# AWS

## Setup and administration

NetApp
September 13, 2023

# Table of Contents

# AWS

## 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 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, but the deployment is initiated directly from the AWS Marketplace, rather than from BlueXP.

- 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.

## Create a Connector in AWS from BlueXP

To create a Connector in AWS from BlueXP, you need to set up your networking, prepare AWS permissions, and then create the Connector.

**Before you begin**

You should review Connector limitations.

### Step 1: Set up networking

Ensure that the network location where you plan to install the Connector supports the following requirements. Meeting these requirements enables the Connector to manage resources and processes within your hybrid cloud environment.

**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. For example, the network where you plan to create Cloud Volumes ONTAP systems or a storage system in your on-premises environment.

**Outbound internet access**

The network location where you deploy the Connector must have an outbound internet connection to contact specific endpoints.

### Endpoints contacted from the Connector

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

| Endpoints | Purpose |
|---|---|
| AWS services (amazonaws.com):<br>• CloudFormation<br>• Elastic Compute Cloud (EC2)<br>• Identity and Access Management (IAM)<br>• Key Management Service (KMS)<br>• Security Token Service (STS)<br>• Simple Storage Service (S3) | To manage resources in AWS. The exact endpoint depends on the AWS region that you're using. 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<br>https://api.bluexp.netapp.com<br>https://*.cloudmanager.cloud.netapp.com<br>https://cloudmanager.cloud.netapp.com<br>https://netapp-cloud-account.auth0.com | To provide SaaS features and services within BlueXP.<br>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<br>https://cloudmanagerinfraprod.azurecr.io | To upgrade the Connector and its Docker components. |

### Endpoints contacted from 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. This includes endpoints that are contacted to deploy the Connector from the BlueXP console.

View the list of endpoints contacted from 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. You'll need to provide this information during installation.

- 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.

## Step 2: Set up AWS permissions

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 manage AWS resources.

**Steps**

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

   As a reminder, this policy contains only the permissions needed to launch the Connector instance in AWS from BlueXP. View permissions required for the Connector instance itself.

```
{
    "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. Select **Next** and add tags, if needed.
6. Select **Next** and enter a name and description.
7. Select **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, select **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, select **Users** and then select the user name.
     b. Select **Add permissions > Attach existing policies directly**.
     c. Select the policy that you created.
     d. Select **Next** and then select **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.

## Step 3: Create the Connector

Create the Connector directly from the BlueXP web-based console.

**About this task**

Creating the Connector from BlueXP deploys an EC2 instance in AWS using a default configuration. Learn about the default configuration for the Connector.

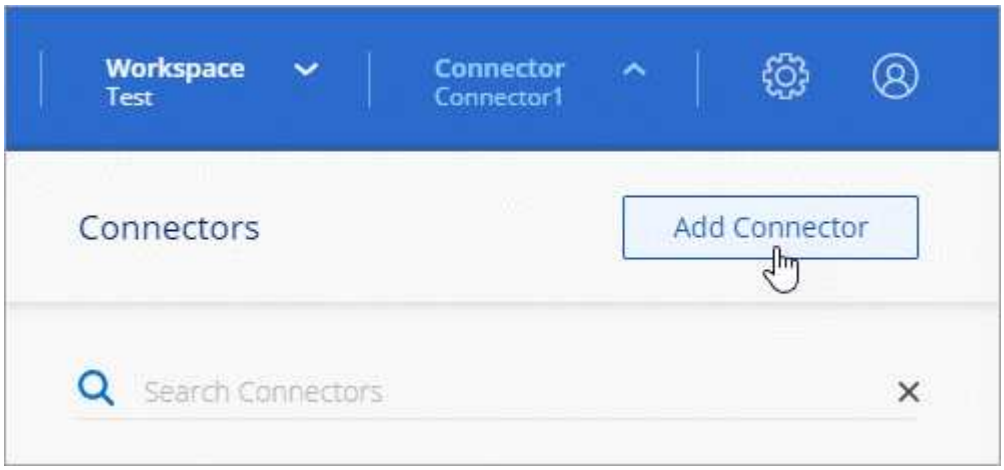
**Before you begin**

You should have the following:

- An AWS authentication method: either an IAM role or access keys for an IAM user with the required permissions.
- A VPC and subnet that meets 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. Select the **Connector** drop-down and select **Add Connector**.




2. Choose **Amazon Web Services** as your cloud provider and select **Continue**.
3. On the **Deploying a Connector** page, review the details about what you'll need. You have two options:
   a. Select **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. Select **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. Select **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.

# Create a Connector from the AWS Marketplace

To create a Connector from the AWS Marketplace, you need to set up your networking, prepare AWS permissions, review instance requirements, and then create the Connector.

**Before you begin**

You should review Connector limitations.

## Step 1: Set up networking

Ensure that the network location where you plan to install the Connector supports the following requirements. Meeting these requirements enables the Connector to manage resources and processes within your hybrid cloud environment.

**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. For example, the network where you plan to create Cloud Volumes ONTAP systems or a storage system in your on-premises environment.

**Outbound internet access**

The network location where you deploy the Connector must have an outbound internet connection to contact specific endpoints.

### Endpoints contacted from the Connector

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

| Endpoints | Purpose |
|---|---|
| AWS services (amazonaws.com):<br>• CloudFormation<br>• Elastic Compute Cloud (EC2)<br>• Identity and Access Management (IAM)<br>• Key Management Service (KMS)<br>• Security Token Service (STS)<br>• Simple Storage Service (S3) | To manage resources in AWS. The exact endpoint depends on the AWS region that you're using. 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<br>https://api.bluexp.netapp.com<br>https://*.cloudmanager.cloud.netapp.com<br>https://cloudmanager.cloud.netapp.com<br>https://netapp-cloud-account.auth0.com | To provide SaaS features and services within BlueXP.<br>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<br>https://cloudmanagerinfraprod.azurecr.io | 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. You'll need to provide this information during installation.

- 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.

## Step 2: Set up AWS permissions

To prepare for a marketplace deployment, 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. 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. 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 that you can associate with the EC2 instance during deployment from the AWS Marketplace.

## Step 3: Review instance requirements

When you create the Connector, you need to choose an EC2 instance type that meets the following requirements.

**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.

## Step 4: Create the Connector

Create the Connector directly from the AWS Marketplace.

### About this task

Creating the Connector from the AWS Marketplace deploys an EC2 instance in AWS using a default configuration. Learn about the default configuration for the Connector.

### Before you begin

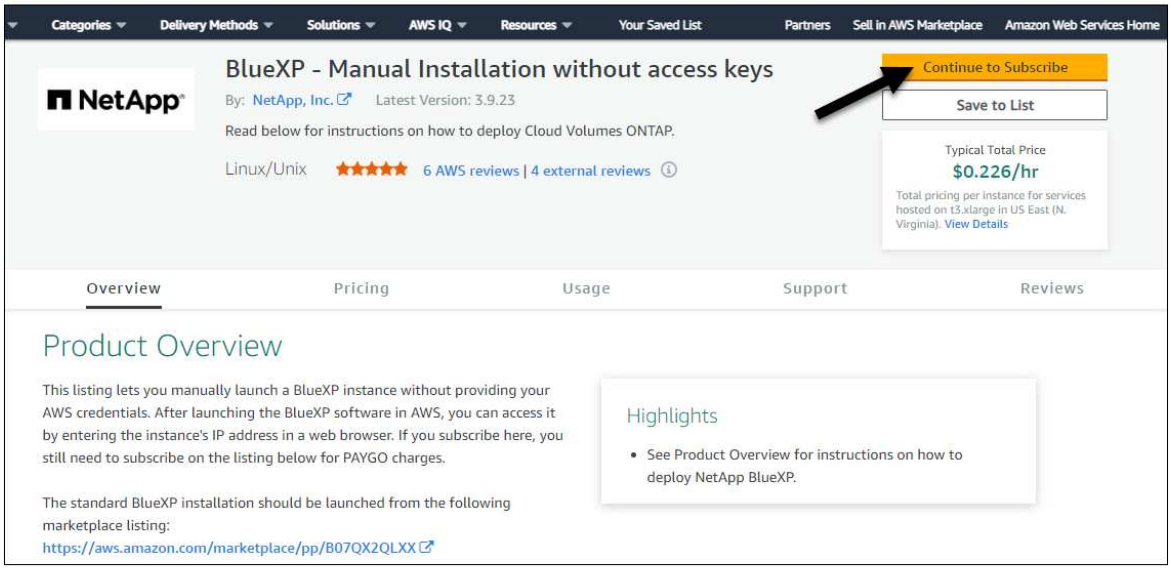
You should have the following:

- A VPC and subnet that meets networking requirements.
- An IAM role with an attached policy that includes the required permissions for the Connector.
- Permissions to subscribe and unsubscribe from the AWS Marketplace for your IAM user.
- An understanding of CPU and RAM requirements for the instance.
- A key pair for the EC2 instance.

### Steps

1. Go to the BlueXP page on the AWS Marketplace
2. On the Marketplace page, select **Continue to Subscribe** and then select **Continue to Configuration**.

a




b

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.xlarge 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 storage options.
   - **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**.

   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. Select **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.

# Manually install the Connector in AWS

To manually install the Connector on your own Linux host, you need to review host requirements, set up your networking, prepare AWS permissions, install the Connector, and then provide the permissions that you prepared.

**Before you begin**

You should review Connector limitations.

## Step 1: 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**

- Ubuntu 22.04
- CentOS 7.6, 7.7, 7.8, and 7.9
- Red Hat Enterprise Linux 7.6, 7.7, 7.8, and 7.9

  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 Ubuntu, 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, 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

## Step 2: Set up networking

Ensure that the network location where you plan to install the Connector supports the following requirements. Meeting these requirements enables the Connector to manage resources and processes within your hybrid cloud environment.

**Connections to target networks**

A Connector requires a network connection to the location where you're planning to create and manage working environments. For example, the network where you plan to create Cloud Volumes ONTAP systems or a storage system in your on-premises environment.

**Outbound internet access**

The network location where you deploy the Connector must have an outbound internet connection to contact specific endpoints.

**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://cloudmanagerinfraprod.azurecr.io

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

**Endpoints contacted from the Connector**

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

| Endpoints | Purpose |
| --- | --- |
| AWS services (amazonaws.com):<br>• CloudFormation<br>• Elastic Compute Cloud (EC2)<br>• Identity and Access Management (IAM)<br>• Key Management Service (KMS)<br>• Security Token Service (STS)<br>• Simple Storage Service (S3) | To manage resources in AWS. The exact endpoint depends on the AWS region that you're using. 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<br>https://api.bluexp.netapp.com<br>https://*.cloudmanager.cloud.netapp.com<br>https://cloudmanager.cloud.netapp.com<br>https://netapp-cloud-account.auth0.com | To provide SaaS features and services within BlueXP.<br>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<br>https://cloudmanagerinfraprod.azurecr.io | 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. You'll need to provide this information during installation.

- 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.

## Step 3: Set up permissions

You need to provide AWS permissions to BlueXP by using one of the following options:

- 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 the AWS access key for an IAM user who has the required permissions.

Follow the steps to prepare permissions for BlueXP.

**IAM role**

**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. 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 that you can associate with the EC2 instance after you install the Connector.

**AWS access key**

**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**

You now have an IAM user that has the required permissions and an access key that you can provide to BlueXP.

## Step 4: Install the Connector

After the pre-requisites are complete, you can manually install the software on your own Linux host.

**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.

- A CA-signed certificate, if the proxy server uses HTTPS or if the proxy is an intercepting proxy.

**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. 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

  The user must be a local user. Domain users are not supported.

--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. Select **Let's start**.

**Result**

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

## Step 5: Provide permissions to BlueXP

Now that you've installed the Connector, you need to provide BlueXP with the AWS permissions that you previously set up. Providing the permissions enables BlueXP to manage your data and storage infrastructure in 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 select **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, select the Settings icon, and select **Credentials**.


3. 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.

Go to the BlueXP console to start using the Connector with BlueXP.

## Copyright information



## Trademark information