



Connectors

Setup and administration

NetApp
July 16, 2024

Table of Contents

- Connectors 1
 - Maintain the Connector VM and operating system 1
 - Install an HTTPS certificate for secure access 3
 - Configure a Connector to use a proxy server 4
 - Require the use of IMDSv2 on Amazon EC2 instances 9
 - Upgrade a Connector when using private mode 11
 - Work with multiple Connectors 11
 - Troubleshoot the Connector 13
 - Uninstall and remove the Connector 15
 - Default configuration for the Connector 17

Connectors

Maintain the Connector VM and operating system

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.



If you have an existing Connector, you should be aware of [changes to supported Linux operating systems](#).

Operating system patches and the Connector

You don't need to stop any services on the Connector host when applying OS security patches.

VM or instance type

If you created a Connector directly from BlueXP, BlueXP deployed a virtual machine instance in your cloud provider using a default configuration. After you create the Connector, you should not change to a smaller VM instance that has less CPU or RAM.

The CPU and RAM requirements are as follows:

CPU

4 cores or 4 vCPUs

RAM

14 GB

[Learn about the default configuration for the Connector.](#)

Stopping the starting the Connector VM

If you need to stop and then start the Connector VM, then 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.](#)

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. The user name for the EC2 Linux instance is ubuntu (for Connectors created prior to May 2023, the user name was ec2-user).

[AWS Docs: Connect to your Linux instance](#)

Azure

When you created the Connector VM in Azure, you specified a user name and 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](#)

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.

You'll need to update the backup location for each Cloud Volumes ONTAP system.

- a. Run the following command from the Cloud Volumes ONTAP CLI to display the current backup target:

```
system configuration backup show
```

- b. Run the following command to update the IP address for the backup target:

```
system configuration backup settings modify -destination <target-  
location>
```

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**.

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 begin

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**.

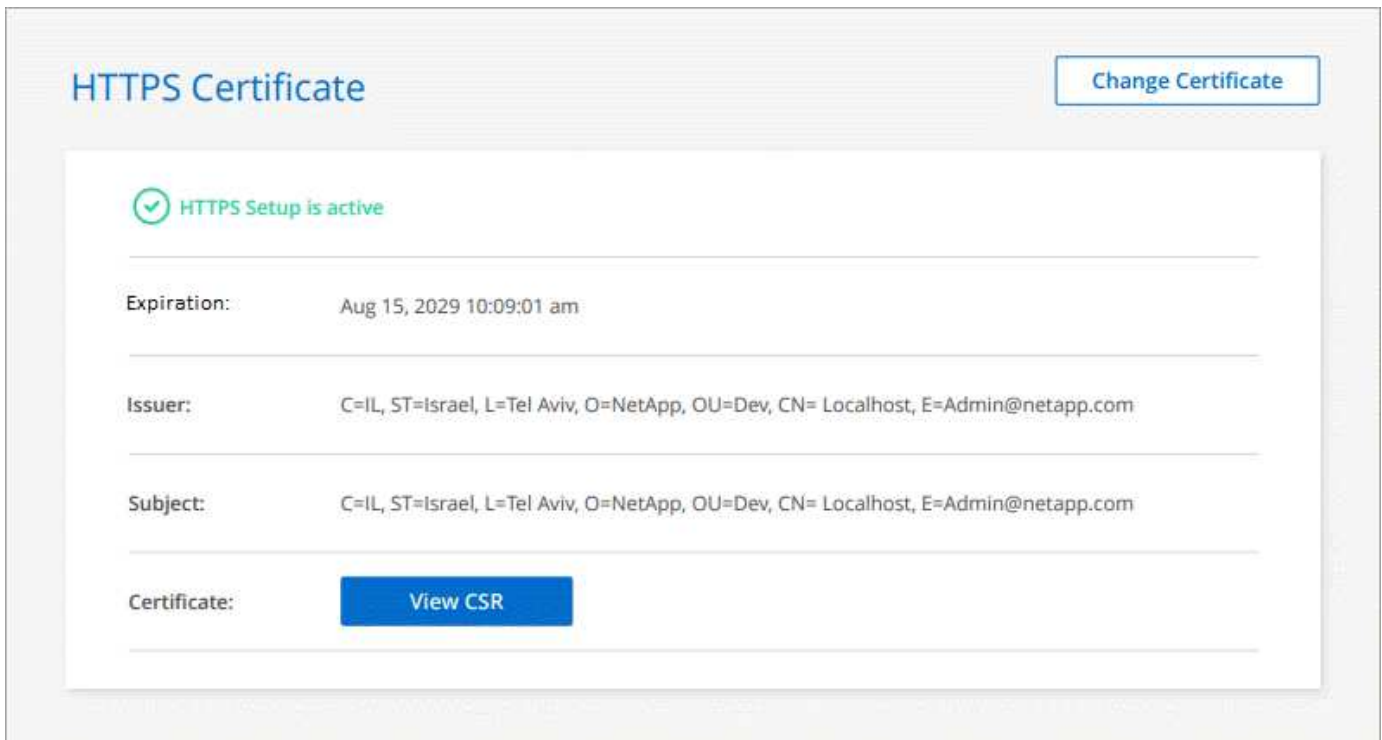


2. In the HTTPS Setup page, install a certificate by generating a certificate signing request (CSR) or by installing your own CA-signed certificate:

Option	Description
Generate a CSR	<ol style="list-style-type: none">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	<ol style="list-style-type: none">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.

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.

Supported configurations

- BlueXP supports HTTP and HTTPS.
- The proxy server can be in the cloud or in your network.
- BlueXP does not support transparent proxy servers.

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.

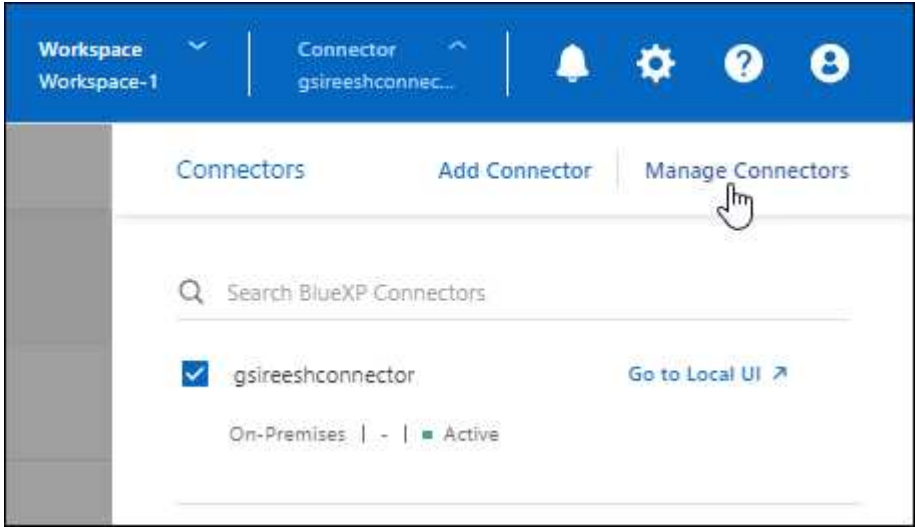
Steps

1. Navigate to the **Edit BlueXP Connector** page.

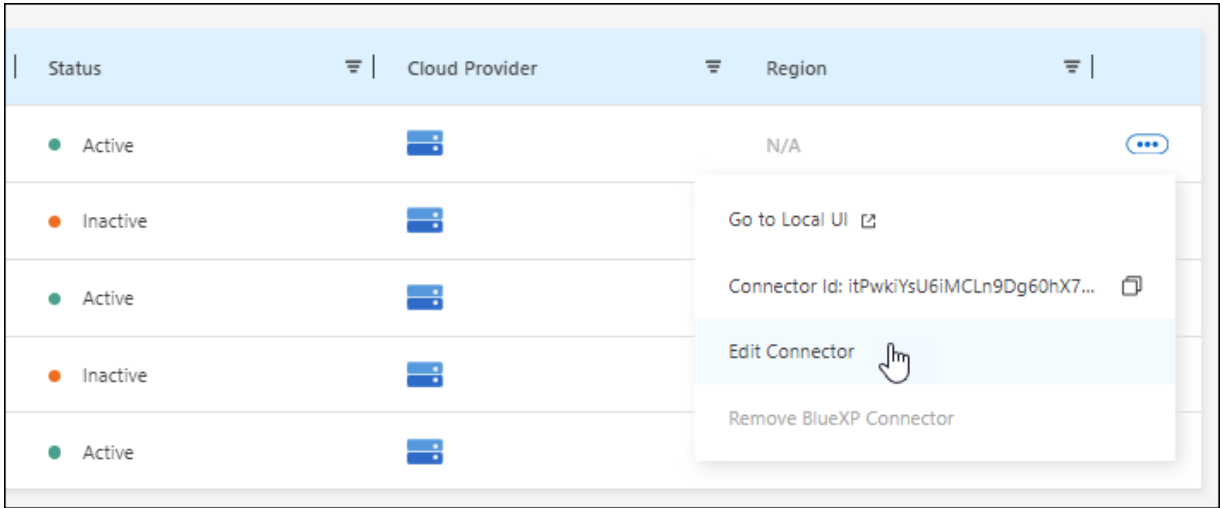
How you navigate depends on whether you're using BlueXP in standard mode (accessing the BlueXP interface from the SaaS website) or using BlueXP in restricted mode or private mode (accessing the BlueXP interface locally from the Connector host).

Standard mode

- a. Select the **Connector** drop-down from the BlueXP header.
- b. Select **Manage Connectors**.

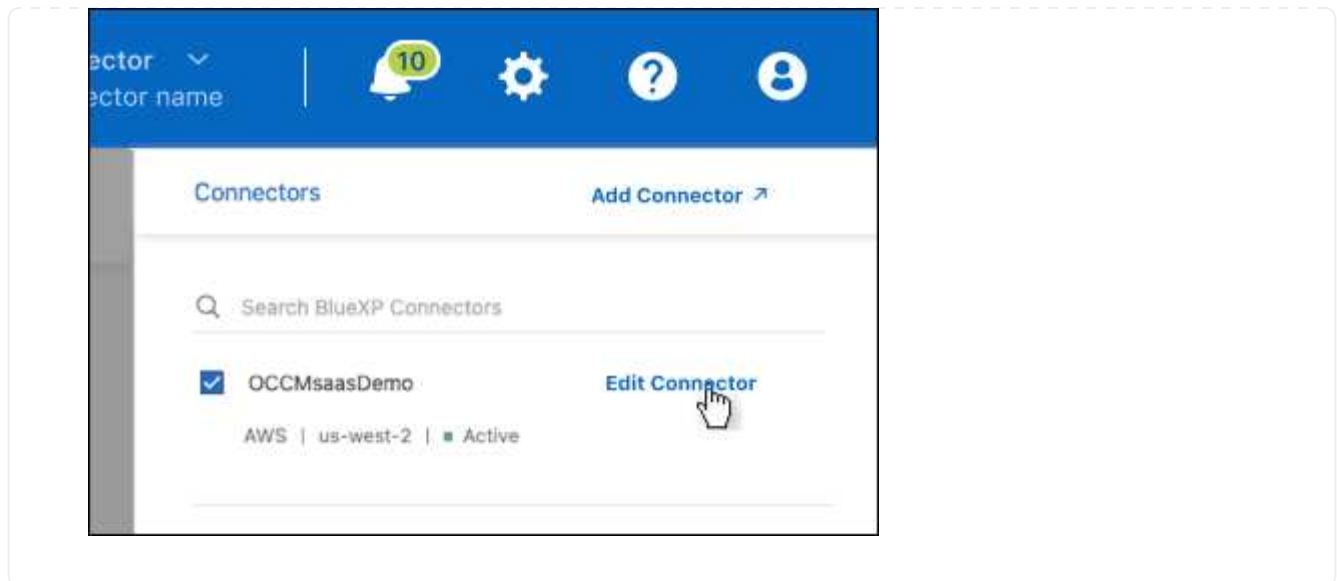


- c. Select the action menu for a Connector and select **Edit Connector**.



Restricted or private mode

- a. Select the **Connector** drop-down from the BlueXP header.
- b. Select **Edit Connector**.



2. 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.

Note the following:

- The user can be a local user or domain user.
- For a domain user, you must enter the ASCII code for the \ as follows: `domain-name%92user-name`

For example: `netapp%92proxy`

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

- d. Select **Save**.

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](#)

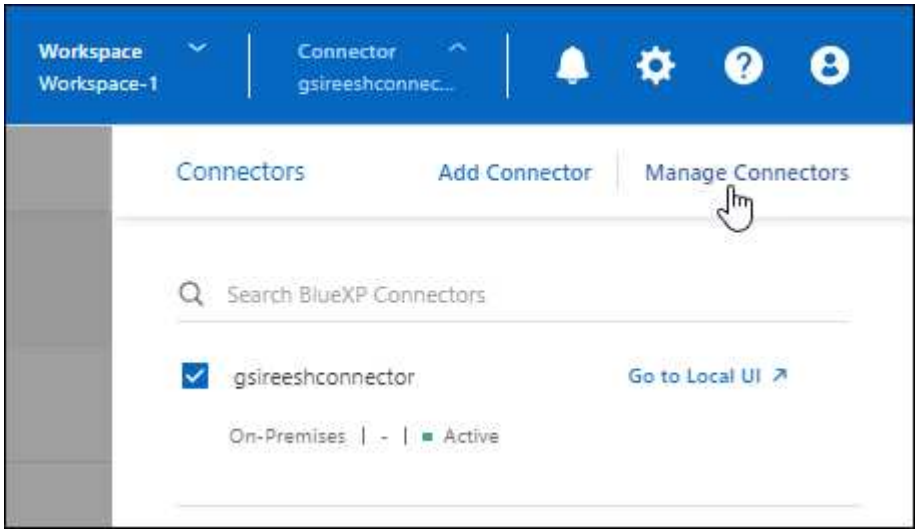
Steps

1. Navigate to the **Edit BlueXP Connector** page:

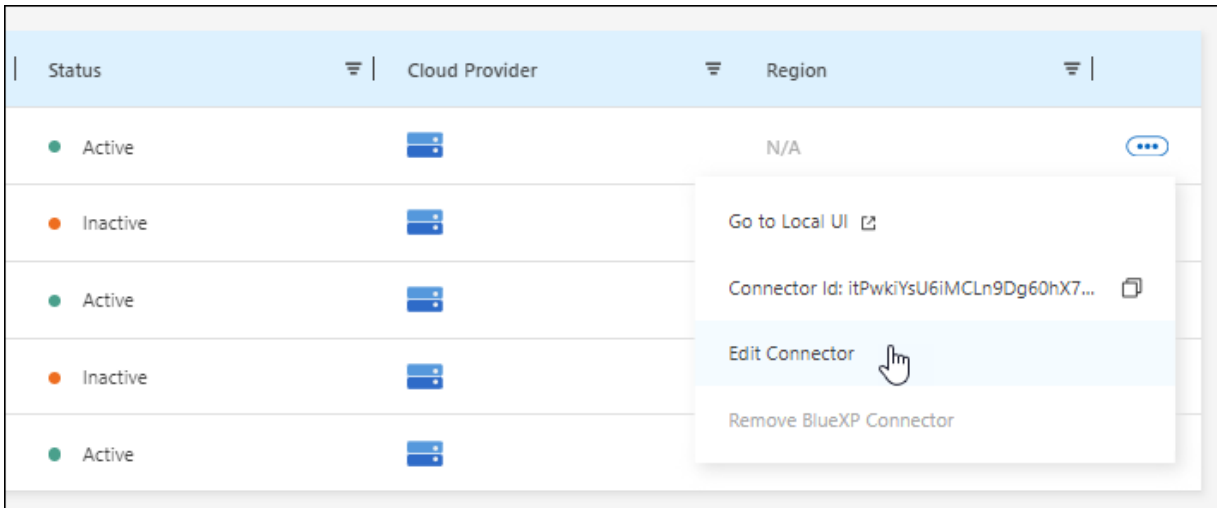
How you navigate depends on whether you're using BlueXP in standard mode (accessing the BlueXP interface from the SaaS website) or using BlueXP in restricted mode or private mode (accessing the BlueXP interface locally from the Connector host).

Standard mode

- a. Select the **Connector** drop-down from the BlueXP header.
- b. Select **Manage Connectors**.

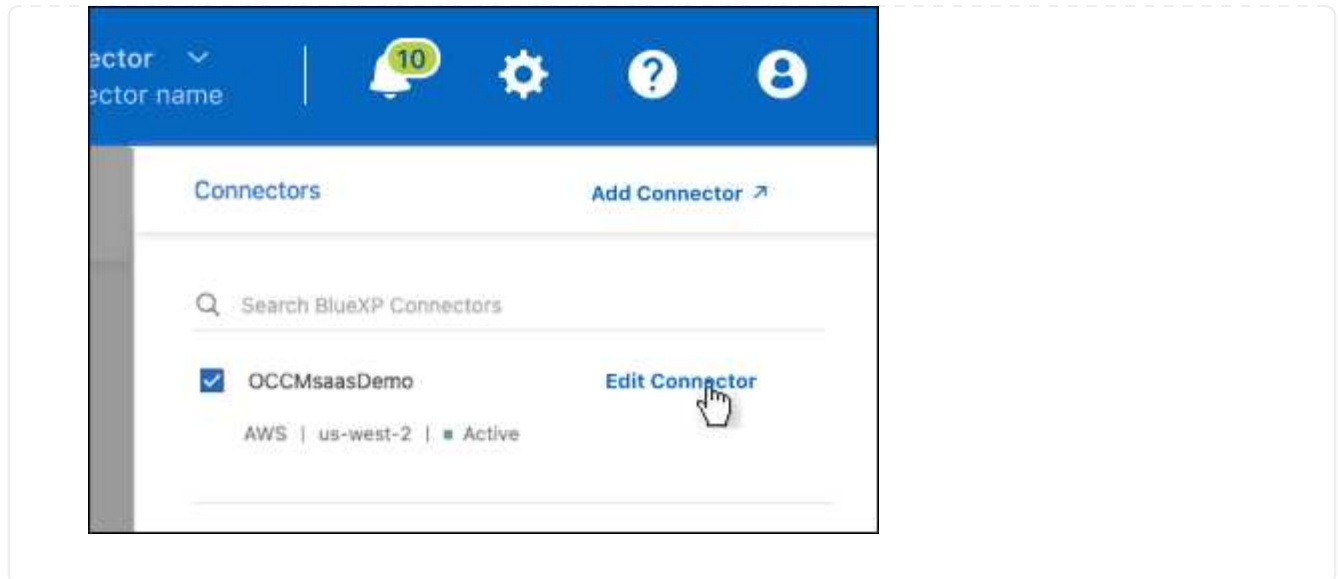


- c. Select the action menu for a Connector and select **Edit Connector**.



Restricted or private mode

- a. Select the **Connector** drop-down from the BlueXP header.
- b. Select **Edit Connector**.



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

Require the use of IMDSv2 on Amazon EC2 instances

BlueXP supports the Amazon EC2 Instance Metadata Service Version 2 (IMDSv2) with the Connector and with Cloud Volumes ONTAP (including the mediator for HA deployments). In most cases, IMDSv2 is automatically configured on new EC2 instances. IMDSv1 was enabled prior to March 2024. If required by your security policies, you might need to manually configure IMDSv2 on your EC2 instances.

Before you begin

- The Connector version must be 3.9.38 or later.
- Cloud Volumes ONTAP must be running one of the following versions:
 - 9.12.1 P2 (or any subsequent patch)
 - 9.13.0 P4 (or any subsequent patch)
 - 9.13.1 or any version after this release
- This change requires you to restart the Cloud Volumes ONTAP instances.
- These steps require the use of the AWS CLI because you must change the response hop limit to 3.

About this task

IMDSv2 provides enhanced protection against vulnerabilities. [Learn more about IMDSv2 from the AWS Security Blog](#)

The Instance Metadata Service (IMDS) is enabled as follows on EC2 instances:

- For new Connector deployments from BlueXP or using [Terraform scripts](#), IMDSv2 is enabled by default on the EC2 instance.
- If you launch a new EC2 instance in AWS and then manually install the Connector software, IMDSv2 is also enabled by default.

- If you launch the Connector from the AWS Marketplace, IMDSv1 is enabled by default. You can manually configure IMDSv2 on the EC2 instance.
- For existing Connectors, IMDSv1 is still supported but you can manually configure IMDSv2 on the EC2 instance if you prefer.
- For Cloud Volumes ONTAP, IMDSv1 is enabled by default on new and existing instances. You can manually configure IMDSv2 on the EC2 instances if you prefer.

Steps

1. Require the use of IMDSv2 on the Connector instance:

a. Connect to the Linux VM for the Connector.

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. The user name for the EC2 Linux instance is ubuntu (for Connectors created prior to May 2023, the user name was ec2-user).

[AWS Docs: Connect to your Linux instance](#)

b. Install the AWS CLI.

[AWS Docs: Install or update to the latest version of the AWS CLI](#)

c. Use the `aws ec2 modify-instance-metadata-options` command to require the use of IMDSv2 and to change the PUT response hop limit to 3.

Example

```
aws ec2 modify-instance-metadata-options \  
  --instance-id <instance-id> \  
  --http-put-response-hop-limit 3 \  
  --http-tokens required \  
  --http-endpoint enabled
```



The `http-tokens` parameter sets IMDSv2 to required. When `http-tokens` is required, you must also set `http-endpoint` to `enabled`.

2. Require the use of IMDSv2 on Cloud Volumes ONTAP instances:

a. Go to the [Amazon EC2 console](#)

b. From the navigation pane, select **Instances**.

c. Select a Cloud Volumes ONTAP instance.

d. Select **Actions > Instance settings > Modify instance metadata options**.

e. On the **Modify instance metadata options** dialog box, select the following:

- For **Instance metadata service**, select **Enable**.
- For **IMDSv2**, select **Required**.
- Select **Save**.

f. Repeat these steps for other Cloud Volumes ONTAP instances, including the HA mediator.

- g. [Stop and start the Cloud Volumes ONTAP instances](#)

Result

The Connector instance and Cloud Volumes ONTAP instances are now configured to use IMDSv2.

Upgrade a 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](#).



When you use BlueXP in standard mode or restricted mode, you don't need to manually upgrade the Connector. BlueXP automatically upgrades a Connector to the latest release, as long as the Connector has outbound internet access to obtain the software update.

About this task

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

Steps

1. Download the Connector software from the [NetApp Support Site](#).

Be sure to download the offline installer for private networks without internet access.

2. Copy the installer to the Linux host.
3. Assign permissions to run the script.

```
chmod +x /path/BlueXP-Connector-offline-<version>
```

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

4. Run the installation script:

```
sudo /path/BlueXP-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**.

Work with multiple Connectors

If you use multiple Connectors, BlueXP enables you to switch between those Connectors directly from the console. You can also manage a single working environment with multiple Connectors.

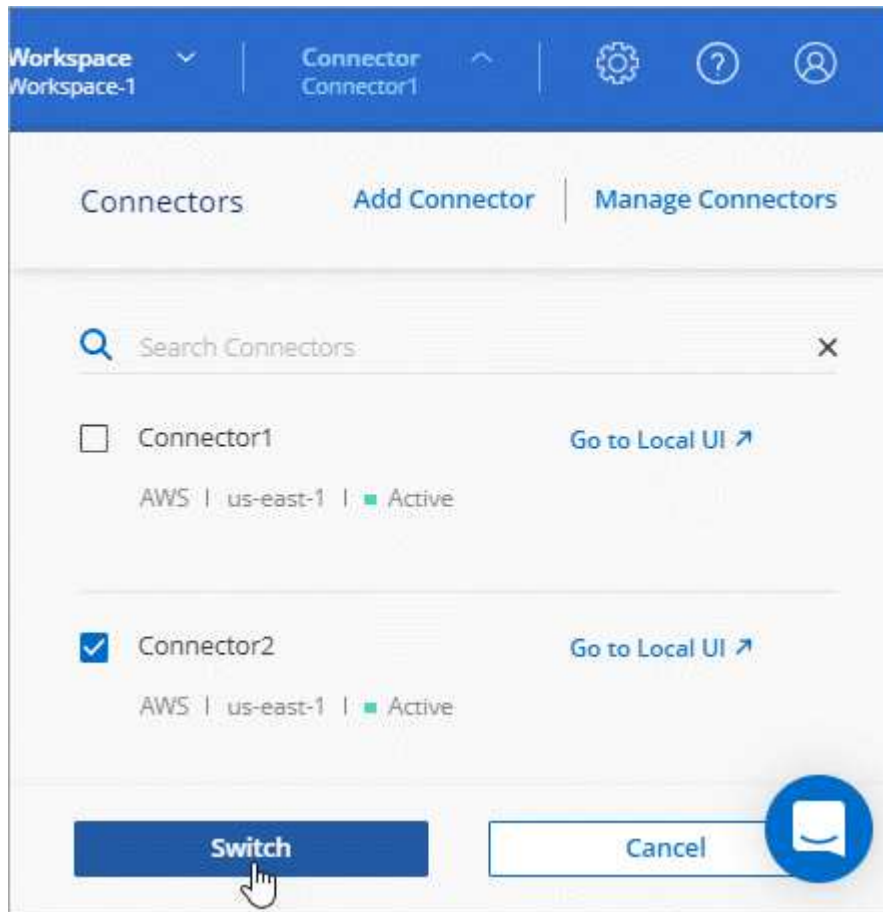
Switch between Connectors

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.

Set up a disaster recovery configuration

You can manage a working environment with multiple Connectors at the same time for disaster recovery purposes. If one Connector goes down, you can switch to the other Connector to immediately manage the working environment.

Steps

1. Switch to the other Connector that you want to manage with the working environment.
2. Discover the existing working environment.

- [Add existing Cloud Volumes ONTAP systems to BlueXP](#)
- [Discover ONTAP clusters](#)

3. If you're managing a Cloud Volumes ONTAP working environment, select **Settings > Connector Settings** and set the Capacity Management Mode to **Manual Mode**.

To avoid contention issues, only the main Connector should be set to **Automatic Mode**.

[Learn more about the capacity management mode](#)

Troubleshoot the Connector

To troubleshoot issues with the Connector, you can work with NetApp Support who might ask for your system ID, Connector version, or the latest AutoSupport messages. You can also view the NetApp Knowledge Base to troubleshoot issues yourself.

Related link

[Get help from NetApp Support.](#)

Find the system ID for a Connector

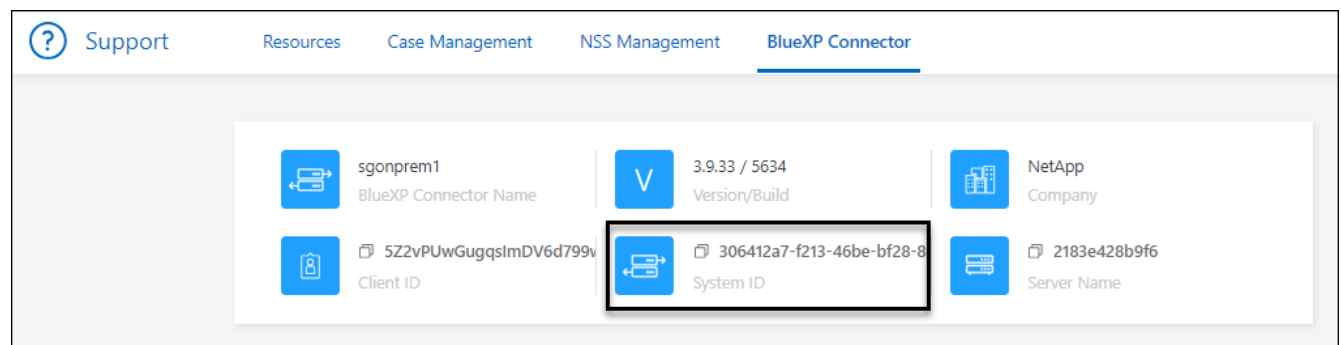
To help you get started, your NetApp representative might ask you for the system ID of your Connector. The ID is typically used for licensing and troubleshooting purposes.

Steps

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

The system ID appears at the top of the page.

Example



View a Connector's version

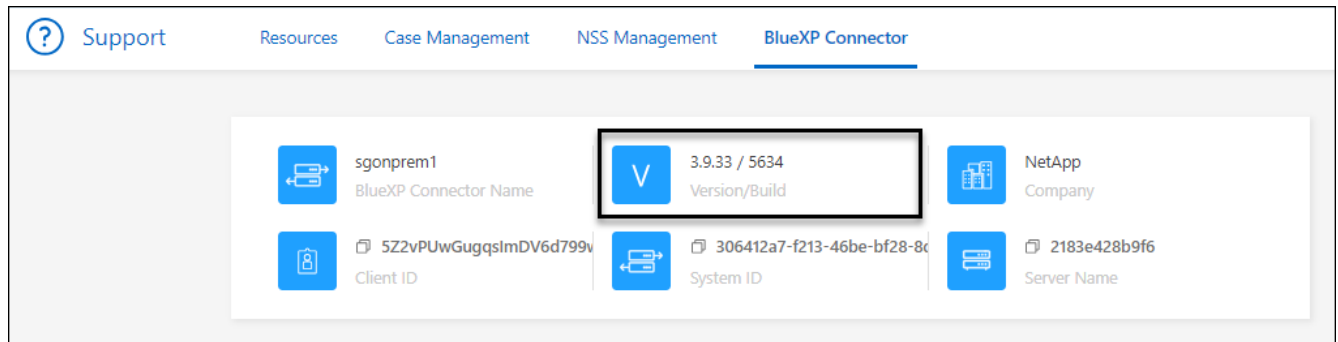
You can view the version of your Connector to verify that the Connector automatically upgraded to the latest release or because you need to share it with your NetApp representative.

Steps

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

2. Select **Support > BlueXP Connector**.

The version displays at the top of the page.

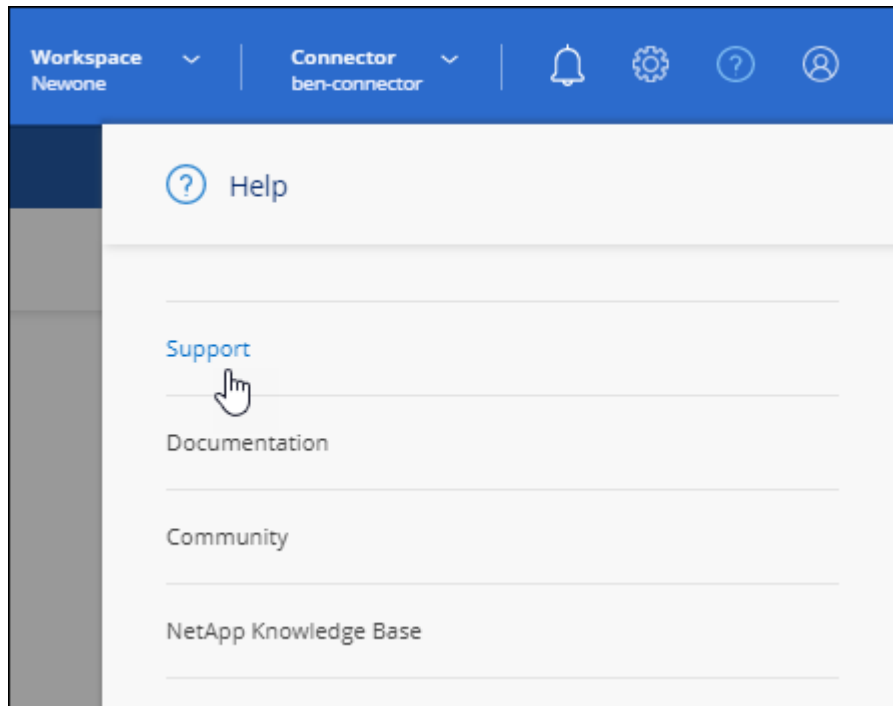


Download or send an AutoSupport message

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

Steps

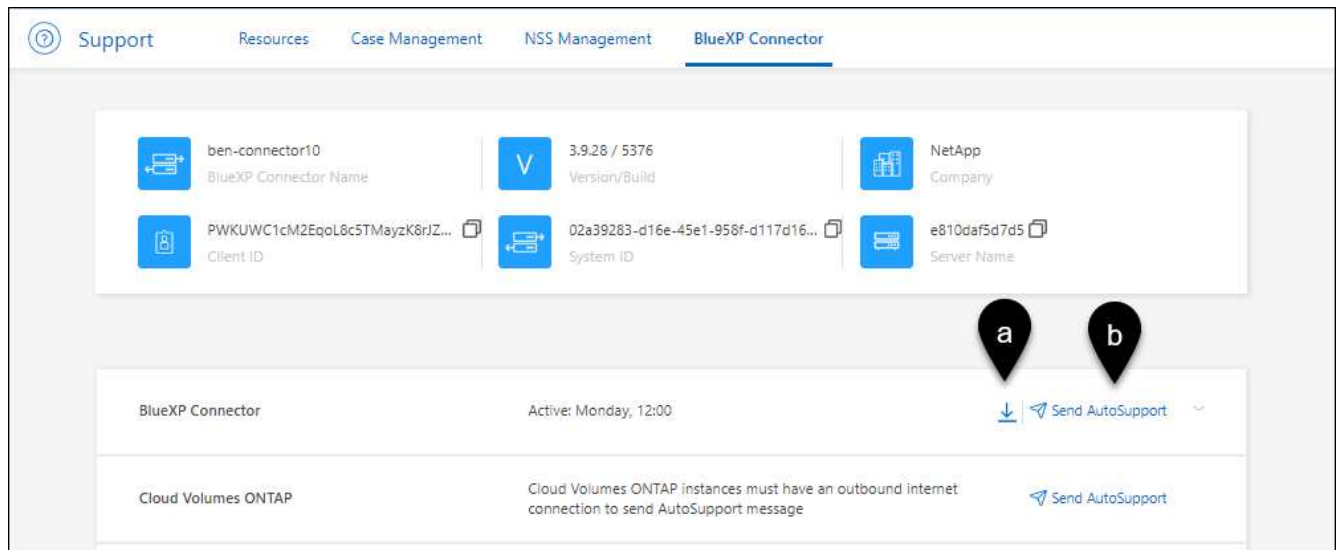
1. In the upper right of the BlueXP console, select the Help icon, and select **Support**.



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.



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](#)

Get help from the NetApp Knowledge Base

[View troubleshooting information created by the NetApp Support team.](#)

Uninstall and remove the Connector

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 the deployment mode that you're using. Once a Connector has been removed from your environment, you can remove it from BlueXP.

[Learn about BlueXP deployment modes.](#)

Uninstall the Connector when using standard or restricted mode

If you're using BlueXP in standard mode or restricted mode (in other words, the Connector host has outbound connectivity), then you should follow the steps below to uninstall the Connector software.

Steps

1. Connect to the Linux VM for the Connector.
2. 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.

Result

The Connector software is now uninstalled from the Linux host.

Uninstall the Connector when using private mode

If you're using BlueXP in private mode (in other words, the Connector host has *no* outbound connectivity), then you should follow the steps below to uninstall the Connector software.

Step

1. Connect to the Linux VM for the Connector.
2. From the Linux host, run the following commands:

```
./opt/application/netapp/ds/cleanup.sh  
rm -rf /opt/application/netapp/ds
```

Result

The Connector software is now uninstalled from the Linux host.

Remove Connectors from BlueXP

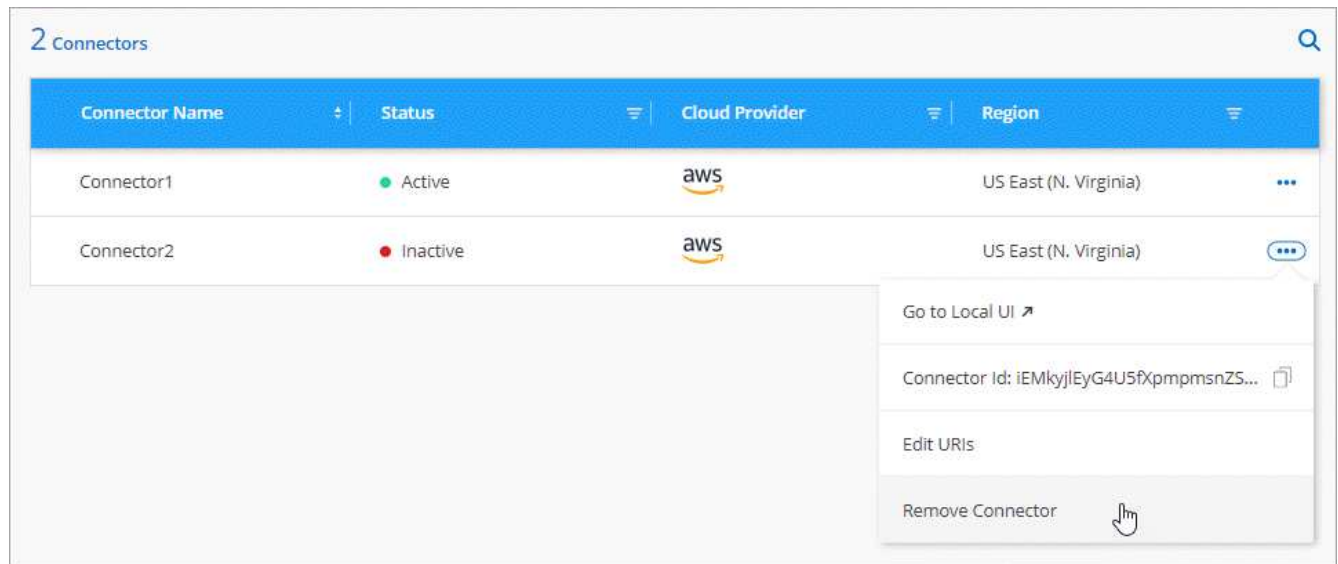
If a Connector is inactive, you can remove it from the list of Connectors in BlueXP. You might do this if you deleted the Connector virtual machine or if you uninstalled the Connector software.

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.

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 LTS.

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

- The installation includes Docker Engine, which is the required container orchestration tool.
- The user name for the EC2 Linux instance is ubuntu (for Connectors created prior to May 2023, the user name was 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 LTS.

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

- The installation includes Docker Engine, which is the required container orchestration tool.
- 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 LTS.

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

- The installation includes Docker Engine, which is the required container orchestration tool.
- 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.

- /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_occndata/_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

Copyright © 2024 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.