Connectors

Setup and administration

NetApp
June 26, 2023

Table of Contents

Connectors

Find the system ID for a Connector

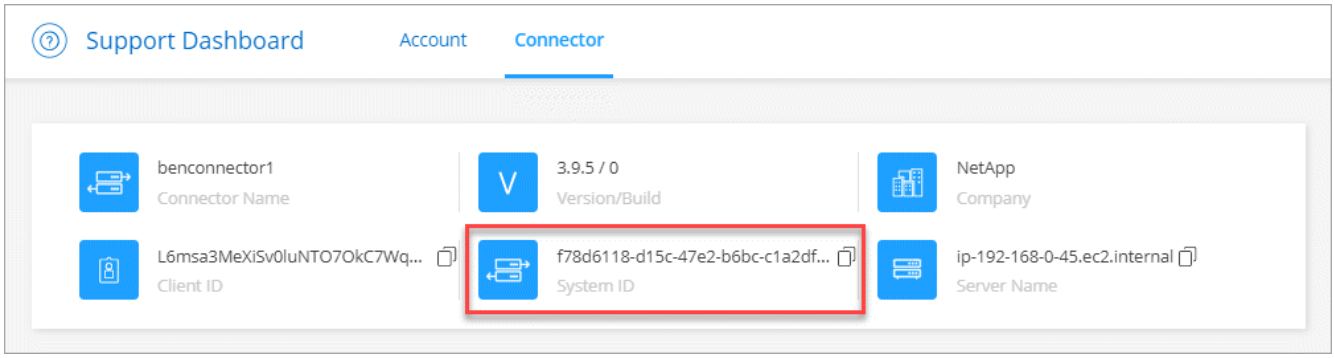
To help you get started, your NetApp representative might ask you for the system ID of your Connector. The ID is typically used for licensing and troubleshooting purposes.

Steps

1. In the upper right of the BlueXP console, select the Help icon.
2. Select **Support > Connector**.

   The system ID appears at the top.

   Example



Manage existing Connectors

After you create a Connector, you might need to manage it every now and then. For example, you might want to switch between Connectors if you have more than one. Or you might need to manually upgrade the Connector when using BlueXP in private mode.

Learn how Connectors work.

Operating system and VM maintenance

Maintaining the operating system on the Connector host is your responsibility. For example, you should apply security updates to the operating system on the Connector host by following your company's standard procedures for operating system distribution.

Note that you don't need to stop any services on the Connector host when running an OS update.

If you need to stop and then start the Connector VM, you should do so from your cloud provider's console or by using the standard procedures for on-premises management.

Be aware that the Connector must be operational at all times.

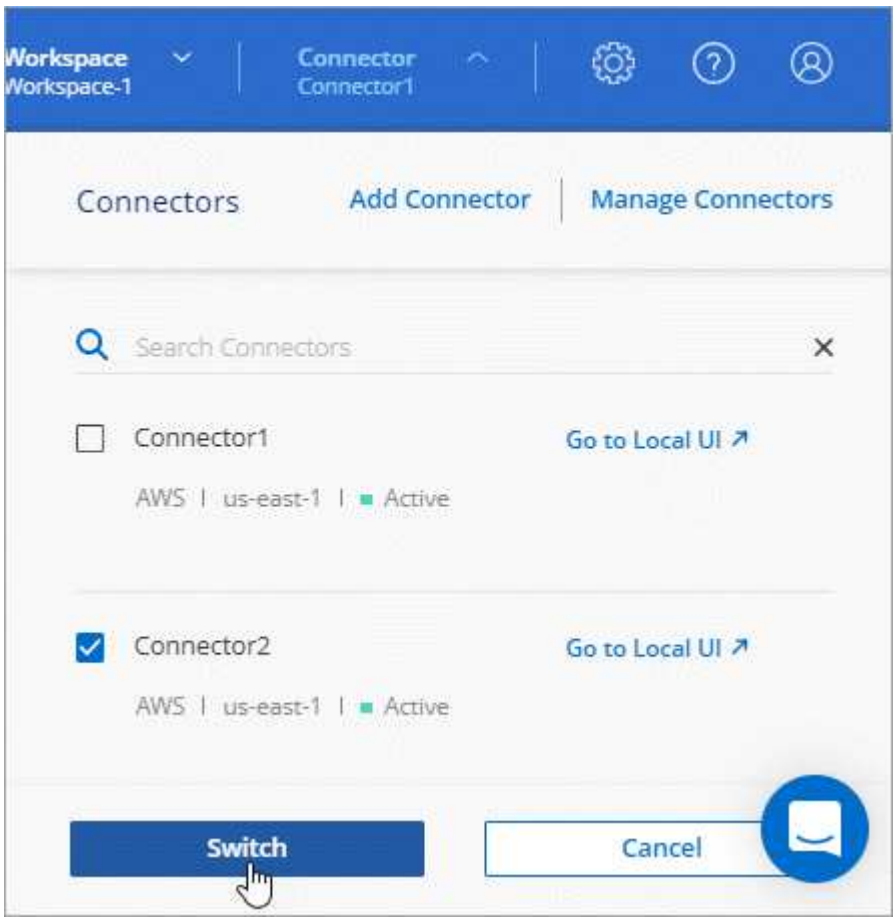
Switch between Connectors

If you have multiple Connectors, you can switch between them to see the Working Environments that are associated with a specific Connector.

For example, let's say that you're working in a multi-cloud environment. You might have one Connector in AWS and another in Google Cloud. You'd need to switch between those Connectors to manage the Cloud Volumes ONTAP systems running in those clouds.

Step

1. Select the **Connector** drop-down, select another Connector, and then select **Switch**.



Result

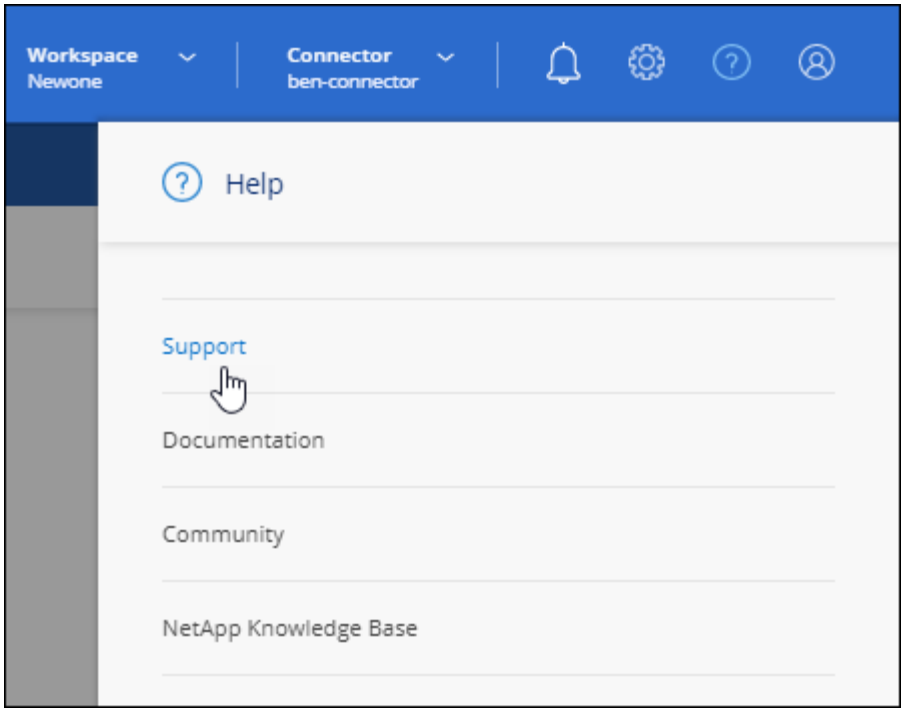
BlueXP refreshes and shows the Working Environments associated with the selected Connector.

Download or send an AutoSupport message

If you're having problems, NetApp personnel might ask you to send an AutoSupport message to NetApp support for troubleshooting purposes.

Steps

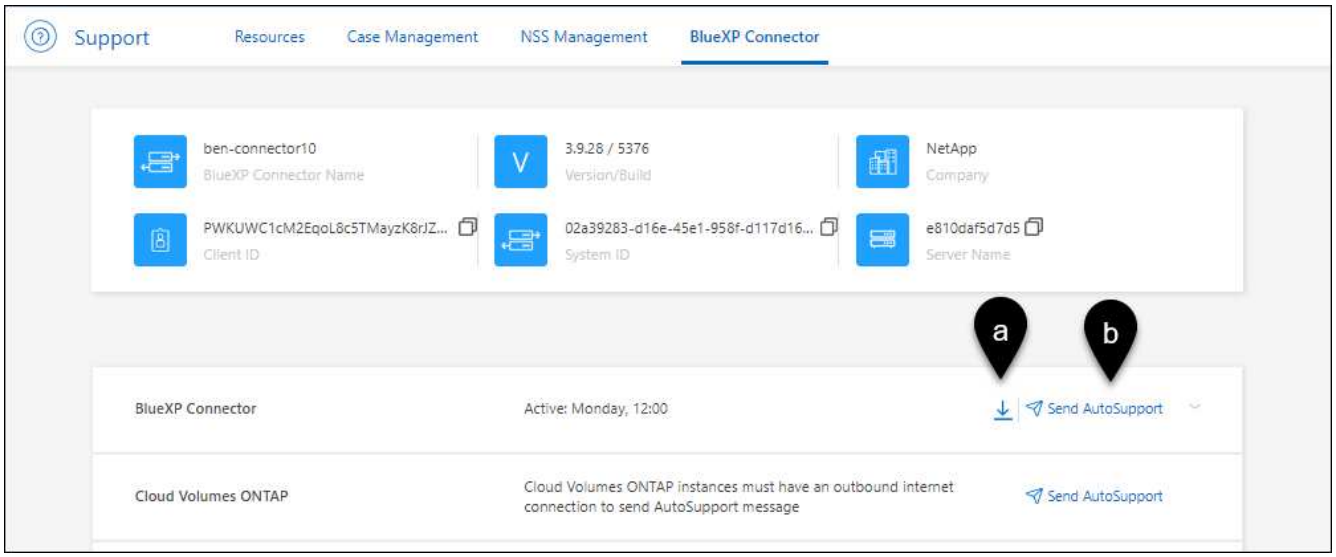
1. In the upper right of the BlueXP console, select the Help icon, and select **Support**.



2. Select **BlueXP Connector**.
3. Depending on how you need to send the information to NetApp support, choose one of the following options:

   a. Select the option to download the AutoSupport message to your local machine. You can then send it to NetApp Support using a preferred method.

   b. Select **Send AutoSupport** to directly send the message to NetApp Support.



Connect to the Linux VM

If you need to connect to the Linux VM that the Connector runs on, you can do so by using the connectivity options available from your cloud provider.

AWS

When you created the Connector instance in AWS, you provided an AWS access key and secret key. You can use this key pair to SSH to the instance.

AWS Docs: Connect to your Linux instance

Azure

When you created the Connector VM in Azure, you chose to authenticate with a password or SSH public key. Use the authentication method that you chose to connect to the VM.

Azure Docs: SSH into your VM

Google Cloud

You can't specify an authentication method when you create a Connector in Google Cloud. However, you can connect to the Linux VM instance using the Google Cloud Console or Google Cloud CLI (gcloud).

Google Cloud Docs: Connect to Linux VMs

Upgrade the Connector when using private mode

If you are using BlueXP in private mode, you can upgrade the Connector when a newer version is available from the NetApp Support Site.

The Connector needs to restart during the upgrade process so the web-based console will be unavailable during the upgrade.

On hosts that have internet access, the Connector automatically updates its software to the latest version, as long as it has outbound internet access to obtain the software update.

Steps

1. Download the Connector software from the NetApp Support Site.
2. Copy the installer to the Linux host.
3. Assign permissions to run the script.

```
chmod +x /path/cloud-manager-connector-offline-<version>
```

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

4. Run the installation script:

```
sudo /path/cloud-manager-connector-offline-<version>
```

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

5. After the upgrade is complete, you can verify the Connector's version by going to **Help > Support > Connector**.

Change the IP address for a Connector

If it's required for your business, you can change the internal IP address and public IP address of the Connector instance that is automatically assigned by your cloud provider.

Steps

1. Follow the instructions from your cloud provider to change the local IP address or public IP address (or both) for the Connector instance.
2. If you changed the public IP address and you need to connect to the local user interface running on the Connector, restart the Connector instance to register the new IP address with BlueXP.
3. If you changed the private IP address, update the backup location for Cloud Volumes ONTAP configuration files so that the backups are being sent to the new private IP address on the Connector.
   a. Run the following command from the Cloud Volumes ONTAP CLI to remove the current backup target:

      ```
      system configuration backup settings modify -destination ""
      ```

   b. Go to BlueXP and open the working environment.
   c. Select the menu and select **Advanced > Configuration Backups**.
   d. Select **Set Backup Target**.

Edit a Connector's URIs

Add and remove the Uniform Resource Identifier (URI) for a Connector.

Steps

1. Select the **Connector** drop-down from the BlueXP header.
2. Select **Manage Connectors**.
3. Select the action menu for a Connector and select **Edit URIs**.
4. Add and remove URIs and then select **Apply**.

Fix download failures when using a Google Cloud NAT gateway

The Connector automatically downloads software updates for Cloud Volumes ONTAP. The download can fail if your configuration uses a Google Cloud NAT gateway. You can correct this issue by limiting the number of parts that the software image is divided into. This step must be completed by using the BlueXP API.

Step

1. Submit a PUT request to /occm/config with the following JSON as body:

   ```
   {
     "maxDownloadSessions": 32
   }
   ```

   The value for *maxDownloadSessions* can be 1 or any integer greater than 1. If the value is 1, then the downloaded image will not be divided.

Note that 32 is an example value. The value that you should use depends on your NAT configuration and the number of sessions that you can have simultaneously.

Learn more about the /occm/config API call

Remove Connectors from BlueXP

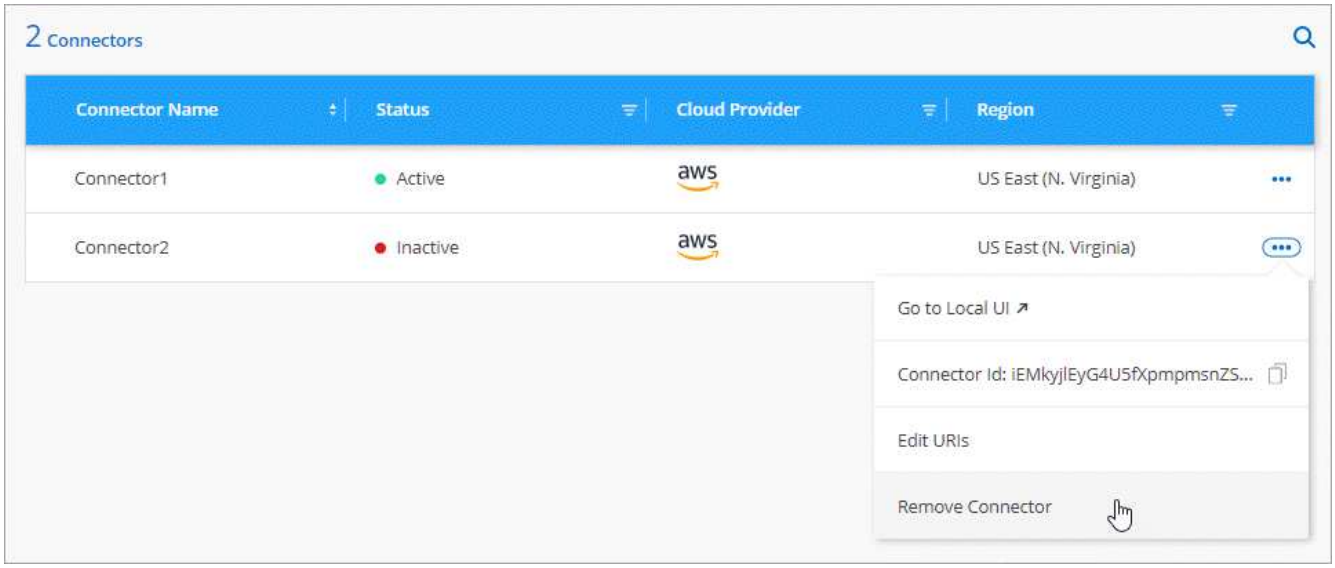
If a Connector is inactive, you can remove it from the list of Connectors in BlueXP. You might do this if you deleted the Connector virtual machine or if you uninstalled the Connector software.

Note the following about removing a Connector:

- This action doesn't delete the virtual machine.
- This action can't be reverted—once you remove a Connector from BlueXP, you can't add it back.

Steps

1. Select the **Connector** drop-down from the BlueXP header.
2. Select **Manage Connectors**.
3. Select the action menu for an inactive Connector and select **Remove Connector**.



4. Enter the name of the Connector to confirm and then select **Remove**.

Result

BlueXP removes the Connector from its records.

Uninstall the Connector software

Uninstall the Connector software to troubleshoot issues or to permanently remove the software from the host. The steps that you need to use depends on whether you installed the Connector on a host that has internet access or a host in a restricted network that doesn't have internet access.

Uninstall from a host with internet access

The online Connector includes an uninstallation script that you can use to uninstall the software.

Step

1. From the Linux host, run the uninstallation script:

```
/opt/application/netapp/service-manager-2/uninstall.sh [silent]
```

silent runs the script without prompting you for confirmation.

Uninstall from a host without internet access

Use these commands if you downloaded the Connector software from the NetApp Support Site and installed it in a restricted network that doesn't have internet access.

Step

1. From the Linux host, run the following commands:

```
docker-compose -f /opt/application/netapp/ds/docker-compose.yml down -v
rm -rf /opt/application/netapp/ds
```

Install an HTTPS certificate for secure access

By default, BlueXP uses a self-signed certificate for HTTPS access to the web console. If required by your business, you can install a certificate signed by a certificate authority (CA), which provides better security protection than a self-signed certificate.

Before you get started

You need to create a Connector before you can change BlueXP settings. Learn how.

Install an HTTPS certificate

Install a certificate signed by a CA for secure access.

Steps

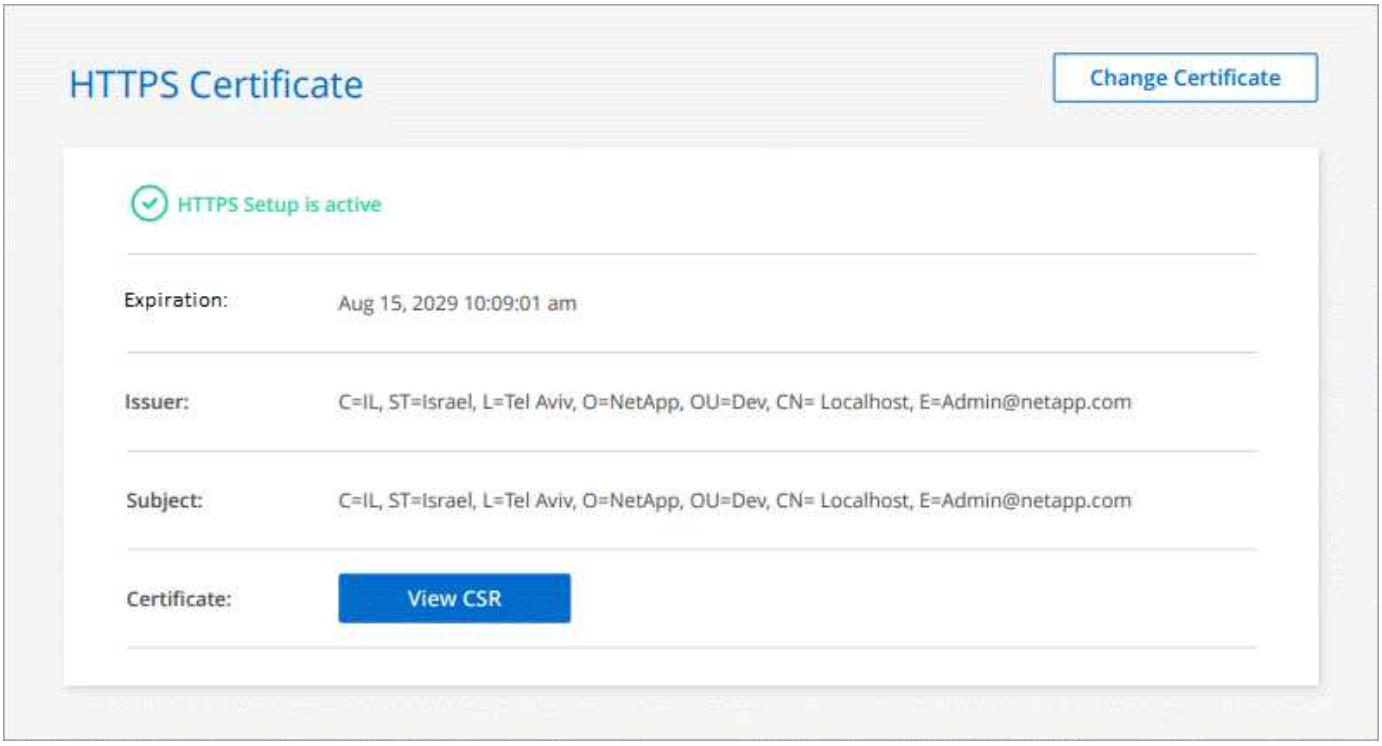
1. In the upper right of the BlueXP console, select the Settings icon, and select **HTTPS Setup**.

2. In the HTTPS Setup page, install a certificate by generating a certificate signing request (CSR) or by installing your own CA-signed certificate:

Option	Description
Generate a CSR	a. Enter the host name or DNS of the Connector host (its Common Name), and then select **Generate CSR**. BlueXP displays a certificate signing request. b. Use the CSR to submit an SSL certificate request to a CA. The certificate must use the Privacy Enhanced Mail (PEM) Base-64 encoded X.509 format. c. Upload the certificate file and then select **Install**.
Install your own CA-signed certificate	a. Select **Install CA-signed certificate**. b. Load both the certificate file and the private key and then select **Install**. The certificate must use the Privacy Enhanced Mail (PEM) Base-64 encoded X.509 format.

Result

BlueXP now uses the CA-signed certificate to provide secure HTTPS access. The following image shows a BlueXP account that is configured for secure access:



Renew the BlueXP HTTPS certificate

You should renew the BlueXP HTTPS certificate before it expires to ensure secure access to the BlueXP console. If you don’t renew the certificate before it expires, a warning appears when users access the web console using HTTPS.

Steps

1. In the upper right of the BlueXP console, select the Settings icon, and select **HTTPS Setup**.

   Details about the BlueXP certificate displays, including the expiration date.

2. Select **Change Certificate** and follow the steps to generate a CSR or install your own CA-signed certificate.

Result

BlueXP uses the new CA-signed certificate to provide secure HTTPS access.

Configure a Connector to use a proxy server

If your corporate policies require you to use a proxy server for all communication to the internet, then you need to configure your Connectors to use that proxy server. If you didn't configure a Connector to use a proxy server during installation, then you can configure the Connector to use that proxy server at any time.

BlueXP supports HTTP and HTTPS. The proxy server can be in the cloud or in your network.

Configuring the Connector to use a proxy server provides outbound internet access if a public IP address or a NAT gateway isn't available. This proxy server provides only the Connector with an outbound connection. It doesn't provide any connectivity for Cloud Volumes ONTAP systems.

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.

Enable a proxy on a Connector

When you configure a Connector to use a proxy server, that Connector and the Cloud Volumes ONTAP systems that it manages (including any HA mediators), all use the proxy server.

Note that this operation restarts the Connector. Ensure that the Connector isn't performing any operations before you proceed.

Steps

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

2. Under **General**, select **HTTP Proxy Configuration**.
3. Set up the proxy:
   a. Select **Enable Proxy**.
   b. Specify the server using the syntax http://*address:port* or https://*address:port*
   c. Specify a user name and password if basic authentication is required for the server

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

d. Select **Save**.

BlueXP doesn't support passwords that include the @ character.

Enable direct API traffic

If you configured a Connector to use a proxy server, you can enable direct API traffic on the Connector in order to send API calls directly to cloud provider services without going through the proxy. This option is supported with Connectors that are running in AWS, in Azure, or in Google Cloud.

If you disabled the use of Azure Private Links with Cloud Volumes ONTAP and are using service endpoints instead, then you must enable direct API traffic. Otherwise, the traffic won't be routed properly.

Learn more about using an Azure Private Link or service endpoints with Cloud Volumes ONTAP

Steps

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

2. Under **General**, select **Support Direct API Traffic**.
3. Select the checkbox to enable the option and then select **Save**.

Default configuration for the Connector

You might want to learn more about the Connector's configuration before you deploy it, or if you need to troubleshoot any issues.

Default configuration with internet access

The following configuration details apply if you deployed the Connector from BlueXP, from your cloud provider's marketplace, or if you manually installed the Connector on an on-premises Linux host that has internet access.

AWS details

If you deployed the Connector from BlueXP or from the cloud provider's marketplace, note the following:

- The EC2 instance type is t3.xlarge.
- The operating system for the image is Ubuntu 22.04.

  The operating system does not include a GUI. You must use a terminal to access the system.

- The user name for the EC2 Linux instance is ec2-user.
- The default system disk is a 100 GiB gp2 disk.

Azure details

If you deployed the Connector from BlueXP or from the cloud provider's marketplace, note the following:

- The VM type is DS3 v2.
- The operating system for the image is Ubuntu 22.04.

  The operating system does not include a GUI. You must use a terminal to access the system.

- The default system disk is a 100 GiB premium SSD disk.

Google Cloud details

If you deployed the Connector from BlueXP, note the following:

- The VM instance is n2-standard-4.
- The operating system for the image is Ubuntu 22.04.

  The operating system does not include a GUI. You must use a terminal to access the system.

- The default system disk is a 100 GiB SSD persistent disk.

Installation folder

The Connector installation folder resides in the following location:

/opt/application/netapp/cloudmanager

Log files

Log files are contained in the following folders:

- /opt/application/netapp/cloudmanager/log
  or
- /opt/application/netapp/service-manager-2/logs (starting with new 3.9.23 installations)

  The logs in these folders provide details about the Connector and docker images.

- /opt/application/netapp/cloudmanager/docker_occm/data/log

  The logs in this folder provide details about cloud services and the BlueXP service that runs on the Connector.

Connector service

- The BlueXP service is named occm.
- The occm service is dependent on the MySQL service.

  If the MySQL service is down, then the occm service is down too.

Ports

The Connector uses the following ports on the Linux host:

- 80 for HTTP access
- 443 for HTTPS access

Default configuration without internet access

The following configuration applies if you manually installed the Connector on an on-premises Linux host that doesn't have internet access. Learn more about this installation option.

- The Connector installation folder resides in the following location:

  /opt/application/netapp/ds

- Log files are contained in the following folders:

  /var/lib/docker/volumes/ds_occmdata/_data/log

  The logs in this folder provide details about the Connector and docker images.

- All services are running inside docker containers

  The services are dependent on the docker runtime service running

- The Connector uses the following ports on the Linux host:
  - 80 for HTTP access
  - 443 for HTTPS access

Copyright information

Trademark information