on the left shows the total cases opened in the past 3 months by the user NSS account you provided.
 - The view on the right shows the total cases opened in the past 3 months at your company level based on your user NSS account.

The results in the table reflect the cases related to the view that you selected.

- You can add or remove columns of interest and you can filter the contents of columns like Priority and Status. Other columns provide just sorting capabilities.

View the steps below for more details.

- At a per-case level, we offer the ability to update case notes or close a case that is not already in Closed or Pending Closed status.

Steps

1. In BlueXP, click **Help > Support**.
2. Click **Case Management** and if you're prompted, add your NSS account to BlueXP.

The **Case management** page shows open cases related to the NSS account that is associated with your BlueXP user account. This is the same NSS account that appears at the top of the **NSS management** page.

3. Optionally modify the information that displays in the table:
 - Under **Organization's cases**, click **View** to view all cases associated with your company.
 - Modify the date range by choosing an exact date range or by choosing a different time frame.

Search icon | Cases opened on the last 3 months | Create a case

| Date created | Last updated | | Status (5) | |
|-------------------|-------------------|---------------|-------------------|-----|
| December 22, 2022 | December 29, 2022 | Last 7 days | Assigned | ... |
| December 21, 2022 | December 28, 2022 | Last 30 days | Active | ... |
| December 15, 2022 | December 27, 2022 | Last 3 months | Pending customer | ... |
| December 14, 2022 | December 26, 2022 | Medium (P3) | Solution proposed | ... |
| | | Low (P4) | | |


Apply | Reset

- Filter the contents of the columns.

Search icon | Cases opened on the last 3 months | Create a case

| Last updated | Priority | Status (5) | |
|-------------------|---------------|-------------------|-----|
| December 29, 2022 | Critical (P1) | Active | ... |
| December 28, 2022 | High (P2) | Pending customer | ... |
| December 27, 2022 | Medium (P3) | Solution proposed | ... |
| December 26, 2022 | Low (P4) | Pending closed | ... |
| | | Closed | ... |

Apply | Reset

- Change the columns that appear in the table by clicking  and then choosing the columns that you'd like to display.

Search icon | Cases opened on the last 3 months | Create a case

| Last updated | Priority | Status (5) | |
|-------------------|---------------|--------------|-----|
| December 29, 2022 | Critical (P1) | Last updated | ... |
| December 28, 2022 | High (P2) | Priority | ... |
| December 27, 2022 | Medium (P3) | Cluster name | ... |
| December 26, 2022 | Low (P4) | Case owner | ... |
| | | Opened by | ... |

Apply | Reset

4. Manage an existing case by clicking ... and selecting one of the available options:

- **View case:** View full details about a specific case.
- **Update case notes:** Provide additional details about your problem or select **Upload files** to attach up to a maximum of five files.

Attachments are limited to 25 MB per file. The following file extensions are supported: txt, log, pdf, jpg/jpeg, rtf, doc/docx, xls/xlsx, and csv.

- **Close case:** Provide details about why you're closing the case and click **Close case**.



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.