



# **Get started with restricted mode**

## **BlueXP setup and administration**

NetApp  
August 15, 2024

# Table of Contents

- Get started with restricted mode ..... 1
  - Getting started workflow (restricted mode) ..... 1
  - Prepare for deployment in restricted mode ..... 1
  - Deploy the Connector in restricted mode ..... 20
  - Subscribe to BlueXP (restricted mode) ..... 32
  - What you can do next (restricted mode) ..... 38

# Get started with restricted mode

## Getting started workflow (restricted mode)

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

Restricted mode is typically used by state and local governments and regulated companies, including deployments in AWS GovCloud and Azure Government regions. Before you get started, you should have an understanding of [BlueXP accounts](#), [Connectors](#), and [deployment modes](#).

1

### Prepare for deployment

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

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.

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.

## 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.

### Step 1: 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.](#)

## Step 2: 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

## Step 3: 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

- Ubuntu 22.04 LTS
- Red Hat Enterprise Linux
  - 8.6 to 8.10
  - 9.1 to 9.3

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 a supported operating system is required.

### CPU

8 cores or 8 vCPUs

### RAM

32 GB

### AWS EC2 instance type

An instance type that meets the CPU and RAM requirements above. We recommend t3.2xlarge.

### Azure VM size

An instance type that meets the CPU and RAM requirements above. We recommend Standard\_D8s\_v3.

## Google Cloud machine type

An instance type that meets the CPU and RAM requirements above. We recommend n2-standard-8.

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

BlueXP uses `/opt` to install the `/opt/application/netapp` directory and its contents.

## Disk space in /var

20 GiB of space must be available

BlueXP requires this space in `/var` because Docker or Podman are architected to create the containers within this directory. Specifically, they will create containers in the `/var/lib/containers/storage` directory. External mounts or symlinks do not work for this space.

## Container orchestration tool

Depending on your operating system, either Podman or Docker Engine is required before you install the Connector.

- Podman is required for Red Hat Enterprise Linux 8 and 9.

RHEL version	Supported Podman version
RHEL 8.6 to 8.9	Podman 4.6.1
RHEL 8.10	Podman 4.6.1 and 4.9.4
RHEL 9.1 to 9.3	Podman 4.6.1

The following prerequisites must be met for Podman:

- The `podman.socket` service must be enabled and started
- `python3` must be installed
- The `podman-compose` package version 1.0.6 must be installed
- `podman-compose` must be added to the `PATH` environment variable
- Docker Engine is required for Ubuntu.
  - The minimum supported version is 23.0.6.
  - The maximum supported version is 25.0.5.

## Step 4: Install Podman or Docker Engine

If you're planning to manually install the Connector software, you need to prepare the host by installing Podman or Docker Engine.

Depending on your operating system, either Podman or Docker Engine is required before you install the Connector.

- Podman is required for Red Hat Enterprise Linux 8 and 9.
- Docker Engine is required for Ubuntu.

## Example 1. Steps

### Podman

Install a supported version of Podman. [View the Podman versions that BlueXP supports.](#)

### Steps

1. Remove the podman-docker package if it's installed on the host.

```
dnf remove podman-docker
rm /var/run/docker.sock
```

2. Install Podman.

Podman is available from official Red Hat Enterprise Linux repositories.

For Red Hat Enterprise Linux 9:

```
sudo dnf install podman-2:<version>
```

Where <version> is the supported version of Podman that you're installing. [View the Podman versions that BlueXP supports.](#)

For Red Hat Enterprise Linux 8:

```
sudo dnf install podman-3:<version>
```

Where <version> is the supported version of Podman that you're installing. [View the Podman versions that BlueXP supports.](#)

3. Enable and start the podman.socket service.

```
sudo systemctl enable --now podman.socket
```

4. Install python3.

```
sudo dnf install python3
```

5. Install the EPEL repository package if it's not already available on your system.

This step is required because podman-compose is available from the Extra Packages for Enterprise Linux (EPEL) repository.

For Red Hat Enterprise Linux 9:

```
sudo dnf install https://dl.fedoraproject.org/pub/epel/epel-release-latest-9.noarch.rpm
```

For Red Hat Enterprise Linux 8:

```
sudo dnf install https://dl.fedoraproject.org/pub/epel/epel-release-latest-8.noarch.rpm
```

6. Install podman-compose package 1.0.6.

```
sudo dnf install podman-compose-1.0.6
```



Using the `dnf install` command meets the requirement for adding podman-compose to the PATH environment variable. The installation command adds podman-compose to `/usr/bin`, which is already included in the `secure_path` option on the host.

## Docker Engine

Install a version of Docker Engine between 23.0.6 and 25.0.5.

### Steps

1. Install Docker Engine.

[View installation instructions from Docker](#)

Be sure to follow the steps to install a specific version of Docker Engine. Installing the latest version will install a version of Docker that BlueXP doesn't support.

2. Verify that Docker is enabled and running.

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

## Step 5: Prepare networking

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

### 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.



## 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. These endpoints are contacted from a user's computer when completing specific actions from the BlueXP console.

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

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

This endpoint is not required in Azure Government regions.

- <https://occmclientinfragov.azurecr.us>

This endpoint is only required in Azure Government regions.

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

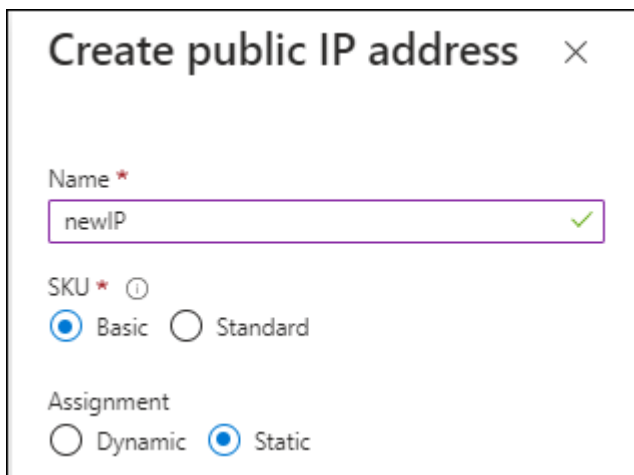
The network location where you deploy the Connector must have an outbound internet connection. The Connector requires outbound internet access to contact the following endpoints in order to manage resources and processes within your public cloud environment.

Endpoints	Purpose
<p>AWS services (amazonaws.com):</p> <ul style="list-style-type: none"> <li>• CloudFormation</li> <li>• Elastic Compute Cloud (EC2)</li> <li>• Identity and Access Management (IAM)</li> <li>• Key Management Service (KMS)</li> <li>• Security Token Service (STS)</li> <li>• Simple Storage Service (S3)</li> </ul>	<p>To manage resources in AWS. The exact endpoint depends on the AWS region that you're using. <a href="#">Refer to AWS documentation for details</a></p>
<p>https://management.azure.com  https://login.microsoftonline.com  https://blob.core.windows.net  https://core.windows.net</p>	<p>To manage resources in Azure public regions.</p>
<p>https://management.usgovcloudapi.net  https://login.microsoftonline.us  https://blob.core.usgovcloudapi.net  https://core.usgovcloudapi.net</p>	<p>To manage resources in Azure Government regions.</p>
<p>https://management.chinacloudapi.cn  https://login.chinacloudapi.cn  https://blob.core.chinacloudapi.cn  https://core.chinacloudapi.cn</p>	<p>To manage resources in Azure China regions.</p>
<p>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</p>	<p>To manage resources in Google Cloud.</p>
<p>https://support.netapp.com  https://mysupport.netapp.com</p>	<p>To obtain licensing information and to send AutoSupport messages to NetApp support.</p>

Endpoints	Purpose
https://*.api.bluexp.netapp.com https://api.bluexp.netapp.com https://*.cloudmanager.cloud.netapp.com https://cloudmanager.cloud.netapp.com https://netapp-cloud-account.auth0.com	To provide SaaS features and services within BlueXP.  Note that the Connector is currently contacting "cloudmanager.cloud.netapp.com" but it will start contacting "api.bluexp.netapp.com" in an upcoming release.
https://*.blob.core.windows.net  https://cloudmanagerinfraprod.azurecr.io This endpoint is not required in Azure Government regions.  https://occmclientinfragov.azurecr.us This endpoint is only required in Azure Government regions.	To upgrade the Connector and its Docker components.

### 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.



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](#)

### 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. You'll need to provide this information during installation. Note that BlueXP does not support transparent proxy servers.

- 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 to send AutoSupport messages from Cloud Volumes ONTAP to NetApp Support.

- 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 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 NTP

If you're planning to use BlueXP classification to scan your corporate data sources, you should enable a Network Time Protocol (NTP) service on both the BlueXP Connector system and the BlueXP classification system so that the time is synchronized between the systems. [Learn more about BlueXP classification](#)

If you're planning to create the Connector from your cloud provider's marketplace, then you'll need to implement this networking requirement after you create the Connector.

## Step 6: 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. Select **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. Select **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. Log in to the AWS console and navigate to the IAM service.
2. Create a policy:
  - a. Select **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](#).

3. Attach the policies to an IAM user.
  - [AWS Documentation: Creating IAM Roles](#)
  - [AWS Documentation: Adding and Removing IAM Policies](#)

4. Ensure that the user has an access key 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.

Note that you can create an Azure custom role using the Azure portal, Azure PowerShell, Azure CLI, or REST API. The following steps show how to create the role using the Azure CLI. If you would prefer to use a different method, refer to [Azure documentation](#)

### 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 that you want to use with BlueXP.

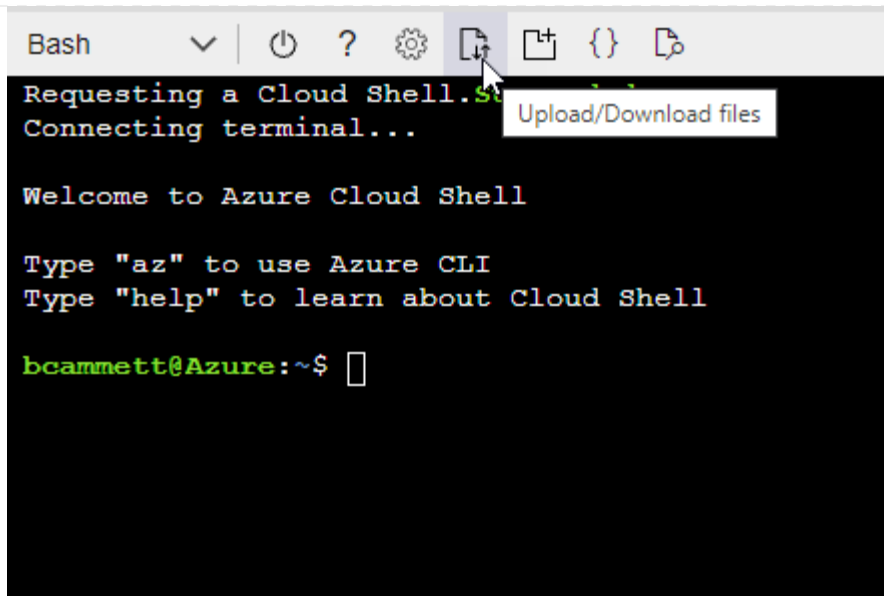
### Example

```
"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

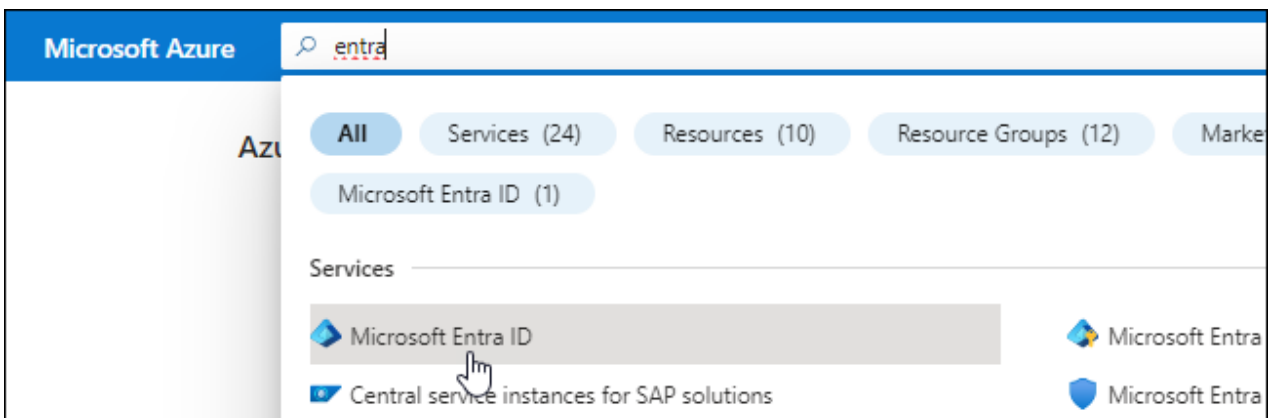
Create and set up a service principal in Microsoft Entra ID and obtain the Azure credentials that BlueXP needs. You'll need to provide BlueXP with these credentials after you install the Connector and set up BlueXP.

### Create a Microsoft Entra 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 **Microsoft Entra ID** service.



3. In the menu, select **App registrations**.
4. Select **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. Select **Register**.

You've created the AD application and service principal.

### Assign the application to a role

1. Create a custom role:

Note that you can create an Azure custom role using the Azure portal, Azure PowerShell, Azure CLI, or REST API. The following steps show how to create the role using the Azure CLI. If you would prefer to use a different method, refer to [Azure documentation](#)

- 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

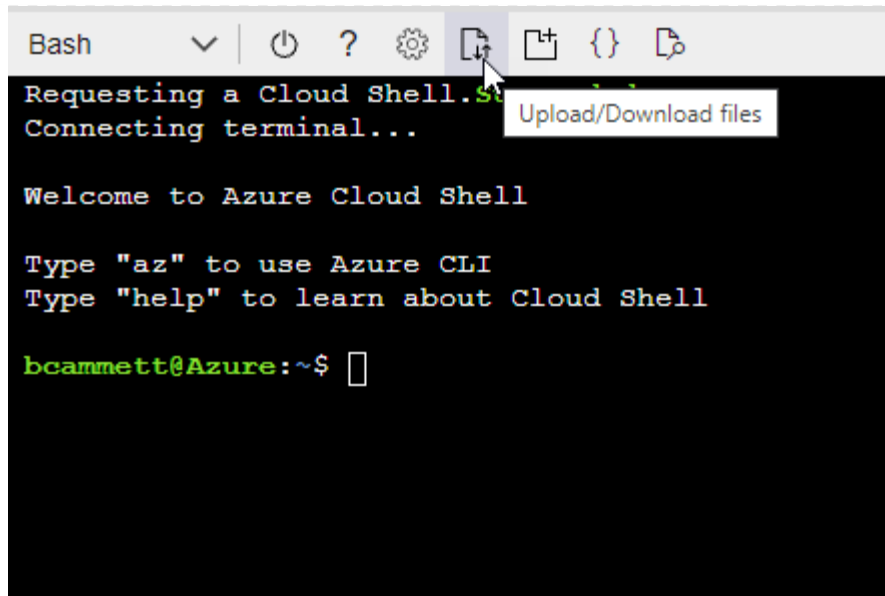
```
"AssignableScopes": [  
  "/subscriptions/d333af45-0d07-4154-943d-c25fbzzzzzzz",  
  "/subscriptions/54b91999-b3e6-4599-908e-416e0zzzzzzz",  
  "/subscriptions/398e471c-3b42-4ae7-9b59-ce5bbzzzzzzz"]
```

- 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.





```
Bash
Requesting a Cloud Shell session...
Connecting terminal...

Welcome to Azure Cloud Shell

Type "az" to use Azure CLI
Type "help" to learn about Cloud Shell

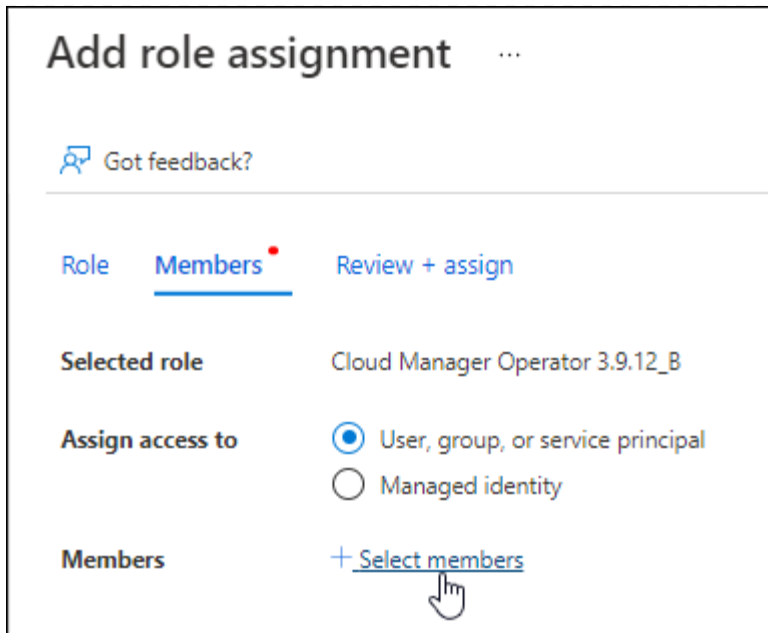
bcammett@Azure:~$
```

- Use the Azure CLI to create the custom role:

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

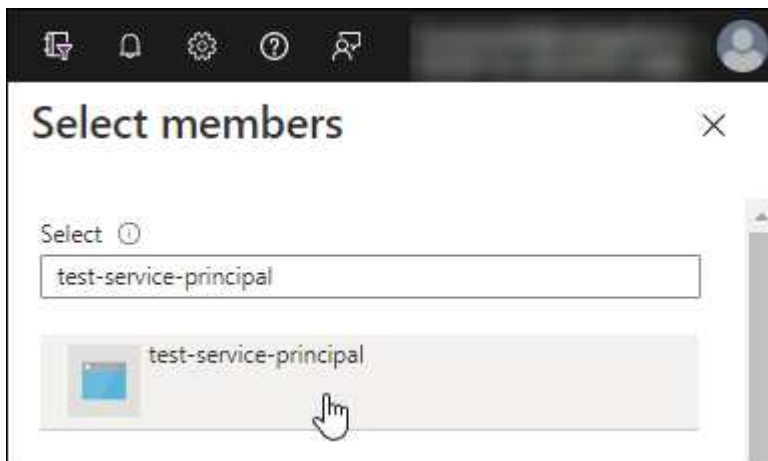
You should now have a custom role called BlueXP Operator that you can assign to the Connector virtual machine.

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



- Search for the name of the application.

Here's an example:



- 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














1. In the **Microsoft Entra ID** 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

<b>Microsoft Graph</b> 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. 		
 <b>Azure Batch</b> Schedule large-scale parallel and HPC applications in the cloud	 <b>Azure Data Catalog</b> Programmatic access to Data Catalog resources to register, annotate and search data assets	 <b>Azure Data Explorer</b> Perform ad-hoc queries on terabytes of data to build near real-time and complex analytics solutions
 <b>Azure Data Lake</b> Access to storage and compute for big data analytic scenarios	 <b>Azure DevOps</b> Integrate with Azure DevOps and Azure DevOps server	 <b>Azure Import/Export</b> Programmatic control of import/export jobs
 <b>Azure Key Vault</b> Manage your key vaults as well as the keys, secrets, and certificates within your Key Vaults	 <b>Azure Rights Management Services</b> Allow validated users to read and write protected content	 <b>Azure Service Management</b> Programmatic access to much of the functionality available through the Azure portal
 <b>Azure Storage</b> Secure, massively scalable object and data lake storage for unstructured and semi-structured data	 <b>Customer Insights</b> Create profile and interaction models for your products	 <b>Data Export Service for Microsoft Dynamics 365</b> 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



user\_impersonation

Access Azure Service Management as organization users (preview)

## Get the application ID and directory ID for the application

1. In the **Microsoft Entra ID** service, select **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 **Microsoft Entra ID** 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	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 Microsoft Entra ID.

### 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, select **Service Accounts > Create Service Account**.
  - b. Enter service account details and select **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.

## Step 7: 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
- Cloud Key Management Service (KMS) API

(Required only if you are planning to use BlueXP backup and recovery with customer-managed encryption keys (CMEK))

## 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.

### Step 1: 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

### Before you begin

You should have the following:

- 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](#)

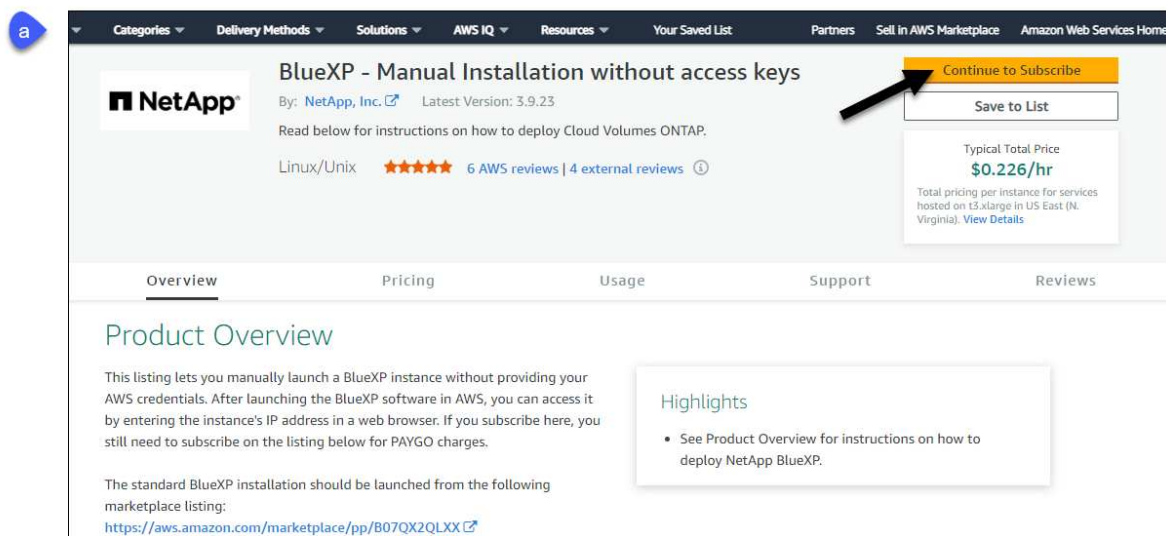
- Permissions to subscribe and unsubscribe from the AWS Marketplace for your IAM user.
- An understanding of CPU and RAM requirements for the instance.

[Review instance requirements.](#)

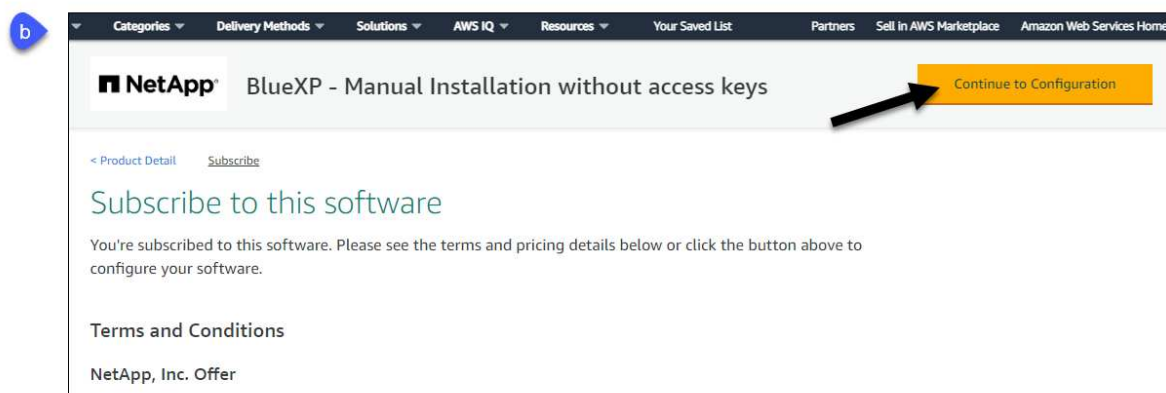
- A key pair for the EC2 instance.

### Steps

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



The screenshot shows the AWS Marketplace listing for NetApp BlueXP. The page header includes navigation links like Categories, Delivery Methods, Solutions, AWS IQ, Resources, Your Saved List, Partners, Sell in AWS Marketplace, and Amazon Web Services Home. The main content area features the NetApp logo, the product name "BlueXP - Manual Installation without access keys", and the version "3.9.23". Below this, there are tabs for Overview, Pricing, Usage, Support, and Reviews. A yellow button labeled "Continue to Subscribe" is highlighted with a black arrow. To the right of this button is a "Save to List" button and a pricing box showing "Typical Total Price \$0.226/hr".



The screenshot shows the "Subscribe to this software" page for NetApp BlueXP. The page header is the same as the previous screenshot. The main content area features the NetApp logo, the product name, and a yellow button labeled "Continue to Configuration" highlighted with a black arrow. Below this, there is a "Terms and Conditions" section with the text "NetApp, Inc. Offer".

3. Change any of the default options and select **Continue to Launch**.
4. Under **Choose Action**, select **Launch through EC2** and then select **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 an instance type that meets RAM and CPU requirements (t3.2xlarge is recommended).
  - **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 size and disk type for the root volume.

If you want to enable Amazon EBS encryption on the root volume, select **Advanced**, expand **Volume 1**, select **Encrypted**, and then choose a KMS key.

- **Advanced details**: Under **IAM instance profile**, choose the IAM role that includes the required permissions for the Connector.
- **Summary**: Review the summary and select **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

### Before you begin

You should have the following:

- 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.

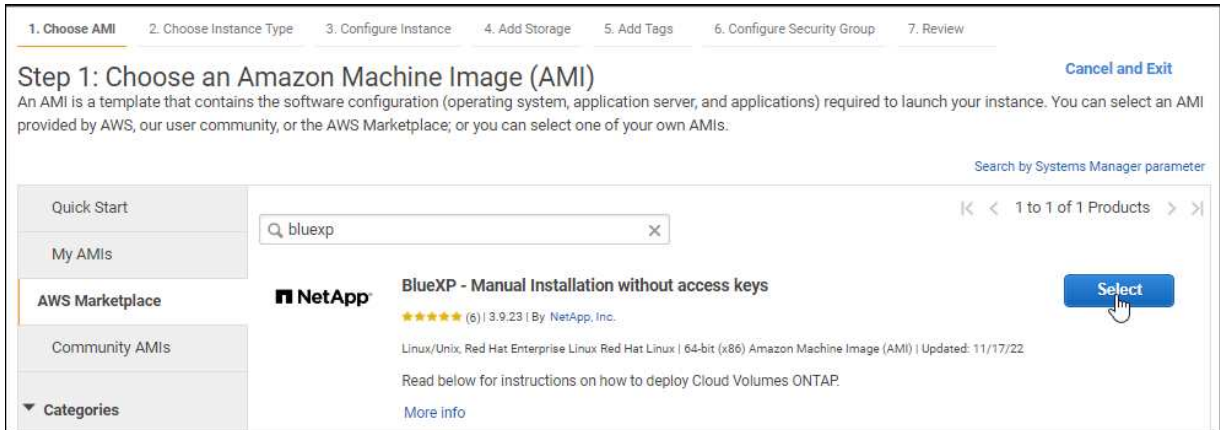
[Learn how to set up AWS permissions](#)



- 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.



- d. Select **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 (t3.2xlarge 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	<input type="text" value="1"/>	<a href="#">Launch into Auto Scaling Group</a>
Purchasing option	<input type="checkbox"/> Request Spot instances	
Network	vpc-a76d91c2   VPC4QA (default)	<a href="#">Create new VPC</a>
Subnet	subnet-39536c13   QASubnet1   us-east-1b 155 IP Addresses available	<a href="#">Create new subnet</a>
Auto-assign Public IP	Enable	
Placement group	<input type="checkbox"/> Add instance to placement group	
Capacity Reservation	Open	<a href="#">Create new Capacity Reservation</a>
IAM role	Cloud_Manager	<a href="#">Create new IAM role</a>
CPU options	<input type="checkbox"/> Specify CPU options	
Shutdown behavior	Stop	
Enable termination protection	<input checked="" type="checkbox"/> Protect against accidental termination	
Monitoring	<input type="checkbox"/> Enable CloudWatch detailed monitoring <a href="#">Additional charges apply.</a>	

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

### Before you begin

You should have the following:

- 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

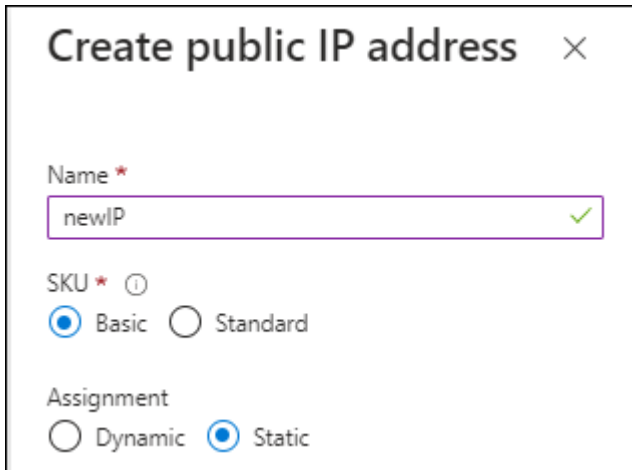
1. Go to the NetApp Connector VM page in the Azure Marketplace.
  - [Azure Marketplace page for commercial regions](#)

- [Azure Marketplace page for Azure Government regions](#)

2. Select **Get it now** and then select **Continue**.
3. From the Azure portal, select **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 Standard\_D8s\_v3.
- **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.



The screenshot shows a dialog box titled "Create public IP address" with a close button (X) in the top right corner. Below the title, there are three sections of configuration options:

- Name \***: A text input field containing "newIP" with a green checkmark on the right side.
- SKU \***: Two radio button options: "Basic" (which is selected) and "Standard".
- Assignment**: Two radio button options: "Dynamic" and "Static" (which is selected).

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.

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

- **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 Microsoft Entra ID without providing any credentials. [Learn more about managed identities for Azure resources.](#)

4. On the **Review + create** page, review your selections and select **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

### Before you begin

You should have the following:

- 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.

Note that BlueXP does not support transparent proxy servers.

- A CA-signed certificate, if the proxy server uses HTTPS or if the proxy is an intercepting proxy.
- Depending on your operating system, either Podman or Docker Engine is required before you install the Connector.

### About this task

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. 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.

2. 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.

3. Assign permissions to run the script.

```
chmod +x BlueXP-Connector-Cloud-<version>
```

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

4. Run the installation script.

```
./BlueXP-Connector-Cloud-<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 parameters 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:

```
./BlueXP-Connector-Cloud-v3.9.40--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://user-name:password@address:port
- http://domain-name%92user-name:password@address:port
- https://address:port
- https://user-name:password@address:port
- https://domain-name%92user-name:password@address:port

Note the following:

- The user can be a local user or domain user.
- For a domain user, you must use the ASCII code for a \ as shown above.
- BlueXP doesn't support user names or passwords that include the @ character.
- If the password includes any of the following special characters, you must escape that special character by prepending it with a backslash: & or !

For example:

```
http://bxpproxyuser:netapp1!\@address:3128
```

--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.

### What's next?

Set up BlueXP.

## Step 2: 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. Select **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.

### **Step 3: 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 select **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, select the Settings icon, and select **Credentials**.



2. Select **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 select **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.

It's important to assign the role from the **Subscriptions** service because this specifies the scope of the role assignment at the subscription level. The *scope* defines the set of resources that the access applies to. If you specify a scope at a different level (for example, at the virtual machine level), your



ability to complete actions from within BlueXP will be affected.

[Microsoft Azure documentation: Understand scope for Azure RBAC](#)

2. Select **Access control (IAM) > Add > Add role assignment**.
3. In the **Role** tab, select the **BlueXP Operator** role and select **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. Select **Select members**, select the subscription in which the Connector virtual machine was created, under **Managed identity**, choose **Virtual machine**, and then select the Connector virtual machine.
  - c. Select **Select**.
  - d. Select **Next**.
  - e. Select **Review + assign**.
  - f. If you want to manage resources in additional Azure 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, select the Settings icon, and select **Credentials**.



2. Select **Add Credentials** and follow the steps in the wizard.
  - a. **Credentials Location:** Select **Microsoft Azure > Connector**.
  - b. **Define Credentials:** Enter information about the Microsoft Entra 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 select **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 manage resources 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.

## **Subscribe to BlueXP (restricted 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 marketplace 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.

A marketplace subscription enables charging for the following BlueXP services with restricted mode:

- Backup and recovery
- Classification
- Cloud Volumes ONTAP

#### **Before you begin**

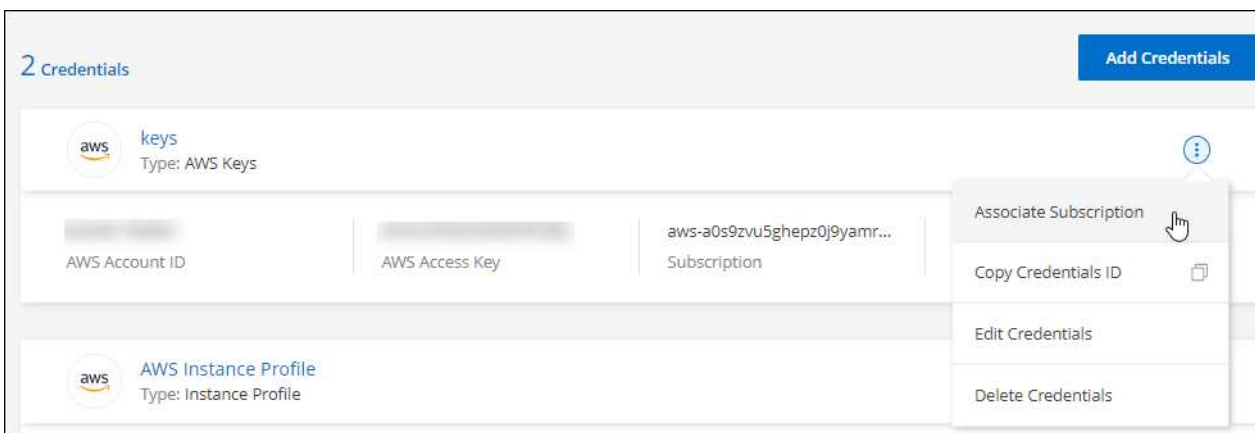
Subscribing to BlueXP involves associating a marketplace subscription with the cloud credentials that are associated with a Connector. If you followed the "Get started with restricted mode" workflow, then you should already have a Connector. To learn more, view the [Quick start for BlueXP in restricted mode](#).

## AWS

### Steps

1. In the upper right of the BlueXP console, select the Settings icon, and select **Credentials**.
2. Select the action menu for a set of credentials and then select **Associate Subscription**.

You must select credentials that are associated with a Connector. You can't associate a marketplace subscription with credentials that are associated with BlueXP.



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 AWS Marketplace:

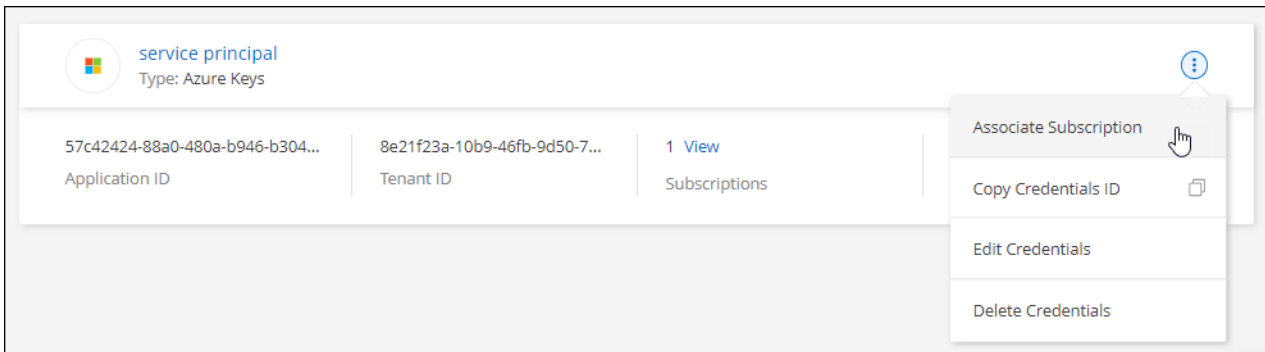
[Subscribe to BlueXP from the AWS Marketplace](#)

## Azure

### Steps

1. In the upper right of the BlueXP console, select the Settings icon, and select **Credentials**.
2. Select the action menu for a set of credentials and then select **Associate Subscription**.

You must select credentials that are associated with a Connector. You can't associate a marketplace subscription with credentials that are associated with BlueXP.



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**.

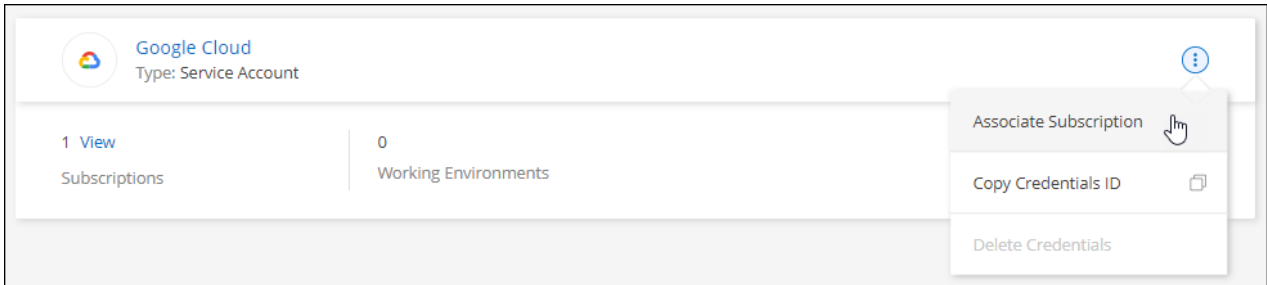
The following video shows the steps to subscribe from the Azure Marketplace:

[Subscribe to BlueXP from the Azure Marketplace](#)

## Google Cloud

### Steps

1. In the upper right of the BlueXP console, select the Settings icon, and select **Credentials**.
2. 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**.

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 Google Cloud product details page for NetApp BlueXP. At the top, there is a Google Cloud logo and a search bar containing 'netapp.com'. Below this is a navigation bar with a back arrow and the text 'Product details'. 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.' Below the description is a prominent blue 'SUBSCRIBE' button. A navigation menu includes links for 'OVERVIEW', '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.' The 'Additional details' section lists: 'Type: [SaaS & APIs](#)', 'Last updated: 12/19/22', and 'Category: [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.

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.

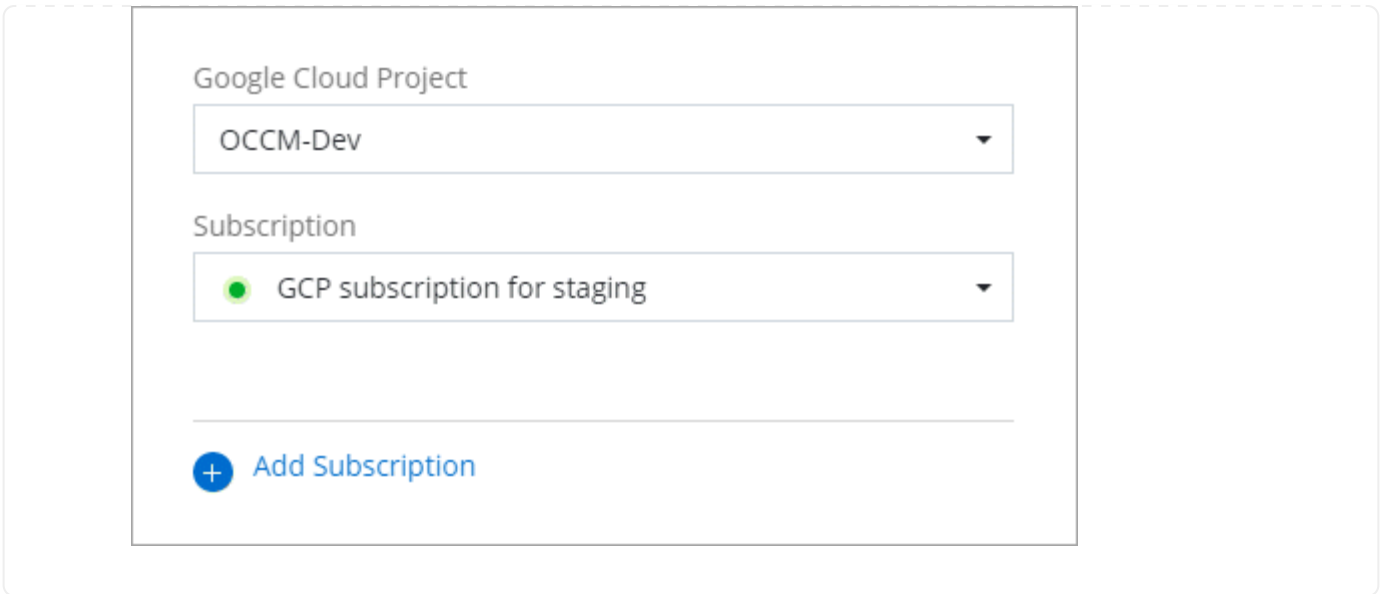
For all other accounts, you'll need to manually associate the subscription by repeating these steps.

- Select **Save**.

The following video shows the steps to subscribe from the Google Cloud Marketplace:

[Subscribe to BlueXP from the Google Cloud Marketplace](#)

g. Once this process is complete, navigate back to the Credentials page in BlueXP and select this new subscription.



### Related links

- [Manage BYOL capacity-based licenses for Cloud Volumes ONTAP](#)
- [Manage BYOL licenses for BlueXP data services](#)
- [Manage AWS credentials and subscriptions for BlueXP](#)
- [Manage Azure credentials and subscriptions for BlueXP](#)
- [Manage Google Cloud credentials and subscriptions for BlueXP](#)

## 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](#)



## Copyright information

Copyright © 2024 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.