



# Create a Connector

## Setup and administration

NetApp  
June 05, 2023

# Table of Contents

- Create a Connector ..... 1
  - AWS ..... 1
  - Azure ..... 18
  - Google Cloud ..... 47
  - On premises ..... 64

# Create a Connector

## AWS

### Quick start to create a Connector in AWS

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

1

#### Understand your installation options

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

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

2

#### Set up networking

Prepare the following for the Connector:

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

[Learn more about networking requirements.](#)

3

#### Review host requirements

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.

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

## Set up AWS networking

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

### VPC and subnet

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

### Connections to target networks

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

### Outbound internet access

The network location where you deploy the Connector must have an outbound internet connection. 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>  <p>The Connector is currently contacting "cloudmanager.cloud.netapp.com" but it will start contacting "api.bluexp.netapp.com" in an upcoming release.</p> </div>
https://cloudmanagerinfraprod.azurecr.io https://*.blob.core.windows.net	To upgrade the Connector and its Docker components.

## Proxy server

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

- IP address
- Credentials
- HTTPS certificate

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

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

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

## Steps

1. Verify that docker is enabled and running.

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

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

```
unset http_proxy
unset https_proxy
```

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

3. Download the Connector software from the [NetApp Support Site](#), and then copy it to the Linux host.

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

4. Assign permissions to run the script.

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

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

5. Run the installation script.

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

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

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

```
./OnCommandCloudManager-V3.9.26 --proxy
https://user:password@10.0.0.30:8080/ --cacert
/tmp/cacert/certificate.cer
```

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

- `http://address:port`

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

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

6. Wait for the installation to complete.

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

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

`https://ipaddress`

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

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

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

### Result

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

### What's next?

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

## Provide AWS permissions to BlueXP

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

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

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

### IAM role

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

### Steps

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

### Result

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

### AWS access key

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

### Steps

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



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

### Result

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

## Azure

### Quick start to create a Connector in Azure

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

## 1

### Understand your installation options

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

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

## 2

### Set up networking

Prepare the following for the Connector:

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

[Learn more about networking requirements.](#)

## 3

### Review host requirements

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 Azure Marketplace, then these requirements are taken care of for you because the software is deployed from an image.

The key requirements are as follows:

- A dedicated host running 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 Azure permissions

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

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

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

## 5

### Create the Connector

Create the Connector using one of the available installation options:

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

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

## 6

### Provide BlueXP with permissions

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

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

## Connector installation options in Azure

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

The following installation options are available:

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

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

- Create a Connector from the Azure Marketplace

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

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

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

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

## Set up Azure networking

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

## VNet and subnet

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

## Azure region

The Connector should be deployed in the same Azure region as the Cloud Volumes ONTAP systems that it manages, or in the [Azure region pair](#) for the Cloud Volumes ONTAP systems. This requirement ensures that an Azure Private Link connection is used between Cloud Volumes ONTAP and its associated storage accounts.

[Learn how Cloud Volumes ONTAP uses an Azure Private Link](#)

## Connections to target networks

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

## Outbound internet access

The network location where you deploy the Connector must have an outbound internet connection. 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
<a href="https://management.azure.com">https://management.azure.com</a> <a href="https://login.microsoftonline.com">https://login.microsoftonline.com</a> <a href="https://blob.core.windows.net">https://blob.core.windows.net</a> <a href="https://core.windows.net">https://core.windows.net</a>	To manage resources in Azure public regions.
<a href="https://management.chinacloudapi.cn">https://management.chinacloudapi.cn</a> <a href="https://login.chinacloudapi.cn">https://login.chinacloudapi.cn</a> <a href="https://blob.core.chinacloudapi.cn">https://blob.core.chinacloudapi.cn</a> <a href="https://core.chinacloudapi.cn">https://core.chinacloudapi.cn</a>	To manage resources in Azure China regions.
<a href="https://support.netapp.com">https://support.netapp.com</a>	To obtain licensing information and to send AutoSupport messages to NetApp support.
<a href="https://*.api.bluexp.netapp.com">https://*.api.bluexp.netapp.com</a> <a href="https://api.bluexp.netapp.com">https://api.bluexp.netapp.com</a> <a href="https://*.cloudmanager.cloud.netapp.com">https://*.cloudmanager.cloud.netapp.com</a> <a href="https://cloudmanager.cloud.netapp.com">https://cloudmanager.cloud.netapp.com</a>	<div>  <p>The Connector is currently contacting "cloudmanager.cloud.netapp.com" but it will start contacting "api.bluexp.netapp.com" in an upcoming release.</p> </div>
<a href="https://cloudmanagerinfraprod.azurecr.io">https://cloudmanagerinfraprod.azurecr.io</a> <a href="https://*.blob.core.windows.net">https://*.blob.core.windows.net</a>	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 Azure installs

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

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

### Dedicated host

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

### Supported operating systems

- 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

### Azure VM size

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

### Disk space in /opt

100 GiB of space must be available

### Disk space in /var

20 GiB of space must be available

### Docker Engine

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

## Set up Azure permissions

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

You can choose from the following installation options:

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

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

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

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

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

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

### Set up permissions to create the Connector from BlueXP

To create a Connector from BlueXP, you need to provide BlueXP with a login that has the required permissions to create the Connector VM in Azure. You have two options:

1. Sign in with your Microsoft account when prompted. This account must have specific Azure permissions. This is the default option.
2. Provide details about an Azure AD service principal. This service principal also requires specific permissions.

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

#### Create a custom role

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

#### Steps

1. Copy the required permissions for a new custom role in Azure and save them in a JSON file.



This policy contains only the permissions needed to launch the Connector VM in Azure from BlueXP. Don't use this policy for other situations. When BlueXP creates the Connector, it applies a new set of permissions to the Connector VM that enables the Connector to manage the resources in your public cloud environment.

```
{  
  "Name": "Azure SetupAsService",  
  "Actions": [  
    "Microsoft.Compute/disks/delete",  
  ]  
}
```

```
"Microsoft.Compute/disks/read",
"Microsoft.Compute/disks/write",
"Microsoft.Compute/locations/operations/read",
"Microsoft.Compute/operations/read",
"Microsoft.Compute/virtualMachines/instanceView/read",
"Microsoft.Compute/virtualMachines/read",
"Microsoft.Compute/virtualMachines/write",
"Microsoft.Compute/virtualMachines/delete",
"Microsoft.Compute/virtualMachines/extensions/write",
"Microsoft.Compute/virtualMachines/extensions/read",
"Microsoft.Compute/availabilitySets/read",
"Microsoft.Network/locations/operationResults/read",
"Microsoft.Network/locations/operations/read",
"Microsoft.Network/networkInterfaces/join/action",
"Microsoft.Network/networkInterfaces/read",
"Microsoft.Network/networkInterfaces/write",
"Microsoft.Network/networkInterfaces/delete",
"Microsoft.Network/networkSecurityGroups/join/action",
"Microsoft.Network/networkSecurityGroups/read",
"Microsoft.Network/networkSecurityGroups/write",

"Microsoft.Network/virtualNetworks/checkIpAddressAvailability/read",
"Microsoft.Network/virtualNetworks/read",
"Microsoft.Network/virtualNetworks/subnets/join/action",
"Microsoft.Network/virtualNetworks/subnets/read",

"Microsoft.Network/virtualNetworks/subnets/virtualMachines/read",
"Microsoft.Network/virtualNetworks/virtualMachines/read",
"Microsoft.Network/publicIPAddresses/write",
"Microsoft.Network/publicIPAddresses/read",
"Microsoft.Network/publicIPAddresses/delete",
"Microsoft.Network/networkSecurityGroups/securityRules/read",
"Microsoft.Network/networkSecurityGroups/securityRules/write",
"Microsoft.Network/networkSecurityGroups/securityRules/delete",
"Microsoft.Network/publicIPAddresses/join/action",

"Microsoft.Network/locations/virtualNetworkAvailableEndpointServices/read",
"Microsoft.Network/networkInterfaces/ipConfigurations/read",
"Microsoft.Resources/deployments/operations/read",
"Microsoft.Resources/deployments/read",
"Microsoft.Resources/deployments/delete",
"Microsoft.Resources/deployments/cancel/action",
"Microsoft.Resources/deployments/validate/action",
"Microsoft.Resources/resources/read",
"Microsoft.Resources/subscriptions/operationresults/read",
```

```

        "Microsoft.Resources/subscriptions/resourceGroups/delete",
        "Microsoft.Resources/subscriptions/resourceGroups/read",

        "Microsoft.Resources/subscriptions/resourcegroups/resources/read",
        "Microsoft.Resources/subscriptions/resourceGroups/write",
        "Microsoft.Authorization/roleDefinitions/write",
        "Microsoft.Authorization/roleAssignments/write",

        "Microsoft.MarketplaceOrdering/offertypes/publishers/offers/plans/agreements/read",

        "Microsoft.MarketplaceOrdering/offertypes/publishers/offers/plans/agreements/write",
        "Microsoft.Network/networkSecurityGroups/delete",
        "Microsoft.Storage/storageAccounts/delete",
        "Microsoft.Storage/storageAccounts/write",
        "Microsoft.Resources/deployments/write",
        "Microsoft.Resources/deployments/operationStatuses/read",
        "Microsoft.Authorization/roleAssignments/read"
    ],
    "NotActions": [],
    "AssignableScopes": [],
    "Description": "Azure SetupAsService",
    "IsCustom": "true"
}

```

2. Modify the JSON by adding your Azure subscription ID to the assignable scope.

### Example

```

"AssignableScopes": [
  "/subscriptions/d333af45-0d07-4154-943d-c25fbzzzzzzz"
],

```

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

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

- a. Start [Azure Cloud Shell](#) and choose the Bash environment.
- b. Upload the JSON file.



c. Enter the following Azure CLI command:

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

You should now have a custom role called *Azure SetupAsService*. You can now apply this custom role to your user account or to a service principal.

#### Set up an authentication method

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

## Azure user account

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

### Steps

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



Azure SetupAsService is the default name provided in the Connector deployment policy for Azure. If you chose a different name for the role, then select that name instead.

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

### Result

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

## Service principal

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

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

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

1. Ensure that you have permissions in Azure to create an Active Directory application and to assign the application to a role.

For details, refer to [Microsoft Azure Documentation: Required permissions](#).

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



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

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

You've created the AD application and service principal.

#### Assign the custom role to the application

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

**Add role assignment** ...

[Got feedback?](#)

**Role** **Members** **Review + assign**

**Selected role** Cloud Manager Operator 3.9.12\_B

**Assign access to** ☒ User, group, or service principal ☐ Managed identity

**Members** [+ Select members](#)

- c. Search for the name of the application.

Here's an example:



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

The service principal now has the required Azure permissions to deploy the Connector.

If you want to deploy Cloud Volumes ONTAP from multiple Azure subscriptions, then you must bind the service principal to each of those subscriptions. BlueXP enables you to select the subscription that you want to use when deploying Cloud Volumes ONTAP.

#### **Add Windows Azure Service Management API permissions**

1. In the **Azure Active Directory** service, click **App registrations** and select the application.
2. Click **API permissions > Add a permission**.
3. Under **Microsoft APIs**, select **Azure Service Management**.



## Request API permissions

### Select an API

Microsoft APIs APIs my organization uses My APIs

#### Commonly used Microsoft APIs

**Microsoft Graph**  
Take advantage of the tremendous amount of data in Office 365, Enterprise Mobility + Security, and Windows 10. Access Azure AD, Excel, Intune, Outlook/Exchange, OneDrive, OneNote, SharePoint, Planner, and more through a single endpoint.



**Azure Batch**  
Schedule large-scale parallel and HPC applications in the cloud

**Azure Data Catalog**  
Programmatic access to Data Catalog resources to register, annotate and search data assets

**Azure Data Explorer**  
Perform ad-hoc queries on terabytes of data to build near real-time and complex analytics solutions

**Azure Data Lake**  
Access to storage and compute for big data analytic scenarios

**Azure DevOps**  
Integrate with Azure DevOps and Azure DevOps server

**Azure Import/Export**  
Programmatic control of import/export jobs

**Azure Key Vault**  
Manage your key vaults as well as the keys, secrets, and certificates within your Key Vaults

**Azure Rights Management Services**  
Allow validated users to read and write protected content

**Azure Service Management**  
Programmatic access to much of the functionality available through the Azure portal

**Azure Storage**  
Secure, massively scalable object and data lake storage for unstructured and semi-structured data

**Customer Insights**  
Create profile and interaction models for your products

**Data Export Service for Microsoft Dynamics 365**  
Export data from Microsoft Dynamics CRM organization to an external destination

- Click **Access Azure Service Management as organization users** and then click **Add permissions**.

## Request API permissions

[< All APIs](#)



Azure Service Management

<https://management.azure.com/> [Docs](#) [🔗](#)

What type of permissions does your application require?

### Delegated permissions

Your application needs to access the API as the signed-in user.

### Application permissions

Your application runs as a background service or daemon without a signed-in user.

Select permissions

[expand all](#)

Type to search

PERMISSION

ADMIN CONSENT REQUIRED



user\_impersonation

Access Azure Service Management as organization users (preview) ⓘ

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

1. In the **Azure Active Directory** service, click **App registrations** and select the application.
2. Copy the **Application (client) ID** and the **Directory (tenant) ID**.



When you add the Azure account to BlueXP, you need to provide the application (client) ID and the directory (tenant) ID for the application. BlueXP uses the IDs to programmatically sign in.


## Create a client secret

1. Open the **Azure Active Directory** service.
2. Click **App registrations** and select your application.
3. Click **Certificates & secrets > New client secret**.
4. Provide a description of the secret and a duration.
5. Click **Add**.
6. Copy the value of the client secret.

## Client secrets

A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.

[+ New client secret](#)

DESCRIPTION	EXPIRES	VALUE	
test secret	8/16/2020	*sZ1jSe2By:D*-ZRoV4NLfdAcY7:+0vA	 <a href="#">Copy to clipboard</a>

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

### Result

Your service principal is now setup and you should have copied the application (client) ID, the directory (tenant) ID, and the value of the client secret. You need to enter this information in BlueXP when you create the Connector.

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

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

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

## Custom role

### Steps

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

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

2. Copy the contents of the [custom role permissions for the Connector](#) and save them in a JSON file.
3. Modify the JSON file by adding Azure subscription IDs to the assignable scope.

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

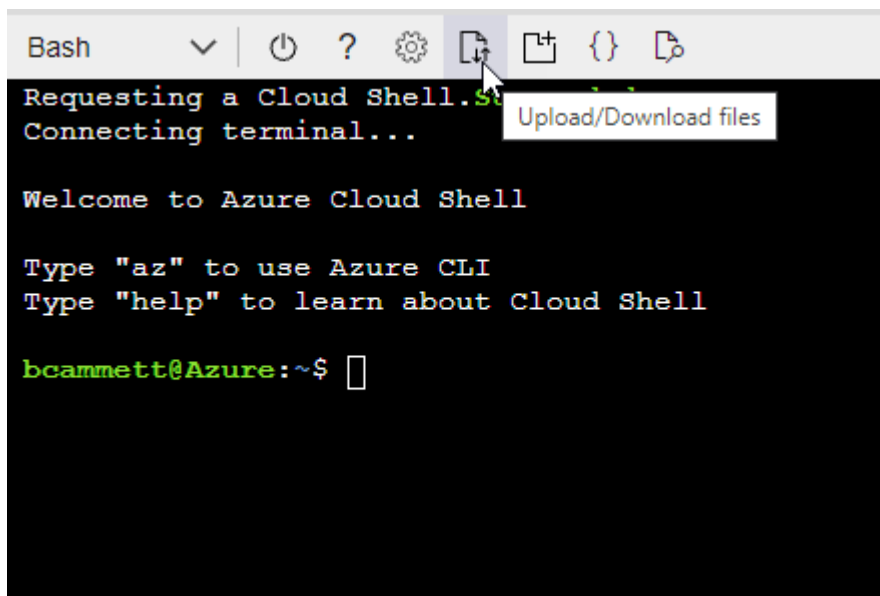
### Example

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

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

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

- a. Start [Azure Cloud Shell](#) and choose the Bash environment.
- b. Upload the JSON file.



- c. Use the Azure CLI to create the custom role:

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

## Result

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

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

## Service principal

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

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

1. Ensure that you have permissions in Azure to create an Active Directory application and to assign the application to a role.

For details, refer to [Microsoft Azure Documentation: Required permissions](#).

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



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

You've created the AD application and service principal.

### Assign the custom role to the application

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

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



- c. Search for the name of the application.

Here's an example:



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

The service principal now has the required Azure permissions to deploy the Connector.

If you want to deploy Cloud Volumes ONTAP from multiple Azure subscriptions, then you must bind the service principal to each of those subscriptions. BlueXP enables you to select the subscription that you want to use when deploying Cloud Volumes ONTAP.

## Add Windows Azure Service Management API permissions

1. In the **Azure Active Directory** service, click **App registrations** and select the application.
2. Click **API permissions > Add a permission**.
3. Under **Microsoft APIs**, select **Azure Service Management**.

### Request API permissions

Select an API

Microsoft APIs APIs my organization uses My APIs

#### Commonly used Microsoft APIs

##### Microsoft Graph

Take advantage of the tremendous amount of data in Office 365, Enterprise Mobility + Security, and Windows 10. Access Azure AD, Excel, Intune, Outlook/Exchange, OneDrive, OneNote, SharePoint, Planner, and more through a single endpoint.



##### Azure Batch

Schedule large-scale parallel and HPC applications in the cloud

##### Azure Data Catalog

Programmatic access to Data Catalog resources to register, annotate and search data assets

##### Azure Data Explorer

Perform ad-hoc queries on terabytes of data to build near real-time and complex analytics solutions

##### Azure Data Lake

Access to storage and compute for big data analytic scenarios

##### Azure DevOps

Integrate with Azure DevOps and Azure DevOps server

##### Azure Import/Export

Programmatic control of import/export jobs

##### Azure Key Vault

Manage your key vaults as well as the keys, secrets, and certificates within your Key Vaults

##### Azure Rights Management Services

Allow validated users to read and write protected content

##### Azure Service Management

Programmatic access to much of the functionality available through the Azure portal

##### Azure Storage

Secure, massively scalable object and data lake storage for unstructured and semi-structured data

##### Customer Insights

Create profile and interaction models for your products

##### Data Export Service for Microsoft Dynamics 365

Export data from Microsoft Dynamics CRM organization to an external destination

4. Click **Access Azure Service Management as organization users** and then click **Add permissions**.



## Request API permissions

[← All APIs](#)



Azure Service Management

<https://management.azure.com/> [Docs](#) [↗](#)

What type of permissions does your application require?

### Delegated permissions

Your application needs to access the API as the signed-in user.

### Application permissions

Your application runs as a background service or daemon without a signed-in user.

Select permissions

[expand all](#)

Type to search

PERMISSION

ADMIN CONSENT REQUIRED



user\_impersonation

Access Azure Service Management as organization users (preview) ⓘ

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

1. In the **Azure Active Directory** service, click **App registrations** and select the application.
2. Copy the **Application (client) ID** and the **Directory (tenant) ID**.

Delete Endpoints

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

Display name : test-service-principal

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

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

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

When you add the Azure account to BlueXP, you need to provide the application (client) ID and the directory (tenant) ID for the application. BlueXP uses the IDs to programmatically sign in.

## Create a client secret

1. Open the **Azure Active Directory** service.
2. Click **App registrations** and select your application.
3. Click **Certificates & secrets > New client secret**.
4. Provide a description of the secret and a duration.
5. Click **Add**.
6. Copy the value of the client secret.



## Client secrets

A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.

[+ New client secret](#)

DESCRIPTION	EXPIRES	VALUE	
test secret	8/16/2020	*sZ1jSe2By:D*-ZRoV4NLfdAcY7:+0vA	 <a href="#">Copy to clipboard</a>

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

### Result

Your service principal is now setup and you should have copied the application (client) ID, the directory (tenant) ID, and the value of the client secret. You need to enter this information in BlueXP when you add an Azure account.

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

## Create a Connector in Azure

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

## BlueXP

### What you'll need

- An Azure subscription.
- A VNet and subnet in your Azure region of choice.
- Details about a proxy server, if your organization requires a proxy for all outgoing internet traffic:
  - IP address
  - Credentials
  - HTTPS certificate
- An SSH public key, if you want to use that authentication method for the Connector virtual machine. The other option for the authentication method is to use a password.

[Learn about connecting to a Linux VM in Azure](#)

- If you don't want BlueXP to automatically create an Azure role for the Connector, then you'll need to create your own [using the policy on this page](#).

These permissions are for the Connector instance itself. It's a different set of permissions than what you previously set up to simply deploy the Connector.

### Steps

1. If you're creating your first Working Environment, click **Add Working Environment** and follow the prompts. Otherwise, click the **Connector** drop-down and select **Add Connector**.



2. Choose **Microsoft Azure** as your cloud provider.
3. On the **Deploying a Connector** page:
  - a. Under **Authentication**, select the authentication option that matches how you set up Azure permissions:
    - Select **Azure user account** to log in to your Microsoft account, which should have the required permissions.

The form is owned and hosted by Microsoft. Your credentials are not provided to NetApp.



If you're already logged in to an Azure account, then BlueXP will automatically use that account. If you have multiple accounts, then you might need to log out first to ensure that you're using the right account.

- Select **Active Directory service principal** to enter information about the Azure Active Directory service principal that grants the required permissions:
  - Application (client) ID
  - Directory (tenant) ID
  - Client Secret

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

4. Follow the steps in the wizard to create the Connector:

- **VM Authentication:** Choose an Azure subscription, a location, a new resource group or an existing resource group, and then choose an authentication method for the Connector virtual machine that you're creating.

The authentication method for the virtual machine can be a password or an SSH public key.

[Learn about connecting to a Linux VM in Azure](#)

- **Details:** Enter a name for the instance, specify tags, and choose whether you want BlueXP to create a new role that has the required permissions, or if you want to select an existing role that you set up with [the required permissions](#).

Note that you can choose the subscriptions associated with this role. Each subscription that you choose provides the Connector with permissions to deploy Cloud Volumes ONTAP in those subscriptions.

- **Network:** Choose a VNet and subnet, whether to enable a public IP address, and optionally specify a proxy configuration.
- **Security Group:** Choose whether to create a new security group or whether to select an existing security group that allows the required inbound and outbound rules.

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

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

5. Click **Add**.

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

## Result

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

## Azure Marketplace

### Steps

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

[Azure Marketplace page for commercial regions](#)

2. Click **Get it now** and then click **Continue**.
3. From the Azure portal, click **Create** and follow the steps to configure the virtual machine.

Note the following as you configure the VM:

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

[Review the VM requirements.](#)

- For the network security group, the Connector requires inbound connections using SSH, HTTP, and HTTPS. A few more rule are required for specific configurations.

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

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

This setting is important because a managed identity allows the Connector virtual machine to identify itself to Azure Active Directory without providing any credentials. After you're done, you'll need to assign the custom role that you created to [Learn more about managed identities for Azure resources](#).

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

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

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

`https://ipaddress`

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

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

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

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

### What's next?

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

### Manual install

### What you'll need

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

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

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

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

### About this task

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

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

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

### Steps

1. Verify that docker is enabled and running.

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

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

```
unset http_proxy
unset https_proxy
```

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

3. Download the Connector software from the [NetApp Support Site](#), and then copy it to the Linux host.

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

4. Assign permissions to run the script.

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

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

5. Run the installation script.

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

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

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

```
./OnCommandCloudManager-V3.9.26 --proxy  
https://user:password@10.0.0.30:8080/ --cacert  
/tmp/cacert/certificate.cer
```

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

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

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

6. Wait for the installation to complete.

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

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

`https://ipaddress`

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

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

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

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

## Result

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

**What's next?**

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

**Provide Azure permissions to BlueXP**

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

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

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

## Custom role

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

### Steps

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



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

4. In the **Members** tab, complete the following steps:
  - a. Assign access to a **Managed identity**.
  - b. Click **Select members**, select the subscription in which the Connector virtual machine was created, choose **Virtual machine**, and then select the Connector virtual machine.
  - c. Click **Select**.
  - d. Click **Next**.
  - e. Click **Review + assign**.
  - f. If you want to deploy Cloud Volumes ONTAP from additional subscriptions, switch to that subscription and then repeat these steps.

## Result

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

## What's next?

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

## Service principal

### Steps

1. Go to the [BlueXP console](#) and log in.
2. In the upper right of the BlueXP console, click the Settings icon, and select **Credentials**.



3. Click **Add Credentials** and follow the steps in the wizard.
  - a. **Credentials Location:** Select **Microsoft Azure > Connector**.
  - b. **Define Credentials:** Enter information about the Azure Active Directory service principal that grants the required permissions:
    - Application (client) ID
    - Directory (tenant) ID
    - Client Secret



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

#### Result

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

## Google Cloud

### Quick start to create a Connector in Google Cloud

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

1

#### Understand your installation options

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

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

2

#### Set up networking

Prepare the following for the Connector:

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

[Learn more about networking requirements.](#)

3

#### Review host requirements

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 by using gcloud, then these requirements are taken care of for you because the software is deployed from an image.

The key requirements are as follows:

- A dedicated host running 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 Google Cloud permissions

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

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

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

5

#### Enable Google Cloud APIs

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

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

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

6

#### Create the Connector

Create the Connector using one of the available installation options:

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

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

7

#### Provide BlueXP with permissions

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

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

## Connector installation options in Google Cloud

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

The following installation options are available:

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

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

- Create the Connector using gcloud

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

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

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

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

## Set up Google Cloud networking

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

### VPC and subnet

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

### Connections to target networks

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

### Outbound internet access

The network location where you deploy the Connector must have an outbound internet connection. 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
<a href="https://www.googleapis.com/compute/v1/">https://www.googleapis.com/compute/v1/</a> <a href="https://compute.googleapis.com/compute/v1">https://compute.googleapis.com/compute/v1</a> <a href="https://cloudresourcemanager.googleapis.com/v1/projects">https://cloudresourcemanager.googleapis.com/v1/projects</a> <a href="https://www.googleapis.com/compute/beta">https://www.googleapis.com/compute/beta</a> <a href="https://storage.googleapis.com/storage/v1">https://storage.googleapis.com/storage/v1</a> <a href="https://www.googleapis.com/storage/v1">https://www.googleapis.com/storage/v1</a> <a href="https://iam.googleapis.com/v1">https://iam.googleapis.com/v1</a> <a href="https://cloudkms.googleapis.com/v1">https://cloudkms.googleapis.com/v1</a> <a href="https://www.googleapis.com/deploymentmanager/v2/projects">https://www.googleapis.com/deploymentmanager/v2/projects</a>	To manage resources in Google Cloud.
<a href="https://support.netapp.com">https://support.netapp.com</a>	To obtain licensing information and to send AutoSupport messages to NetApp support.
<a href="https://*.api.bluelxp.netapp.com">https://*.api.bluelxp.netapp.com</a> <a href="https://api.bluelxp.netapp.com">https://api.bluelxp.netapp.com</a> <a href="https://*.cloudmanager.cloud.netapp.com">https://*.cloudmanager.cloud.netapp.com</a> <a href="https://cloudmanager.cloud.netapp.com">https://cloudmanager.cloud.netapp.com</a>	To provide SaaS features and services within BlueXP.   The Connector is currently contacting "cloudmanager.cloud.netapp.com" but it will start contacting "api.bluelxp.netapp.com" in an upcoming release.
<a href="https://cloudmanagerinfraproduct.azurecr.io">https://cloudmanagerinfraproduct.azurecr.io</a> <a href="https://*.blob.core.windows.net">https://*.blob.core.windows.net</a>	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 Google Cloud installs

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

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

### Dedicated host

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

### Supported operating systems

- 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

## Google Cloud machine type

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

The Connector is supported in Google Cloud on a VM instance with an OS that supports [Shielded VM features](#)

## Disk space in /opt

100 GiB of space must be available

## Disk space in /var

20 GiB of space must be available

## Docker Engine

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

## Set up Google Cloud permissions

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

You need to set up Google Cloud permissions as follows:

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

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

Depending on your configuration, you might need to complete the following steps as well:

- Set up permissions across projects
- Set up permissions for a shared VPC

## Set up permissions to create the Connector from BlueXP or gcloud

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

## Steps

1. Create a custom role in Google Cloud:
  - a. Create a YAML file that includes the following permissions:

```
title: Connector deployment policy
description: Permissions for the user who deploys the Connector from
BlueXP
stage: GA
includedPermissions:
- compute.disks.create
- compute.disks.get
- compute.disks.list
- compute.disks.setLabels
- compute.disks.use
- compute.firewalls.create
- compute.firewalls.delete
- compute.firewalls.get
- compute.firewalls.list
- compute.globalOperations.get
- compute.images.get
- compute.images.getFromFamily
- compute.images.list
- compute.images.useReadOnly
- compute.instances.attachDisk
- compute.instances.create
- compute.instances.get
- compute.instances.list
- compute.instances.setDeletionProtection
- compute.instances.setLabels
- compute.instances.setMachineType
- compute.instances.setMetadata
- compute.instances.setTags
- compute.instances.start
- compute.instances.updateDisplayDevice
- compute.machineTypes.get
- compute.networks.get
- compute.networks.list
- compute.networks.updatePolicy
- compute.projects.get
- compute.regions.get
- compute.regions.list
- compute.subnetworks.get
- compute.subnetworks.list
- compute.zoneOperations.get
- compute.zones.get
- compute.zones.list
- deploymentmanager.compositeTypes.get
```

```

- deploymentmanager.compositeTypes.list
- deploymentmanager.deployments.create
- deploymentmanager.deployments.delete
- deploymentmanager.deployments.get
- deploymentmanager.deployments.list
- deploymentmanager.manifests.get
- deploymentmanager.manifests.list
- deploymentmanager.operations.get
- deploymentmanager.operations.list
- deploymentmanager.resources.get
- deploymentmanager.resources.list
- deploymentmanager.typeProviders.get
- deploymentmanager.typeProviders.list
- deploymentmanager.types.get
- deploymentmanager.types.list
- resourcemanager.projects.get
- compute.instances.setServiceAccount
- iam.serviceAccounts.list

```

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

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

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

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

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

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

## Result

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

## Set up permissions for the Connector

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

## Steps

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



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

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

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

2. Create a service account in Google Cloud:

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

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

## Result

The service account for the Connector VM is set up.

## Set up permissions across projects

If you plan to deploy Cloud Volumes ONTAP systems in different projects than the project where the Connector resides, then you'll need to provide the Connector's service account with access to those projects.

For example, let's say the Connector is in project 1 and you want to create Cloud Volumes ONTAP systems in project 2. You'll need to grant access to the service account in project 2.

## Steps

1. In the Google Cloud console, go to the IAM service and select the project where you want to create Cloud Volumes ONTAP systems.
2. On the **IAM** page, select **Grant Access** and provide the required details.
  - Enter the email of the Connector's service account.
  - Select the Connector's custom role.
  - Click **Save**.

For more details, refer to [Google Cloud documentation](#)

## Set up shared VPC permissions

If you are using a shared VPC to deploy resources into a service project, then you'll need to prepare your permissions.

This table is for reference and your environment should reflect the permissions table when IAM configuration is complete.

Identity	Creator	Hosted in	Service project permissions	Host project permissions	Purpose
Google account to deploy the Connector	Custom	Service Project	<a href="#">Connector deployment policy</a>	compute.networkUser	Deploying the Connector in the service project
Connector service account	Custom	Service project	<a href="#">Connector service account policy</a>	<ul style="list-style-type: none"> <li>• compute.networkUser</li> <li>• deploymentmanager.editor</li> </ul>	Deploying and maintaining Cloud Volumes ONTAP and services in the service project
Cloud Volumes ONTAP service account	Custom	Service project	<ul style="list-style-type: none"> <li>• storage.admin</li> <li>• member: BlueXP service account as serviceAccount.user</li> </ul>	N/A	(Optional) For data tiering and BlueXP backup and recovery
Google APIs service agent	Google Cloud	Service project	(Default) Editor	compute.networkUser	Interacts with Google Cloud APIs on behalf of deployment. Allows BlueXP to use the shared network.
Google Compute Engine default service account	Google Cloud	Service project	(Default) Editor	compute.networkUser	Deploys Google Cloud instances and compute infrastructure on behalf of deployment. Allows BlueXP to use the shared network.

#### Notes:

1. deploymentmanager.editor is only required at the host project if you are not passing firewall rules to the deployment and are choosing to let BlueXP create them for you. BlueXP will create a deployment in the host project which contains the VPC0 firewall rule if no rule is specified.
2. firewall.create and firewall.delete are only required if you are not passing firewall rules to the deployment and are choosing to let BlueXP create them for you. These permissions reside in the BlueXP account .yaml file. If you are deploying an HA pair using a shared VPC, these permissions will be used to create the firewall rules for VPC1, 2 and 3. For all other deployments, these permissions will also be used to create rules for VPC0.
3. For data tiering, the tiering service account must have the serviceAccount.user role on the service account, not just at the project level. Currently if you assign serviceAccount.user at the project level, the permissions don't show when you query the service account with getIAMPolicy.

## Enable Google Cloud APIs

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

### Step

1. Enable the following Google Cloud APIs in your project:

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

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

[Google Cloud documentation: Enabling APIs](#)

## Create a Connector in Google Cloud

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

## BlueXP

### What you'll need

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

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

- A VPC and subnet that meets networking requirements.

[Learn about networking requirements](#)

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

### Steps

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



2. Choose **Google Cloud Platform** as your cloud provider.
3. On the **Deploying a Connector** page, review the details about what you'll need. You have two options:
  - a. Click **Continue** to prepare for deployment by using the in-product guide. Each step in the in-product guide includes the information that's contained on this page of the documentation.
  - b. Click **Skip to Deployment** if you already prepared by following the steps on this page.
4. Follow the steps in the wizard to create the Connector:
  - If you're prompted, log in to your Google account, which should have the required permissions to create the virtual machine instance.

The form is owned and hosted by Google. Your credentials are not provided to NetApp.

- **Details:** Enter a name for the virtual machine instance, specify tags, select a project, and then select the service account that has the required permissions (refer to the section above for details).
- **Location:** Specify a region, zone, VPC, and subnet for the instance.
- **Network:** Choose whether to enable a public IP address and optionally specify a proxy configuration.
- **Firewall Policy:** Choose whether to create a new firewall policy or whether to select an existing

firewall policy that allows the required inbound and outbound rules.

### [Firewall rules in Google Cloud](#)

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

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

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

### **Result**

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

### **gcloud**

#### **What you'll need**

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

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

- A VPC and subnet that meets networking requirements.

[Learn about networking requirements](#)

### **Steps**

#### 1. Log in to the gcloud SDK using your preferred methodology.

In our examples, we'll use a local shell with the gcloud SDK installed, but you could use the native Google Cloud Shell in the Google Cloud console.

For more information about the Google Cloud SDK, visit the [Google Cloud SDK documentation page](#).

#### 2. Verify that you are logged in as a user who has the required permissions that are defined in the section above:

```
gcloud auth list
```

The output should show the following where the \* user account is the desired user account to be logged in as:

## Credentialed Accounts

ACTIVE ACCOUNT

some\_user\_account@domain.com

\* desired\_user\_account@domain.com

To set the active account, run:

```
$ gcloud config set account `ACCOUNT`
```

Updates are available for some Cloud SDK components. To install them,

please run:

```
$ gcloud components update
```

### 3. Run the `gcloud compute instances create` command:

```
gcloud compute instances create <instance-name>
  --machine-type=n2-standard-4
  --image-project=netapp-cloudmanager
  --image-family=cloudmanager
  --scopes=cloud-platform
  --project=<project>
  --service-account=<service-account>
  --zone=<zone>
  --no-address
  --tags <network-tag>
  --network <network-path>
  --subnet <subnet-path>
  --boot-disk-kms-key <kms-key-path>
```

#### **instance-name**

The desired instance name for the VM instance.

#### **project**

(Optional) The project where you want to deploy the VM.

#### **service-account**

The service account specified in the output from step 2.

#### **zone**

The zone where you want to deploy the VM

#### **no-address**

(Optional) No external IP address is used (you need a cloud NAT or proxy to route traffic to the public internet)

#### **network-tag**

(Optional) Add network tagging to link a firewall rule using tags to the Connector instance

**network-path**

(Optional) Add the name of the network to deploy the Connector into (for a Shared VPC, you need the full path)

**subnet-path**

(Optional) Add the name of the subnet to deploy the Connector into (for a Shared VPC, you need the full path)

**kms-key-path**

(Optional) Add a KMS key to encrypt the Connector's disks (IAM permissions also need to be applied)

For more information about these flags, visit the [Google Cloud compute SDK documentation](#).

Running the command deploys the Connector using the NetApp golden image. The Connector instance and software should be running in approximately five minutes.

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

`https://ipaddress`

5. After you log in, set up the Connector:
  - a. Specify the BlueXP account to associate with the Connector.

[Learn about BlueXP accounts](#).

- b. Enter a name for the system.

**Result**

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

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

**Manual install****What you'll need**

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

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

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

**About this task**

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

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

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

## Steps

1. Verify that docker is enabled and running.

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

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

```
unset http_proxy
unset https_proxy
```

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

3. Download the Connector software from the [NetApp Support Site](#), and then copy it to the Linux host.

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

4. Assign permissions to run the script.

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

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

5. Run the installation script.

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

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

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

```
./OnCommandCloudManager-V3.9.26 --proxy
https://user:password@10.0.0.30:8080/ --cacert
/tmp/cacert/certificate.cer
```

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

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



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

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

6. Wait for the installation to complete.

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

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

`https://ipaddress`

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

- 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 Google Cloud permissions to BlueXP

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

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

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

### Steps

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

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

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

## Result

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

# On premises

## Quick start to create a Connector on premises

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

1

### Set up networking

Prepare the following for the Connector:

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

[Learn more about networking requirements.](#)

2

### Review host requirements

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

- A dedicated host running 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.](#)

3

### Set up cloud permissions

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

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

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

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

## 4

### Install the Connector software

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

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

## 5

### Provide BlueXP with permissions

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

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

## Set up on-prem networking

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

### Connections to target networks

A Connector requires a network connection to the type of working environment that you're creating and the services that you're planning to enable.

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

### Outbound internet access

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

### Endpoints contacted during manual installation

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

- <https://support.netapp.com>
- <https://mysupport.netapp.com>
- <https://cloudmanager.cloud.netapp.com/tenancy>
- <https://stream.cloudmanager.cloud.netapp.com>
- <https://cloudmanagerinfraproduct.azurecr.io>
- <https://production-artifacts.cloudmanager.cloud.netapp.com>
- [https://\\*.blob.core.windows.net](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>
<a href="https://management.azure.com">https://management.azure.com</a> <a href="https://login.microsoftonline.com">https://login.microsoftonline.com</a>	To manage resources in Azure public regions.
<a href="https://management.chinacloudapi.cn">https://management.chinacloudapi.cn</a> <a href="https://login.chinacloudapi.cn">https://login.chinacloudapi.cn</a>	To manage resources in Azure China regions.
<a href="https://www.googleapis.com/compute/v1/">https://www.googleapis.com/compute/v1/</a> <a href="https://compute.googleapis.com/compute/v1">https://compute.googleapis.com/compute/v1</a> <a href="https://cloudresourcemanager.googleapis.com/v1/projects">https://cloudresourcemanager.googleapis.com/v1/projects</a> <a href="https://www.googleapis.com/compute/beta">https://www.googleapis.com/compute/beta</a> <a href="https://storage.googleapis.com/storage/v1">https://storage.googleapis.com/storage/v1</a> <a href="https://www.googleapis.com/storage/v1">https://www.googleapis.com/storage/v1</a> <a href="https://iam.googleapis.com/v1">https://iam.googleapis.com/v1</a> <a href="https://cloudkms.googleapis.com/v1">https://cloudkms.googleapis.com/v1</a> <a href="https://www.googleapis.com/deploymentmanager/v2/projects">https://www.googleapis.com/deploymentmanager/v2/projects</a>	To manage resources in Google Cloud.
<a href="https://support.netapp.com">https://support.netapp.com</a>	To obtain licensing information and to send AutoSupport messages to NetApp support.
<a href="https://*.api.blueexp.netapp.com">https://*.api.blueexp.netapp.com</a> <a href="https://api.blueexp.netapp.com">https://api.blueexp.netapp.com</a> <a href="https://*.cloudmanager.cloud.netapp.com">https://*.cloudmanager.cloud.netapp.com</a> <a href="https://cloudmanager.cloud.netapp.com">https://cloudmanager.cloud.netapp.com</a>	<div>The Connector is currently contacting "cloudmanager.cloud.netapp.com" but it will start contacting "api.blueexp.netapp.com" in an upcoming release.</div>
<a href="https://cloudmanagerinfraprod.azurecr.io">https://cloudmanagerinfraprod.azurecr.io</a> <a href="https://*.blob.core.windows.net">https://*.blob.core.windows.net</a>	To upgrade the Connector and its Docker components.

## Related link

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

## Proxy server

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

- IP address
- Credentials
- HTTPS certificate

## Ports

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

- HTTP (80) and HTTPS (443) provide access to the local UI, which you'll use in rare circumstances.
- SSH (22) is only needed if you need to connect to the host for troubleshooting.
- Inbound connections over port 3128 are required if you deploy Cloud Volumes ONTAP systems in a subnet where an outbound internet connection isn't available. If Cloud Volumes ONTAP systems don't have an outbound internet connection to send AutoSupport messages, BlueXP automatically configures those Cloud Volumes ONTAP systems to use a proxy server that's included with the Connector. The only requirement is to ensure that the Connector's security group allows inbound connections over port 3128. You'll need to open this port after you deploy the Connector.

## IP address limitation

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

## Review Connector host requirements for on-prem installs

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

### Dedicated host

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

### Supported operating systems

- 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.

**CPU**

4 cores or 4 vCPUs

**RAM**

14 GB

**Disk space in /opt**

100 GiB of space must be available

**Disk space in /var**

20 GiB of space must be available

**Docker Engine**

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

**Set up cloud permissions for on-prem deployments**

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



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

## AWS

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

You must use this authentication method if the Connector is installed on premises. You can't use an IAM role.

### Steps

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

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

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

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

### Result

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

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

## Azure

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

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

1. Ensure that you have permissions in Azure to create an Active Directory application and to assign the application to a role.

For details, refer to [Microsoft Azure Documentation: Required permissions](#).

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



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

You've created the AD application and service principal.

#### Assign the application to a role

1. Create a custom role:
  - a. Copy the contents of the [custom role permissions for the Connector](#) and save them in a JSON file.
  - b. Modify the JSON file by adding Azure subscription IDs to the assignable scope.

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

#### Example

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

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

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

- Start [Azure Cloud Shell](#) and choose the Bash environment.
- Upload the JSON file.





- Use the Azure CLI to create the custom role:

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

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

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

**Add role assignment** ...

[Got feedback?](#)

**Role**   **Members**   [Review + assign](#)

**Selected role**   Cloud Manager Operator 3.9.12\_B

**Assign access to**   ☒ User, group, or service principal  
☐ Managed identity

**Members**   [+ Select members](#)

- Search for the name of the application.

Here's an example:

**Select members** ×

Select ⓘ

test-service-principal

test-service-principal

- Select the application and click **Select**.
  - Click **Next**.
- f. Click **Review + assign**.

The service principal now has the required Azure permissions to deploy the Connector.

If you want to deploy Cloud Volumes ONTAP from multiple Azure subscriptions, then you must bind the service principal to each of those subscriptions. BlueXP enables you to select the subscription that you want to use when deploying Cloud Volumes ONTAP.

#### Add Windows Azure Service Management API permissions

1. In the **Azure Active Directory** service, click **App registrations** and select the application.
2. Click **API permissions > Add a permission**.
3. Under **Microsoft APIs**, select **Azure Service Management**.

## Request API permissions

Select an API

Microsoft APIs APIs my organization uses My APIs

### Commonly used Microsoft APIs

#### Microsoft Graph

Take advantage of the tremendous amount of data in Office 365, Enterprise Mobility + Security, and Windows 10. Access Azure AD, Excel, Intune, Outlook/Exchange, OneDrive, OneNote, SharePoint, Planner, and more through a single endpoint.



#### Azure Batch

Schedule large-scale parallel and HPC applications in the cloud

#### Azure Data Catalog

Programmatic access to Data Catalog resources to register, annotate and search data assets

#### Azure Data Explorer

Perform ad-hoc queries on terabytes of data to build near real-time and complex analytics solutions

#### Azure Data Lake

Access to storage and compute for big data analytic scenarios

#### Azure DevOps

Integrate with Azure DevOps and Azure DevOps server

#### Azure Import/Export

Programmatic control of import/export jobs

#### Azure Key Vault

Manage your key vaults as well as the keys, secrets, and certificates within your Key Vaults

#### Azure Rights Management Services

Allow validated users to read and write protected content

#### Azure Service Management

Programmatic access to much of the functionality available through the Azure portal

#### Azure Storage

Secure, massively scalable object and data lake storage for unstructured and semi-structured data

#### Customer Insights

Create profile and interaction models for your products

#### Data Export Service for Microsoft Dynamics 365

Export data from Microsoft Dynamics CRM organization to an external destination

- Click **Access Azure Service Management as organization users** and then click **Add permissions**.

## Request API permissions

[← All APIs](#)



Azure Service Management

<https://management.azure.com/> [Docs](#) [↗](#)

What type of permissions does your application require?

### Delegated permissions

Your application needs to access the API as the signed-in user.

### Application permissions

Your application runs as a background service or daemon without a signed-in user.

Select permissions

[expand all](#)

Type to search

PERMISSION

ADMIN CONSENT REQUIRED



user\_impersonation

Access Azure Service Management as organization users (preview) ⓘ

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

1. In the **Azure Active Directory** service, click **App registrations** and select the application.
2. Copy the **Application (client) ID** and the **Directory (tenant) ID**.



When you add the Azure account to BlueXP, you need to provide the application (client) ID and the directory (tenant) ID for the application. BlueXP uses the IDs to programmatically sign in.

## Create a client secret

1. Open the **Azure Active Directory** service.
2. Click **App registrations** and select your application.
3. Click **Certificates & secrets > New client secret**.
4. Provide a description of the secret and a duration.
5. Click **Add**.
6. Copy the value of the client secret.

## Client secrets

A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.

[+ New client secret](#)

DESCRIPTION	EXPIRES	VALUE	Copy to clipboard
test secret	8/16/2020	*sZ1jSe2By:D*-ZRoV4NLfdAcY7:+0vA	

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

### Result

Your service principal is now setup and you should have copied the application (client) ID, the directory (tenant) ID, and the value of the client secret. After you install the Connector, you'll need to associate these credentials with the Connector from BlueXP.

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

## Install and set up a Connector on premises

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

### Install the Connector

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

### What you'll need

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

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

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

### About this task

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

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

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

### Steps

1. Verify that docker is enabled and running.

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

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

```
unset http_proxy
unset https_proxy
```

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

3. Download the Connector software from the [NetApp Support Site](#), and then copy it to the Linux host.

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

4. Assign permissions to run the script.

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

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

5. Run the installation script.

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

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

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

```
./OnCommandCloudManager-V3.9.26 --proxy
https://user:password@10.0.0.30:8080/ --cacert
/tmp/cacert/certificate.cer
```

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

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

`--cacert` specifies a CA-signed certificate to use for HTTPS access between the Connector and the proxy

server. This parameter is required only if you specify an HTTPS proxy server or if the proxy is an intercepting proxy.

## Result

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

## Set up the Connector

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

## Steps

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

`https://ipaddress`

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

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

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

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

## Result

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

## What's next?

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

## Provide permissions to BlueXP for on-prem installs

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



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

## AWS

### Before you get started

If you just created these credentials in AWS, it might take a few minutes until they are available for use. Wait a few minutes before you add the credentials to BlueXP.

### Steps

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



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

### Result

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

## Azure

### Before you get started

If you just created these credentials in Azure, it might take a few minutes until they are available for use. Wait a few minutes before you add the credentials to BlueXP.

### Steps

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



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



**Result**

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

## 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.