# NetApp

# Advanced deployment

Set up and administration

NetApp
April 03, 2023

# Table of Contents

# Advanced deployment

## Create a Connector from the AWS Marketplace

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

> 💡 You can also download and install the Connector software on an existing Linux host in your network or in the cloud. Learn how to install the Connector on an existing Linux host.

### Create the Connector in an AWS commercial region

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

**Before you get started**

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

**Steps**

1. Set up permissions in AWS:

   a. From the IAM console, create the required policies by copying and pasting the contents of the IAM policies for the Connector.

   b. Create an IAM role with the role type Amazon EC2 and attach the policies that you created in the previous step to the role.

2. Go to the BlueXP page on the AWS Marketplace to deploy the Connector from an AMI:

3. On the Marketplace page, click **Continue to Subscribe** and then click **Continue to Configuration**.

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

5. Under **Choose Action**, select **Launch through EC2** and then click **Launch**.

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

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

   ◦ **Name and tags**: Enter a name and tags for the instance.

   ◦ **Application and OS Image**: Skip this section. The Connector AMI is already selected.

   ◦ **Instance type**: Depending on region availability, choose one of the supported instance types (t3.xlarge is recommended).

   Review the instance requirements.

   ◦ **Key pair (login)**: Select the key pair that you want to use to securely connect to the instance.

   ◦ **Network settings**: Edit the network settings as needed:

     ▪ Choose the desired VPC and subnet.

     ▪ Specify whether the instance should have a public IP address.

     ▪ Specify firewall settings that enable the required connection methods for the Connector instance: SSH, HTTP, and HTTPS.

- ◦ **Configure storage**: Keep the default storage options.
- ◦ **Advanced details**: Under **IAM instance profile**, choose the IAM role that you created in step 1.
- ◦ **Summary**: Review the summary and click **Launch instance**.

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

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

   https://*ipaddress*

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

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

      Learn about NetApp accounts.

   b. Enter a name for the system.

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

**Result**

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

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

## Create the Connector in an AWS Government region

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

**Steps**

1. Set up permissions in AWS:

   a. From the IAM console, create your own policy by copying and pasting the contents of the IAM policy for the Connector.

   b. Create an IAM role with the role type Amazon EC2 and attach the policy that you created in the previous step to the role.

2. Go to the BlueXP offering in the AWS Marketplace.

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

   a. Open the EC2 service and select **Launch instance**.

   b. Select **AWS Marketplace**.

   c. Search for BlueXP and select the offering.

    d. Click **Continue**.

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

- **Choose an Instance Type**: Depending on region availability, choose one of the supported instance types (t3.xlarge is recommended).

  Review the instance requirements.

- **Configure Instance Details**: Select a VPC and subnet, choose the IAM role that you created in step 1, enable termination protection (recommended), and choose any other configuration options that meet your requirements.



- **Add Storage**: Keep the default storage options.
- **Add Tags**: Enter tags for the instance, if desired.
- **Configure Security Group**: Specify the required connection methods for the Connector instance:

SSH, HTTP, and HTTPS.

  ◦ **Review**: Review your selections and click **Launch**.

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

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

  https://*ipaddress*

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

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

    Learn about NetApp accounts.

  b. Enter a name for the system.

**Result**

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

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

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

## Open port 3128 for AutoSupport messages

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

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

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

# Create a Connector from the Azure Marketplace

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

> 💡 You can also download and install the Connector software on an existing Linux host in your network or in the cloud. Learn how to install the Connector on an existing Linux host.

# Creating a Connector in Azure

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

**Steps**

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

   - Azure Marketplace page for commercial regions
   - Azure Marketplace page for Azure Government regions

2. Click **Get it now** and then click **Continue**.

3. From the Azure portal, click **Create** and follow the steps to configure the virtual machine.

   Note the following as you configure the VM:

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

     Review the VM requirements.

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

     Learn more about security group rules for the Connector.

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

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

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

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

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

   https://*ipaddress*

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

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

      Learn about NetApp accounts.

   b. Enter a name for the system.

**Result**

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

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

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

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

## Granting Azure permissions

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

**Steps**

1. Create a custom role:

   a. Copy the contents of the custom role permissions for the Connector and save them in a JSON file.

   b. Modify the JSON file by adding Azure subscription IDs to the assignable scope.

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

      **Example**

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

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

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

      - Start Azure Cloud Shell and choose the Bash environment.
      - Upload the JSON file.

- Use the Azure CLI to create the custom role:

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

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

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

   a. Open the **Subscriptions** service and then select the subscription in which you want to deploy Cloud Volumes ONTAP systems.

   b. Click **Access control (IAM)** > **Add** > **Add role assignment**.

   c. In the **Role** tab, select the **BlueXP Operator** role and click **Next**.

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

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

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

   e. Click **Review + assign**.

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

**Result**

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

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

## Open port 3128 for AutoSupport messages

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

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

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

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

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

Learn about other ways to deploy a Connector.

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

## Verify host requirements

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

**A dedicated host is required**

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

**CPU**

4 cores or 4 vCPUs

**RAM**

14 GB

**AWS EC2 instance type**

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

**Azure VM size**

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

**GCP machine type**

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

The Connector is supported in Google Cloud on a VM instance with an OS that supports Shielded VM features

**Supported operating systems**

- CentOS 7.6, 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 Red Hat Enterprise Linux system must be registered with Red Hat Subscription Management. If it is not registered, the system cannot access repositories to update required 3rd party software during Connector installation.

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

**Hypervisor**

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

**Disk space in /opt**

100 GiB of space must be available

**Disk space in /var**

20 GiB of space must be available

**Docker Engine**

Docker Engine version 19.3.1 or later is required on the host before you install the Connector. View installation instructions

**Outbound internet access**

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

- https://support.netapp.com

- https://mysupport.netapp.com

- https://cloudmanager.cloud.netapp.com/tenancy

- https://stream.cloudmanager.cloud.netapp.com

- https://cloudmanagerinfraprod.azurecr.io

- https://production-artifacts.cloudmanager.cloud.netapp.com

- https://*.blob.core.windows.net

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

# Install the Connector

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

**What you'll need**

- Root privileges to install the Connector.

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

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

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

**About this task**

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

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

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

**Steps**

1. Verify that docker is enabled and running.

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

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

   ```
   unset http_proxy
   unset https_proxy
   ```

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

3. Download the Connector software from the NetApp Support Site, and then copy it to the Linux host.

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

4. Assign permissions to run the script.

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

5. Run the installation script.

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

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

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

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

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

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

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

### Result

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

## Set up the Connector

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

### Steps

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

   https://*ipaddress*

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

2. Sign up or log in.

3. If you installed the Connector in Google Cloud, set up a service account that has the permissions that BlueXP needs to create and manage Cloud Volumes ONTAP systems in projects.

   a. Create a role in GCP that includes the permissions defined in the Connector policy for GCP.

   b. Create a GCP service account and apply the custom role that you just created.

   c. Associate this service account with the Connector VM.

d. If you want to deploy Cloud Volumes ONTAP in other projects, grant access by adding the service account with the BlueXP role to that project. You'll need to repeat this step for each project.

4. After you log in, set up BlueXP:

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

Learn about NetApp accounts.

b. Enter a name for the system.

**Result**

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

**After you finish**

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

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

# Install the Connector in a location with no internet access

You can install the Connector in a location that has complete isolation from the internet, either on premises or in a cloud region. You can then use the BlueXP services that are supported in that environment.

## On premises overview

In an on-premises environment without internet, you can use BlueXP to discover on-prem ONTAP clusters, replicate data between them, back up volumes using Cloud Backup, and scan them with Cloud Data Sense. No other BlueXP services are supported in this type of deployment, except for the Digital Wallet.

## Cloud overview

In a cloud region without internet, you can use BlueXP to deploy Cloud Volumes ONTAP systems and to discover on-premises ONTAP clusters (if there's a connection from your cloud environment to on your on-premises environment). You can also use Cloud Backup to back up Cloud Volumes ONTAP volumes in AWS and Azure commercial regions (Backup is not supported in AWS and Azure secret regions at this time). No other BlueXP services are supported in this type of deployment, except for the Digital Wallet.

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

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

## Verify host requirements

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

**A dedicated host is required**

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

**CPU**

4 cores or 4 vCPUs

**RAM**

14 GB

**Supported operating systems**

- CentOS 7.6, 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 Red Hat Enterprise Linux system must be registered with Red Hat Subscription Management. If it is not registered, the system cannot access repositories to update required 3rd party software during Connector installation.

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

**Hypervisor**

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

**Disk type**

An SSD is required

**Disk space in /opt**

100 GiB of space must be available

**Disk space in /var**

20 GiB of space must be available

**Docker Engine**

Docker Engine version 19 or later is required on the host before you install the Connector. View installation instructions

## Install the Connector

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

**Required privileges**

Root privileges are required to install the Connector.

**Steps**

1. Verify that docker is enabled and running.

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

2. Download the Connector installer for restricted networks without internet access from the NetApp Support Site

3. Copy the installer to the Linux host.

4. Assign permissions to run the script.

```
chmod +x /path/Cloud-Manager-Connector-offline-<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.

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

You should see the following screen.
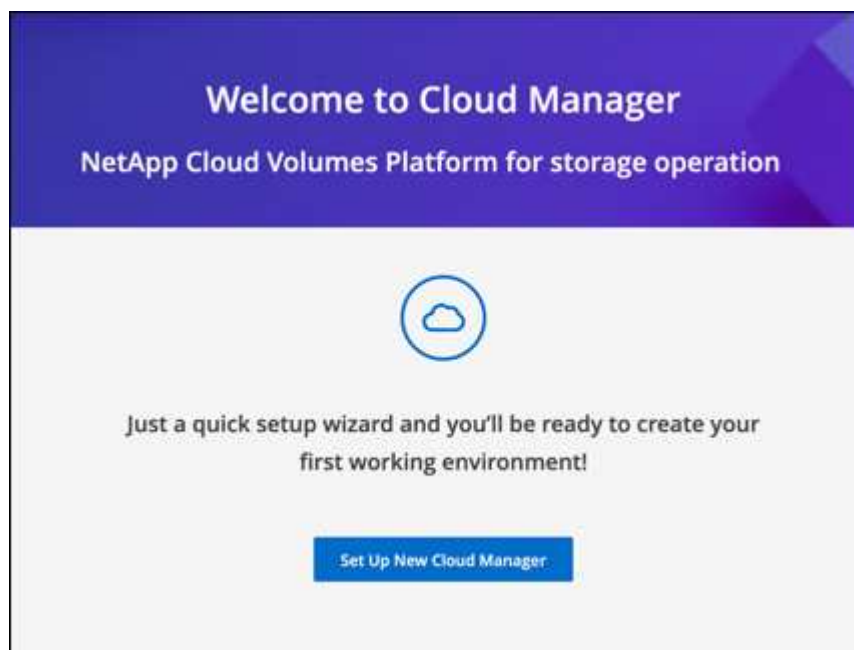


7. Click **Set Up New BlueXP** and follow the prompts to set up the system.
   ◦ **System Details**: Enter a name for the Connector and your company name.

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

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

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

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

**Result**

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

**What's next?**

In an on-prem environment:

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

In a cloud environment, you can deploy Cloud Volumes ONTAP

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