NetApp

Administer BlueXP

Set up and administration

NetApp
January 18, 2023

Table of Contents

Administer BlueXP

NetApp accounts

Managing your NetApp account

After you perform initial setup, you can administer your account settings later by managing users, service accounts, workspaces, and Connectors.

Learn more about how NetApp accounts work.

Managing your account with the Tenancy API

If you want to manage your account settings by sending API requests, then you'll need to use the *Tenancy* API. This API is different than the BlueXP API, which you use to create and manage Cloud Volumes ONTAP working environments.

View endpoints for the Tenancy API

Creating and managing users

The user's in your account can access the manage the resources in your account's workspaces.

Adding users

Associate users with your NetApp account so those users can create and manage working environments in BlueXP.

Steps

1. If the user hasn't already done so, ask the user to go to NetApp BlueXP website and sign up.

2. From the top of BlueXP, click the **Account** drop-down.

3. Click **Manage Account** next to the currently selected account.

4. From the Members tab, click **Associate User**.

5. Enter the user's email address and select a role for the user:

   ◦ **Account Admin**: Can perform any action in BlueXP.

   ◦ **Workspace Admin**: Can create and manage resources in assigned workspaces.

   ◦ **Compliance Viewer**: Can only view Cloud Data Sense compliance information and generate reports for workspaces that they have permission to access.

   ◦ **SnapCenter Admin**: Can use the SnapCenter Service to create application consistent backups and restore data using those backups. *This service is currently in Beta.*

6. If you selected Workspace Admin or Compliance Viewer, select one or more workspaces to associate with that user.

7. Click **Associate**.

Result

The user should receive an email from NetApp BlueXP titled "Account Association." The email includes the information needed to access BlueXP.

Removing users

Disassociating a user makes it so they can no longer access the resources in a NetApp account.

Steps

1. From the top of BlueXP, click the **Account** drop-down and click **Manage Account**.

2. From the Members tab, click the action menu in the row that corresponds to the user.

3. Click **Disassociate User** and click **Disassociate** to confirm.

Result

The user can no longer access the resources in this NetApp account.

Managing a Workspace Admin's workspaces

You can associate and disassociate Workspace Admins with workspaces at any time. Associating the user enables them to create and view the working environments in that workspace.

Steps

1. From the top of BlueXP, click the **Account** drop-down and click **Manage Account**.

2. From the Members tab, click the action menu in the row that corresponds to the user.

3. Click **Manage Workspaces**.

4. Select the workspaces to associate with the user and click **Apply**.

Result

The user can now access those workspaces from BlueXP, as long as the Connector was also associated with the workspaces.

Creating and managing service accounts

A service account acts as a "user" that can make authorized API calls to BlueXP for automation purposes. This makes it easier to manage automation because you don't need to build automation scripts based on a real person's user account who can leave the company at any time. And if you're using federation, you can create a token without generating a refresh token from the cloud.

You give permissions to a service account by assigning it a role, just like any other BlueXP user. You can also associate the service account with specific workspaces in order to control the working environments (resources) that the service can access.

When you create the service account, BlueXP enables you to copy or download a client ID and client secret for the service account. This key pair is used for authentication with BlueXP.

Creating a service account

Create as many service accounts as you need to manage the resources in your working environments.

Steps

1. From the top of BlueXP, click the **Account** drop-down.

2. Click **Manage Account** next to the currently selected account.

3. From the Members tab, click **Create Service Account**.

4. Enter a name and select a role. If you chose a role other than Account Admin, choose the workspace to associate with this service account.

5. Click **Create**.

6. Copy or download the client ID and client secret.

   The client secret is visible only once and is not stored anywhere by BlueXP. Copy or download the secret and store it safely.

7. Click **Close**.

Obtaining a bearer token for a service account

In order to make API calls to the Tenancy API, you'll need to obtain a bearer token for a service account.

Learn how to create a service account token

Copying the client ID

You can copy a service account's client ID at any time.

Steps

1. From the Members tab, click the action menu in the row that corresponds to the service account.

2. Click **Client ID**.

3. The ID is copied to your clipboard.

Recreating keys

Recreating the key will delete the existing key for this service account and then create a new key. You won't be able to use the previous key.

Steps

1. From the Members tab, click the action menu in the row that corresponds to the service account.

2. Click **Recreate Key**.

3. Click **Recreate** to confirm.

4. Copy or download the client ID and client secret.

   The client secret is visible only once and is not stored anywhere by BlueXP. Copy or download the secret and store it safely.
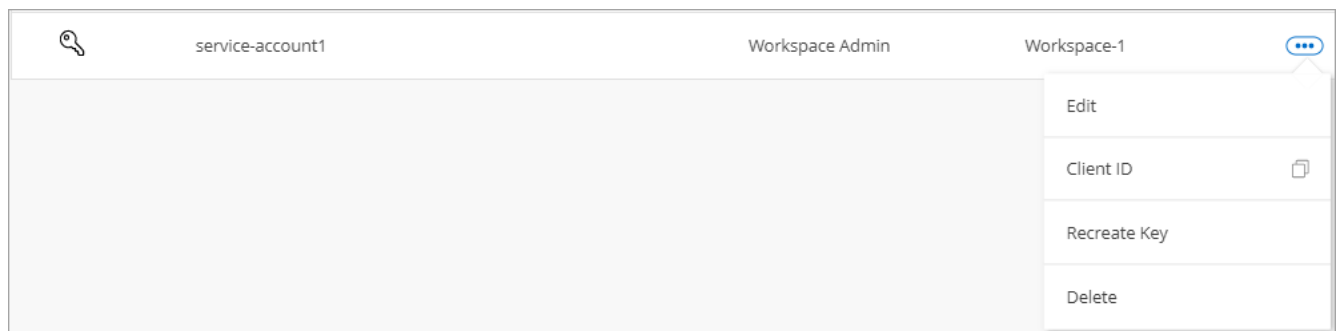
5. Click **Close**.

Deleting a service account

Delete a service account if you no longer need to use it.

Steps

1. From the Members tab, click the action menu in the row that corresponds to the service account.

2. Click **Delete**.

3. Click **Delete** again to confirm.

Managing workspaces

Manage your workspaces by creating, renaming, and deleting them. Note that you can't delete a workspace if it contains any resources. It must be empty.

Steps

1. From the top of BlueXP, click the **Account** drop-down and click **Manage Account**.

2. Click **Workspaces**.

3. Choose one of the following options:

   ◦ Click **Add New Workspace** to create a new workspace.

   ◦ Click **Rename** to rename the workspace.

   ◦ Click **Delete** to delete the workspace.

Managing a Connector's workspaces

You need to associate the Connector with workspaces so Workspace Admins can access those workspaces from BlueXP.

If you only have Account Admins, then associating the Connector with workspaces isn't required. Account Admins have the ability to access all workspaces in BlueXP by default.

Learn more about users, workspaces, and Connectors.

Steps

1. From the top of BlueXP, click the **Account** drop-down and click **Manage Account**.

2. Click **Connector**.

3. Click **Manage Workspaces** for the Connector that you want to associate.

4. Select the workspaces to associate with the Connector and click **Apply**.

Changing your account name

Change you account name at any time to change it to something meaningful for you.

Steps

1. From the top of BlueXP, click the **Account** drop-down and click **Manage Account**.

2. In the **Overview** tab, click the edit icon next to the account name.

3. Type a new account name and click **Save**.

Allowing private previews

Allow private previews in your account to get access to new NetApp cloud services that are made available as a preview in BlueXP.

Services in private preview are not guaranteed to behave as expected and might sustain outages and be missing functionality.

Steps

1. From the top of BlueXP, click the **Account** drop-down and click **Manage Account**.

2. In the **Overview** tab, enable the **Allow Private Preview** setting.

Allowing third-party services

Allow third-party services in your account to get access to third-party services that are available in BlueXP. Third-party services are cloud services similar to the services that NetApp offers, but they're managed and

supported by third-party companies.

Steps

1. From the top of BlueXP, click the **Account** drop-down and click **Manage Account**.
2. In the **Overview** tab, enable the **Allow Third Party Services** setting.

Disabling the SaaS platform

We don't recommend disabling the SaaS platform unless you need to in order to comply with your company's security policies. Disabling the SaaS platform limits your ability to use NetApp's integrated cloud services.

The following services aren't available from BlueXP if you disable the SaaS platform:

- Cloud Data Sense
- Kubernetes
- Cloud Tiering
- Global File Cache

If you do disable the SaaS platform, you'll need to perform all tasks from the local user interface that is available on a Connector.

> ⚠️ This is an irreversible action that will prevent you from using the BlueXP SaaS platform. You'll need to perform actions from the local Connector. You won't have the ability to use many of NetApp's integrated cloud services, and re-enabling the SaaS platform will require the help of NetApp support.

Steps

1. From the top of BlueXP, click the **Account** drop-down and click **Manage Account**.
2. In the Overview tab, toggle the option to disable use of the SaaS platform.

Monitoring operations in your account

You can monitor the status of the operations that BlueXP is performing to see if there are any issues that you need to address. You can view the status in the Notification Center, in the Timeline, or have notifications sent to your email.

This table provides a comparison of the Notification Center and the Timeline so you can understand what each has to offer.

Notification Center	Timeline
Shows high level status for events and actions	Provides details for each event or action for further investigation
Shows status for the current login session - the information won't appear in the Notification Center after you log off	Retains status for the last month
Shows only actions initiated in the user interface	Shows all actions from the UI or APIs
Shows user-initiated actions	Shows all actions, whether user-initiated or system-initiated

Notification Center	Timeline
Filter results by importance	Filter by service, action, user, status, and more
Provides the ability to email notifications to Account users and to others	No email capability

Monitoring activities using the Notification Center

Notifications track the progress of operations that you've initiated in BlueXP so you can verify whether the operation was successful or not. They enable you to view the status for many BlueXP actions that you initiated during your current login session. Not all services report information into the Notification Center at this time.

You can display the notifications by clicking the notification bell ( ) in the menu bar. The color of the little bubble in the bell indicates the highest level severity notification that is active. So if you see a red bubble, it means there's an important notification that you should look at.
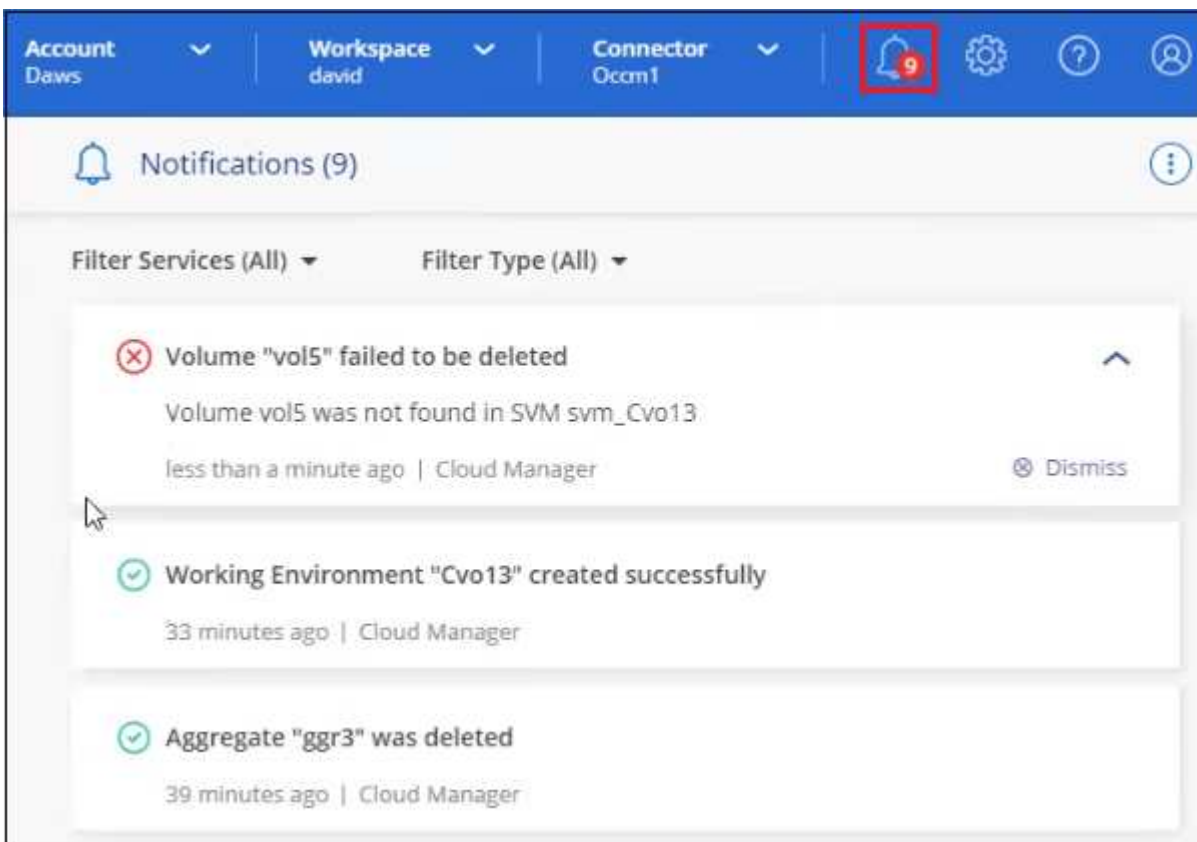
You can also configure BlueXP to send notifications by email so you can be informed of important system activity even when you're not logged into the system. Emails can be sent to any users who are part of your NetApp Cloud Account, or to any other recipients who need to be aware of certain types of system activity. See Setting email notification settings below.

Notification types

Notifications are classified in the following categories:

Notification type	Description
Critical	A problem occurred that might lead to service disruption if corrective action is not taken immediately.
Error	An action or process ended with failure, or could lead to failure if corrective action is not taken.
Warning	An issue that you should be aware of to make sure it does not reach the critical severity. Notifications of this severity do not cause service disruption, and immediate corrective action might not be required.
Recommendation	A system recommendation for you to take an action to improve the system or a certain service; for example: costs saving, suggestion for new services, recommended security configuration, etc.
Information	A message that provides additional information about an action or process.
Success	An action or process completed successfully.

Filtering notifications

By default you'll see all notifications. You can filter the notifications that you see in the Notification Center to show only those notifications that are important to you. You can filter by BlueXP "Service" and by notification "Type".

For example, if you want to see only "Error" and "Warning" notifications for BlueXP operations, select those entries and you'll see only those types of notifications.

Setting email notification settings

You can send specific types of notifications by email so you can be informed of important system activity even when you're not logged into BlueXP. Emails can be sent to any users who are part of your NetApp Account, or to any other recipients who need to be aware of certain types of system activity.

(i)

- At this time, only Cloud Sync, Cloud Backup, and Ransomware Protection are sending notifications by email. Additional services will be added in future releases.
- Sending email notifications is not supported when the Connector is installed in a site without internet access.

By default, BlueXP Account Admins will receive emails for all "Critical" and "Recommendation" notifications. All other users and recipients are configured, by default, not to receive any notification emails.

You must be an Account Admin to customize the notifications settings.

Steps

1. From the BlueXP menu bar, click **Settings > Alerts and Notifications Settings**.
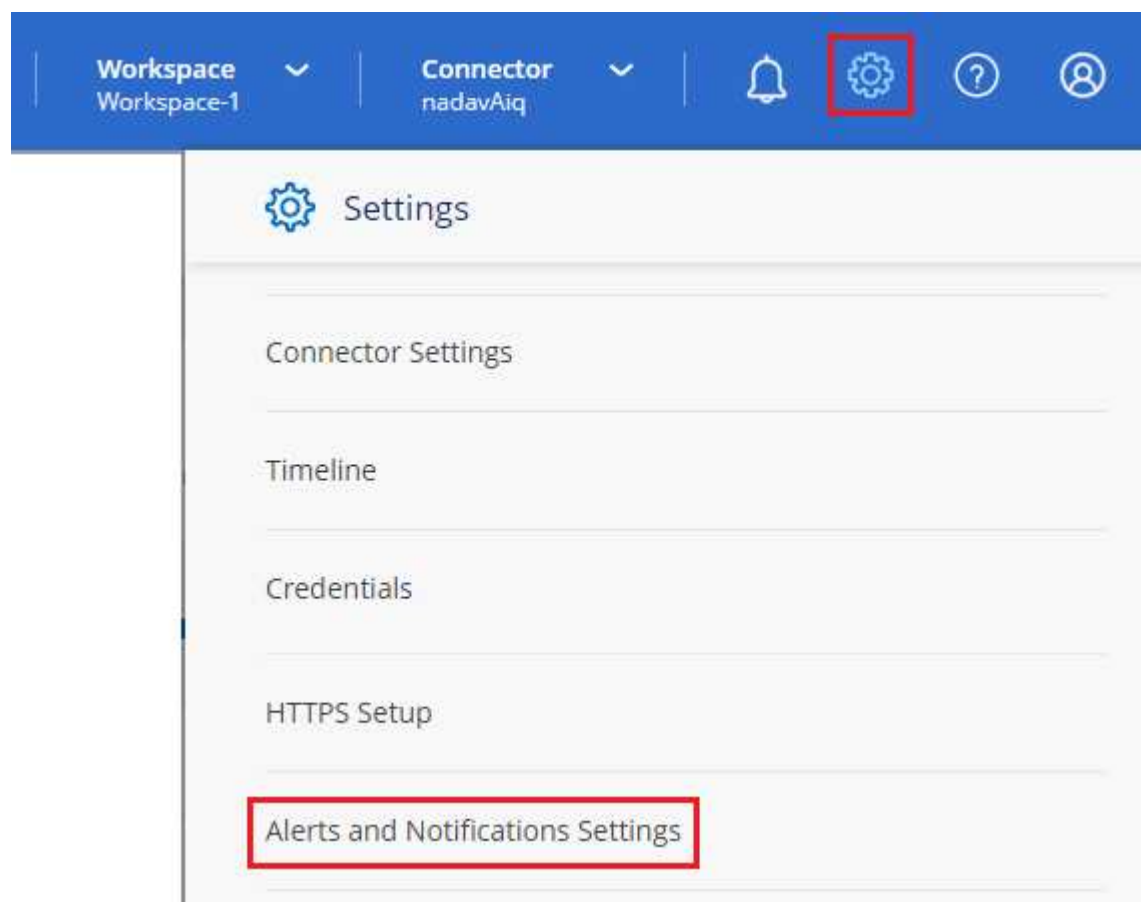
2. Select a user, or multiple users, from either the *Account Users* tab or the *Additional Recipients* tab, and choose the type of notifications to be sent:

   ◦ To make changes for a single user, click the menu in the Notifications column for that user, check the types of Notifications to be sent, and click **Apply**.

   ◦ To make changes for multiple users, check the box for each user, click **Manage Email Notifications**, check the types of Notifications to be sent, and click **Apply**.

Adding additional email recipients

The users who appear in the *Account Users* tab are populated automatically from the users in your NetApp Account (from the Manage Account page). You can add email addresses in the *Additional Recipients* tab for other people, or groups, who do not have access to BlueXP, but who need to be notified about certain types of alerts and notifications.

Steps

1. From the Alerts and Notifications Settings page, click **Add New Recipients**.

2. Enter the name, email address, and select the types of Notifications that recipient will receive, and click **Add New Recipient**.

Dismissing notifications

You can remove notifications from the page if you no longer need to see them. You can dismiss all notifications at once, or you can dismiss individual notifications.

To dismiss all notifications, in the Notification Center, click ⋮ and select **Dismiss All**.

To dismiss individual notifications, hover your cursor over the notification and click **Dismiss**.

Auditing user activity in your account

The Timeline in BlueXP shows the actions that users completed to manage your account. This includes management actions such as associating users, creating workspaces, creating Connectors, and more.

Checking the Timeline can be helpful if you need to identify who performed a specific action, or if you need to identify the status of an action.

Steps

1. From the BlueXP menu bar, click **Settings > Timeline**.
2. Under the Filters, click **Service**, enable **Tenancy**, and click **Apply**.

Result

The Timeline updates to show you account management actions.

Roles

The Account Admin, Workspace Admin, Compliance Viewer, and SnapCenter Admin roles provide specific permissions to users.

The Compliance Viewer role is for read-only Cloud Data Sense access.

Task	Account Admin	Workspace Admin	Compliance Viewer	SnapCenter Admin
Manage working environments	Yes	Yes	No	No
Enable services on working environments	Yes	Yes	No	No
View data replication status	Yes	Yes	No	No
View the timeline	Yes	Yes	No	No
Switch between workspaces	Yes	Yes	Yes	No

Task	Account Admin	Workspace Admin	Compliance Viewer	SnapCenter Admin
View Data Sense scan results	Yes	Yes	Yes	No
Delete working environments	Yes	No	No	No
Connect Kubernetes clusters to working environments	Yes	No	No	No
Receive the Cloud Volumes ONTAP report	Yes	No	No	No
Create Connectors	Yes	No	No	No
Manage NetApp accounts	Yes	No	No	No
Manage credentials	Yes	No	No	No
Modify BlueXP settings	Yes	No	No	No
View and manage the Support Dashboard	Yes	No	No	No
Remove working environments from BlueXP	Yes	No	No	No
Install an HTTPS certificate	Yes	No	No	No
Use the SnapCenter Service	Yes	Yes	No	Yes

Related links

- Setting up workspaces and users in the NetApp account
- Managing workspaces and users in the NetApp account

Connectors

Advanced deployment

Create a Connector from the AWS Marketplace

For an AWS commercial region, it's best to create a Connector directly from BlueXP, but you can launch a Connector from the AWS Marketplace, if you prefer. For AWS Government regions, you can't deploy the Connector in a Government region from the BlueXP SaaS website, so the next best option is to do so from the AWS Marketplace.

> 💡 You can also download and install the Connector software on an existing Linux host in your network or in the cloud. Learn how to install the Connector on an existing Linux host.

Create the Connector in an AWS commercial region

You can launch the Connector instance in an AWS commercial region directly from the AWS Marketplace offering for BlueXP.

Before you get started

The IAM user who creates the Connector must have AWS Marketplace permissions to subscribe and unsubscribe.

Steps

1. Set up permissions in AWS:

   a. From the IAM console, create the required policies by copying and pasting the contents of the IAM policies for the Connector.

   b. Create an IAM role with the role type Amazon EC2 and attach the policies that you created in the previous step to the role.

2. Go to the BlueXP page on the AWS Marketplace to deploy the Connector from an AMI:

3. On the Marketplace page, click **Continue to Subscribe** and then click **Continue to Configuration**.
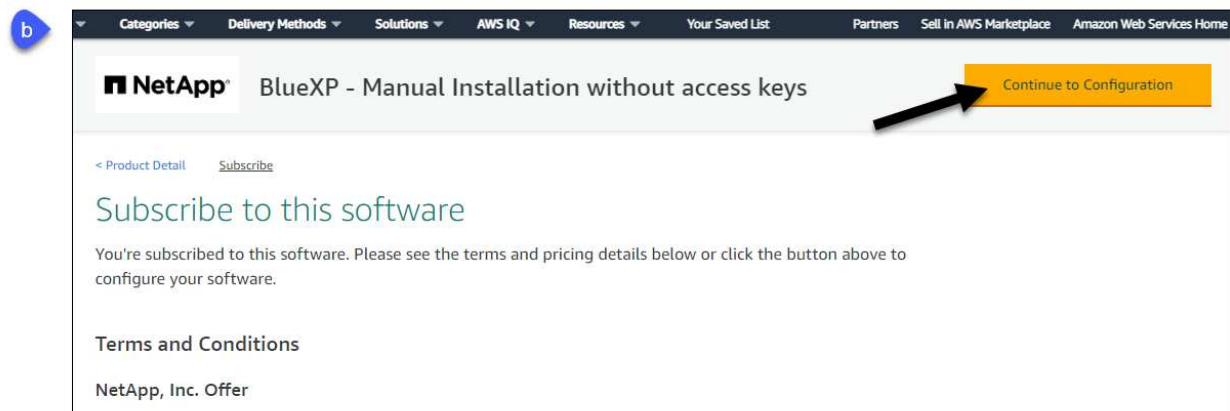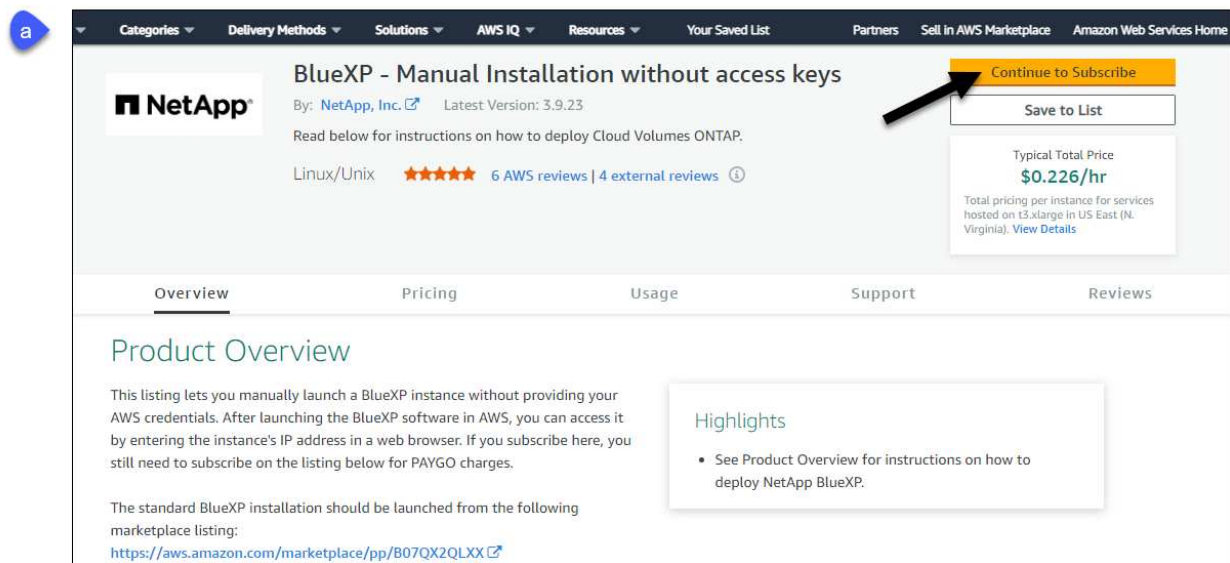
4. Change any of the default options and click **Continue to Launch**.

5. 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.

6. 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.

   ◦ **Configure storage**: Keep the default storage options.

   ◦ **Advanced details**: Under **IAM instance profile**, choose the IAM role that you created in step 1.

   ◦ **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.

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

   https://*ipaddress*

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

   a. Specify the NetApp account to associate with the Connector.

   Learn about NetApp accounts.

   b. Enter a name for the system.

9. Open a web browser and go to https://console.bluexp.netapp.com to start using the Connector with BlueXP.

Result

The Connector is now installed and set up with your NetApp account. BlueXP will automatically use this Connector when you create new working environments. But if you have more than one Connector, you'll need to switch between them.

If you have Amazon S3 buckets in the same AWS account where you created the Connector, you'll see an Amazon S3 working environment appear on the Canvas automatically. Learn more about what you can do with this working environment.

Create the Connector in an AWS Government region

To deploy the Connector in an AWS Government region, you need to go to the EC2 service and select the BlueXP offering from the AWS Marketplace.

Steps

1. Set up permissions in AWS:

   a. From the IAM console, create your own policy by copying and pasting the contents of the IAM policy for the Connector.

   b. Create an IAM role with the role type Amazon EC2 and attach the policy that you created in the previous step to the role.

2. Go to the BlueXP offering in the AWS Marketplace.

   The IAM user must have AWS Marketplace permissions to subscribe and unsubscribe.

   a. Open the EC2 service and select **Launch instance**.

   b. Select **AWS Marketplace**.

   c. Search for BlueXP and select the offering.

   d. Click **Continue**.

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

   ◦ **Choose an Instance Type**: Depending on region availability, choose one of the supported instance types (t3.xlarge is recommended).

     Review the instance requirements.

   ◦ **Configure Instance Details**: Select a VPC and subnet, choose the IAM role that you created in step 1, enable termination protection (recommended), and choose any other configuration options that meet your requirements.

- **Add Storage**: Keep the default storage options.

- **Add Tags**: Enter tags for the instance, if desired.

- **Configure Security Group**: Specify the required connection methods for the Connector instance: SSH, HTTP, and HTTPS.

- **Review**: Review your selections and click **Launch**.

AWS launches the software with the specified settings. 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 NetApp account to associate with the Connector.

    Learn about NetApp accounts.

    b. Enter a name for the system.

Result

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

Any time that you want to use BlueXP, open your web browser and connect to the IP address of the Connector instance: https://*ipaddress*

Since the Connector was deployed in a Government region, it's not accessible from https://console.bluexp.netapp.com.

Open port 3128 for AutoSupport messages

If you plan to deploy Cloud Volumes ONTAP systems in a subnet where an outbound internet connection won't be available, then BlueXP automatically configures Cloud Volumes ONTAP to use the Connector as a proxy server.

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.

If you use the default security group for Cloud Volumes ONTAP, then no changes are needed to its security group. But if you plan to define strict outbound rules for Cloud Volumes ONTAP, then you'll also need to ensure that the Cloud Volumes ONTAP security group allows *outbound* connections over port 3128.

Create a Connector from the Azure Marketplace

For an Azure commercial region, it's best to create a Connector directly from BlueXP, but you can launch a Connector from the Azure Marketplace, if you prefer. For Azure Government regions, you can't deploy the Connector in a Government region from the BlueXP SaaS website, so the next best option is to do so from the Azure Marketplace.

> You can also download and install the Connector software on an existing Linux host in your network or in the cloud. Learn how to install the Connector on an existing Linux host.

Creating a Connector in Azure

Deploy the Connector in Azure using the image in the Azure Marketplace and then log in to the Connector to specify your NetApp account.

Steps

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

   ◦ Azure Marketplace page for commercial regions

   ◦ Azure Marketplace page for Azure Government 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.

     Learn more about security group rules for the Connector.

   ◦ Under **Management**, enable **System assigned managed identity** for the Connector 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. Learn more about managed identities

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 NetApp account to associate with the Connector.

      Learn about NetApp accounts.

   b. Enter a name for the system.

Result

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

If the Connector is in an Azure commercial region, open a web browser and go to https://console.bluexp.netapp.com to start using the Connector with BlueXP.

If the Connector is in an Azure Government region, you can use BlueXP by opening your web browser and connecting to the IP address of the Connector instance: https://*ipaddress*

Since the Connector was deployed in a Government region, it's not accessible from https://console.bluexp.netapp.com.

Granting Azure permissions

When you deployed the Connector in Azure, you should have enabled a system-assigned managed identity. You must now grant the required Azure permissions by creating a custom role and then by assigning the role to the Connector virtual machine for one or more subscriptions.

Steps

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.
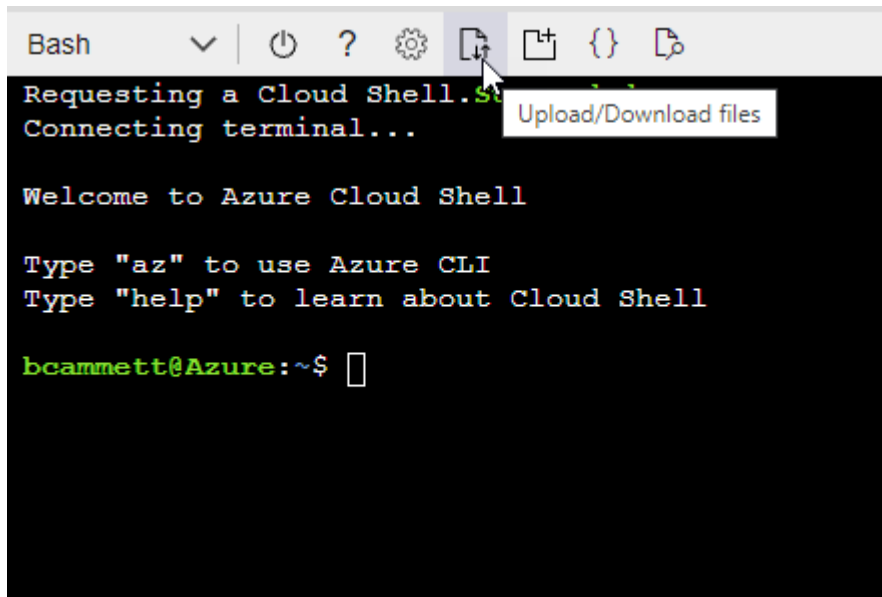
      Example

```
"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 role to the Connector virtual machine for one or more subscriptions:

a. Open the **Subscriptions** service and then select the subscription in which you want to deploy Cloud Volumes ONTAP systems.

b. Click **Access control (IAM)** > **Add** > **Add role assignment**.

c. 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.

d. In the **Members** tab, complete the following steps:

- Assign access to a **Managed identity**.
- Click **Select members**, select the subscription in which the Connector virtual machine was created, choose **Virtual machine**, and then select the Connector virtual machine.
- Click **Select**.
- Click **Next**.

e. Click **Review + assign**.

Result

The Connector now has the permissions that it needs to manage resources and processes within your public cloud environment. BlueXP will automatically use this Connector when you create new working environments. But if you have more than one Connector, you'll need to switch between them.

If you have Azure Blob storage in the same Azure account where you created the Connector, you'll see an Azure Blob working environment appear on the Canvas automatically. Learn more about what you can do with this working environment.

Open port 3128 for AutoSupport messages

If you plan to deploy Cloud Volumes ONTAP systems in a subnet where an outbound internet connection won't be available, then BlueXP automatically configures Cloud Volumes ONTAP to use the Connector as a proxy server.

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.

If you use the default security group for Cloud Volumes ONTAP, then no changes are needed to its security group. But if you plan to define strict outbound rules for Cloud Volumes ONTAP, then you'll also need to ensure that the Cloud Volumes ONTAP security group allows *outbound* connections over port 3128.

Install the Connector on an existing Linux host that has internet access

The most common way to create a Connector is directly from BlueXP or from a cloud provider's marketplace. But you have the option to download and install the Connector software on an existing Linux host in your network or in the cloud. These steps are specific to hosts that have internet access.

Learn about other ways to deploy a Connector.

> If you want to create a Cloud Volumes ONTAP system in Google Cloud, then you must have a Connector that's running in Google Cloud as well. You can't use a Connector that's running in AWS, Azure, or on-prem.

Verify host requirements

The Connector software must run on a host that meets specific operating system requirements, RAM requirements, port requirements, and so on.

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

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.

Azure VM size

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

GCP 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

Supported operating systems

- CentOS 7.6
- CentOS 7.7
- CentOS 7.8
- CentOS 7.9
- Red Hat Enterprise Linux 7.6
- Red Hat Enterprise Linux 7.7
- Red Hat Enterprise Linux 7.8
- Red Hat Enterprise Linux 7.9
- Red Hat Enterprise Linux 8.6

  The Red Hat Enterprise Linux system must be registered with Red Hat Subscription Management. If it is not registered, the system cannot 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 CentOS or Red Hat Enterprise Linux
Red Hat Solution: Which hypervisors are certified to run Red Hat Enterprise Linux?

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

Outbound internet access

The installer for the Connector must access 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://cloudmanagerinfraprod.azurecr.io
- https://production-artifacts.cloudmanager.cloud.netapp.com
- 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.

Install the Connector

After you verify that you have a supported Linux host, you can obtain the Connector software and then install it.

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.

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. Download the Connector software from the NetApp Support Site, and then copy it to the Linux host.

   You should download the Connector installer that's meant for use in your network or in the cloud.

3. Assign permissions to run the script.

   ```
   chmod +x OnCommandCloudManager-V3.9.23
   ```

4. Run the installation script.

```
  ./OnCommandCloudManager-V3.9.23 --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-V3.9.23 --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.

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. If you installed the Connector in Google Cloud, set up a service account that has the permissions that BlueXP needs to create and manage Cloud Volumes ONTAP systems in projects.

   a. Create a role in GCP that includes the permissions defined in the Connector policy for GCP.

   b. Create a GCP service account and apply the custom role that you just created.

   c. Associate this service account with the Connector VM.

d. 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.

4. After you log in, set up BlueXP:

a. Specify the NetApp account to associate with the Connector.

Learn about NetApp accounts.

b. Enter a name for the system.

Result

The Connector is now installed and set up with your NetApp account. BlueXP will automatically use this Connector when you create new working environments.

After you finish

Set up permissions so BlueXP can manage resources and processes within your public cloud environment:

- AWS: Set up an AWS account and then add it to BlueXP
- Azure: Set up an Azure account and then add it to BlueXP
- Google Cloud: See step 3 above

Install the Connector on-prem without internet access

You can install the Connector on an on-premises Linux host that doesn't have internet access. You can then discover on-prem ONTAP clusters, replicate data between them, back up volumes using Cloud Backup, and scan them with Cloud Data Sense.

These installation instructions are specifically for the use case described above. Learn about other ways to deploy a Connector.

Verify host requirements

The Connector software must run on a host that meets specific operating system requirements, RAM requirements, port requirements, and so on.

A dedicated host is required

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

CPU

4 cores or 4 vCPUs

RAM

14 GB

Supported operating systems

- CentOS 7.6
- CentOS 7.7
- CentOS 7.8
- CentOS 7.9

- Red Hat Enterprise Linux 7.6
- Red Hat Enterprise Linux 7.7
- Red Hat Enterprise Linux 7.8
- Red Hat Enterprise Linux 7.9
- Red Hat Enterprise Linux 8.6

  The Red Hat Enterprise Linux system must be registered with Red Hat Subscription Management. If it is not registered, the system cannot 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 CentOS or Red Hat Enterprise Linux
Red Hat Solution: Which hypervisors are certified to run Red Hat Enterprise Linux?

Disk type

An SSD is required

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 or later is required on the host before you install the Connector. View installation instructions

Install the Connector

After you verify that you have a supported Linux host, you can obtain the Connector software and then install it.

Required privileges

Root privileges are required to install the Connector.

Steps

1. Verify that docker is enabled and running.

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

2. Download the Connector software from the NetApp Support Site

3. Copy the installer to the Linux host.

4. Assign permissions to run the script.

   ```
   chmod +x /path/cloud-manager-connector-offline-v3.9.23
   ```

5. Run the installation script:

```
sudo /path/cloud-manager-connector-offline-v3.9.23
```
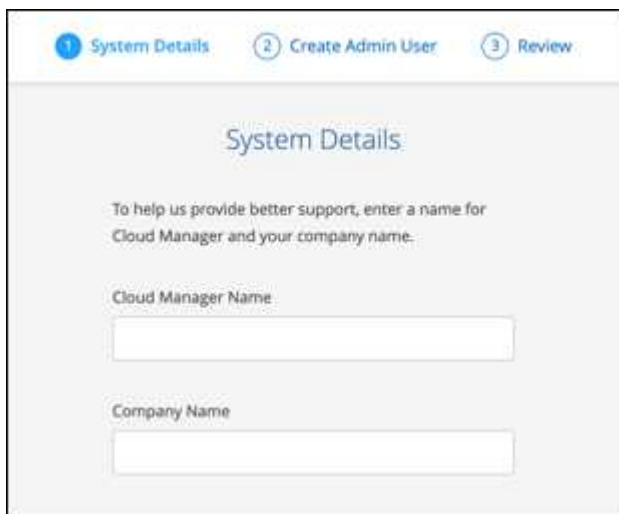
6. Open a web browser and enter https://*ipaddress* where *ipaddress* is the IP address of the Linux host.

   You should see the following screen.
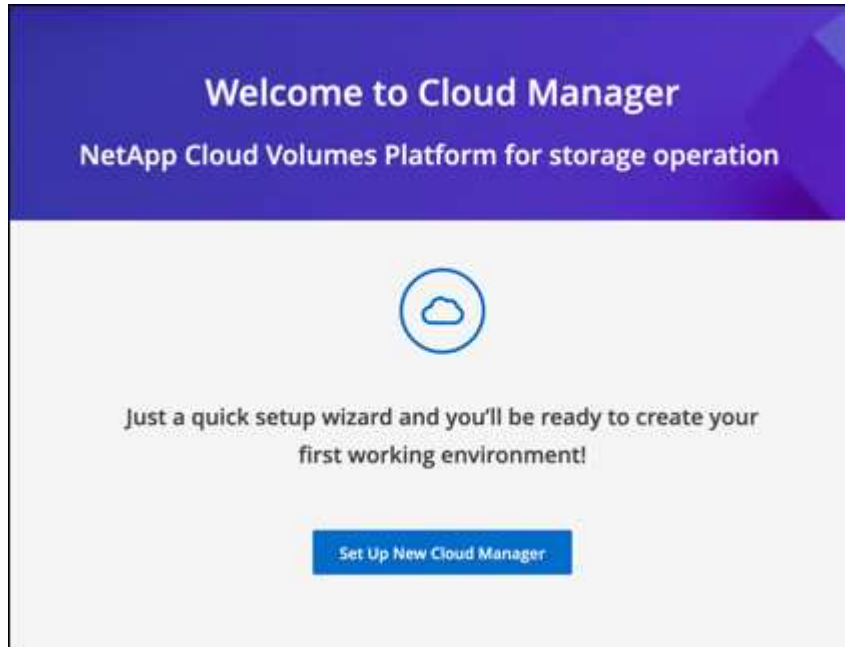
7. Click **Set Up New BlueXP** and follow the prompts to set up the system.

   ◦ **System Details**: Enter a name for the Connector and your company name.

   ◦ **Create Admin User**: Create the admin user for the system.

   This user account runs locally on the system. There's no connection to the auth0 service available through BlueXP.

◦ **Review**: Review the details, accept the license agreement, and then click **Set Up**.

8. Log in to BlueXP using the admin user that you just created.

Result

The Connector is now installed and you can start using the BlueXP features that are available in a dark site deployment.

What's next?

- Discover on-prem ONTAP clusters
- Replicate data between on-prem ONTAP clusters
- Back up on-prem ONTAP volume data to StorageGRID using Cloud Backup
- Scan on-prem ONTAP volume data using Cloud Data Sense

When new versions of the Connector software are available, they'll be posted to the NetApp Support Site. Learn how to upgrade the Connector.

Finding the system ID for a Connector

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

Steps

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

2. Click **Support > Connector**.

   The system ID appears at the top.

   Example
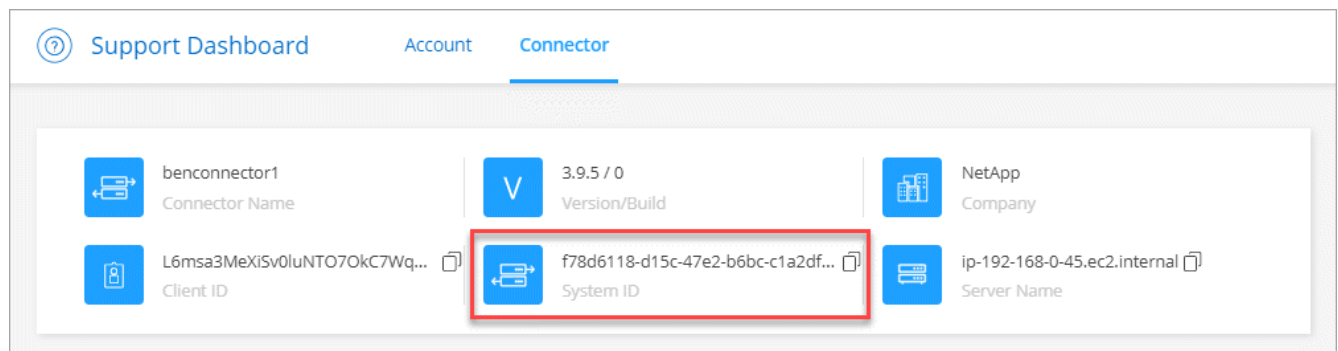
Managing existing Connectors

After you create one or more Connectors, you can manage them by switching between Connectors, connecting to the local user interface running on a Connector, and more.

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. Click the **Connector** drop-down, select another Connector, and then click **Switch**.
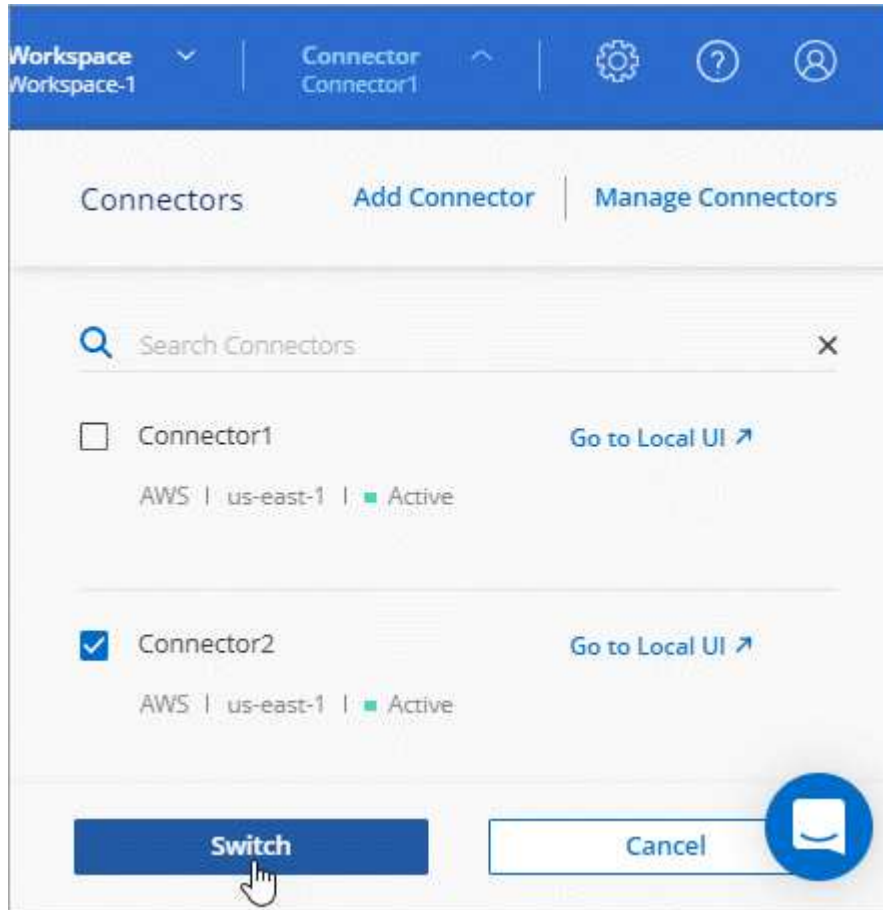
BlueXP refreshes and shows the Working Environments associated with the selected Connector.

Access the local UI

While you should perform almost all tasks from the SaaS user interface, a local user interface is still available on the Connector. If you're accessing BlueXP from a Government region or a site that doesn't have outbound internet access, then you need to use the local user interface running on the Connector.

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. Enter your user name and password to log in.

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. Connect to the Connector local UI, as described in the section above.

2. In the upper right of the BlueXP console, click the Help icon, and select **Support**.
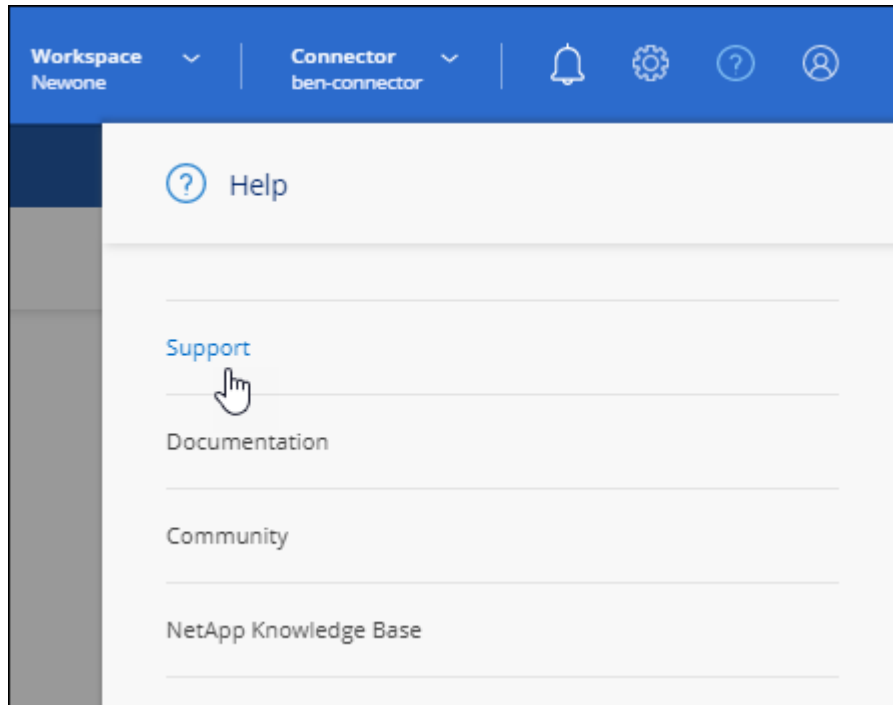
3. Click **Connector**.

4. 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. Click **Send AutoSupport** to directly send the message to NetApp Support.
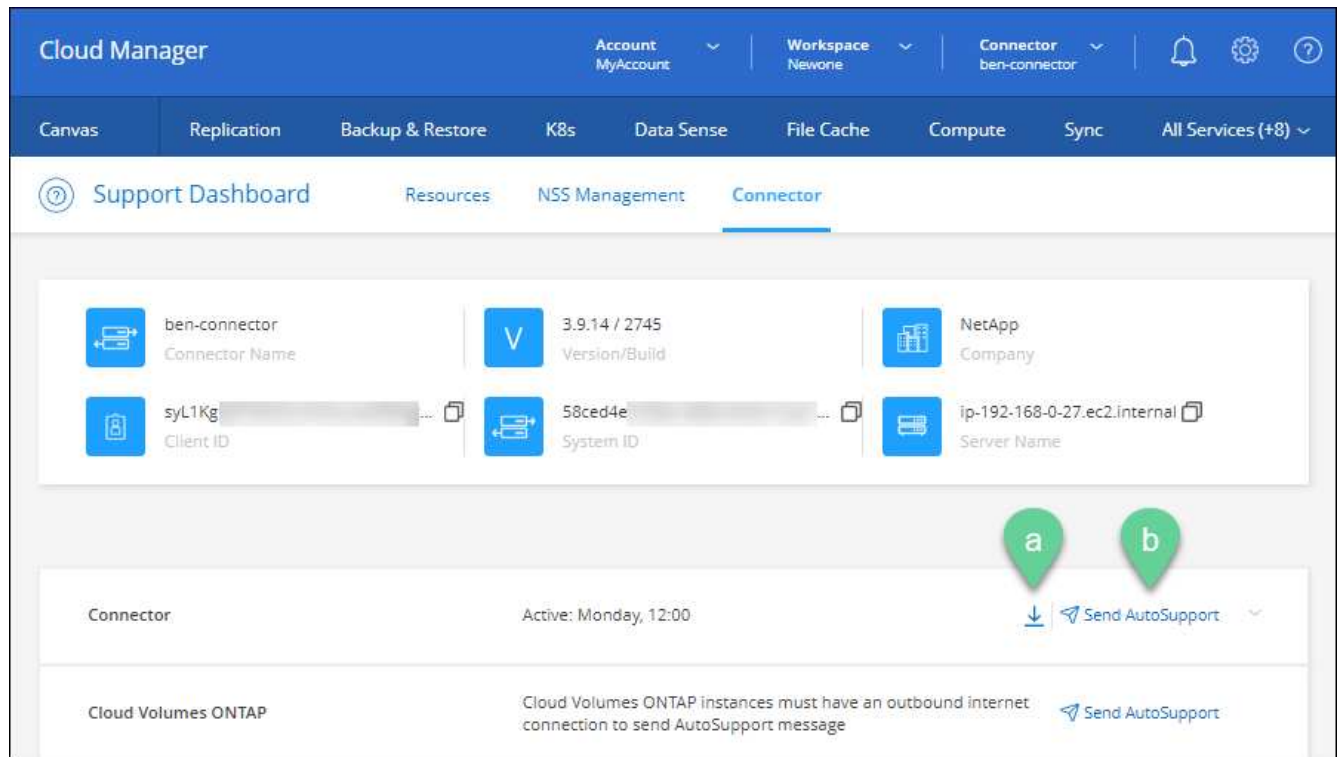
Connect to the Linux VM

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](#)

Apply security updates

Update the operating system on the Connector to ensure that it's patched with the latest security updates.

Steps

1. Access the CLI shell on the Connector host.

2. Run the following commands with elevated privileges:

```
sudo -s
service netapp-service-manager stop
yum -y update --security
service netapp-service-manager start
```

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. Click the menu and select **Advanced > Configuration Backups**.

   d. Click **Set Backup Target**.

Edit a Connector's URIs

Add and remove the URIs for a Connector.

Steps

1. Click the **Connector** drop-down from the BlueXP header.

2. Click **Manage Connectors**.

3. Click the action menu for a Connector and click **Edit URIs**.

4. Add and remove URIs and then click **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.

Upgrade the Connector on-prem without internet access

If you installed the Connector on an on-premises host that doesn't have internet access, 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 user interface will be unavailable during the upgrade.

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-v3.9.14
```

4. Run the installation script:

```
sudo /path/cloud-manager-connector-offline-v3.9.14
```

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

What about software upgrades 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.

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. Click the **Connector** drop-down from the BlueXP header.
2. Click **Manage Connectors**.
3. Click the action menu for an inactive Connector and click **Remove Connector**.
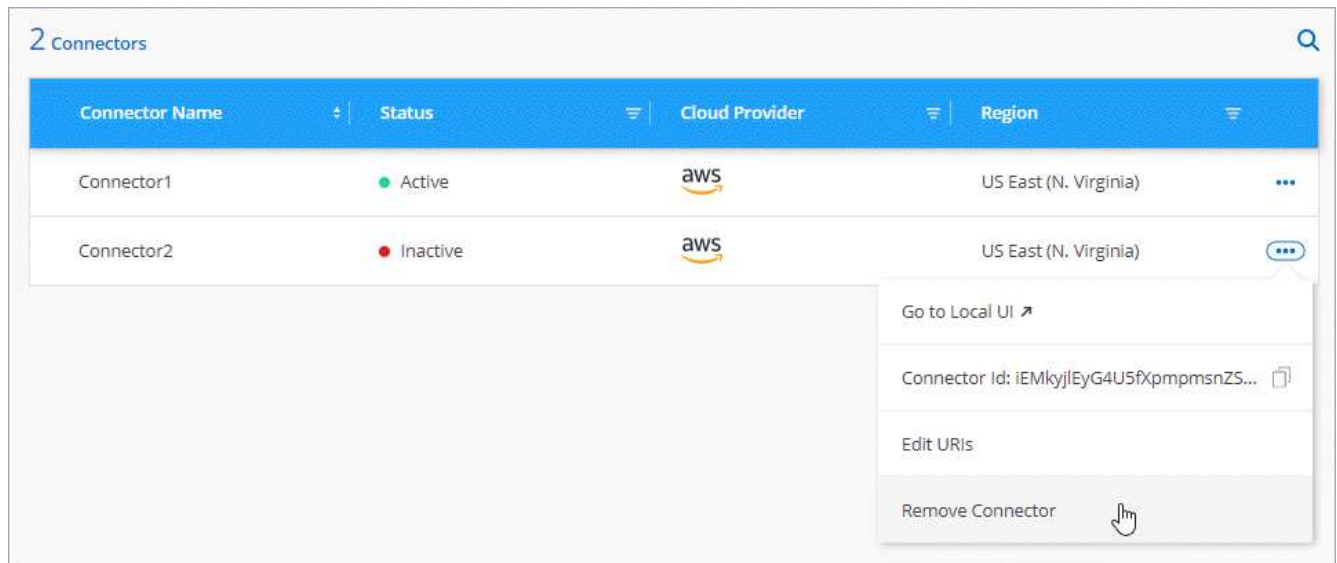
4. Enter the name of the Connector to confirm and then click Remove.

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
```

Managing an HTTPS certificate for secure access

By default, BlueXP uses a self-signed certificate for HTTPS access to the web console. 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.

Installing an HTTPS certificate

Install a certificate signed by a CA for secure access.

Steps

1. In the upper right of the BlueXP console, click 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 click **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 click **Install**.

Option	Description
Install your own CA-signed certificate	a. Select **Install CA-signed certificate**. b. Load both the certificate file and the private key and then click **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:
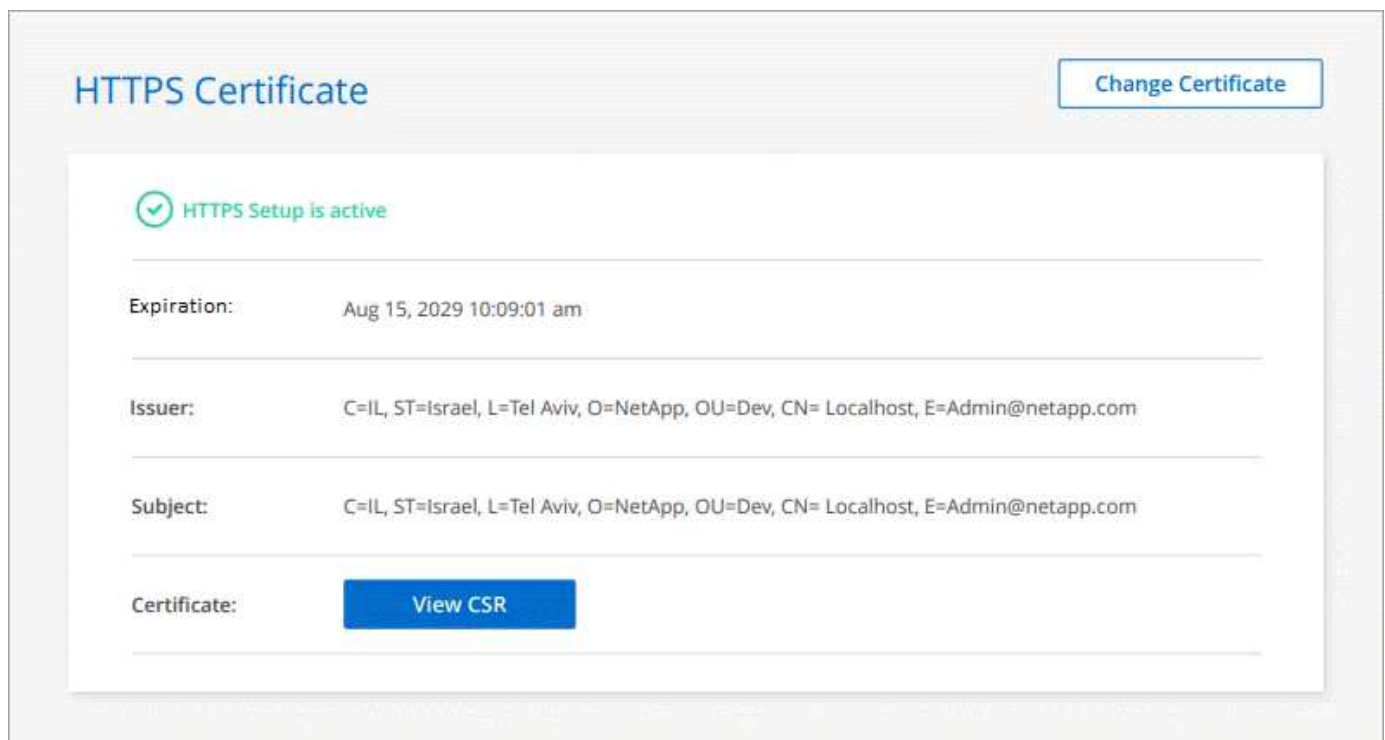
Renewing the BlueXP HTTPS certificate

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, click the Settings icon, and select **HTTPS Setup**.

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

2. Click **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.

Configuring a Connector to use an HTTP proxy server

If your corporate policies require you to use a proxy server for all HTTP communication to the internet, then you must configure your Connectors to use an HTTP proxy server. The proxy server can be in the cloud or in your network.

> ⓘ   BlueXP doesn't support using an HTTPS proxy with the Connector.

Configuring the Connector to use an HTTP 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. Log in to the BlueXP SaaS interface from a machine that has a network connection to the Connector instance.

   If the Connector doesn't have a public IP address, you'll need a VPN connection or you'll need to connect from a jump host that's in the same network as the Connector.

2. Click the **Connector** drop-down and then click **Go to local UI** for a specific Connector.

The BlueXP interface running on the Connector loads in a new browser tab.

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

4. Under **General**, click **HTTP Proxy Configuration**.

5. Set up the proxy:

   a. Click **Enable Proxy**.

   b. Specify the server using the syntax http://*address:port*

   c. Specify a user name and password if basic authentication is required for the server

   d. Click **Save**.

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

Enable direct API traffic

If you configured a proxy server, you can send API calls directly to BlueXP without going through the proxy. This option is supported with Connectors that are running in AWS, in Azure, or in Google Cloud.

Steps

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

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

Default configuration for the Connector

You might want to learn more about the Connector 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 Red Hat Enterprise Linux 7.6 (HVM).

  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 CentOS 7.6.

  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 or from the cloud provider's marketplace, note the following:

- The VM instance is n2-standard-4.
- The operating system for the image is Red Hat Enterprise Linux 8.6.

  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

Manage PAYGO subscriptions and contracts

When you subscribe to BlueXP from a cloud provider's marketplace, you're redirected to the BlueXP website where you need to save your subscription and associate it with specific accounts. After you've subscribed, each subscription is available to manage from the Digital Wallet.

View your subscriptions
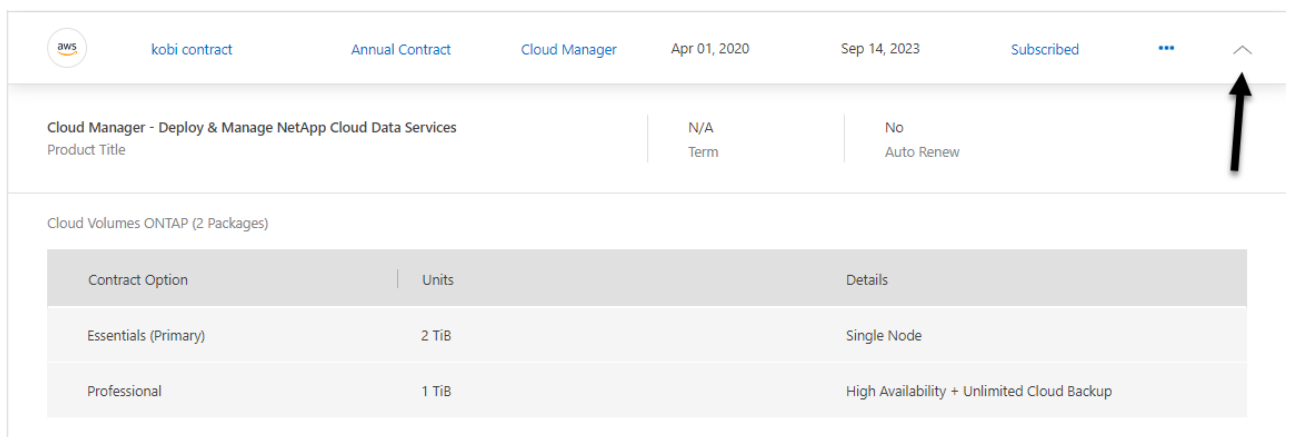
The Digital Wallet provides details about each PAYGO subscription and annual contract associated with your BlueXP account and with Astra (Astra uses BlueXP's charging service).

Steps

1. From the BlueXP navigation menu, select **Governance > Digital wallet**.
2. Select **Subscriptions**.

   You'll only see the subscriptions that are associated with the account that you're currently viewing.

3. As you view the information about your subscriptions, you can interact with the details in the table as follows:

   - Expand a row to view more details.

   -
   Click [+] to choose which columns appear in the table.

   Note that the Term and Auto Renew columns don't appear by default. The Auto Renew column displays renewal information for Azure contracts only.

   Note the following about what you see in the table:

Start date

> The start date is when you successfully associated the subscription with your account and charging started.

N/A

> If you see N/A in the table, the information isn't available from the cloud provider's API at this time.

Contracts

> ◦ If you expand the details for a contract, the Digital Wallet shows what's available for your current plan: the contract options and units (capacity or number of nodes).
>
> ◦ The Digital Wallet will identify the end date and whether the contract will renew soon, end soon, or whether it has already ended.
>
> ◦ If you have an AWS contract and you changed any of the contract's options after the start date, be sure to validate your contract options from the AWS.

Manage your subscriptions

You can manage your subscriptions from the Digital Wallet by renaming a subscription and choosing the accounts that are associated with the subscription.

For example, let's say that you have two accounts and each is billed through separate subscriptions. You might disassociate a subscription from one of the accounts so the users in that account don't accidentally choose the wrong subscription when creating a Cloud Volume ONTAP working environment.

Steps

1. From the BlueXP navigation menu, select **Governance > Digital wallet**.

2. Select **Subscriptions**.

3. Click the action menu in the row that corresponds to the subscription that you want to manage.

Provider ⇕	Name	Type	Service	Start Date	End Date	Status	⊕
aws	aws-sub-a2	PAYGO	Cloud Manager	Apr 02, 2020	N/A	Subscribed	⋯ ∨
aws	Aleksey_aws_marketplace	Annual Contract	Astra	Oct 18, 2022	Oct 18, 2023		∨
aws	By Capacity By Node 3	PAYGO	Cloud Manager	Mar 31, 2020	N/A	Subscribed	⋯ ∨

Associate Subscription

Rename Subscription

4. Choose to rename the subscription or to manage the NetApp accounts that are associated with the subscription.

Discovered cloud storage

Viewing your Amazon S3 buckets

After you install a Connector in AWS, BlueXP can automatically discover information about the Amazon S3 buckets that reside in the AWS account where the Connector is installed. An Amazon S3 working environment is added to the Canvas so you can view this information.

You can see details about your S3 buckets, including the region, access policy, account, total and used capacity, and more. These buckets can be used as destinations for Cloud Backup, Cloud Tiering, or Cloud Sync operations. Additionally, you can use Cloud Data Sense to scan these buckets.

Steps

1. Install a Connector in the AWS account where you want to view your Amazon S3 buckets.

2. From the navigation menu, select **Storage > Canvas**.

   You should automatically see an Amazon S3 working environment shortly after.
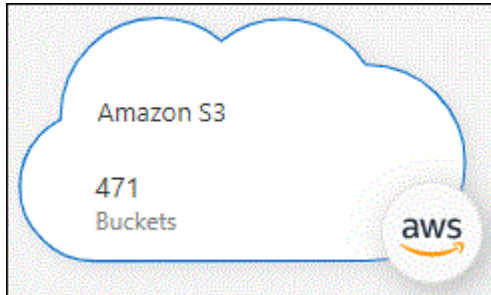
3. Click the working environment and select an action from the right pane.
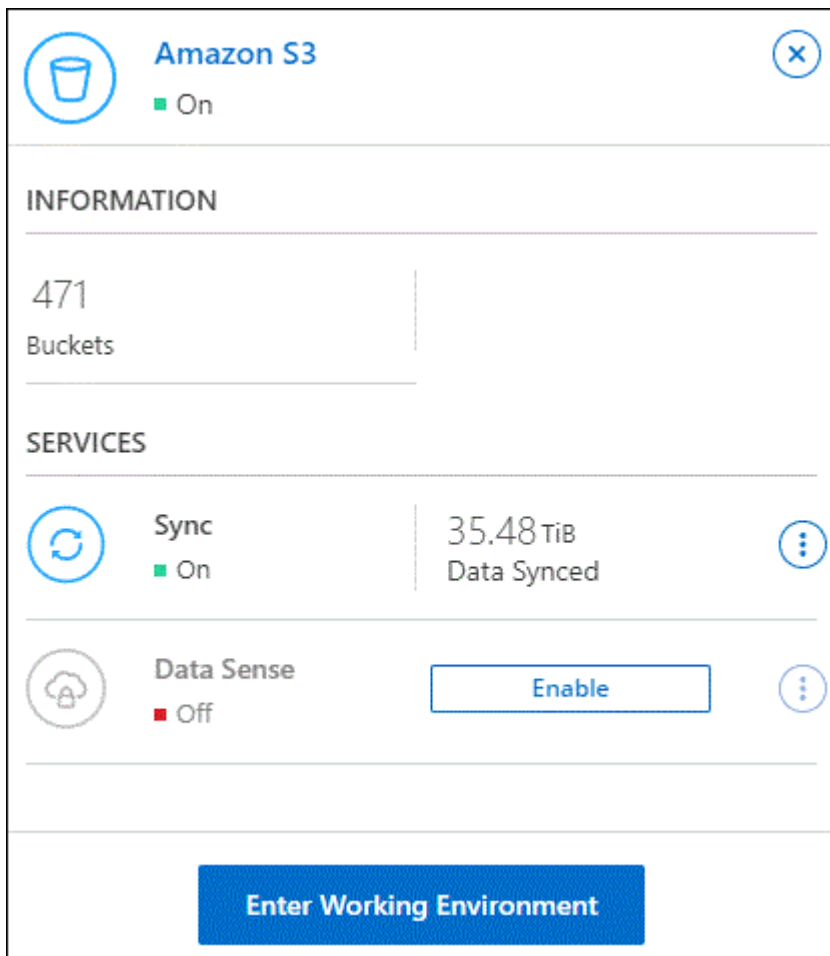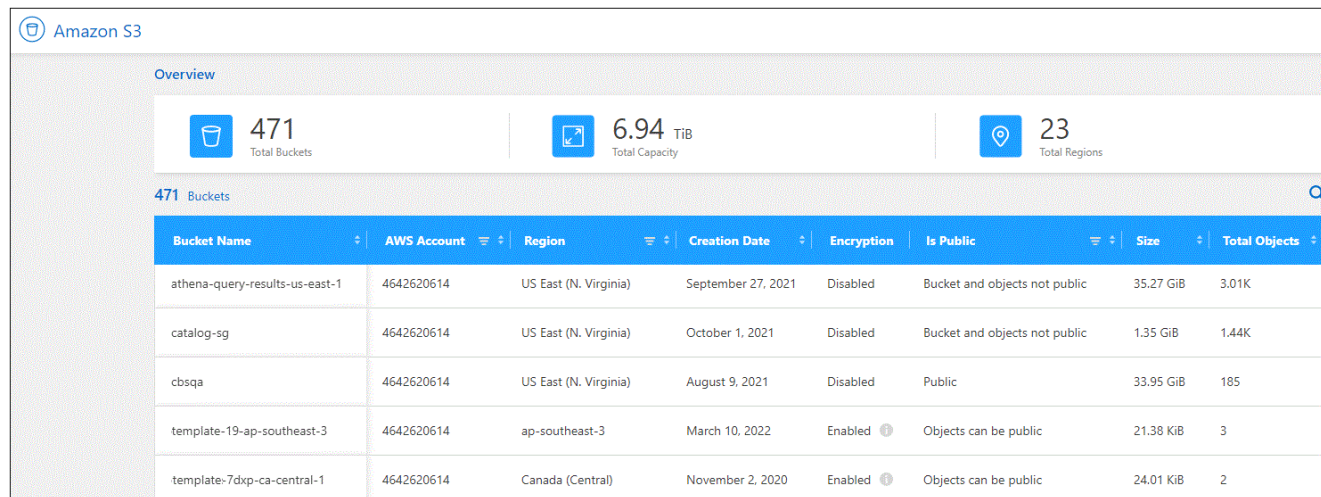
4. Click **Sync data** to synchronize data to or from S3 buckets.

   For more details, see the overview for the Cloud Sync service.

5. Click **Enable** if you want Cloud Data Sense to scan the S3 buckets for personal and sensitive data.

   For more details, see Getting started with Cloud Data Sense for Amazon S3.

6. Click **Enter Working Environment** to view details about the S3 buckets in your AWS account.

Viewing your Azure Blob accounts

After you install a Connector in Azure, BlueXP can automatically discover information about the Azure storage accounts that reside in the Azure Subscriptions where the Connector is installed. An Azure Blob working environment is added to the Canvas so you can view this information.

You can see details about your Azure storage accounts, including the location, resource group, total and used capacity, and more. These accounts can be used as destinations for Cloud Backup, Cloud Tiering, or Cloud Sync operations.

Steps

1. Install a Connector in the Azure account where you want to view your Azure storage accounts.

2. From the navigation menu, select **Storage > Canvas**.

   You should automatically see an Azure Blob working environment shortly after.

3. Click the working environment and select an action from the right pane.

4. Click **Sync data** to synchronize data to or from Azure Blob storage.

   For more details, see the overview for the Cloud Sync service.

5. Click **Enter Working Environment** to view details about the Azure storage accounts in your Azure Blobs.

Viewing your Google Cloud Storage buckets

After you install a Connector in Google Cloud, BlueXP can automatically discover information about the Google Cloud Storage buckets that reside in the Google account where the Connector is installed. A Google Cloud Storage working environment is added to the Canvas so you can view this information.

You can see details about your Google Cloud Storage buckets, including the location, access status, storage class, total and used capacity, and more. These buckets can be used as destinations for Cloud Backup, Cloud Tiering, or Cloud Sync operations.

Steps

1. Install a Connector in the Google account where you want to view your Google Cloud Storage buckets.

2. From the navigation menu, select **Storage > Canvas**.

   You should automatically see a Google Cloud Storage working environment shortly after.
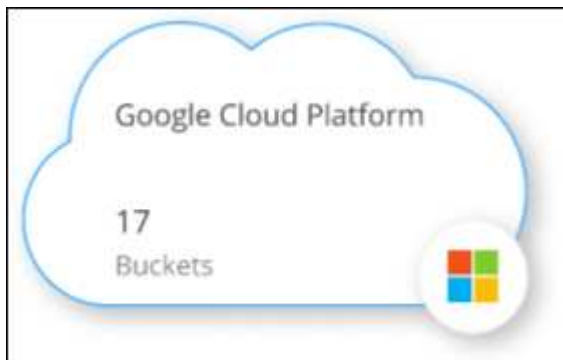
3. Click the working environment and select an action from the right pane.

4. Click **Sync data** to synchronize data to or from Google Cloud Storage buckets.

   For more details, see the overview for the Cloud Sync service.

5. Click **Enter Working Environment** to view details about the buckets in your Google account.

AWS credentials

AWS credentials and permissions

BlueXP enables you to choose the AWS credentials to use when deploying Cloud Volumes ONTAP. You can deploy all of your Cloud Volumes ONTAP systems using the initial AWS credentials, or you can add additional credentials.

Initial AWS credentials

When you deploy a Connector from BlueXP, you need to provide the ARN of an IAM role or access keys for an IAM user. The authentication method that you use must have the required permissions to deploy the Connector instance in AWS. The required permissions are listed in the Connector deployment policy for AWS.

When BlueXP launches the Connector instance in AWS, it creates an IAM role and an instance profile for the instance. It also attaches a policy that provides the Connector with permissions to manage resources and processes within that AWS account. Review how BlueXP uses the permissions.
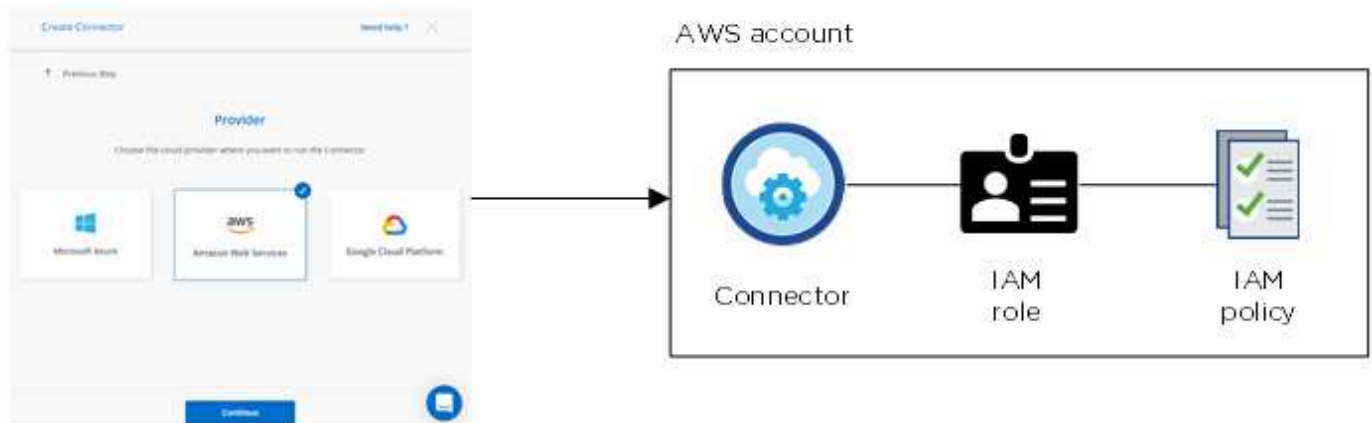
BlueXP selects these AWS credentials by default when you create a new working environment for Cloud Volumes ONTAP:

Additional AWS credentials

There are two ways to add additional AWS credentials.

Add AWS credentials to an existing Connector

If you want to launch Cloud Volumes ONTAP in different AWS accounts, then you can either provide AWS keys for an IAM user or the ARN of a role in a trusted account. The following image shows two additional accounts, one providing permissions through an IAM role in a trusted account and another through the AWS keys of an IAM user:
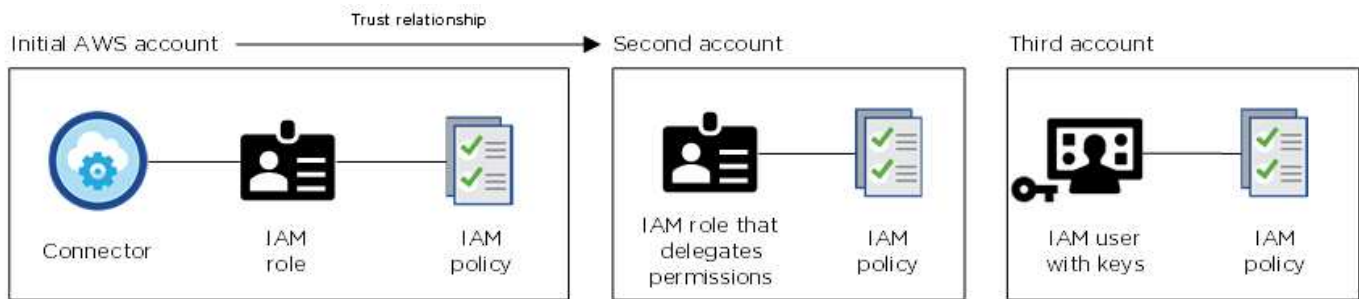
You would then add the account credentials to BlueXP by specifying the Amazon Resource Name (ARN) of the IAM role, or the AWS keys for the IAM user.

After you add another set of credentials, you can switch to them when creating a new working environment:

Add AWS credentials directly to BlueXP

Adding new AWS credentials to BlueXP provides the permissions needed to create and manage an FSx for ONTAP working environment or to create a Connector.

What about Marketplace deployments and on-prem deployments?

The sections above describe the recommended deployment method for the Connector, which is from BlueXP. You can also deploy a Connector in AWS from the AWS Marketplace and you can install the Connector on-premises.

If you use the Marketplace, permissions are provided in the same way. You just need to manually create and set up the IAM role, and then provide permissions for any additional accounts.

For on-premises deployments, you can't set up an IAM role for the BlueXP system, but you can provide permissions just like you would for additional AWS accounts.

How can I securely rotate my AWS credentials?

As described above, BlueXP enables you to provide AWS credentials in a few ways: an IAM role associated with the Connector instance, by assuming an IAM role in a trusted account, or by providing AWS access keys.

With the first two options, BlueXP uses the AWS Security Token Service to obtain temporary credentials that rotate constantly. This process is the best practice—it's automatic and it's secure.

If you provide BlueXP with AWS access keys, you should rotate the keys by updating them in BlueXP at a regular interval. This is a completely manual process.

Manage AWS credentials and subscriptions for BlueXP

Add and manage AWS credentials so that BlueXP has the permissions that it needs to deploy and manage cloud resources in your AWS accounts. If you manage multiple AWS subscriptions, you can assign each one of them to different AWS credentials from the Credentials page.

Overview

You can add AWS credentials to an existing Connector or directly to BlueXP:

- Add additional AWS credentials to an existing Connector

  Adding AWS credentials to an existing Connector provides the permissions needed to manage resources and processes within your public cloud environment. Learn how to add AWS credentials to a Connector.

- Add AWS credentials to BlueXP for creating a Connector

  Adding new AWS credentials to BlueXP gives BlueXP the permissions needed to create a Connector. Learn how to add AWS credentials to BlueXP.

- Add AWS credentials to BlueXP for FSx for ONTAP

  Adding new AWS credentials to BlueXP gives BlueXP the permissions needed to create and manage FSx for ONTAP. Learn how to set up permissions for FSx for ONTAP

How to rotate credentials

BlueXP enables you to provide AWS credentials in a few ways: an IAM role associated with the Connector instance, by assuming an IAM role in a trusted account, or by providing AWS access keys. Learn more about AWS credentials and permissions.

With the first two options, BlueXP uses the AWS Security Token Service to obtain temporary credentials that rotate constantly. This process is the best practice because it's automatic and it's secure.

If you provide BlueXP with AWS access keys, you should rotate the keys by updating them in BlueXP at a

regular interval. This is a completely manual process.

Add credentials to a Connector

Add AWS credentials to a Connector so that it has the permissions needed to manage resources and processes within your public cloud environment. You can either provide the ARN of an IAM role in another account or provide AWS access keys.

Grant permissions

Before you add AWS credentials to a Connector, you need to provide the required permissions. The permissions enable BlueXP to manage resources and processes within that AWS account. How you provide the permissions depends on whether you want to provide BlueXP with the ARN of a role in a trusted account or AWS keys.

> ⓘ If you deployed a Connector from BlueXP, BlueXP automatically added AWS credentials for the account in which you deployed the Connector. This initial account is not added if you deployed the Connector from the AWS Marketplace or if you manually installed the Connector software on an existing system. Learn about AWS credentials and permissions.

Choices

- Grant permissions by assuming an IAM role in another account
- Grant permissions by providing AWS keys

Grant permissions by assuming an IAM role in another account

You can set up a trust relationship between the source AWS account in which you deployed the Connector instance and other AWS accounts by using IAM roles. You would then provide BlueXP with the ARN of the IAM roles from the trusted accounts.

Steps

1. Go to the IAM console in the target account in which you want to provide the Connector with permissions.

2. Under Access Management, click **Roles > Create Role** and follow the steps to create the role.

   Be sure to do the following:

   - Under **Trusted entity type**, select **AWS account**.
   - Select **Another AWS account** and enter the ID of the account where the Connector instance resides.
   - Create the required policies by copying and pasting the contents of the IAM policies for the Connector.

3. Copy the Role ARN of the IAM role so that you can paste it in BlueXP later on.

Result

The account now has the required permissions. You can now add the credentials to a Connector.

Grant permissions by providing AWS keys

If you want to provide BlueXP with AWS keys for an IAM user, then you need to grant the required permissions to that user. The BlueXP IAM policy defines the AWS actions and resources that BlueXP is allowed to use.

Steps

1. From the IAM console, create policies by copying and pasting the contents of the IAM policies for the Connector.

   AWS Documentation: Creating IAM Policies

2. Attach the policies to an IAM role or an IAM user.
   - AWS Documentation: Creating IAM Roles
   - AWS Documentation: Adding and Removing IAM Policies

Result

The account now has the required permissions. You can now add the credentials to a Connector.

Add the credentials

After you provide an AWS account with the required permissions, you can add the credentials for that account to an existing Connector. This enables you to launch Cloud Volumes ONTAP systems in that account using the same Connector.

Before you get started

If you just created these credentials in your cloud provider, 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. 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**: Provide the ARN (Amazon Resource Name) of a trusted IAM role, or 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.

   To pay for Cloud Volumes ONTAP at an hourly rate (PAYGO) or with an annual contract, AWS credentials must be associated with a subscription to Cloud Volumes ONTAP from the AWS Marketplace.

   d. **Review**: Confirm the details about the new credentials and click **Add**.

Result

You can now switch to a different set of credentials from the Details and Credentials page when creating a new working environment:

Add credentials to BlueXP for creating a Connector

Add AWS credentials to BlueXP by providing the ARN of an IAM role that gives BlueXP the permissions needed to create a Connector. You can choose these credentials when creating a new Connector.

Set up the IAM role

Set up an IAM role that enables the BlueXP SaaS to assume the role.

Steps

1. Go to the IAM console in the target account.

2. Under Access Management, click **Roles > Create Role** and follow the steps to create the role.

   Be sure to do the following:

   - Under **Trusted entity type**, select **AWS account**.
   - Select **Another AWS account** and enter the ID of the BlueXP SaaS: 952013314444
   - Create a policy that includes the permissions required to create a Connector.
     - View the permissions needed for FSx for ONTAP
     - View the Connector deployment policy

3. Copy the Role ARN of the IAM role so that you can paste it in BlueXP in the next step.

Result

The IAM role now has the required permissions. You can now add it to BlueXP.

Add the credentials

After you provide the IAM role with the required permissions, add the role ARN to BlueXP.

Before you get started

If you just created the IAM role, 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 > BlueXP**.

   b. **Define Credentials**: Provide the ARN (Amazon Resource Name) of the IAM role.

   c. **Review**: Confirm the details about the new credentials and click **Add**.

Result

You can now use the credentials when creating a new Connector.

Associate an AWS subscription

After you add your AWS credentials to BlueXP, you can associate an AWS Marketplace subscription with those credentials. The subscription enables you to pay for Cloud Volumes ONTAP at an hourly rate (PAYGO) or using an annual contract, and to use other NetApp cloud services.

There are two scenarios in which you might associate an AWS Marketplace subscription after you've already added the credentials to BlueXP:

- You didn't associate a subscription when you initially added the credentials to BlueXP.
- You want to replace an existing AWS Marketplace subscription with a new subscription.

What you'll need

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

Steps

1. In the upper right of the BlueXP console, click the Settings icon, and select **Credentials**.
2. Click the action menu for a set of credentials and then select **Associate Subscription**.

3. Select an existing subscription from the down-down list or click **Add Subscription** and follow the steps to create a new subscription.

   ► https://docs.netapp.com/us-en/cloud-manager-setup-admin//media/video_subscribing_aws.mp4 *(video)*

Edit credentials

Edit your AWS credentials in BlueXP by changing the account type (AWS keys or assume role), by editing the name, or by updating the credentials themselves (the keys or the role ARN).

> You can't edit the credentials for an instance profile that is associated with a Connector instance.

Steps

1. In the upper right of the BlueXP console, click the Settings icon, and select **Credentials**.
2. Click the action menu for a set of credentials and then select **Edit Credentials**.
3. Make the required changes and then click **Apply**.

Deleting credentials

If you no longer need a set of credentials, you can delete them from BlueXP. You can only delete credentials that aren't associated with a working environment.

> You can't delete the credentials for an instance profile that is associated with a Connector instance.

Steps

1. In the upper right of the BlueXP console, click the Settings icon, and select **Credentials**.
2. Click the action menu for a set of credentials and then select **Delete Credentials**.
3. Click **Delete** to confirm.

Azure credentials

Azure credentials and permissions

BlueXP enables you to choose the Azure credentials to use when deploying Cloud Volumes ONTAP. You can deploy all of your Cloud Volumes ONTAP systems using the initial Azure credentials, or you can add additional credentials.

Initial Azure credentials

When you deploy a Connector from BlueXP, you need to use an Azure account or service principal that has permissions to deploy the Connector virtual machine. The required permissions are listed in the Connector deployment policy for Azure.

When BlueXP deploys the Connector virtual machine in Azure, it enables a system-assigned managed identity on virtual machine, creates a custom role, and assigns it to the virtual machine. The role provides BlueXP with the permissions required to manage resources and processes within that Azure subscription. Review how BlueXP uses the permissions.

BlueXP selects these Azure credentials by default when you create a new working environment for Cloud Volumes ONTAP:

Additional Azure subscriptions for a managed identity

The managed identity is associated with the subscription in which you launched the Connector. If you want to select a different Azure subscription, then you need to associate the managed identity with those subscriptions.

Additional Azure credentials

If you want to deploy Cloud Volumes ONTAP using different Azure credentials, then you must grant the required permissions by creating and setting up a service principal in Azure Active Directory for each Azure account. The following image shows two additional accounts, each set up with a service principal and custom

role that provides permissions:

You would then add the account credentials to BlueXP by providing details about the AD service principal.

After you add another set of credentials, you can switch to them when creating a new working environment:

Managing Azure credentials and subscriptions for BlueXP

When you create a Cloud Volumes ONTAP system, you need to select the Azure credentials to use with that system. You also need to choose a Marketplace subscription,

if you're using pay-as-you-go licensing. Follow the steps on this page if you need to use multiple Azure credentials or multiple Azure Marketplace subscriptions for Cloud Volumes ONTAP.

There are two ways to add additional Azure subscriptions and credentials in BlueXP.

1. Associate additional Azure subscriptions with the Azure managed identity.

2. If you want to deploy Cloud Volumes ONTAP using different Azure credentials, grant Azure permissions using a service principal and add its credentials to BlueXP.

Associating additional Azure subscriptions with a managed identity

BlueXP enables you to choose the Azure credentials and Azure subscription in which you want to deploy Cloud Volumes ONTAP. You can't select a different Azure subscription for the managed identity profile unless you associate the managed identity with those subscriptions.

About this task

A managed identity is the initial Azure account when you deploy a Connector from BlueXP. When you deployed the Connector, BlueXP created the BlueXP Operator role and assigned it to the Connector virtual machine.

Steps

1. Log in to the Azure portal.

2. Open the **Subscriptions** service and then select the subscription in which you want to deploy Cloud Volumes ONTAP.

3. Click **Access control (IAM)**.

   a. Click **Add** > **Add role assignment** and then add the permissions:

      ▪ Select the **BlueXP Operator** role.

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

      ▪ Assign access to a **Virtual Machine**.

      ▪ Select the subscription in which the Connector virtual machine was created.

      ▪ Select the Connector virtual machine.

      ▪ Click **Save**.

4. Repeat these steps for additional subscriptions.

Result

When you create a new working environment, you should now have the ability to select from multiple Azure subscriptions for the managed identity profile.

Adding additional Azure credentials to BlueXP

When you deploy a Connector from BlueXP, BlueXP enables a system-assigned managed identity on the virtual machine that has the required permissions. BlueXP selects these Azure credentials by default when you create a new working environment for Cloud Volumes ONTAP.

> 💡 An initial set of credentials isn't added if you manually installed the Connector software on an existing system. Learn about Azure credentials and permissions.

If you want to deploy Cloud Volumes ONTAP using *different* Azure credentials, then you must grant the required permissions by creating and setting up a service principal in Azure Active Directory for each Azure account. You can then add the new credentials to BlueXP.

Granting Azure permissions using a service principal

BlueXP needs permissions to perform actions in Azure. You can grant the required permissions to an Azure account by creating and setting up a service principal in Azure Active Directory and by obtaining the Azure credentials that BlueXP needs.

About this task

The following image depicts how BlueXP obtains permissions to perform operations in Azure. A service principal object, which is tied to one or more Azure subscriptions, represents BlueXP in Azure Active Directory and is assigned to a custom role that allows the required permissions.

Cloud Manager → Active Directory authentication and authorization → Azure REST API calls to manage Cloud Volumes ONTAP

```
curl http://localhost/occm/api/
azure/vsa/working-
environments -X POST --header
"Content-Type:application/json"
```

Azure subscriptions ↔ Service principal that represents Cloud Manager with AD ↔ Custom role with the required permissions

Steps

1. Create an Azure Active Directory application.
2. Assign the application to a role.
3. Add Windows Azure Service Management API permissions.
4. Get the application ID and directory ID.
5. Create a client secret.

Creating an Azure Active Directory application

Create an Azure Active Directory (AD) application and service principal that BlueXP can use for role-based access control.

Before you begin

You must have the right 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.

Steps

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

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

3. Click **New registration**.

4. 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.

5. Click **Register**.

Result

You've created the AD application and service principal.

Assigning the application to a role

You must bind the service principal to one or more Azure subscriptions and assign it the custom "BlueXP Operator" role so BlueXP has permissions in Azure.

Steps

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**.

- Search for the name of the application.

  Here's an example:

- 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.

Adding Windows Azure Service Management API permissions

The service principal must have "Windows Azure Service Management API" permissions.

Steps

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**.

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

Getting the application ID and directory 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.

Steps

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**.

Creating a client secret

You need to create a client secret and then provide BlueXP with the value of the secret so BlueXP can use it to authenticate with Azure AD.

Steps

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.

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.

Adding the credentials to BlueXP

After you provide an Azure account with the required permissions, you can add the credentials for that account to BlueXP. Completing this step enables you to launch Cloud Volumes ONTAP using different Azure credentials.

Before you get started

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

What you'll need

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

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: See Getting the application ID and directory ID.

      ▪ Directory (tenant) ID: See Getting the application ID and directory ID.

      ▪ Client Secret: See Creating a client secret.

   c. **Marketplace Subscription**: Associate a Marketplace subscription with these credentials by subscribing now or by selecting an existing subscription.

To pay for Cloud Volumes ONTAP at an hourly rate (PAYGO), these Azure credentials must be associated with a subscription from the Azure Marketplace.

   d. **Review**: Confirm the details about the new credentials and click **Add**.

Result

You can now switch to different set of credentials from the Details and Credentials page when creating a new working environment

Manage existing credentials

Manage the Azure credentials that you've already added to BlueXP by associating a Marketplace subscription, editing credentials, and deleting them.

Associating an Azure Marketplace subscription to credentials

After you add your Azure credentials to BlueXP, you can associate an Azure Marketplace subscription to those credentials. The subscription enables you to create a pay-as-you-go Cloud Volumes ONTAP system, and to use other NetApp cloud services.

There are two scenarios in which you might associate an Azure Marketplace subscription after you've already added the credentials to BlueXP:

   • You didn't associate a subscription when you initially added the credentials to BlueXP.

   • You want to replace an existing Azure Marketplace subscription with a new subscription.

What you'll need

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

Steps

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

2. Click the action menu for a set of credentials and then select **Associate Subscription**.

3. Select a subscription from the down-down list or click **Add Subscription** and follow the steps to create a new subscription.

   The following video starts from the context of the working environment wizard, but shows you the same workflow after you click **Add Subscription**:

   ► https://docs.netapp.com/us-en/cloud-manager-setup-admin//media/video_subscribing_azure.mp4

(video)

Editing credentials

Edit your Azure credentials in BlueXP by modifying the details about your Azure service credentials. For example, you might need to update the client secret if a new secret was created for the service principal application.

Steps

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

2. Click the action menu for a set of credentials and then select **Edit Credentials**.

3. Make the required changes and then click **Apply**.

Deleting credentials

If you no longer need a set of credentials, you can delete them from BlueXP. You can only delete credentials that aren't associated with a working environment.

Steps

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

2. Click the action menu for a set of credentials and then select **Delete Credentials**.

3. Click **Delete** to confirm.

Google Cloud credentials

Google Cloud projects, permissions, and accounts

A service account provides BlueXP with permissions to deploy and manage Cloud Volumes ONTAP systems that are in the same project as the Connector, or in different projects.

Project and permissions for BlueXP

Before you can deploy Cloud Volumes ONTAP in Google Cloud, you must first deploy a Connector in a Google Cloud project. The Connector can't be running on your premises, or in a different cloud provider.

Two sets of permissions must be in place before you deploy a Connector directly from BlueXP:

1. You need to deploy a Connector using a Google account that has permissions to launch the Connector VM instance from BlueXP.

2. When deploying the Connector, you are prompted to select a service account for the VM instance. BlueXP gets permissions from the service account to create and manage Cloud Volumes ONTAP systems on your behalf. Permissions are provided by attaching a custom role to the service account.

We have set up two YAML files that include the required permissions for the user and the service account. Learn how to use the YAML files to set up permissions.

The following image depicts the permission requirements described in numbers 1 and 2 above:
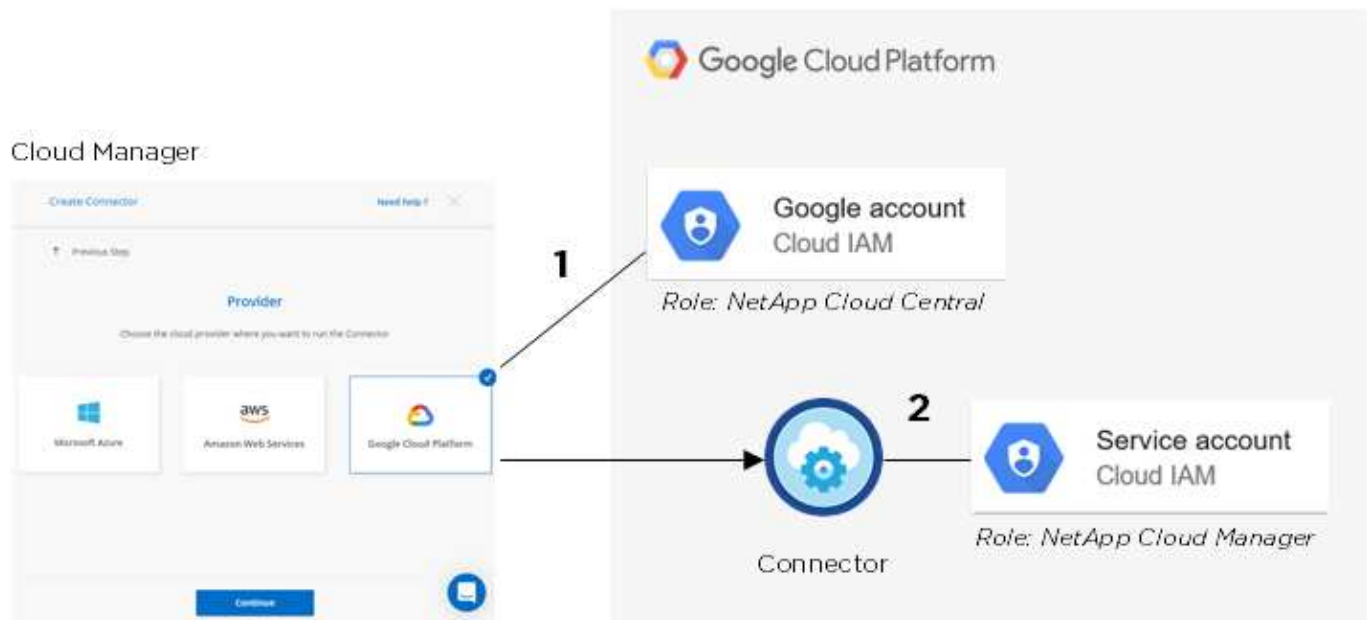
Project for Cloud Volumes ONTAP

Cloud Volumes ONTAP can reside in the same project as the Connector, or in a different project. To deploy Cloud Volumes ONTAP in a different project, you need to first add the Connector service account and role to that project.

- Learn how to set up service account
- Learn how to deploy Cloud Volumes ONTAP in GCP and select a project

Managing Google Cloud credentials and subscriptions for BlueXP

You can manage the credentials that are associated with the Connector VM instance.

Associating a Marketplace subscription with Google Cloud credentials

When you deploy a Connector in Google Cloud, BlueXP creates a default set of credentials that are associated with the Connector VM instance. These are the credentials that BlueXP uses to deploy Cloud Volumes ONTAP.

At any time, you can change the Marketplace subscription that's associated with these credentials. The subscription enables you to create a pay-as-you-go Cloud Volumes ONTAP system, and to use other NetApp cloud services.

Steps

1. In the upper right of the BlueXP console, click the Settings icon, and select **Credentials**.
2. Click the action menu for a set of credentials and then select **Associate Subscription**.

3. Select a Google Cloud project and subscription from the down-down list.

4. Click **Associate**.

5. If you don't already have a subscription, click **Add Subscription** and follow the steps to create a new subscription below.

> (i) Before you complete the following steps, ensure that you have both Billing Admin privileges in your Google Cloud account as well as a BlueXP login.

6. Reivew the subscription steps and click **Continue**.

Add Subscription

Subscription Steps:

1. **Cloud Manager**
   Clicking **Continue** to create your subscription from the Google Cloud Marketplace.

2. **Google Cloud Marketplace**
   Subscribe and then then click **Register With NetApp** to configure your account from Cloud Central.

3. **Cloud Central**
   Save your subscription.

4. **Cloud Manager**
   Associate the Marketplace subscription with your Google Cloud project.

▶ View video instructions

[Continue] [Cancel]

7. After you're redirected to the NetApp BlueXP page on the Google Cloud Marketplace, ensure that the correct project is selected at the top navigation menu.

8. Click **Subscribe**.

9. Select the appropriate billing account and agree to the terms and conditions.

2. Purchase details

Select a billing account *
Secondary_Billing_Account

3. Terms

Cancellation and change policy

- Usage fee is billed every month.
- You can cancel the service at any time and it will take effect immediately. You will be billed by the amount you used for that month.

Additional terms

☑ I understand this subscription will be automatically renewed at the end of the current term.

☑ I authorize Google LLC and its affiliates ("Google") to share my purchase, usage, operational (e.g., project lifecycle events), support ticket, and account information with NetApp, Inc., its affiliates and subcontractors, for the purposes of providing the service, sales attribution, and technical support. I represent that I have the authority to bind my company.

☑ By deploying the software or accessing the service you are agreeing to comply with the End User License Agreement ⬀, GCP Marketplace Terms of Service, and the terms of applicable open source software licenses bundled with the software or service. Please review these terms and licenses carefully for details about any obligations you may have related to the software or service. To the limited extent an open source software license related to the software or service expressly supersedes the GCP Marketplace Terms of Service, that open source software license governs your use of that software or service.

By using this product, you understand that certain account and usage information may be shared with NetApp, Inc. for the purposes of financial accounting, sales attribution, performance analysis, and support. ❓

Google is providing this software or service "as-is" and any support for this software or service will be provided by NetApp, Inc. under their terms of service.

SUBSCRIBE

10. Click **Subscribe**.

    This step sends your transfer request to NetApp.

11. On the pop-up dialog box, click **Register with NetApp, Inc.** to be redirected to the NetApp BlueXP website.

> ℹ This step must be completed to link the Google Cloud subscription to your NetApp account. The process of linking a subscription isn't complete until you are redirected from this page and then sign in to BlueXP.

12. After you're redirected to BlueXP, log in or sign up, and then click **Done** to proceed.

    The Google Cloud subscription will be linked to all NetApp accounts that your user login is associated with. If you need to limit access to the new subscription, you can manage the NetApp accounts that are associated with the subscription from the Digital Wallet. Learn how to manage your subscriptions.
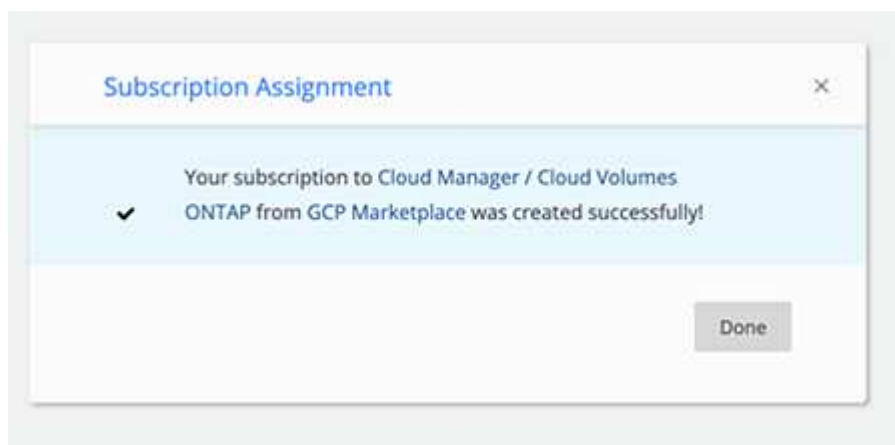
> ℹ If someone from your organization has already subscribed to the NetApp BlueXP subscription from your billing account, then you will be redirected to the Cloud Volumes ONTAP page on the BlueXP website instead. If this is unexpected, contact your NetApp sales team. Google enables only one subscription per Google billing account.

13. Once this process is complete, navigate back to the Credentials page in BlueXP and select this new subscription.

Troubleshooting the Marketplace subscription process

Sometimes subscribing to Cloud Volumes ONTAP through the Google Cloud Marketplace can become fragmented due to incorrect permissions or accidentally not following the redirection to the BlueXP website. If this happens, use the following steps to complete the subscription process.

Steps

1. Navigate to the NetApp BlueXP page on the Google Cloud Marketplace to check on the state of the order. If the page states **Manage on Provider**, scroll down and click **Manage Orders**.

   a. If the order shows a green check mark and this is unexpected, somebody else from the organization using the same billing account might already be subscribed. If this is unexpected or you require the details of this subscription, contact your NetApp sales team.

   b. If the order shows a clock and **Pending** status, go back to the marketplace page and choose **Manage on Provider** to complete the process as documented above.

Add and manage NetApp Support Site accounts in BlueXP

Provide the credentials for your NetApp Support Site (NSS) accounts to register for support, enable key workflows for Cloud Volumes ONTAP, and more.

Overview

Adding your NetApp Support Site account to BlueXP is required to enable the following tasks:

- To register for support
- To deploy Cloud Volumes ONTAP when you bring your own license (BYOL)

  Providing your NSS account is required so that BlueXP can upload your license key and to enable the subscription for the term that you purchased. This includes automatic updates for term renewals.

- To register pay-as-you-go Cloud Volumes ONTAP systems

  Providing your NSS account is required to activate support for your system and to gain access to NetApp technical support resources.

- To upgrade Cloud Volumes ONTAP software to the latest release

You'll also need to enter your NSS credentials to use Digital Advisor (formerly Active IQ) from within BlueXP. These credentials are associated directly with your user account and are for use with Digital Advisor only. Review more details in the section that follows.

Manage an NSS account associated with Digital Advisor

When you access Digital Advisor in BlueXP, you're prompted to log in to Digital Advisor by entering your NSS credentials. After you enter your NSS credentials, you'll see this NSS account listed at the top of the NSS Management page. You can then manage those credentials as needed.

Note the following about this NSS account:

- The account is managed at the user level, which means it isn't viewable by other users who log in.
- The account can't be used with any other BlueXP feature: not with Cloud Volumes ONTAP creation, licensing, or support.
- There can be only one NSS account associated with Digital Advisor, per user.

Steps

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

2. Click **NSS Management**.

3. Under **Your NSS Credentials**, click **Action** and choose any of the following options:

   ◦ **Associate NSS user**: Add credentials for a NetApp Support Site account so that you can access Digital Advisor in BlueXP.

   ◦ **Update existing credentials**: Update the credentials for your NetApp Support Site account.

   ◦ **Delete**: Remove the account associated with Digital Advisor.

Result

BlueXP updates the NSS account associated with Digital Advisor.

Add an NSS account

The Support Dashboard enables you to add and manage your NetApp Support Site accounts for use with BlueXP at the NetApp account level.

- If you have a customer-level account, you can add one or more NSS accounts.

- If you have a partner or reseller account, you can add one or more NSS accounts, but they can't be added alongside customer-level accounts.

Steps

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

2. Click **NSS Management > Add NSS Account**.

3. When you're prompted, click **Continue** to be redirected to a Microsoft login page.

   NetApp uses Microsoft Azure Active Directory as the identity provider for authentication services specific to support and licensing.

4. At the login page, provide your NetApp Support Site registered email address and password to perform the authentication process.

   These actions enable BlueXP to use your NSS account for things like license downloads, software upgrade verification, and future support registrations.

   Note the following:

   ◦ The account must be a customer-level account (not a guest or temp account).

   ◦ Upon successful login, NetApp will store the NSS user name. This is a system generated ID that maps to your email. On the **NSS Management** page, you can display your email from the ••• menu.

   ◦ If you ever need to refresh your login credential tokens, there is also an **Update Credentials** option in the ••• menu. Using this option prompts you to log in again.

What's next?

Users can now select the account when creating new Cloud Volumes ONTAP systems, when registering existing Cloud Volumes ONTAP systems, and when registering for support.

- Launching Cloud Volumes ONTAP in AWS
- Launching Cloud Volumes ONTAP in Azure
- Launching Cloud Volumes ONTAP in GCP
- Registering pay-as-you-go systems

Update an NSS account for the new authentication method

Starting in November 2021, NetApp now uses Microsoft Azure Active Directory as the identity provider for authentication services specific to support and licensing. As a result of this update, BlueXP will prompt you to update the credentials for any existing accounts that you previously added.

Steps

1. If you haven't already done so, create a Microsoft Azure Active Directory B2C account that will be linked to your current NetApp account.

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

3. Click **NSS Management**.

4. For the NSS account that you want to update, click **Update Account**.
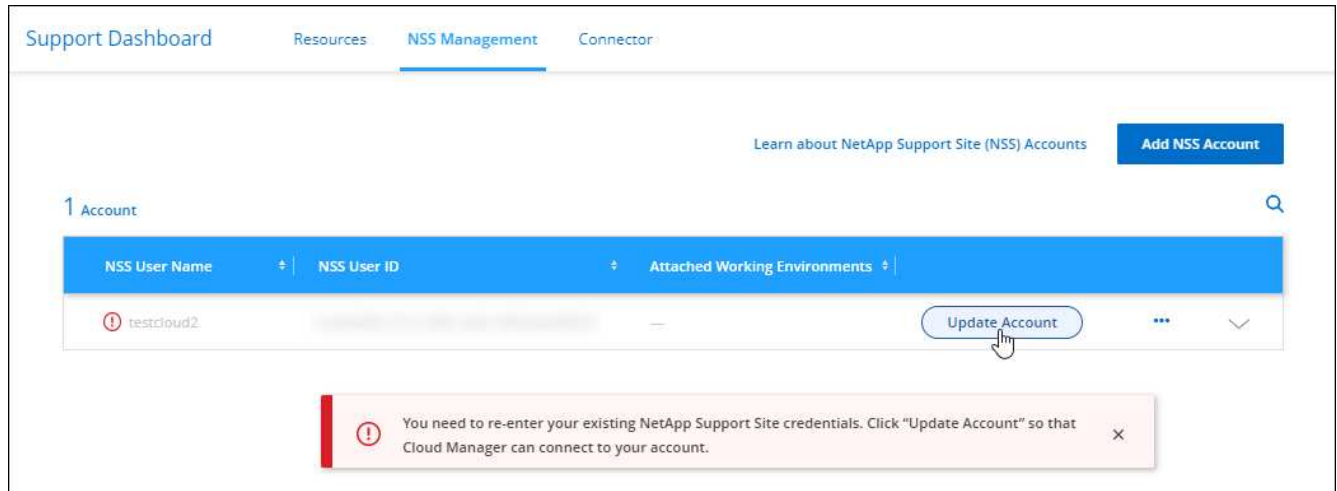
5. When you're prompted, click **Continue** to be redirected to a Microsoft login page.

   NetApp uses Microsoft Azure Active Directory as the identity provider for authentication services specific to support and licensing.

6. At the login page, provide your NetApp Support Site registered email address and password to perform the authentication process.

   After the process is complete, the account that you updated should now be listed as a *new* account in the table. The *older* version of the account is still listed in the table, along with any existing working environment associations.

7. If existing Cloud Volumes ONTAP working environments are attached to the older version of the account, follow the steps below to attach those working environments to a different NSS account.

8. Go to the older version of the NSS account, click ••• and then select **Delete**.

Update NSS credentials

You'll need to update the credentials for your NSS accounts in BlueXP when either of the following happens:

- You change the credentials for the account

- The refresh token associated with your account expires after 3 months

Steps

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

2. Click **NSS Management**.

3. For the NSS account that you want to update, click ••• and then select **Update Credentials**.
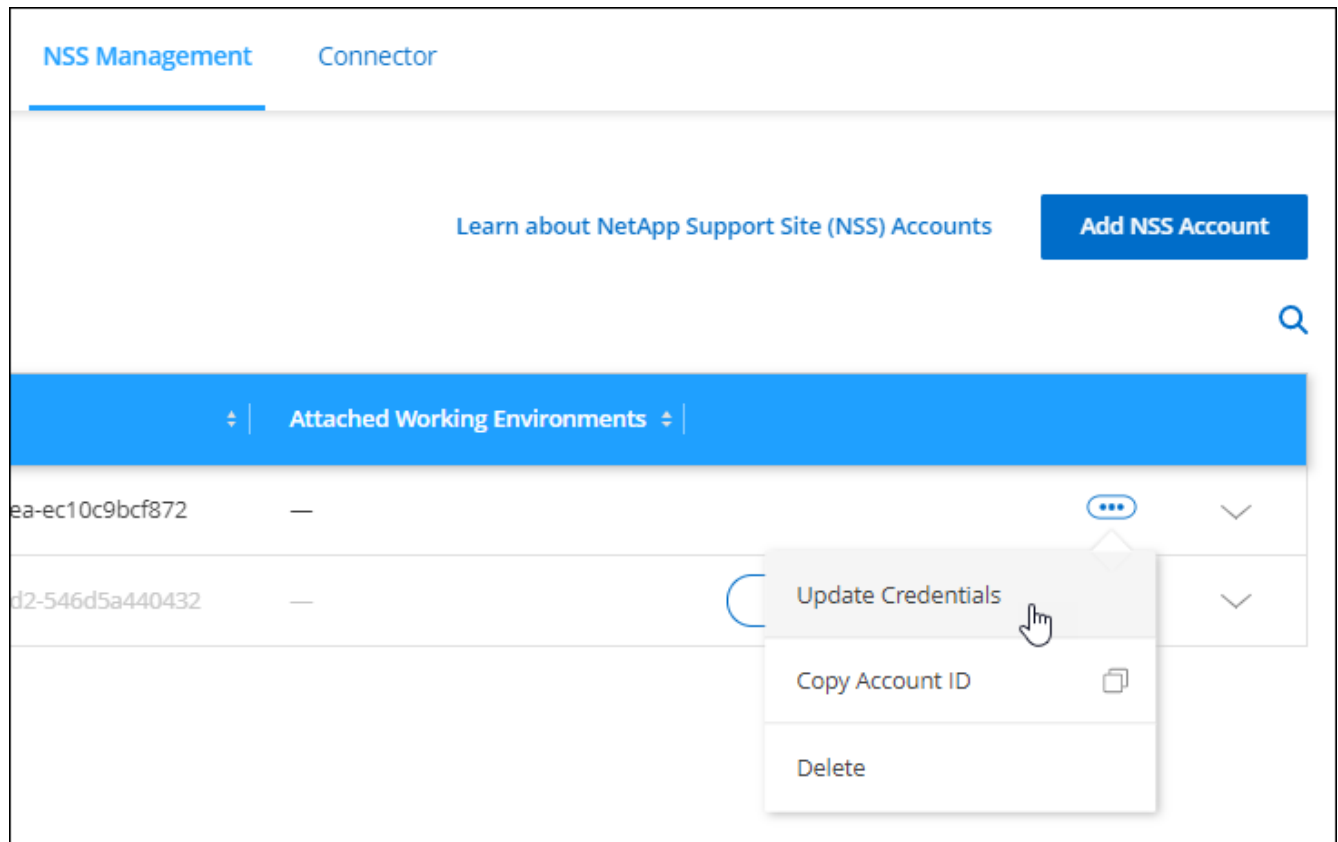
4. When you're prompted, click **Continue** to be redirected to a Microsoft login page.

   NetApp uses Microsoft Azure Active Directory as the identity provider for authentication services specific to support and licensing.

5. At the login page, provide your NetApp Support Site registered email address and password to perform the authentication process.

Attach a working environment to a different NSS account

If your organization has multiple NetApp Support Site accounts, you can change which account is associated with a Cloud Volumes ONTAP system.

This feature is only supported with NSS accounts that are configured to use Microsoft Azure AD adopted by NetApp for identity management. Before you can use this feature, you need click **Add NSS Account** or **Update Account**.

Steps

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

2. Click **NSS Management**.

3. Complete the following steps to change the NSS account:

   a. Expand the row for the NetApp Support Site account that the working environment is currently associated with.

   b. For the working environment that you want to change the association for, click •••

   c. Select **Change to a different NSS account**.
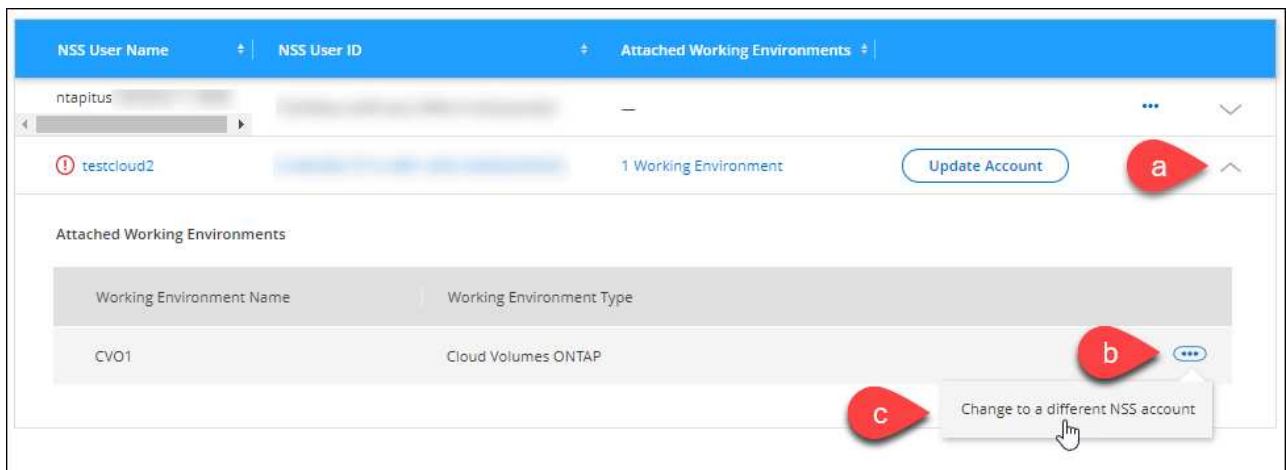
d. Select the account and then click **Save**.

Display the email address for an NSS account

Now that NetApp Support Site accounts use Microsoft Azure Active Directory for authentication services, the NSS user name that displays in BlueXP is typically an identifier generated by Azure AD. As a result, you might not immediately know the email address associated with that account. But BlueXP has an option to show you the associated email address.

> When you go to the NSS Management page, BlueXP generates a token for each account in the table. That token includes information about the associated email address. The token is then removed when you leave the page. The information is never cached, which helps protect your privacy.

Steps

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

2. Click **NSS Management**.

3. For the NSS account that you want to update, click ••• and then select **Display Email Address**.

Result

BlueXP displays the NetApp Support Site user name and the associated email address. You can use the copy button to copy the email address.

Remove an NSS account

Delete any of the NSS accounts that you no longer want to use with BlueXP.

Note that you can't delete an account that is currently associated with a Cloud Volumes ONTAP working environment. You first need to attach those working environments to a different NSS account.

Steps

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

2. Click **NSS Management**.

3. For the NSS account that you want to delete, click ••• and then select **Delete**.
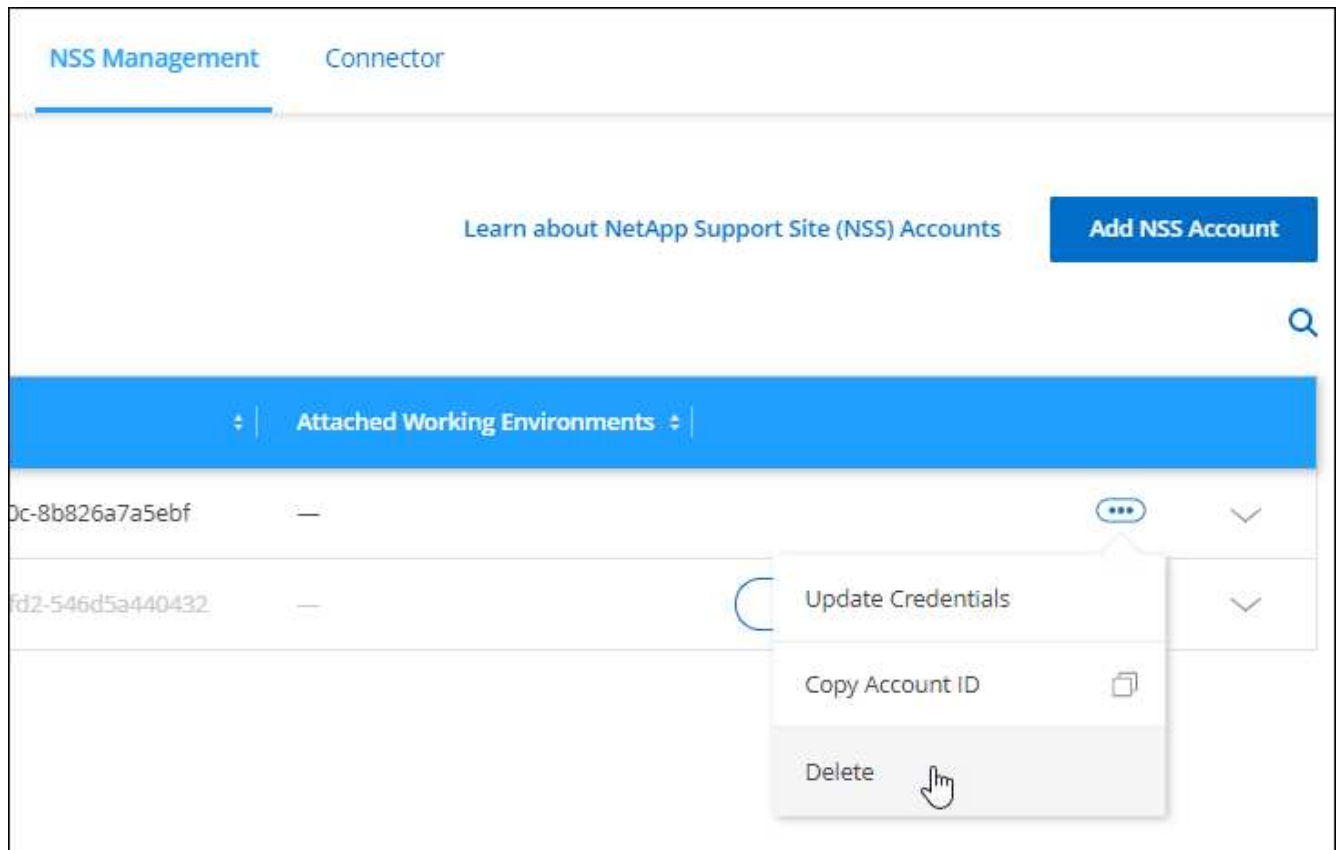
4. Click **Delete** to confirm.

My Opportunities

On the Canvas, the **My Opportunities** tab provides a centralized location to discover existing resources that you can add to BlueXP for consistent data services and operations across your hybrid multicloud.

Currently, My Opportunities enables you to discover existing FSx for ONTAP file systems in your AWS account.

Learn how to discover FSx for ONTAP using My Opportunities