



## **AWS**

### **Setup and administration**

NetApp  
June 19, 2023

# Table of Contents

- AWS ..... 1
  - Quick start to create a Connector in AWS ..... 1
  - Connector installation options in AWS ..... 2
  - Set up AWS networking ..... 3
  - Review Connector host requirements for AWS installs ..... 5
  - Set up AWS permissions ..... 6
  - Create a Connector in AWS ..... 11
  - Provide AWS permissions to BlueXP ..... 17

# AWS

## Quick start to create a Connector in AWS

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

1

### Understand your installation options

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

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

2

### Set up networking

Prepare the following for the Connector:

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

[Learn more about networking requirements.](#)

3

### Review host requirements

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

The key requirements are as follows:

- A dedicated host running Ubuntu 22.04, CentOS 7.6 to 7.9, or RHEL 7.6 to 7.9
- 4 CPUs
- 14 GB of RAM
- Docker Engine 19.3.1 or later

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

4

### Set up AWS permissions

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

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

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

5

### Create the Connector

Create the Connector using one of the available installation options:

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

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

6

### Provide BlueXP with permissions

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

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

## Connector installation options in AWS

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

The following installation options are available:

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

This action launches an EC2 instance running Linux and the Connector software in a VPC of your choice.

- Create a Connector from the AWS Marketplace

This action also launches an EC2 instance running Linux and the Connector software.

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

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

## Set up AWS networking

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

### VPC and subnet

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

### Connections to target networks

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

### Outbound internet access

The network location where you deploy the Connector must have an outbound internet connection. Outbound internet access is also required from your web browser when deploying the Connector from the BlueXP console.

### 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.](#)

### Endpoints contacted during manual installation


If you plan to manually install the Connector on your own Linux host, the installer for the Connector requires access to the following URLs during the installation process:

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

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

## Endpoints contacted 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): <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>	To manage resources in AWS. The exact endpoint depends on the region in which you deploy the Connector. <a href="#">Refer to AWS documentation for details</a>
https://support.netapp.com	To obtain licensing information and to send AutoSupport messages to NetApp support.
https://*.api.bluexp.netapp.com https://api.bluexp.netapp.com https://*.cloudmanager.cloud.netapp.com https://cloudmanager.cloud.netapp.com	To provide SaaS features and services within BlueXP. <div>The Connector is currently contacting "cloudmanager.cloud.netapp.com" but it will start contacting "api.bluexp.netapp.com" in an upcoming release.</div>
https://cloudmanagerinfraprod.azurecr.io https://*.blob.core.windows.net	To upgrade the Connector and its Docker components.

## Proxy server

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

- IP address
- Credentials
- HTTPS certificate

## Ports

There's no incoming traffic to the Connector, unless you initiate it or if the Connector is used as a proxy for AutoSupport messages.

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

outbound internet connection to send AutoSupport messages, BlueXP automatically configures those Cloud Volumes ONTAP systems to use a proxy server that's included with the Connector. The only requirement is to ensure that the Connector's security group allows inbound connections over port 3128. You'll need to open this port after you deploy the Connector.

## IP address limitation

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

# Review Connector host requirements for AWS installs

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

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

## Dedicated host

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

## Supported operating systems

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

### Disk space in /opt

100 GiB of space must be available

### Disk space in /var

20 GiB of space must be available

### Docker Engine

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

## Set up AWS permissions

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

You can choose from the following installation options:

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

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

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

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

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

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

## Set up permissions to create the Connector from BlueXP

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

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

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

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



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

### Steps

1. Go to the AWS IAM console.



2. Click **Policies > Create policy**.
3. Click **JSON**.
4. Copy and paste the following policy:

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](#).

```
{
  "Version": "2012-10-17",
  "Statement": [{
    "Effect": "Allow",
    "Action": [
      "iam:CreateRole",
      "iam>DeleteRole",
      "iam:PutRolePolicy",
      "iam:CreateInstanceProfile",
      "iam>DeleteRolePolicy",
      "iam:AddRoleToInstanceProfile",
      "iam:RemoveRoleFromInstanceProfile",
      "iam>DeleteInstanceProfile",
      "iam:PassRole",
      "ec2:DescribeInstanceStatus",
      "ec2:RunInstances",
      "ec2:ModifyInstanceAttribute",
      "ec2:CreateSecurityGroup",
      "ec2>DeleteSecurityGroup",
      "ec2:DescribeSecurityGroups",
      "ec2:RevokeSecurityGroupEgress",
      "ec2:AuthorizeSecurityGroupEgress",
      "ec2:AuthorizeSecurityGroupIngress",
      "ec2:RevokeSecurityGroupIngress",
      "ec2:CreateNetworkInterface",
      "ec2:DescribeNetworkInterfaces",
      "ec2>DeleteNetworkInterface",
      "ec2:ModifyNetworkInterfaceAttribute",
      "ec2:DescribeSubnets",
      "ec2:DescribeVpcs",
      "ec2:DescribeDhcpOptions",
      "ec2:DescribeKeyPairs",
      "ec2:DescribeRegions",
      "ec2:DescribeInstances",
      "ec2:CreateTags",
      "ec2:DescribeImages",
      "cloudformation:CreateStack",
      "cloudformation>DeleteStack",
      "cloudformation:DescribeStacks",
```

```

        "cloudformation:DescribeStackEvents",
        "cloudformation:ValidateTemplate",
        "ec2:AssociateIamInstanceProfile",
        "ec2:DescribeIamInstanceProfileAssociations",
        "ec2:DisassociateIamInstanceProfile",
        "iam:GetRole",
        "iam:TagRole",
        "iam:ListRoles",
        "kms:ListAliases"
    ],
    "Resource": "*"
},
{
    "Effect": "Allow",
    "Action": [
        "ec2:TerminateInstances"
    ],
    "Condition": {
        "StringLike": {
            "ec2:ResourceTag/OCCMInstance": "*"
        }
    },
    "Resource": [
        "arn:aws:ec2:*:*:instance/*"
    ]
}
]
}

```

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

- a. From the AWS IAM console, click **Users** and then select the user name.
- b. Click **Add permissions > Attach existing policies directly**.
- c. Select the policy that you created.
- d. Click **Next** and then click **Add permissions**.
- e. Ensure that you have the access key and secret key for the IAM user.

### Result

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

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

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

### Steps

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

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

For standard regions, the permissions are spread across two policies. Two policies are required due to a maximum character size limit for managed policies in AWS.

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

### Result

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

## Set up permissions to assign after manual installation

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

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

## IAM role

### Steps

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

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

For standard regions, the permissions are spread across two policies. Two policies are required due to a maximum character size limit for managed policies in AWS. [Learn more about IAM policies for the Connector](#).

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

### Result

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

## AWS access key

### Steps

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

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

For standard regions, the permissions are spread across two policies. Two policies are required due to a maximum character size limit for managed policies in AWS. [Learn more about IAM policies for the Connector](#).

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

### Result

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

## Create a Connector in AWS

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

## BlueXP

### What you'll need

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

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

- A VPC and subnet that meets networking requirements.

[Learn about networking requirements](#)

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

### Steps

1. Click the **Connector** drop-down and select **Add Connector**.



2. Choose **Amazon Web Services** as your cloud provider and click **Continue**.
3. On the **Deploying a Connector** page, review the details about what you'll need. You have two options:
  - a. Click **Continue** to prepare for deployment by using the in-product guide. Each step in the in-product guide includes the information that's contained on this page of the documentation.
  - b. Click **Skip to Deployment** if you already prepared by following the steps on this page.
4. Follow the steps in the wizard to create the Connector:
  - **Get Ready**: Review what you'll need.
  - **AWS Credentials**: Specify your AWS region and then choose an authentication method, which is either an IAM role that BlueXP can assume or an AWS access key and secret key.



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

- **Details**: Provide details about the Connector.

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

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

- **Security Group:** Choose whether to create a new security group or whether to select an existing security group that allows the required inbound and outbound rules.

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

- **Review:** Review your selections to verify that your set up is correct.

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

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

### Result

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

### AWS Marketplace

#### What you'll need

- A VPC and subnet that meets networking requirements.

[Learn about networking requirements.](#)

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

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

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

### Steps

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



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

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

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

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

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

[Review the instance requirements.](#)

- **Key pair (login):** Select the key pair that you want to use to securely connect to the instance.
- **Network settings:** Edit the network settings as needed:
  - Choose the desired VPC and subnet.
  - Specify whether the instance should have a public IP address.
  - Specify firewall settings that enable the required connection methods for the Connector instance: SSH, HTTP, and HTTPS.



A few more rule are required for specific configurations.

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

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

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

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

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

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

`https://ipaddress`

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

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

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

## Result

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

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

## Manual install

### What you'll need

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

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

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

### About this task

The 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. Click **Let's start**.

### Result

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

### What's next?

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

## Provide AWS permissions to BlueXP

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

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

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

### IAM role

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

### Steps

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

### Result

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

### AWS access key

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

### Steps

1. Ensure that the correct Connector is currently selected in BlueXP.
2. In the upper right of the BlueXP console, click the Settings icon, and select **Credentials**.



3. Click **Add Credentials** and follow the steps in the wizard.
  - a. **Credentials Location**: Select **Amazon Web Services > Connector**.
  - b. **Define Credentials**: Enter an AWS access key and secret key.
  - c. **Marketplace Subscription**: Associate a Marketplace subscription with these credentials by subscribing now or by selecting an existing subscription.
  - d. **Review**: Confirm the details about the new credentials and click **Add**.

### Result

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

## Copyright information

Copyright © 2023 NetApp, Inc. All Rights Reserved. Printed in the U.S. No part of this document covered by copyright may be reproduced in any form or by any means—graphic, electronic, or mechanical, including photocopying, recording, taping, or storage in an electronic retrieval system—without prior written permission of the copyright owner.

Software derived from copyrighted NetApp material is subject to the following license and disclaimer:

THIS SOFTWARE IS PROVIDED BY NETAPP “AS IS” AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, WHICH ARE HEREBY DISCLAIMED. IN NO EVENT SHALL NETAPP BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

NetApp reserves the right to change any products described herein at any time, and without notice. NetApp assumes no responsibility or liability arising from the use of products described herein, except as expressly agreed to in writing by NetApp. The use or purchase of this product does not convey a license under any patent rights, trademark rights, or any other intellectual property rights of NetApp.

The product described in this manual may be protected by one or more U.S. patents, foreign patents, or pending applications.

LIMITED RIGHTS LEGEND: Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (b)(3) of the Rights in Technical Data -Noncommercial Items at DFARS 252.227-7013 (FEB 2014) and FAR 52.227-19 (DEC 2007).

Data contained herein pertains to a commercial product and/or commercial service (as defined in FAR 2.101) and is proprietary to NetApp, Inc. All NetApp technical data and computer software provided under this Agreement is commercial in nature and developed solely at private expense. The U.S. Government has a non-exclusive, non-transferrable, nonsublicensable, worldwide, limited irrevocable license to use the Data only in connection with and in support of the U.S. Government contract under which the Data was delivered. Except as provided herein, the Data may not be used, disclosed, reproduced, modified, performed, or displayed without the prior written approval of NetApp, Inc. United States Government license rights for the Department of Defense are limited to those rights identified in DFARS clause 252.227-7015(b) (FEB 2014).

## Trademark information

NETAPP, the NETAPP logo, and the marks listed at <http://www.netapp.com/TM> are trademarks of NetApp, Inc. Other company and product names may be trademarks of their respective owners.