



BlueXP setup and administration documentation

BlueXP setup and administration

NetApp
August 29, 2025

This PDF was generated from <https://docs.netapp.com/us-en/bluexp-setup-admin/index.html> on August 29, 2025. Always check docs.netapp.com for the latest.

Table of Contents

- BlueXP setup and administration documentation 1
- Release notes 2
 - What's new 2
 - 11 August 2025 2
 - 31 July 2025 2
 - 21 July 2025 3
 - 14 July 2025 3
 - 9 June 2025 4
 - 29 May 2025 5
 - 12 May 2025 6
 - 14 April 2025 7
 - 28 March 2025 7
 - 10 March 2025 8
 - 6 March 2025 8
 - 18 February 2025 9
 - 10 February 2025 9
 - 13 January 2025 12
 - 16 December 2024 12
 - 9 December 2024 13
 - 26 November 2024 13
 - 11 November 2024 14
 - 10 October 2024 14
 - 7 October 2024 14
 - 30 September 2024 17
 - 9 September 2024 18
 - 22 August 2024 19
 - 8 August 2024 19
 - 31 July 2024 20
 - 15 July 2024 21
 - 8 July 2024 21
 - 12 June 2024 22
 - 4 June 2024 22
 - 17 May 2024 22
 - Known limitations 23
 - Connector limitations 23
 - Changes to supported Linux operating systems 24
 - Supported operating systems 24
 - Support for RHEL 8 and 9 25
 - End of support for RHEL 7 and CentOS 7 26
 - Related information 26
- Get started 28
 - Learn the basics 28
 - Learn about BlueXP 28

Learn about BlueXP Connectors	31
Learn about BlueXP deployment modes	35
Get started with standard mode	45
Getting started workflow (standard mode)	45
Prepare networking for the BlueXP console	46
Sign up or log in to BlueXP	48
Create a Connector	50
Subscribe to NetApp Intelligent Services (standard mode)	166
What you can do next (standard mode)	171
Get started with restricted mode	171
Getting started workflow (restricted mode)	171
Prepare for deployment in restricted mode	172
Deploy the Connector in restricted mode	191
Subscribe to NetApp Intelligent Services (restricted mode)	203
What you can do next (restricted mode)	208
Get started with private mode	209
Getting started workflow (private mode)	209
Prepare for deployment in private mode	209
Deploy the Connector in private mode	225
What you can do next (private mode)	230
Use BlueXP	231
Log in to BlueXP	231
Manage your BlueXP user settings	233
Change your display name	233
Configure multi-factor authentication	233
Regenerate your MFA recovery code	234
Delete your MFA configuration	234
Contact your Organization administrator	235
Configure dark mode (dark theme)	235
Administer BlueXP	236
Identity and access management	236
Learn about BlueXP identity and access management	236
Get started with BlueXP identity and access management	243
Organize your resources in BlueXP IAM with folders and projects	244
Add BlueXP members and service accounts	249
Use roles to manage user access to resources	254
Manage the resource hierarchy in your BlueXP organization	255
Associate a BlueXP Connector with other folders and projects	258
Switch between BlueXP organizations, projects, and Connectors	259
Organization and project IDs	261
Monitor or audit IAM activity from the BlueXP timeline	262
BlueXP access roles	263
Identity federation	275
Enable single sign-on by using identity federation with BlueXP	275
Domain verification	277

Configure federations	278
Manage federations in BBlueXP	285
Import your federation to BlueXP	287
Connectors	287
Maintain the Connector VM and operating system	287
Install a CA-signed certificate for web-based console access	290
Configure a Connector to use a proxy server	292
Require the use of IMDSv2 on Amazon EC2 instances	299
Manage connector upgrades	301
Work with multiple Connectors	303
Troubleshoot the Connector	304
Uninstall and remove the Connector	307
Default configuration for the Connector	309
Enforce ONTAP permissions for ONTAP Advanced View (ONTAP System Manager)	311
Credentials and subscriptions	312
AWS	312
Azure	326
Google Cloud	340
Manage NSS credentials associated with BlueXP	346
Manage credentials associated with your BlueXP login	351
Monitor BlueXP operations	353
Audit user activity from the BlueXP timeline	353
Monitor activities using the Notification Center	354
Reference	359
Connector maintenance console	359
Connector maintenance console	359
Permissions	360
Permissions summary for BlueXP	360
AWS permissions for the Connector	364
Azure permissions for the Connector	395
Google Cloud permissions for the Connector	414
Ports	420
Connector security group rules in AWS	420
Connector security group rules in Azure	421
Connector firewall rules in Google Cloud	423
Ports for the on-premisesConnector	424
Knowledge and support	425
Register for support	425
Support registration overview	425
Register BlueXP for NetApp support	425
Associate NSS credentials for Cloud Volumes ONTAP support	427
Get help	429
Get support for a cloud provider file service	429
Use self-support options	429
Create a case with NetApp support	429

Manage your support cases (Preview)	432
Legal notices	435
Copyright	435
Trademarks	435
Patents	435
Privacy policy	435
Open source	435

BlueXP setup and administration documentation

Release notes

What's new

Learn what's new with BlueXP administration features: identity and access management (IAM), Connectors, cloud provider credentials, and more.

11 August 2025

Connector 3.9.55

This release of the BlueXP Connector includes security improvements, and bug fixes.

The 3.9.55 release is available for standard mode and restricted mode.

Japanese language support

The BlueXP UI is now available in the Japanese language. If your browser language is Japanese, BlueXP displays in Japanese. To access documentation in Japanese, use the language menu on the documentation website.

Operational resiliency feature

The Operational resiliency feature has been removed from BlueXP. Contact NetApp support if you encounter issues.

BlueXP Identity and Access Management (IAM)

Identity and Access Management in BlueXP now provides the following feature.

New access role for operational support

BlueXP now supports an Operational support analyst role. This role grants a user permissions to monitor storage alerts, view the BlueXP audit timeline, and enter and track NetApp Support cases.

[Learn more about using access roles.](#)

31 July 2025

Private mode release (3.9.54)

A new private mode release is now available to download from the [NetApp Support Site](#)

The 3.9.54 release includes updates to the following BlueXP components and services.

Component or service	Version included in this release	Changes since the previous private mode release
Connector	3.9.54, 3.9.53	Go to the what's new in BlueXP page and refer to the changes included for versions 3.9.54 and 3.9.53.

Component or service	Version included in this release	Changes since the previous private mode release
Backup and recovery	28 July 2025	Go to the what's new in BlueXP backup and recovery page and refer to the changes included in the July 2025 release.
Classification	14 July 2025 (version 1.45)	Go to the what's new in BlueXP classification page .

For more details about private mode, including how to upgrade, refer to the following:

- [Learn about private mode](#)
- [Learn how to get started with BlueXP in private mode](#)
- [Learn how to upgrade the Connector when using private mode](#)

21 July 2025

Support for Google Cloud NetApp Volumes

You can now view Google Cloud NetApp Volumes in BlueXP. [Learn more about Google Cloud NetApp Volumes](#).

BlueXP Identity and Access Management (IAM)

New access role for Google Cloud NetApp Volumes

BlueXP now supports using an access role for the following storage system:

- Google Cloud NetApp Volumes

[Learn more about using access roles](#).

14 July 2025

Connector 3.9.54

This release of the BlueXP Connector includes security improvements, bug fixes, and the following new features:

- Support for transparent proxies for Connectors dedicated to supporting Cloud Volumes ONTAP services. [Learn more about configuring a transparent proxy](#).
- Ability to use network tags to help route Connector traffic when the Connector is deployed in a Google Cloud environment.
- Additional in-product notifications for Connector health monitoring, including CPU and RAM usage.

At this time, the 3.9.54 release is available for standard mode and restricted mode.

BlueXP Identity and Access Management (IAM)

Identity and Access Management in BlueXP now provides the following features:

- Support for IAM in private mode, allowing you to manage user access and permissions for BlueXP services and applications.

- Streamlined management of identity federations, including easier navigation, clearer options for configuring federated connections, and improved visibility into existing federations.
- Access roles for BlueXP backup and recovery, BlueXP disaster recovery, and federation management.

Support for IAM in private mode

BlueXP now supports IAM in private mode, allowing you to manage user access and permissions for BlueXP services and applications. This enhancement enables private mode customers to leverage role-based access control (RBAC) for better security and compliance.

[Learn more about IAM in BlueXP.](#)

Streamlined management of identity federations

BlueXP now offers a more intuitive interface for managing identity federation. This includes easier navigation, clearer options for configuring federated connections, and improved visibility into existing federations.

Enabling single sign-on (SSO) through identity federation lets users log in to BlueXP with their corporate credentials. This improves security, reduces password use, and simplifies onboarding.

You'll be prompted to import any existing federated connections to the new interface to gain access to the new management features. This allows you to take advantage of the latest enhancements without having to recreate your federated connections. [Learn more about importing your existing federated connection to BlueXP.](#)

Improved federation management allows you to:

- Add more than one verified domain to a federated connection, allowing you to use multiple domains with the same identity provider (IdP).
- Disable or delete federated connections when needed, giving you control over user access and security.
- Control access to federation management with IAM roles.

[Learn more about identity federation in BlueXP.](#)

New access roles for BlueXP backup and recovery, BlueXP disaster recovery, and federation management

BlueXP now supports using IAM roles for the following features and data services:

- BlueXP backup and recovery
- BlueXP disaster recovery
- Federation

[Learn more about using access roles.](#)

9 June 2025

Connector 3.9.53

This release of the BlueXP Connector includes security improvements and bug fixes.

The 3.9.53 release is available for standard mode and restricted mode.

Disk space usage alerts

The Notifications Center now includes alerts for disk space usage on the Connector. [Learn more.](#)

Audit improvements

The Timeline now includes login and logout events for users. You can see when login activity, which can help with auditing and security monitoring. API users who have the Organization administrator role can view the email address of the user who logged in by including the `includeUserData=true`` parameter as in the following: `/audit/<account_id>?includeUserData=true`.

Keystone subscription management available in BlueXP

You can manage your NetApp Keystone subscription from BlueXP.

[Learn about Keystone subscription management in BlueXP.](#)

BlueXP Identity and Access Management (IAM)

Multi-factor authentication (MFA)

Unfederated users can enable MFA for their BlueXP accounts to improve security. Administrators can manage MFA settings, including resetting or disabling MFA for users as needed. This is supported in standard mode only.

[Learn about setting up multi-factor authentication for yourself.](#)
[Learn about administering multi-factor authentication for users.](#)

Workloads

You can now view and delete Amazon FSx for NetApp ONTAP credentials from the Credentials page in BlueXP.

29 May 2025

Private mode release (3.9.52)

A new private mode release is now available to download from the [NetApp Support Site](#)

The 3.9.52 release includes updates to the following BlueXP components and services.

Component or service	Version included in this release	Changes since the previous private mode release
Connector	3.9.52, 3.9.51	Go to the what's new in BlueXP connector page and refer to the changes included for versions 3.9.52 and 3.9.50.
Backup and recovery	12 May 2025	Go to the what's new in BlueXP backup and recovery page and refer to the changes included in the May 2025 release.
Classification	12 May 2025 (version 1.43)	Go to the what's new in BlueXP classification page and refer to the changes included in the 1.38 to 1.371.41 releases.

For more details about private mode, including how to upgrade, refer to the following:

- [Learn about private mode](#)
- [Learn how to get started with BlueXP in private mode](#)
- [Learn how to upgrade the Connector when using private mode](#)

12 May 2025

Connector 3.9.52

This release of the BlueXP Connector includes minor security improvements and bug fixes, as well as some additional updates.

At this time, the 3.9.52 release is available for standard mode and restricted mode.

Support for Docker 27 and Docker 28

Docker 27 and Docker 28 are now supported with the Connector.

Cloud Volumes ONTAP

Cloud Volumes ONTAP nodes no longer shutdown when the Connector is out of compliance or down for more than 14 days. Cloud Volumes ONTAP still sends Event Management messages when it loses access to the Connector. This change is to ensure that Cloud Volumes ONTAP can continue to operate even if the Connector is down for an extended period of time. It does not change compliance requirements for the Connector.

Keystone administration available in BlueXP

The beta for NetApp Keystone in BlueXP has added access to Keystone administration. You can access the sign-up page for the NetApp Keystone beta from the left navigation bar of BlueXP.

BlueXP Identity and Access Management (IAM)

New storage management roles

The Storage admin, System health specialist, and Storage viewer roles are available and can be assigned to users.

These roles enable you to manage who in your organization can discover and manage storage resources, as well as view storage health information and perform software updates.

These roles are supported for controlling access to the following storage resources:

- E-Series systems
- StorageGRID systems
- On-premises ONTAP systems

You can also use these roles to control access to the following BlueXP services:

- Software updates
- Digital advisor
- Operational resiliency
- Economic efficiency

- Sustainability

The following roles have been added:

- **Storage admin**

Administer storage health, governance, and discovery for the storage resources in the organization. This role can also perform software updates on storage resources.

- **System health specialist**

Administer storage health and governance for the storage resources in the organization. This role can also perform software updates on storage resources. This role cannot modify or delete working environments.

- **Storage viewer**

View storage health information and governance data.

[Learn about access roles.](#)

14 April 2025

Connector 3.9.51

This release of the BlueXP Connector includes minor security improvements and bug fixes.

At this time, the 3.9.51 release is available for standard mode and restricted mode.

Secure endpoints for Connector downloads now supported for Backup and recovery and Ransomware protection

If you are using Backup and recovery or Ransomware protection, you can now use secure endpoints for Connector downloads. [Learn about secure endpoints for Connector downloads.](#)

BlueXP Identity and Access Management (IAM)

- Users without the Org admin or Folder or project admin must be assigned a Ransomware protection role to have access to Ransomware protection. You can assign a user one of two roles: Ransomware protection admin or Ransomware protection viewer.
- Users without the Org admin or Folder or project admin must be assigned a Keystone role to have access to Keystone. You can assign a user one of two roles: Keystone admin or Keystone viewer.

[Learn about access roles.](#)

- If you have the Org admin or Folder or project admin role, you can now associate a Keystone subscription with an IAM project. Associating a Keystone subscription with an IAM project allows you to control access to Keystone within BlueXP.

28 March 2025

Private mode release (3.9.50)

A new private mode release is now available to download from the [NetApp Support Site](#)

The 3.9.50 release includes updates to the following BlueXP components and services.

Component or service	Version included in this release	Changes since the previous private mode release
Connector	3.9.50, 3.9.49	Go to the what's new in BlueXP connector page and refer to the changes included for versions 3.9.50 and 3.9.49.
Backup and recovery	17 March 2025	Go to the what's new in BlueXP backup and recovery page and refer to the changes included in the March 2024 release.
Classification	10 March 2025 (version 1.41)	Go to the what's new in BlueXP classification page and refer to the changes included in the 1.38 to 1.371.41 releases.

For more details about private mode, including how to upgrade, refer to the following:

- [Learn about private mode](#)
- [Learn how to get started with BlueXP in private mode](#)
- [Learn how to upgrade the Connector when using private mode](#)

10 March 2025

Connector 3.9.50

This release of the BlueXP Connector includes minor security improvements and bug fixes.

- Management of Cloud Volumes ONTAP systems is now supported by Connectors that have SELinux enabled on the operating system.

[Learn more about SELinux](#)

At this time, the 3.9.50 release is available for standard mode and restricted mode.

NetApp Keystone beta available in BlueXP

NetApp Keystone will soon be available from BlueXP and is now in beta. You can access the sign-up page for the NetApp Keystone beta from the left navigation bar of BlueXP.

6 March 2025

Connector 3.9.49 update

ONTAP System Manager access when BlueXP uses a Connector

A BlueXP administrator (users with the Organization admin role) can configure BlueXP to prompt users to enter their ONTAP credentials in order to access ONTAP system manager. When this setting is enabled, users need enter their ONTAP credentials each time as they are not stored in BlueXP.

This feature is available in Connector version 3.9.49 and higher. [Learn how to configure credentials settings..](#)

Connector 3.9.48 update

Ability to disable the auto-upgrade setting for the Connector

You can disable the auto-upgrade feature of the Connector.

When you use BlueXP in standard mode or restricted mode, BlueXP automatically upgrades your Connector to the latest release, as long as the Connector has outbound internet access to obtain the software update. If you need to manually manage when the connector is upgraded, you can now disable automatic upgrades for standard mode or restricted mode.



This change does not impact BlueXP private mode where you must always upgrade the connector yourself.

This feature is available in Connector version 3.9.48 and higher.

[Learn how disable auto-upgrade for the Connector.](#)

18 February 2025

Private mode release (3.9.48)

A new private mode release is now available to download from the [NetApp Support Site](#)

The 3.9.48 release includes updates to the following BlueXP components and services.

Component or service	Version included in this release	Changes since the previous private mode release
Connector	3.9.48	Go to the what's new in BlueXP connector page and refer to the changes included for versions 3.9.48.
Backup and recovery	21 February 2025	Go to the what's new in BlueXP backup and recovery page and refer to the changes included in the February 2025 release.
Classification	22 January 2025 (version 1.39)	Go to the what's new in BlueXP classification page and refer to the changes included in the 1.39 release.

10 February 2025

Connector 3.9.49

This release of the BlueXP Connector includes minor security improvements and bug fixes.

At this time, the 3.9.49 release is available for standard mode and restricted mode.

BlueXP identity and access management (IAM)

- Support for assigning multiple roles to a BlueXP user.
- Support for assigning a role on multiple resources of the BlueXP organization (Org/folder/project)
- Roles are now associated with one of two categories: platform and data service.

Restricted mode now uses BlueXP IAM

BlueXP identity and access management (IAM) is now used in restricted mode.

BlueXP identity and access management (IAM) is a resource and access management model that replaces and enhances the previous functionality provided by BlueXP accounts when using BlueXP in standard and restricted mode.

Related information

- [Learn about BlueXP IAM](#)
- [Get started with BlueXP IAM](#)

BlueXP IAM provides more granular management of resources and permissions:

- A top-level *organization* enables you to manage access across your various *projects*.
- *Folders* enable you to group related projects together.
- Enhanced resource management enables you to associate a resource with one or more folders or projects.

For example, you can associate a Cloud Volumes ONTAP system with multiple projects.

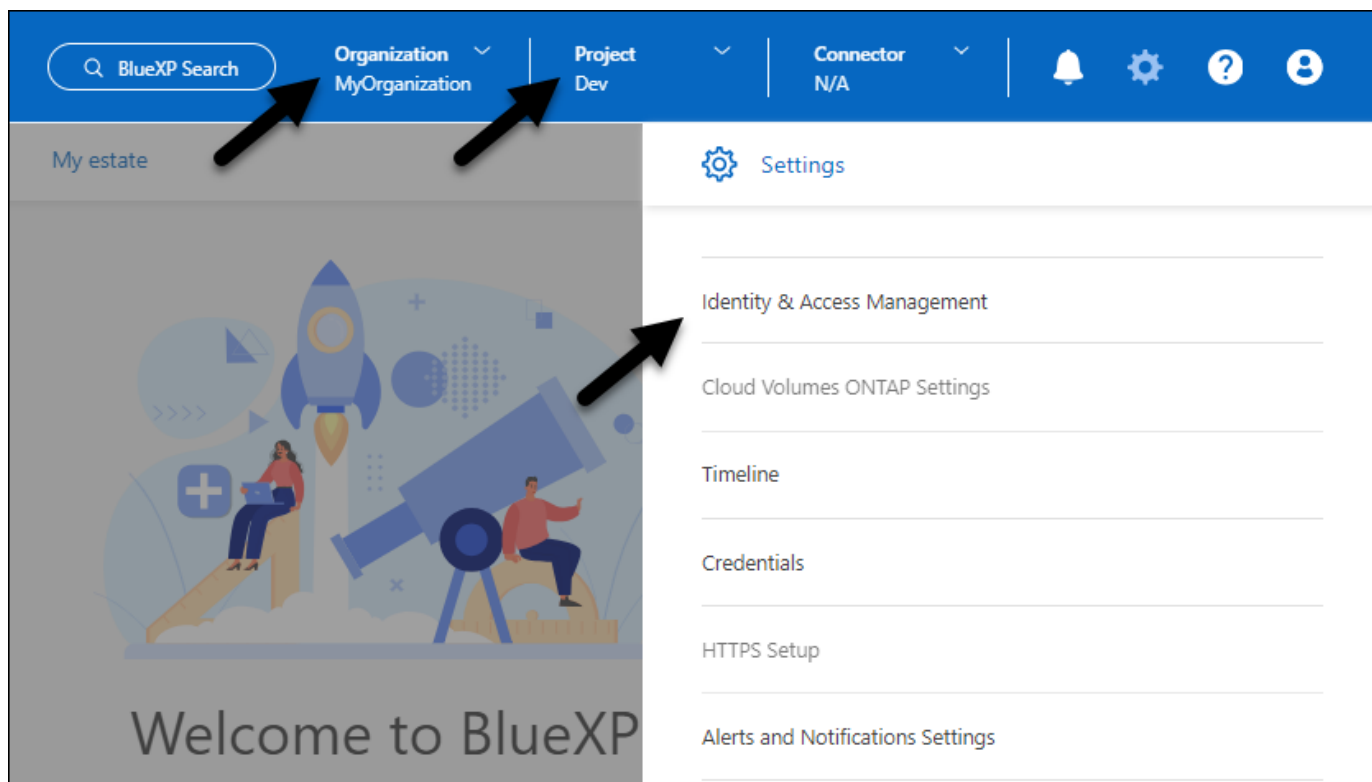
- Enhanced access management enables you to assign a role to members at different levels of the organization hierarchy.

These enhancements provide better control over the actions that users can perform and the resources that they can access.

How BlueXP IAM affects your existing account in restricted mode

When you log in to BlueXP, you'll notice these changes:

- Your *account* is now called an *organization*
- Your *workspaces* are now called *projects*
- The names of user roles have changed:
 - *Account admin* is now *Organization admin*
 - *Workspace admin* is now *Folder or project admin*
 - *Compliance viewer* is now *Classification viewer*
- Under Settings, you can access BlueXP identity and access management to take advantage of these enhancements



Note the following:

- There are no changes to your existing users or working environments.
- While the names of the roles have changed, there are no differences from a permissions perspective. Users will continue to have access to the same working environments as before.
- There are no changes to how you log in to BlueXP. BlueXP IAM works with NetApp cloud logins, NetApp Support Site credentials, and federated connections just like BlueXP accounts did.
- If you had multiple BlueXP accounts, you now have multiple BlueXP organizations.

API for BlueXP IAM

This change introduces a new API for BlueXP IAM, but it is backwards compatible with the previous tenancy API. [Learn about the API for BlueXP IAM](#)

Supported deployment modes

BlueXP IAM is supported when using BlueXP in standard and restricted mode. If you're using BlueXP in private mode, then you'll continue using a BlueXP *account* to manage workspaces, users, and resources.

Private mode release (3.9.48)

A new private mode release is now available to download from the [NetApp Support Site](#)

The 3.9.48 release includes updates to the following BlueXP components and services.

Component or service	Version included in this release	Changes since the previous private mode release
Connector	3.9.48	Go to the what's new in BlueXP connector page and refer to the changes included for versions 3.9.48.

Component or service	Version included in this release	Changes since the previous private mode release
Backup and recovery	21 February 2025	Go to the what's new in BlueXP backup and recovery page and refer to the changes included in the February 2025 release.
Classification	22 January 2025 (version 1.39)	Go to the what's new in BlueXP classification page and refer to the changes included in the 1.39 release.

13 January 2025

Connector 3.9.48

This release of the BlueXP Connector includes minor security improvements and bug fixes.

At this time, the 3.9.48 release is available for standard mode and restricted mode.

BlueXP identity and access management

- The Resources page now displays undiscovered resources. Undiscovered resources are storage resources that BlueXP knows about but you have not created working environments for. For example, resources that display in digital advisor that do not yet have working environments display on the Resources page as undiscovered resources.
- Amazon FSx for NetApp ONTAP resources aren't displayed on the IAM resources page as you cannot associate them with an IAM role. You can view these resources on their respective canvas or from workloads.

Create a support case for additional BlueXP services

After you register BlueXP for support, you can create a support case directly from the BlueXP web-based console. When you create the case, you need to select the service that the issue is associated with.

Starting with this release, you can now create a support case and associate it with additional BlueXP services:

- BlueXP disaster recovery
- BlueXP ransomware protection

[Learn more about creating a support case.](#)

16 December 2024

New secure endpoints to obtain Connector images

When you install the Connector, or when an automatic upgrade occurs, the Connector contacts repositories to download images for the installation or upgrade. By default, the Connector has always contacted the following endpoints:

- https://*.blob.core.windows.net
- <https://cloudmanagerinfraproduct.azurecr.io>

The first endpoint includes a wild card because we can't provide a definitive location. The load balancing of the repository is managed by the service provider, which means the downloads can happen from different endpoints.

For increased security, the Connector can now download installation and upgrades images from dedicated endpoints:

- <https://bluexpinfraprod.eastus2.data.azurecr.io>
- <https://bluexpinfraprod.azurecr.io>

We recommend that you start using these new endpoints by removing the existing endpoints from your firewall rules and allowing the new endpoints.

These new endpoints are supported starting with the 3.9.47 release of the Connector. There is no backwards compatibility with previous releases of the Connector.

Note the following:

- The existing endpoints are still supported. If you don't want to use the new endpoints, no changes are required.
- The Connector contacts the existing endpoints first. If those endpoints aren't accessible, the Connector automatically contacts the new endpoints.
- The new endpoints are not supported in the following scenarios:
 - If the Connector is installed in a Government region.
 - If you use the Connector with BlueXP backup and recovery or BlueXP ransomware protection.

For both of these scenarios, you can continue to use the existing endpoints.

9 December 2024

Connector 3.9.47

This release of the BlueXP Connector includes bug fixes and a change to the endpoints contacted during Connector installation.

At this time, the 3.9.47 release is available for standard mode and restricted mode.

Endpoint to contact NetApp support during installation

When you manually install the Connector, the installer no longer contacts <https://support.netapp.com>.

The installer still contacts <https://mysupport.netapp.com>.

BlueXP identity and access management

The Connectors page lists only currently available Connectors. It no longer displays Connectors that you have removed.

26 November 2024

Private mode release (3.9.46)

A new private mode release is now available to download from the [NetApp Support Site](#)

The 3.9.46 release includes updates to the following BlueXP components and services.

Component or service	Version included in this release	Changes since the previous private mode release
Connector	3.9.46	Minor security improvements and bug fixes
Backup and recovery	22 November 2024	Go to the what's new in BlueXP backup and recovery page and refer to the changes included in the November 2024 release
Classification	4 November 2024 (version 1.37)	Go to the what's new in BlueXP classification page and refer to the changes included in the 1.32 to 1.37 releases
Cloud Volumes ONTAP management	11 November 2024	Go to the what's new with Cloud Volumes ONTAP management page and refer to the changes included in the October 2024 and November 2024 releases
On-premises ONTAP cluster management	26 November 2024	Go to the what's new with on-premises ONTAP cluster management page and refer to the changes included in the November 2024 release

While the BlueXP digital wallet and BlueXP replication are also included with private mode, there are no changes from the previous private mode release.

For more details about private mode, including how to upgrade, refer to the following:

- [Learn about private mode](#)
- [Learn how to get started with BlueXP in private mode](#)
- [Learn how to upgrade the Connector when using private mode](#)

11 November 2024

Connector 3.9.46

This release of the BlueXP Connector includes minor security improvements and bug fixes.

At this time, the 3.9.46 release is available for standard mode and restricted mode.

ID for IAM projects

You can now view the ID for a project from BlueXP identity and access management. You might need to use the ID when making an API call.

[Learn how to obtain the ID for a project.](#)

10 October 2024

Connector 3.9.45 patch

This patch includes bug fixes.

7 October 2024

BlueXP identity and access management

BlueXP identity and access management (IAM) is a new resource and access management model that

replaces and enhances the previous functionality provided by BlueXP accounts when using BlueXP in standard mode.

BlueXP IAM provides more granular management of resources and permissions:

- A top-level *organization* enables you to manage access across your various *projects*.
- *Folders* enable you to group related projects together.
- Enhanced resource management enables you to associate a resource with one or more folders or projects.

For example, you can associate a Cloud Volumes ONTAP system with multiple projects.

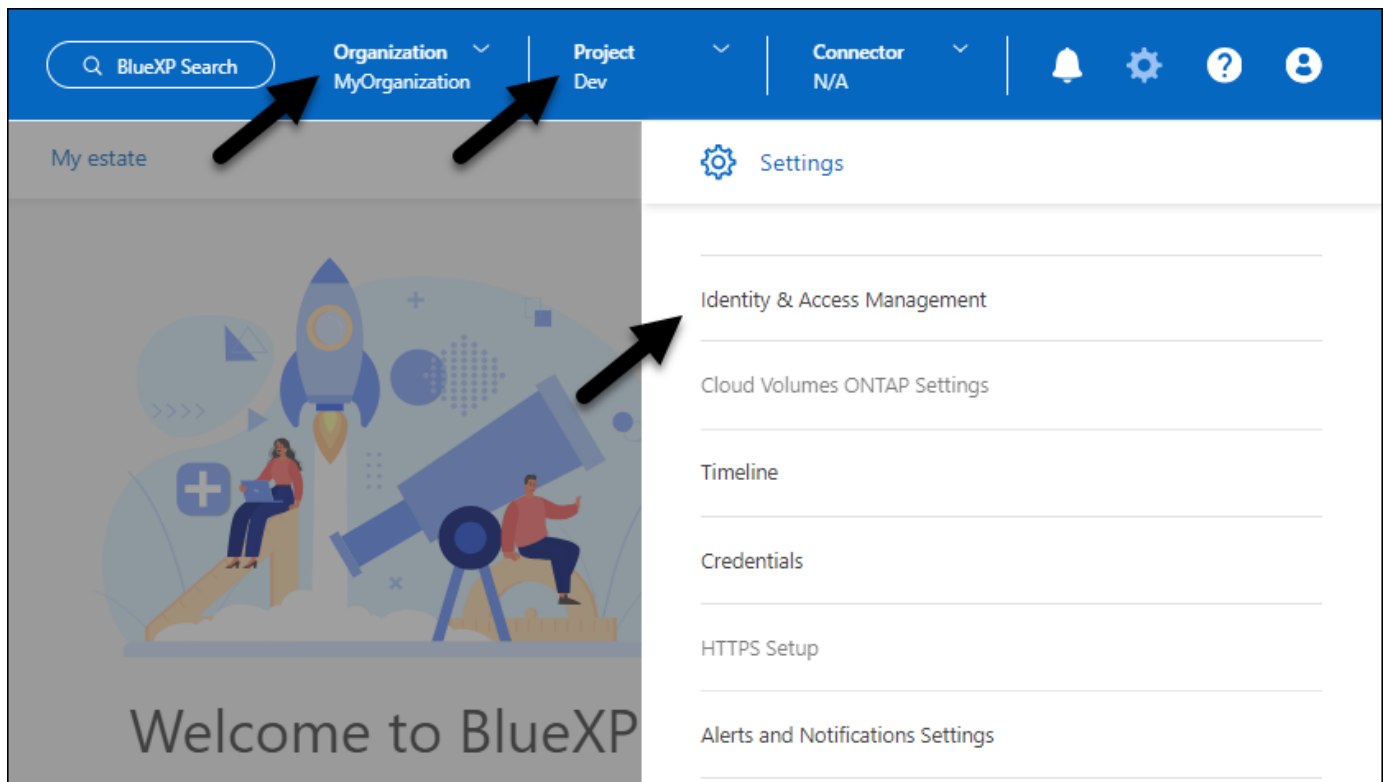
- Enhanced access management enables you to assign a role to members at different levels of the organization hierarchy.

These enhancements provide better control over the actions that users can perform and the resources that they can access.

How BlueXP IAM affects your existing account

When you log in to BlueXP, you'll notice these changes:

- Your *account* is now called an *organization*
- Your *workspaces* are now called *projects*
- The names of user roles have changed:
 - *Account admin* is now *Organization admin*
 - *Workspace admin* is now *Folder or project admin*
 - *Compliance viewer* is now *Classification viewer*
- Under Settings, you can access BlueXP identity and access management to take advantage of these enhancements



Note the following:

- There are no changes to your existing users or working environments.
- While the names of the roles have changed, there are no differences from a permissions perspective. Users will continue to have access to the same working environments as before.
- There are no changes to how you log in to BlueXP. BlueXP IAM works with NetApp cloud logins, NetApp Support Site credentials, and federated connections just like BlueXP accounts did.
- If you had multiple BlueXP accounts, you now have multiple BlueXP organizations.

API for BlueXP IAM

This change introduces a new API for BlueXP IAM, but it is backwards compatible with the previous tenancy API. [Learn about the API for BlueXP IAM](#)

Supported deployment modes

BlueXP IAM is supported when using BlueXP in standard mode. If you're using BlueXP in restricted mode or private mode, then you'll continue using a BlueXP *account* to manage workspaces, users, and resources.

Where to go next

- [Learn about BlueXP IAM](#)
- [Get started with BlueXP IAM](#)

Connector 3.9.45

This release includes expanded operating system support and bug fixes.

The 3.9.45 release is available for standard mode and restricted mode.

Support for Ubuntu 24.04 LTS

Starting with the 3.9.45 release, BlueXP now supports new installations of the Connector on Ubuntu 24.04 LTS hosts when using BlueXP in standard mode or restricted mode.

[View Connector host requirements.](#)

Support for SELinux with RHEL hosts

BlueXP now supports the Connector with Red Hat Enterprise Linux hosts that have SELinux enabled in either enforcing mode or permissive mode.

Support for SELinux starts with the 3.9.40 release for standard mode and restricted mode and with the 3.9.42 release for private mode.

Note the following limitations:

- BlueXP does not support SELinux with Ubuntu hosts.
- Management of Cloud Volumes ONTAP systems it not supported by Connectors that have SELinux enabled on the operating system.

[Learn more about SELinux](#)

30 September 2024

Private mode release (3.9.44)

A new private mode release is now available to download from the NetApp Support Site.

This release includes the following versions of the BlueXP components and services that are supported with private mode.

Service	Version included
Connector	3.9.44
Backup and recovery	27 September 2024
Classification	15 May 2024 (version 1.31)
Cloud Volumes ONTAP management	9 September 2024
Digital wallet	30 July 2023
On-premises ONTAP cluster management	22 April 2024
Replication	18 Sept 2022

For the Connector, the 3.9.44 private mode release includes the updates introduced in the August 2024 and September 2024 releases. Most notably, support for Red Hat Enterprise Linux 9.4.

To learn more about what’s included in the versions of these BlueXP components and services, refer to the release notes for each BlueXP service:

- [What’s new in the September 2024 release of the Connector](#)
- [What’s new in the August 2024 release of the Connector](#)
- [What’s new with BlueXP backup and recovery](#)

- [What's new with BlueXP classification](#)
- [What's new with Cloud Volumes ONTAP management in BlueXP](#)

For more details about private mode, including how to upgrade, refer to the following:

- [Learn about private mode](#)
- [Learn how to get started with BlueXP in private mode](#)
- [Learn how to upgrade the Connector when using private mode](#)

9 September 2024

Connector 3.9.44

This release includes support for Docker Engine 26, an enhancement to SSL certificates, and bug fixes.

The 3.9.44 release is available for standard mode and restricted mode.

Support for Docker Engine 26 with new installations

Starting with the 3.9.44 release of the Connector, Docker Engine 26 is now supported with *new* Connector installations on Ubuntu hosts.

If you have an existing Connector created prior to the 3.9.44 release, then Docker Engine 25.0.5 is still the maximum supported version on Ubuntu hosts.

[Learn more about Docker Engine requirements.](#)

Updated SSL certificate for local UI access

When you use BlueXP in restricted mode or private mode, the user interface is accessible from the Connector virtual machine that's deployed in your cloud region or on-premises. By default, BlueXP uses a self-signed SSL certificate to provide secure HTTPS access to the web-based console running on the Connector.

In this release, we made changes to the SSL certificate for new and existing Connectors:

- The Common Name for the certificate now matches the short host name
- The Certificate Subject Alternative Name is the Fully Qualified Domain Name (FQDN) of the host machine

Support for RHEL 9.4

BlueXP now supports installing the Connector on a Red Hat Enterprise Linux 9.4 host when using BlueXP in standard mode or restricted mode.

Support for RHEL 9.4 starts with the 3.9.40 release of the Connector.

The updated list of supported RHEL versions for standard mode and restricted mode now includes the following:

- 8.6 to 8.10
- 9.1 to 9.4

[Learn about support for RHEL 8 and 9 with the Connector.](#)

Support for Podman 4.9.4 with all RHEL versions

Podman 4.9.4 is now supported with all supported versions of Red Hat Enterprise Linux. Version 4.9.4 was previously supported with only RHEL 8.10.

The updated list of supported Podman versions includes 4.6.1 and 4.9.4 with Red Hat Enterprise Linux hosts.

Podman is required for RHEL hosts starting with the 3.9.40 release of the Connector.

[Learn about support for RHEL 8 and 9 with the Connector.](#)

Updated AWS and Azure permissions

We updated the AWS and Azure policies for the Connector to remove permissions that are no longer required. The permissions were related to BlueXP edge caching and discovery and management of Kubernetes clusters, which are no longer supported as of August, 2024.

- [Learn what changed in the AWS policy.](#)
- [Learn what changed in the Azure policy.](#)

22 August 2024

Connector 3.9.43 patch

We updated the Connector to support the Cloud Volumes ONTAP 9.15.1 release.

Support for this release includes an update to the Connector policy for Azure. The policy now includes the following permissions:

```
"Microsoft.Compute/virtualMachineScaleSets/write",  
"Microsoft.Compute/virtualMachineScaleSets/read",  
"Microsoft.Compute/virtualMachineScaleSets/delete"
```

These permissions are required for Cloud Volumes ONTAP support of Virtual Machine Scale Sets. If you have existing Connectors and you want to use this new feature, you'll need to add these permissions to the custom roles that are associated with your Azure credentials.

- [Learn about the Cloud Volumes ONTAP 9.15.1 release](#)
- [View Azure permissions for the Connector.](#)

8 August 2024

Connector 3.9.43

This release includes minor improvements and bug fixes.

The 3.9.43 release is available for standard mode and restricted mode.

Updated CPU and RAM requirements

To provide higher reliability and to improve the performance of BlueXP and the Connector, we now require

additional CPU and RAM for the Connector virtual machine:

- CPU: 8 cores or 8 vCPUs (the previous requirement was 4)
- RAM: 32 GB (the previous requirement was 14 GB)

As a result of this change, the default VM instance type when deploying the Connector from BlueXP or from the cloud provider's marketplace is as follows:

- AWS: t3.2xlarge
- Azure: Standard_D8s_v3
- Google Cloud: n2-standard-8

The updated CPU and RAM requirements apply to all new Connectors. For existing Connectors, increasing the CPU and RAM is recommended to provide improved performance and reliability.

Support for Podman 4.9.4 with RHEL 8.10

Podman version 4.9.4 is now supported when installing the Connector on a Red Hat Enterprise Linux 8.10 host.

User validation for identity federation

If you use identity federation with BlueXP, each user who logs in to BlueXP for the first time will need to complete a quick form to validate their identity.

31 July 2024

Private mode release (3.9.42)

A new private mode release is now available to download from the NetApp Support Site.

Support for RHEL 8 and 9

This release includes support for installing the Connector on a Red Hat Enterprise Linux 8 or 9 host when using BlueXP in private mode. The following versions of RHEL are supported:

- 8.6 to 8.10
- 9.1 to 9.3

Podman is required as the container orchestration tool for these operating systems.

You should be aware of Podman requirements, known limitations, a summary of operating system support, what to do if you have a RHEL 7 host, how to get started, and more.

[Learn about support for RHEL 8 and 9 with the Connector.](#)

Versions included in this release

This release includes the following versions of the BlueXP services that are supported with private mode.

Service	Version included
Connector	3.9.42
Backup and recovery	18 July 2024

Service	Version included
Classification	1 July 2024 (version 1.33)
Cloud Volumes ONTAP management	10 June 2024
Digital wallet	30 July 2023
On-premises ONTAP cluster management	30 July 2023
Replication	18 Sept 2022

To learn more about what's included in the versions of these BlueXP services, refer to the release notes for each BlueXP service.

- [Learn about private mode](#)
- [Learn how to get started with BlueXP in private mode](#)
- [Learn how to upgrade the Connector when using private mode](#)
- [Learn what's new with BlueXP backup and recovery](#)
- [Learn what's new with BlueXP classification](#)
- [Learn what's new with Cloud Volumes ONTAP management in BlueXP](#)

15 July 2024

Support for RHEL 8.10

BlueXP now supports installing the Connector on a Red Hat Enterprise Linux 8.10 host when using standard mode or restricted mode.

Support for RHEL 8.10 starts with the 3.9.40 release of the Connector.

[Learn about support for RHEL 8 and 9 with the Connector.](#)

8 July 2024

Connector 3.9.42

This release includes minor improvements, bug fixes, and support for the Connector in the AWS Canada West (Calgary) region.

The 3.9.42 release is available for standard mode and restricted mode.

Updated Docker Engine requirements

When the Connector is installed on an Ubuntu host, the minimum supported version of Docker Engine is now 23.0.6. It was previously 19.3.1.

The maximum supported version is still 25.0.5.

[View Connector host requirements.](#)

Email verification now required

New users who sign up to BlueXP are now required to verify their email address before they can log in.

12 June 2024

Connector 3.9.41

This release of the BlueXP Connector includes minor security improvements and bug fixes.

The 3.9.41 release is available for standard mode and restricted mode.

4 June 2024

Private mode release (3.9.40)

A new private mode release is now available to download from the NetApp Support Site. This release includes the following versions of the BlueXP services that are supported with private mode.

Note that this private mode release does *not* include support for the Connector with Red Hat Enterprise Linux 8 and 9.

Service	Version included
Connector	3.9.40
Backup and recovery	17 May 2024
Classification	15 May 2024 (version 1.31)
Cloud Volumes ONTAP management	17 May 2024
Digital wallet	30 July 2023
On-premises ONTAP cluster management	30 July 2023
Replication	18 Sept 2022

To learn more about what's included in the versions of these BlueXP services, refer to the release notes for each BlueXP service.

- [Learn about private mode](#)
- [Learn how to get started with BlueXP in private mode](#)
- [Learn how to upgrade the Connector when using private mode](#)
- [Learn what's new with BlueXP backup and recovery](#)
- [Learn what's new with BlueXP classification](#)
- [Learn what's new with Cloud Volumes ONTAP management in BlueXP](#)

17 May 2024

Connector 3.9.40

This release of the BlueXP Connector includes support for additional operating systems, minor security improvements, and bug fixes.

At this time, the 3.9.40 release is available for standard mode and restricted mode.

Support for RHEL 8 and 9

The Connector is now supported on hosts running the following versions of Red Hat Enterprise Linux with *new* Connector installations when using BlueXP in standard mode or restricted mode:

- 8.6 to 8.9
- 9.1 to 9.3

Podman is required as the container orchestration tool for these operating systems.

You should be aware of Podman requirements, known limitations, a summary of operating system support, what to do if you have a RHEL 7 host, how to get started, and more.

[Learn about support for RHEL 8 and 9 with the Connector.](#)

End of support for RHEL 7 and CentOS 7

On June 30, 2024, RHEL 7 will reach end of maintenance (EOM), while CentOS 7 will reach end of life (EOL). NetApp will continue to support the Connector on these Linux distributions until June 30, 2024.

[Learn what to do if you have an existing Connector running on RHEL 7 or CentOS 7.](#)

AWS permissions update

In the 3.9.38 release, we updated the Connector policy for AWS to include the "ec2:DescribeAvailabilityZones" permission. This permission is now required to support AWS Local Zones with Cloud Volumes ONTAP.

- [View AWS permissions for the Connector.](#)
- [Learn more about support for AWS Local Zones](#)

Known limitations

Known limitations identify platforms, devices, or functions that are not supported by this release of the product, or that do not interoperate correctly with it. Review these limitations carefully.

These limitations are specific to BlueXP set up and administration: the Connector, the software as a service (SaaS) platform, and more.

Connector limitations

Possible conflict with IP addresses in the 172 range

BlueXP deploys the Connector with two interfaces that have IP addresses in the 172.17.0.0/16 and 172.18.0.0/16 ranges.

If your network has a subnet configured with either of these ranges, then you might experience connectivity failures from BlueXP. For example, discovering on-premises ONTAP clusters in BlueXP might fail.

See Knowledge Base article [BlueXP Connector IP conflict with existing network](#) for instructions on how to change the IP address of the Connector's interfaces.

SSL decryption isn't supported

BlueXP doesn't support firewall configurations that have SSL decryption enabled. If SSL decryption is enabled, error messages appear in BlueXP and the Connector instance displays as inactive.

For enhanced security, you have the option to [install an HTTPS certificate signed by a certificate authority \(CA\)](#).

Blank page when loading the local UI

If you load the web-based console that's running on a Connector, the interface might fail to display sometimes, and you just get a blank page.

This issue is related to a caching problem. The workaround is to use an incognito or private web browser session.

Shared Linux hosts are not supported

The Connector isn't supported on a VM that is shared with other applications. The VM must be dedicated to the Connector software.

3rd-party agents and extensions

3rd-party agents or VM extensions are not supported on the Connector VM.

Changes to supported Linux operating systems

As we add and remove support for the Connector on specific Linux operating systems, you might have questions about how this support affects your existing Connector deployments.

Supported operating systems

NetApp supports the BlueXP Connector with the following Linux operating systems.

Standard mode

Manual installation

- Ubuntu 24.04 LTS
- Ubuntu 22.04 LTS
- Red Hat Enterprise Linux
 - 8.6 to 8.10
 - 9.1 to 9.4

Deployment from BlueXP

Ubuntu 22.04 LTS

Deployment from the AWS Marketplace

Ubuntu 22.04 LTS

Deployment from the Azure Marketplace

Ubuntu 22.04 LTS

Restricted mode

Manual installation

- Ubuntu 24.04 LTS
- Ubuntu 22.04 LTS
- Red Hat Enterprise Linux
 - 8.6 to 8.10
 - 9.1 to 9.4

Deployment from the AWS Marketplace

Ubuntu 22.04 LTS

Deployment from the Azure Marketplace

Ubuntu 22.04 LTS

Private mode

Manual installation

- Ubuntu 22.04 LTS
- Red Hat Enterprise Linux
 - 8.6 to 8.10
 - 9.1 to 9.4

Support for RHEL 8 and 9

Note the following about support for RHEL 8 and 9:

Limitations

BlueXP classification is supported if you install the Connector on a RHEL 8 or 9 host that resides on-premises. It's not supported if the RHEL 8 or 9 host resides in AWS, Azure, or Google Cloud.

Container orchestration tool

You must use the Podman tool as the container orchestration tool when installing the Connector on a RHEL 8 or 9 host. Docker Engine is not supported with RHEL 8 and 9.

Deployment mode

RHEL 8 and 9 are supported when using BlueXP in standard mode, restricted mode, and private mode.

Supported Connector versions

NetApp supports RHEL 8 and 9 beginning with the following versions of the Connector:

- 3.9.40 when using BlueXP in standard mode or restricted mode
- 3.9.42 when using BlueXP in private mode

New manual installations only

RHEL 8 and 9 are supported with *new* Connector installations when manually installing the Connector on hosts running on your premises or in the cloud.

RHEL upgrades

If you have an existing Connector running on a RHEL 7 host, we don't support upgrading the RHEL 7 operating system to RHEL 8 or 9. [Learn more about existing Connectors on RHEL 7 or CentOS 7.](#)

End of support for RHEL 7 and CentOS 7

On June 30, 2024, RHEL 7 reached end of maintenance (EOM), while CentOS 7 reached end of life (EOL). NetApp stopped supporting the Connector on these Linux distributions on June 30, 2024.

[Red Hat: What to know about Red Hat Enterprise Linux 7 End of Maintenance](#)

Existing Connectors on RHEL 7 or CentOS 7

If you have an existing Connector running on RHEL 7 or CentOS 7, we don't support upgrading or converting the operating system to RHEL 8 or 9. You need to create a new Connector on a supported operating system.

1. Set up a RHEL 8 or 9 host.
2. Install Podman.
3. Perform a *new* Connector installation.
4. Configure the Connector to discover the working environments that the old Connector was managing.

Related information

How to get started with RHEL 8 and 9

Refer to the following pages for details about host requirements, Podman requirements, and steps to install Podman and the Connector:

Standard mode

- [Install and set up a Connector on-premises](#)
- [Manually install the Connector in AWS](#)
- [Manually install the Connector in Azure](#)
- [Manually install the Connector in Google Cloud](#)

Restricted mode

[Prepare for deployment in restricted mode](#)

Private mode

[Prepare for deployment in private mode](#)

How to rediscover your working environments

Refer to the following pages to rediscover your working environments after a new Connector deployment.

- [Add existing Cloud Volumes ONTAP systems to BlueXP](#)
- [Discover on-premises ONTAP clusters](#)
- [Create or discover an FSx for ONTAP working environment](#)
- [Create an Azure NetApp Files working environment](#)
- [Discover E-Series systems](#)
- [Discover StorageGRID systems](#)

Get started

Learn the basics

Learn about BlueXP

NetApp BlueXP provides your organization with a single control plane that helps you build, protect, and govern data across your on-premises and cloud environments. The BlueXP software as a service (SaaS) platform includes services that provide storage management, data mobility, data protection, and data analysis and control. Management capabilities are provided through a web-based console and APIs.

Features

BlueXP provides unified control of storage across your hybrid multicloud and integrated data services to protect, secure, and optimize data.

Unified control of storage from the BlueXP canvas

The *BlueXP canvas* lets you discover, deploy, and manage cloud and on-premises storage. The canvas centralizes storage management.

Supported cloud and on-premises storage

BlueXP enables you to manage the following types of storage from the BlueXP canvas:

Cloud storage solutions

- Amazon FSx for NetApp ONTAP
- Azure NetApp Files
- Cloud Volumes ONTAP
- Google Cloud NetApp Volumes

On-premises flash and object storage

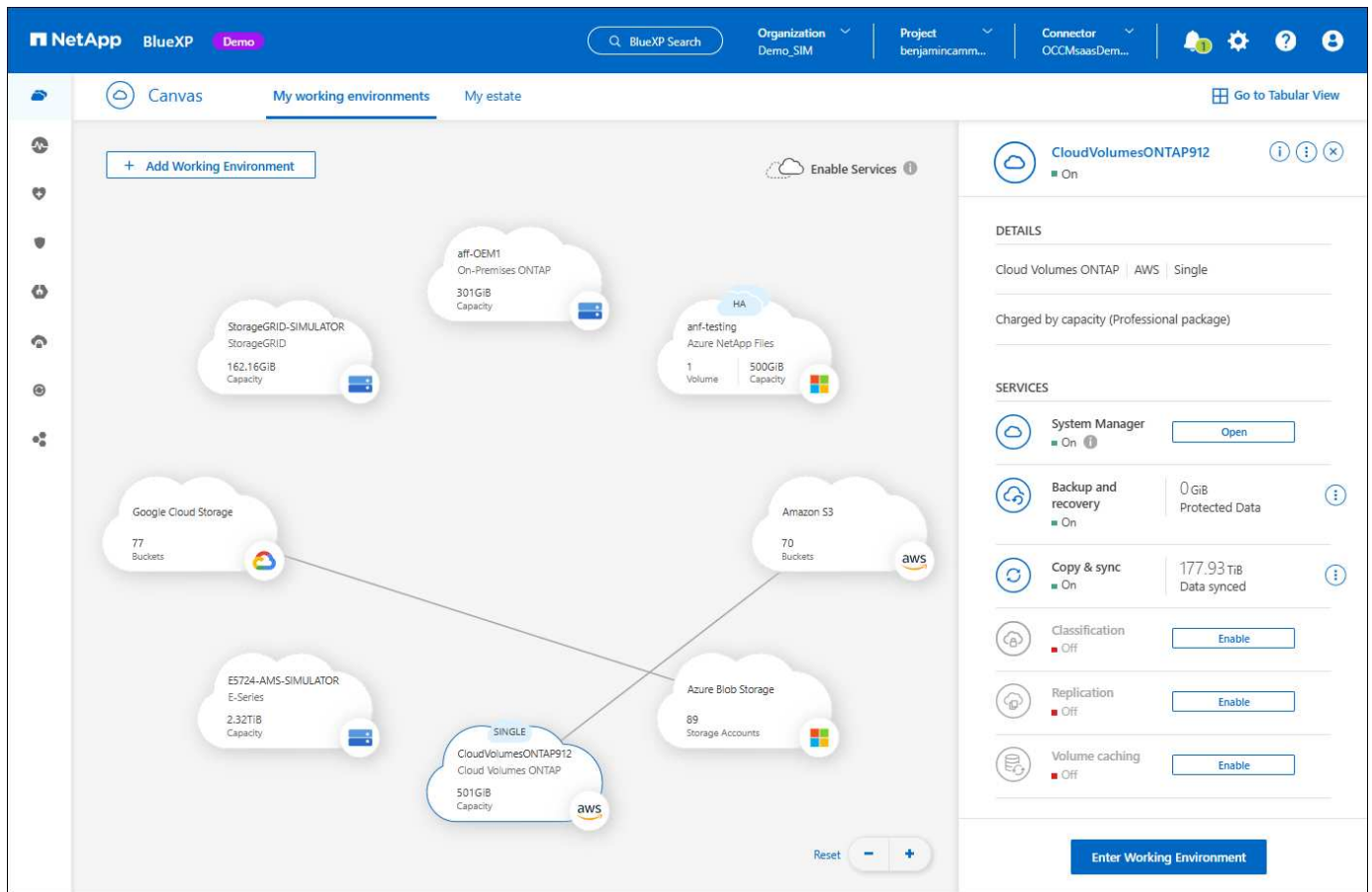
- E-Series systems
- ONTAP clusters
- StorageGRID systems

Cloud object storage

- Amazon S3 storage
- Azure Blob storage
- Google Cloud Storage

Storage management from working environments

On the BlueXP canvas, *working environments* represent discovered or deployed storage. You can select a *working environment* to integrate it with BlueXP data services or manage storage, such as adding volumes.



Integrated services to protect, secure, and optimize data

BlueXP includes data services to secure and maintain data availability across storage.

BlueXP alerts

View issues related to capacity, availability, performance, protection, and security in your ONTAP environment.

BlueXP automation catalog

Use scripted solutions to automate the deployment and integration of NetApp products and services.

BlueXP backup and recovery

Back up and restore cloud and on-premises data.

BlueXP classification

Get your application data and cloud environments privacy ready.

BlueXP copy and sync

Sync data between on-premises and cloud data stores.

BlueXP digital advisor

Use predictive analytics and proactive support to optimize your data infrastructure.

BlueXP digital wallet

Manage and monitor your licenses and subscriptions.

BlueXP disaster recovery

Protect on-premises VMware workloads using VMware Cloud on Amazon FSx for ONTAP as a disaster recovery site.

BlueXP economic efficiency

Identify clusters with current or forecasted low capacity and implement data tiering or additional capacity recommendations.

BlueXP ransomware protection

Detect anomalies that might result in ransomware attacks. Protect and recover workloads.

BlueXP replication

Replicate data between storage systems to support backup and disaster recovery.

BlueXP software updates

Automate the assessment, planning, and execution of ONTAP upgrades.

BlueXP sustainability dashboard

Analyze the sustainability of your storage systems.

BlueXP tiering

Extend your on-premises ONTAP storage to the cloud.

BlueXP volume caching

Create a writable cache volume to speed up access to data or offload traffic from heavily accessed volumes.

BlueXP workload factory

Design, set up, and operate key workloads using Amazon FSx for NetApp ONTAP.

[Learn more about BlueXP and the available data services](#)

Supported cloud providers

BlueXP enables you to manage cloud storage and use cloud services in Amazon Web Services, Microsoft Azure, and Google Cloud.

Cost

Pricing for BlueXP depends on the services that you use.

[Learn about BlueXP pricing](#)

How BlueXP works

BlueXP includes a web-based console that's provided through the SaaS layer, a resource and access management system, Connectors that manage working environments and enable BlueXP cloud services, and different deployment modes to meet your business requirements.

Software-as-a-service

BlueXP is accessible through a [web-based console](#) and APIs. This SaaS experience enables you to automatically access the latest features as they're released and to easily switch between your BlueXP organizations, projects, and Connectors.

BlueXP identity and access management (IAM)

BlueXP identity and access management (IAM) is a resource and access management model that provides granular management of resources and permissions:

- A top-level *organization* enables you to manage access across your various *projects*
- *Folders* enable you to group related projects together
- Resource management enables you to associate a resource with one or more folders or projects
- Access management enables you to assign a role to members at different levels of the organization hierarchy

BlueXP IAM is supported when using BlueXP in standard or restricted mode. If you're using BlueXP in private mode, then you use a BlueXP *account* to manage workspaces, users, and resources.

- [Learn more about BlueXP IAM](#)

Connectors

You don't need a Connector to get started with BlueXP, but you'll need to create a Connector to unlock all BlueXP features and services. A Connector enables you to manage resources and processes across your on-premises and cloud environments. You need it to manage working environments (for example, Cloud Volumes ONTAP) and to use many BlueXP services.

[Learn more about Connectors.](#)

Deployment modes

BlueXP offers three deployment modes. *Standard mode* leverages the BlueXP software as a service (SaaS) layer to provide full functionality. If your environment has security and connectivity restrictions, *restricted mode* and *private mode* limit outbound connectivity to the BlueXP SaaS layer.

[Learn more about BlueXP deployment modes.](#)

SOC 2 Type 2 certification

An independent certified public accountant firm and services auditor examined BlueXP and affirmed that BlueXP achieved SOC 2 Type 2 reports based on the applicable Trust Services criteria.

[View NetApp's SOC 2 reports](#)

Learn about BlueXP Connectors

A *Connector* is NetApp software running in your cloud network or on-premises network. It's used to connect BlueXP's services to your storage environments.

What you can do without a Connector

A Connector isn't required to get started with BlueXP. You can use several features and services within BlueXP without ever creating a Connector.

You can use the following BlueXP features and services without a Connector:

- Amazon FSx for NetApp ONTAP

Some actions require a Connector or a BlueXP workload factory link. [Learn which actions require a Connector or link](#)

- Automation catalog
- Azure NetApp Files

While a Connector isn't required to set up and manage Azure NetApp Files, a Connector is required if you want to use BlueXP classification to scan Azure NetApp Files data.

- Cloud Volumes Service for Google Cloud
- Copy and sync
- Digital advisor
- Digital wallet (licenses only, subscription monitoring requires a Connector)

In almost all cases, you can add a license to the digital wallet without a Connector.

The only time that a Connector is required to add a license to the digital wallet is for Cloud Volumes ONTAP *node-based* licenses. A Connector is required in this case because the data is taken from the licenses installed on Cloud Volumes ONTAP systems.

- Direct discovery of on-premises ONTAP clusters

While a Connector isn't required for direct discovery of an on-premises ONTAP cluster, a Connector is required if you want to take advantage of additional BlueXP features.

[Learn more about discovery and management options for on-premises ONTAP clusters](#)

- Software updates
- Sustainability
- Workload factory

When a Connector is required

When you use BlueXP in standard mode, a Connector is required for the following features and services in BlueXP:

- Alerts
- Amazon FSx for ONTAP management features
- Amazon S3 storage
- Azure Blob storage
- Backup and recovery
- Classification
- Cloud Volumes ONTAP
- Disaster recovery
- E-Series systems
- Economic efficiency ¹
- Google Cloud Storage buckets

- On-premises ONTAP cluster integration with BlueXP data services
- Ransomware protection
- StorageGRID systems
- Tiering
- Volume caching

¹ While you can access these services without a Connector, a Connector is required to initiate actions from the services.

A Connector is required to use BlueXP in restricted mode or private mode.

Connectors must be operational at all times

Connectors are a fundamental part of the BlueXP service architecture. It's your responsibility to ensure that relevant Connectors are up, operational, and accessible at all times. While the service is designed to overcome short outages of Connector availability, you must take immediate action when required to remedy infrastructure failures.

This documentation is governed by the EULA. If the product is not operated in accordance with the documentation, the functionality and operation of the product, as well as your rights under the EULA, might be adversely impacted.

Supported locations

A Connector is supported in the following locations:

- Amazon Web Services
- Microsoft Azure

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

- Google Cloud

If you want to use BlueXP services with Google Cloud, then you must use a Connector that's running in Google Cloud.

- On your premises

Communication with cloud providers

The Connector uses TLS 1.3 for all communication to AWS, Azure, and Google Cloud.

Restricted mode and private mode

To use BlueXP in restricted mode or private mode, you get started with BlueXP by installing the Connector and then accessing the user interface that's running locally on the Connector.

[Learn about BlueXP deployment modes.](#)

How to install a Connector

You can install a Connector directly from BlueXP, from your cloud provider's marketplace, or by manually installing the software on your own Linux host. How you get started depends on whether you're using BlueXP in standard mode, restricted mode, or private mode.

- [Learn about BlueXP deployment modes](#)
- [Get started with BlueXP in standard mode](#)
- [Get started with BlueXP in restricted mode](#)
- [Get started with BlueXP in private mode](#)

Permissions

Specific permissions are needed to create the Connector directly from BlueXP and another set of permissions are needed for the Connector instance itself. If you create the Connector in AWS or Azure directly from BlueXP, then BlueXP creates the Connector with the permissions that it needs.

When using BlueXP in standard mode, how you provide permissions depends on how you plan to create the Connector.

To learn how to set up permissions, refer to the following:

- Standard mode
 - [Connector installation options in AWS](#)
 - [Connector installation options in Azure](#)
 - [Connector installation options in Google Cloud](#)
 - [Set up cloud permissions for on-premises deployments](#)
- [Set up permissions for restricted mode](#)
- [Set up permissions for private mode](#)

To view the exact permissions that the Connector needs for day-to-day operations, refer to the following pages:

- [Learn how the Connector uses AWS permissions](#)
- [Learn how the Connector uses Azure permissions](#)
- [Learn how the Connector uses Google Cloud permissions](#)

It's your responsibility to update the Connector policies as new permissions are added in subsequent releases. If new permissions are required, they will be listed in the release notes.

Connector upgrades

We typically update the Connector software each month to introduce new features and to provide stability improvements. While most of the services and features in the BlueXP platform are offered through SaaS-based software, a few features are dependent on the version of the Connector. That includes Cloud Volumes ONTAP management, on-premises ONTAP cluster management, settings, and help.

When you use BlueXP in standard mode or restricted mode, the Connector automatically updates its software to the latest version, as long as it has outbound internet access to obtain the software update. If you're using BlueXP in private mode, then you'll need to manually upgrade the Connector.

[Learn how to manually upgrade the Connector software when using private mode.](#)

Operating system and VM maintenance

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

Note that you (customer) don't need to stop any services on the Connector host when applying minor security updates.

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

[Be aware that the Connector must be operational at all times.](#)

Multiple working environments and Connectors

A Connector can manage multiple working environments in BlueXP. The maximum number of working environments that a single Connector should manage varies. It depends on the type of working environments, the number of volumes, the amount of capacity being managed, and the number of users.

If you have a large-scale deployment, work with your NetApp representative to size your environment. If you experience any issues along the way, reach out to us by using the in-product chat.

In some cases, you might only need one Connector, but you might find yourself needing two or more Connectors.

Here are a few examples:

- You have a multicloud environment (for example, AWS and Azure) and you prefer to have one Connector in AWS and another in Azure. Each manages the Cloud Volumes ONTAP systems running in those environments.
- A service provider might use one BlueXP organization to provide services for their customers, while using another organization to provide disaster recovery for one of their business units. Each organization would have separate Connectors.

Learn about BlueXP deployment modes

BlueXP offers *deployment modes* that enable you to meet your business and security requirements. *Standard mode* leverages a software as a service (SaaS) layer to provide full functionality, while *restricted mode* and *private mode* are available for organizations that have connectivity restrictions.

While BlueXP inhibits the flow of traffic, communication, and data when using restricted mode or private mode, it's your responsibility to ensure that your environment (on-premises and in the cloud) is in compliance with the required regulations for your business.

Overview

Each deployment mode differs in outbound connectivity, location, installation, authentication, data services, and charging methods.

Standard mode

You use a SaaS service from the web-based console. Depending on the data services and features that you plan to use, a BlueXP admin creates one or more Connectors to manage data within your hybrid cloud environment.

This mode uses encrypted data transmission over the public internet.

Restricted mode

You install a BlueXP Connector in the cloud (in a government, sovereign, or commercial region), and it has limited outbound connectivity to the BlueXP SaaS layer.

This mode is typically used by state and local governments and regulated companies.

[Learn more about outbound connectivity to the SaaS layer.](#)

Private mode

You install a BlueXP Connector on-premises or in the cloud (in a secure region, sovereign cloud region, or commercial region) and has *no* connectivity to the BlueXP SaaS layer. Users access the BlueXP console provided by the Connector locally, not the SaaS layer.

A secure region includes [AWS Secret Cloud](#), [AWS Top Secret Cloud](#), and [Azure IL6](#)

The following table provides a comparison of these modes.

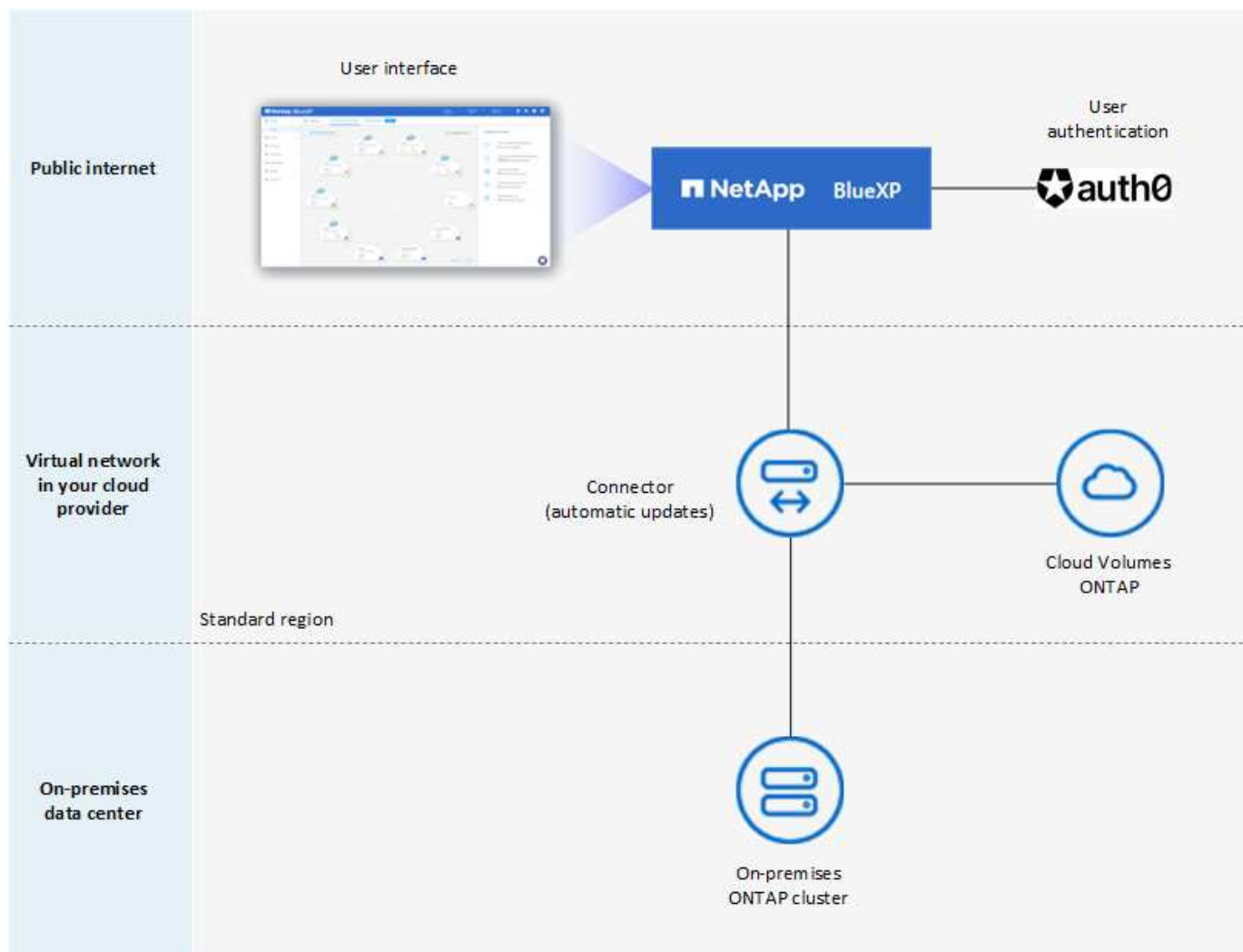
	Standard mode	Restricted mode	Private mode
Connection required to BlueXP SaaS layer?	Yes	Outbound only	No
Connection required to your cloud provider?	Yes	Yes, within the region	Yes, within the region (if using Cloud Volumes ONTAP)
Connector installation	From BlueXP, cloud marketplace, or manual install	Cloud marketplace or manual install	Manual install
Connector upgrades	Automatic upgrades of NetApp Connector software	Automatic upgrades of NetApp Connector software	Manual upgrade required
UI access	From the BlueXP SaaS layer	Locally from the Connector VM	Locally from the Connector VM
API endpoint	The BlueXP SaaS layer	The Connector	The Connector
Authentication	Through SaaS using auth0, NSS login, or identity federation	Through SaaS using auth0 or identity federation	Local user authentication
Multi-factor authentication	Available for local users	Not available	Not available
Storage and data services	All are supported	Many are supported	Several are supported

	Standard mode	Restricted mode	Private mode
Data service licensing options	Marketplace subscriptions and BYOL	Marketplace subscriptions and BYOL	BYOL

Read through the following sections to learn more about these modes, including which BlueXP features and services are supported.

Standard mode

The following image is an example of a standard mode deployment.



BlueXP works as follows in standard mode:

Outbound communication

Connectivity is required from the Connector to the BlueXP SaaS layer, to your cloud provider's publicly available resources, and to other essential components for day-to-day operations.

- [Endpoints that the Connector contacts in AWS](#)
- [Endpoints that the Connector contacts in Azure](#)

- [Endpoints that the Connector contacts in Google Cloud](#)

Supported location for the Connector

In standard mode, the Connector is supported in the cloud or on your premises.

Connector installation

You can install the Connector using the BlueXP setup wizard, AWS or Azure Marketplace, the Google Cloud SDK, or a manual installer on a Linux host in your data center or cloud.

Connector upgrades

BlueXP provides automated upgrades of the Connector software with monthly updates.

User interface access

The user interface is accessible from the web-based console that's provided through the SaaS layer.

API endpoint

API calls are made to the following endpoint:
<https://cloudmanager.cloud.netapp.com>

Authentication

BlueXP provides authentication with auth0 or NetApp Support Site (NSS) logins. Identity federation is available.

Supported BlueXP services

All BlueXP services are available to users.

Supported licensing options

Marketplace subscriptions and BYOL are supported with standard mode; however, the supported licensing options depends on which BlueXP service you are using. Review the documentation for each service to learn more about the available licensing options.

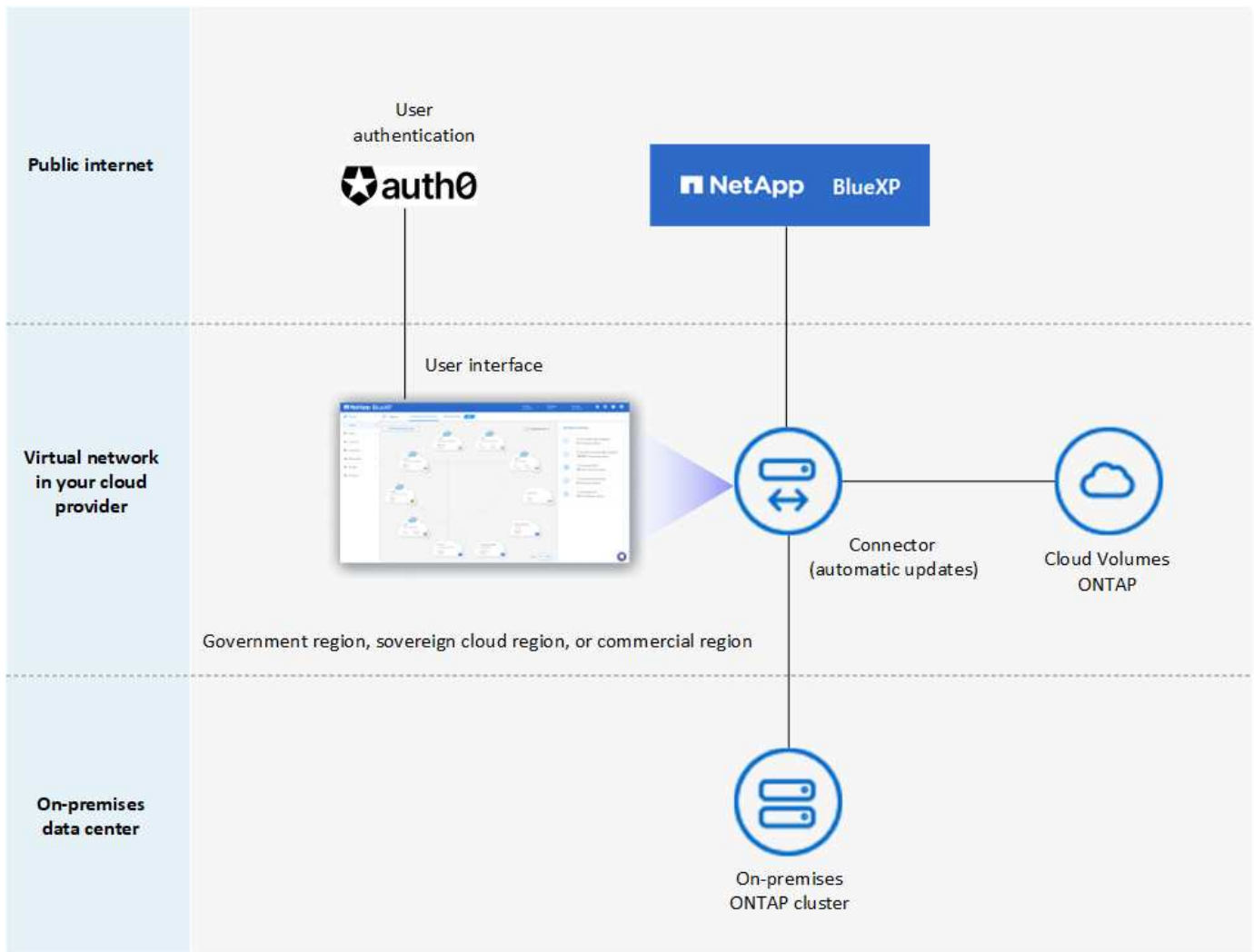
How to get started with standard mode

Go to the [BlueXP web-based console](#) and sign up.

[Learn how to get started with standard mode.](#)

Restricted mode

The following image is an example of a restricted mode deployment.



BlueXP works as follows in restricted mode:

Outbound communication

The Connector requires outbound connectivity to the BlueXP SaaS layer for data services, software upgrades, authentication, and metadata transmission.

The BlueXP SaaS layer does not initiate communication to the Connector. All communication is initiated by the Connector, which can pull or push data from or to the SaaS layer as required.

A connection is also required to cloud provider resources from within the region.

Supported location for the Connector

In restricted mode, the Connector is supported in the cloud: in a government region, sovereign region, or commercial region.

Connector installation

Connector installation is possible from the AWS or Azure Marketplace or a manual installation on your own Linux host.

Connector upgrades

BlueXP provides automated upgrades of the Connector software with monthly updates.

User interface access

The user interface is accessible from the Connector virtual machine that's deployed in your cloud region.

API endpoint

API calls are made to the Connector virtual machine.

Authentication

Authentication is provided through BlueXP's cloud service using auth0. Identity federation is also available.

Supported BlueXP services

BlueXP supports the following storage and data services with restricted mode:

Supported services	Notes
Azure NetApp Files	Full support
Backup and recovery	<p>Supported in Government regions and commercial regions with restricted mode. Not supported in sovereign regions with restricted mode.</p> <p>In restricted mode, BlueXP backup and recovery supports back up and restore of ONTAP volume data only. View the list of supported backup destinations for ONTAP data</p> <p>In restricted mode, BlueXP backup and recovery supports back up and restore of ONTAP volume data only. View the list of supported backup destinations for ONTAP data</p> <p>Back up and restore of application data and virtual machine data is not supported.</p>
Classification	Supported in Government regions with restricted mode. Not supported in commercial regions or in sovereign regions with restricted mode.
Cloud Volumes ONTAP	Full support
Digital wallet	You can use the digital wallet with the supported licensing options listed below for restricted mode.
On-premises ONTAP clusters	<p>Discovery with a Connector and discovery without a Connector (direct discovery) are both supported.</p> <p>When you discover an on-premises cluster with a Connector, the Advanced view (System Manager) is not supported.</p>
Replication	Supported in Government regions with restricted mode. Not supported in commercial regions or in sovereign regions with restricted mode.

Supported licensing options

The following licensing options are supported with restricted mode:

- Marketplace subscriptions (hourly and annual contracts)

Note the following:

- For Cloud Volumes ONTAP, only capacity-based licensing is supported.
- In Azure, annual contracts are not supported with government regions.

- BYOL

For Cloud Volumes ONTAP, both capacity-based licensing and node-based licensing are supported with BYOL.

How to get started with restricted mode

You need to enable restricted mode when you create your BlueXP account.

If you don't have an organization yet, you are prompted to create your organization and enable restricted mode when you log in to BlueXP for the first time from a Connector that you manually installed or that you created from your cloud provider's marketplace.

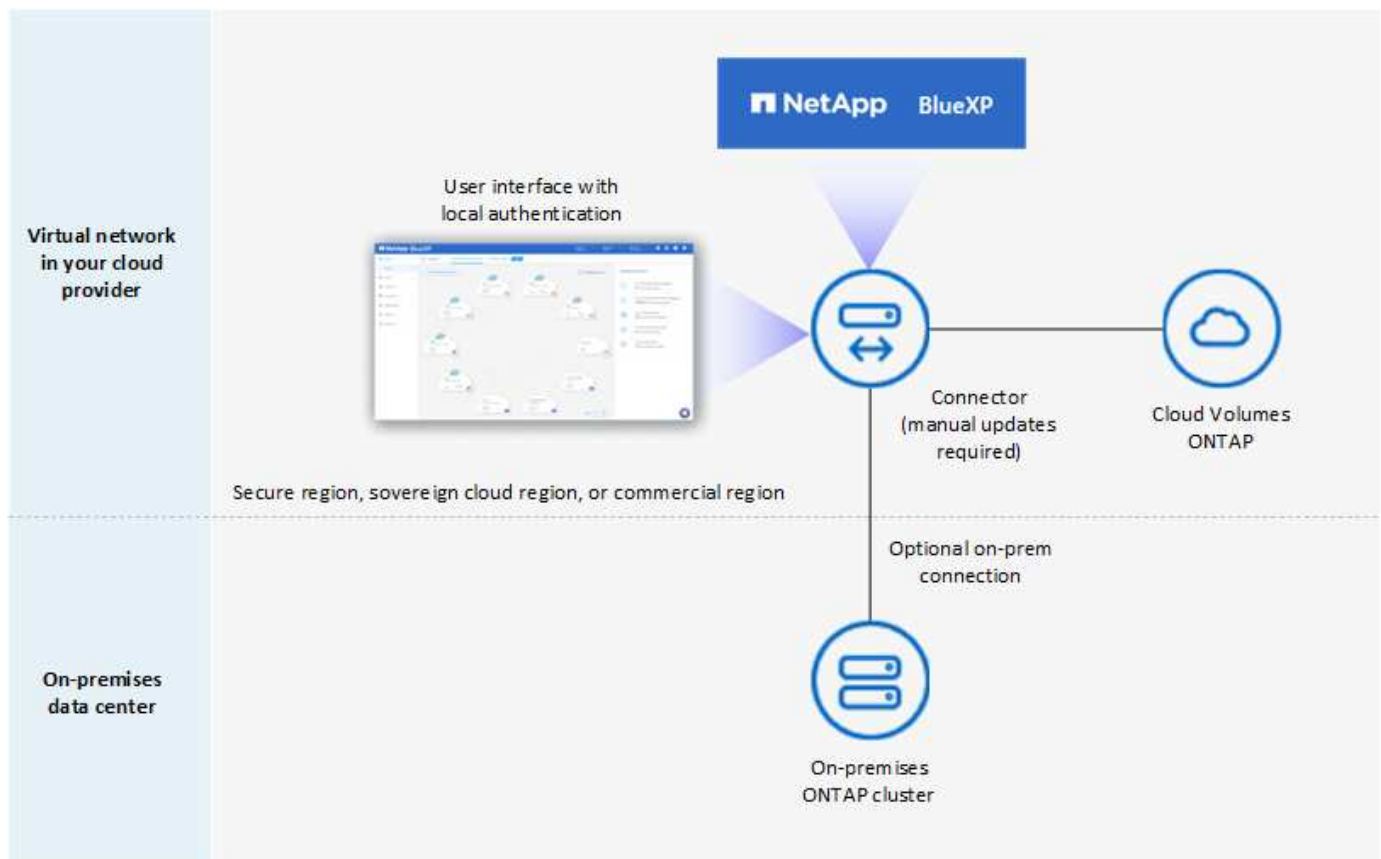
Note that you can't change the restricted mode setting after BlueXP creates the organization. You can't enable restricted mode later and you can't disable it later.

- [Learn how to get started with restricted mode.](#)

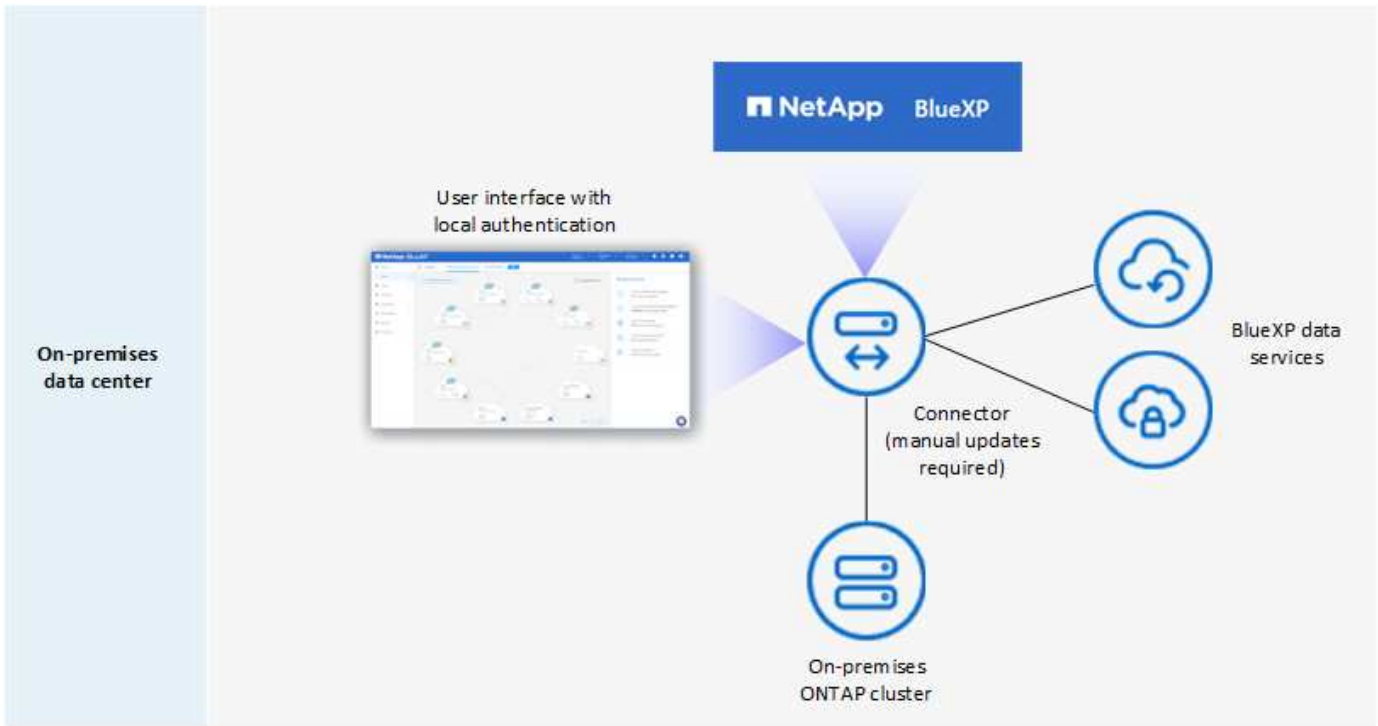
Private mode

In private mode, you can install a Connector either on-premises or in the cloud and then use BlueXP to manage data across your hybrid cloud. There is no connectivity to the BlueXP SaaS layer.

The following image shows an example of a private mode deployment where the Connector is installed in the cloud and manages both Cloud Volumes ONTAP and an on-premises ONTAP cluster.



Meanwhile, the second image shows an example of a private mode deployment where the Connector is installed on-premises, manages an on-premises ONTAP cluster, and provides access to supported BlueXP data services.



BlueXP works as follows in private mode:

Outbound communication

No outbound connectivity is required to the BlueXP SaaS layer. All packages, dependencies, and essential components are packaged with the Connector and served from the local machine. Connectivity to your cloud provider's publicly available resources is required only if you are deploying Cloud Volumes ONTAP.

Supported location for the Connector

In private mode, the Connector is supported in the cloud or on-premises.

Connector installation

Manual installations of the Connector are supported on your own Linux host in the cloud or on-premises.

Connector upgrades

You need to upgrade the Connector software manually. The Connector software is published to the NetApp Support Site at undefined intervals.

User interface access

The user interface is accessible from the Connector that's deployed in your cloud region or on-premises.

API endpoint

API calls are made to the Connector virtual machine.

Authentication

Authentication is provided through local user management and access. Authentication is not provided through BlueXP's cloud service.

Supported BlueXP services in cloud deployments

BlueXP supports the following storage and data services with private mode when the Connector is installed in the cloud:

Supported services	Notes
Backup and recovery	<p>Supported in AWS and Azure commercial regions.</p> <p>Not supported in Google Cloud or in AWS Secret Cloud, AWS Top Secret Cloud, or Azure IL6</p> <p>In private mode, BlueXP backup and recovery supports back up and restore of ONTAP volume data only. View the list of supported backup destinations for ONTAP data</p> <p>Back up and restore of application data and virtual machine data is not supported.</p>
Cloud Volumes ONTAP	Because there's no internet access, the following features aren't available: automated software upgrades and AutoSupport.
Digital wallet	You can use the digital wallet with the supported licensing options listed below for private mode.
On-premises ONTAP clusters	<p>Requires connectivity from the cloud (where the Connector is installed) to the on-premises environment.</p> <p>Discovery without a Connector (direct discovery) is not supported.</p>

Supported BlueXP services in on-premises deployments

BlueXP supports the following storage and data services with private mode when the Connector is installed on your premises:

Supported services	Notes
Backup and recovery	<p>In private mode, BlueXP backup and recovery supports back up and restore of ONTAP volume data only. View the list of supported backup destinations for ONTAP volume data</p> <p>Back up and restore of application data and virtual machine data is not supported.</p>
Classification	<ul style="list-style-type: none"> The only supported data sources are the ones that you can discover locally. View the sources that you can discover locally Features that require outbound internet access are not supported. View the feature limitations
Digital wallet	You can use the digital wallet with the supported licensing options listed below for private mode.
On-premises ONTAP clusters	Discovery without a Connector (direct discovery) is not supported.
Replication	Full support

Supported licensing options

Only BYOL is supported with private mode.

For Cloud Volumes ONTAP BYOL, only node-based licensing is supported. Capacity-based licensing is not supported. Because an outbound internet connection isn't available, you need to manually upload your Cloud Volumes ONTAP licensing file in the BlueXP digital wallet.

[Learn how to add licenses to the BlueXP digital wallet](#)

How to get started with private mode

Private mode is available by downloading the "offline" installer from the NetApp Support Site.

[Learn how to get started with private mode.](#)



If you want to use BlueXP in the [AWS Secret Cloud](#) or the [AWS Top Secret Cloud](#), then you should follow separate instructions to get started in those environments. [Learn how to get started with Cloud Volumes ONTAP in the AWS Secret Cloud or Top Secret Cloud](#)

Service and feature comparison

The following table can help you quickly identify which BlueXP services and features are supported with restricted mode and private mode.

Note that some services might be supported with limitations. For more details about how these services are supported with restricted mode and private mode, refer to the sections above.

Product area	BlueXP service or feature	Restricted mode	Private mode
Working environments This portion of the table lists support for working environment management from the BlueXP canvas. It does not indicate the supported backup destinations for BlueXP backup and recovery.	Amazon FSx for ONTAP	No	No
	Amazon S3	No	No
	Azure Blob	No	No
	Azure NetApp Files	Yes	No
	Cloud Volumes ONTAP	Yes	Yes
	Google Cloud NetApp Volumes	No	No
	Google Cloud Storage	No	No
	On-premisesONTAP clusters	Yes	Yes
	E-Series	No	No
	StorageGRID	No	No

Product area	BlueXP service or feature	Restricted mode	Private mode
Services	Alerts	No	No
	Backup and recovery	Yes View the list of supported backup destinations for ONTAP volume data	Yes View the list of supported backup destinations for ONTAP volume data
	Classification	Yes	Yes
	Copy and sync	No	No
	Digital advisor	No	No
	Digital wallet	Yes	Yes
	Disaster recovery	No	No
	Economic efficiency	No	No
	Ransomware protection	No	No
	Replication	Yes	Yes
	Software updates	No	No
	Sustainability	No	No
	Tiering	No	No
	Volume caching	No	No
	Workload factory	No	No
Features	Identity and access management	Yes	Yes
	Credentials	Yes	Yes
	Federation	Yes	No
	Multi-factor authentication	Yes	No
	NSS accounts	Yes	No
	Notifications	Yes	No
	Search	Yes	No
	Timeline	Yes	Yes

Get started with standard mode

Getting started workflow (standard mode)

Get started with BlueXP in standard mode by preparing networking for the BlueXP console, signing up and creating an account, optionally creating a Connector, and subscribing to NetApp Intelligent Services.

In standard mode, you access a web-based console that is hosted as a Software-as-a-service (SaaS) product

from NetApp. Before you get started, you should have an understanding of [deployment modes](#) and [Connectors](#).

1

Prepare networking for using the BlueXP console

Computers that access the BlueXP console should have connections to specific endpoints to complete a few administrative tasks. If your network restricts outbound access, you should ensure that these endpoints are allowed.

2

Sign up and create an organization

Go to the [BlueXP console](#) and sign up. You'll be given the option to create an organization, but you can skip that step if you're being invited to an existing organization.

At this point, you're logged in and can start using several BlueXP services like Digital Advisor, Amazon FSx for ONTAP, Azure NetApp Files, and more. [Learn what you can do without a Connector](#).

3

Create a Connector

You don't need a Connector to get started with BlueXP, but you can create a Connector to unlock all BlueXP features and services. The Connector is NetApp software that enables BlueXP to manage resources and processes within your hybrid cloud environment.

You can create a Connector in your cloud or on-premises network.

- [Learn more about when Connectors are required and how they work](#)
- [Learn how to create a Connector in AWS](#)
- [Learn how to create a Connector in Azure](#)
- [Learn how to create a Connector in Google Cloud](#)
- [Learn how to create a Connector on-premises](#)

Note that if you want to use NetApp Intelligent Data Services to manage storage and data in Google Cloud, then the Connector must be running in Google Cloud.

Note that if you want to use NetApp's intelligent data services to manage storage and data in Google Cloud, then the Connector must be running in Google Cloud.

4

Subscribe to NetApp Intelligent Services (optional)

Subscribe to NetApp Intelligent Services from your cloud provider's marketplace to pay for data services at an hourly rate (PAYGO) or through an annual contract. NetApp Intelligent Services include Backup and recovery, Cloud Volumes ONTAP, Tiering, Ransomware protection, and Disaster recovery. Classification is included with your subscription at no additional cost.

Prepare networking for the BlueXP console

When you log in and use the web-based console, BlueXP contacts several endpoints to complete the actions that you initiate. Computers that access the console must have connections to these endpoints.

These endpoints are contacted in two scenarios:

- From a user's computer when completing sections from the [BlueXP web-based console](#) that's available as software as a service (SaaS).
- From a user's computer when opening a web browser, entering the IP address of the Connector host, and then logging in and setting up the Connector. These steps are required if you manually install the Connector.

Endpoints	Purpose
https://console.bluexp.netapp.com https://*.console.bluexp.netapp.com	This is the endpoint that you enter in your web browser to use the web-based console.
https://api.bluexp.netapp.com	The web-based console contacts this endpoint to interact with the API for actions related to authorization, licensing, subscriptions, credentials, notifications, and more.
https://aiq.netapp.com	Required to access digital advisor.
AWS services (amazonaws.com): <ul style="list-style-type: none"> • CloudFormation • Elastic Compute Cloud (EC2) • Key Management Service (KMS) • Security Token Service (STS) • Simple Storage Service (S3) 	Required to deploy a Connector from BlueXP in AWS. The exact endpoint depends on the region in which you deploy the Connector. See AWS documentation for details. Suggestion: See AWS documentation for details.
https://management.azure.com https://login.microsoftonline.com	Required to deploy a Connector from BlueXP in most Azure regions.
https://management.microsoftazure.de https://login.microsoftonline.de	Required to deploy a Connector from BlueXP in Azure Germany regions.
https://management.usgovcloudapi.net https://login.microsoftonline.com	Required to deploy a Connector from BlueXP in Azure US Gov regions.
https://www.googleapis.com	Required to deploy a Connector from BlueXP in Google Cloud.
https://signin.b2c.netapp.com	Required to update NetApp Support Site (NSS) credentials or to add new NSS credentials to BlueXP.
https://netapp-cloud-account.auth0.com https://cdn.auth0.com https://services.cloud.netapp.com	Your web browser connects to these endpoints for centralized user authentication through BlueXP.
https://widget.intercom.io	For in-product chat that enables you to talk to NetApp support.

Ensure the Connector has outbound internet access to contact endpoints for daily operations. Follow the links in the next section below to find the list of these endpoints.

Related information

- Prepare networking for the Connector
 - [Set up AWS networking](#)
 - [Set up Azure networking](#)
 - [Set up Google Cloud networking](#)
 - [Set up on-premises networking](#)
- Prepare networking for BlueXP services

Refer to the documentation for each BlueXP service.

[BlueXP documentation](#)

Sign up or log in to BlueXP

BlueXP is accessible from a web-based console. When you get started with BlueXP, your first step is to sign up or to log in using your NetApp Support Site credentials or SSO credentials from your corporate directory.

About this task

When you access BlueXP for the first time, BlueXP enables you to sign up or log in using one of the following options:

BlueXP login

You can sign up by creating a BlueXP login. This authentication method requires you to specify your email address and a password. After you verify your email address, you can log in and then create a BlueXP organization, if you don't already belong to one.

NetApp Support Site (NSS) credentials

If you have existing NetApp Support Site credentials, you don't need to sign up to BlueXP. You log in using your NSS credentials and then BlueXP prompts you to create a BlueXP organization, if you don't already belong to one.

Note that the default password experience is a one-time passcode (OTP) to the registered email address. A new OTP is generated with each sign-in attempt.

Federated connection

You can use single sign-on to log in using credentials from your corporate directory (federated identity). The first user in your organization's account must sign up to BlueXP or log in using NSS credentials, and then set up identity federation. After that, you can add members from your corporate identity to your organization. Those users can then log in using their SSO credentials.

[Learn how to use identity federation with BlueXP.](#)

Steps

1. Open a web browser and go to the [BlueXP console](#)
2. If you have a NetApp Support Site account or if you already set up identity federation, enter the email address associated with your account directly on the **Log in** page.

In both of these cases, BlueXP will sign you up as part of this initial login.

3. If you want to sign up by creating a BlueXP login, select **Sign up**.
 - a. On the **Sign up** page, enter the required information and select **Next**.

Note that only English characters are allowed in the sign up form.

- b. Check your inbox for an email from NetApp that includes instructions to verify your email address.

This step is required before you can log in to BlueXP.

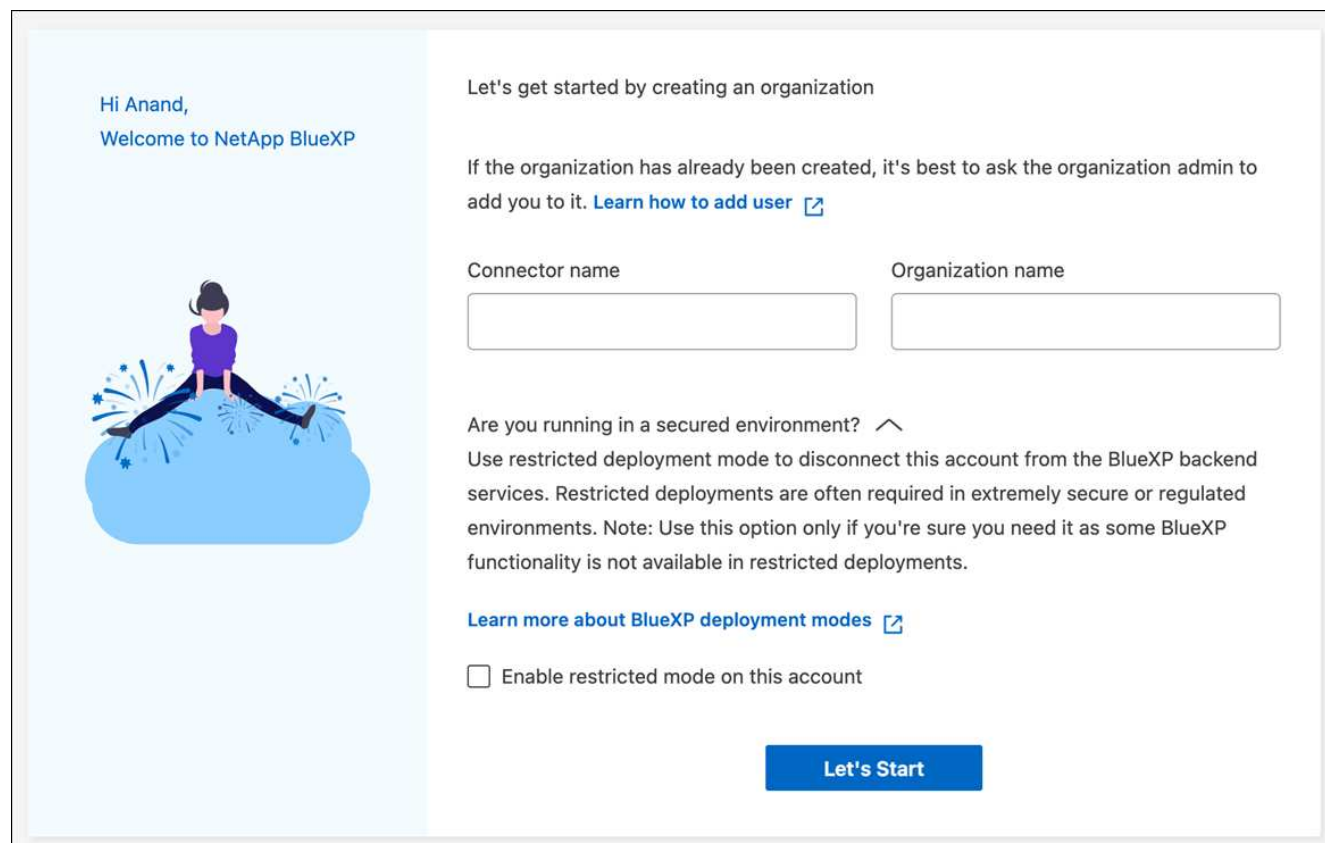
4. After you log in, review the End User License Agreement and accept the terms.

If your user account doesn't already belong to a BlueXP organization, you'll be prompted to create one.

5. On the **Welcome** page, enter a name for your BlueXP organization.

An organization is the top-level element in BlueXP identity and access management (IAM). [Learn about BlueXP IAM](#).

If your business already has a BlueXP organization and you want to join it, then you should close out of BlueXP and ask the owner to associate you with the organization. After the owner adds you, you can log in and you'll have access to the account. [Learn how to add members to an existing organization](#).



The screenshot shows the BlueXP Welcome page. On the left, there is a light blue vertical banner with the text "Hi Anand, Welcome to NetApp BlueXP" and an illustration of a person sitting on a cloud with fireworks. The main content area has a white background. At the top, it says "Let's get started by creating an organization". Below this, it says "If the organization has already been created, it's best to ask the organization admin to add you to it. [Learn how to add user](#)". There are two input fields: "Connector name" and "Organization name". Below these fields, there is a section titled "Are you running in a secured environment?" with a chevron icon. The text below this title says "Use restricted deployment mode to disconnect this account from the BlueXP backend services. Restricted deployments are often required in extremely secure or regulated environments. Note: Use this option only if you're sure you need it as some BlueXP functionality is not available in restricted deployments." There is a link "[Learn more about BlueXP deployment modes](#)" and a checkbox labeled "Enable restricted mode on this account". At the bottom right, there is a blue button labeled "Let's Start".

6. Select **Let's Start**.

Result

You now have a BlueXP login and an organization. In most cases, the next step is to create a Connector, which connects BlueXP's services to your hybrid cloud environment.

Create a Connector

AWS

Connector installation options in AWS

There are a few different ways to create a Connector in AWS. Directly from BlueXP is the most common way.

The following installation options are available:

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

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

- [Create a Connector from the AWS Marketplace](#)

This action also launches an EC2 instance running Linux and the Connector software, but the deployment is initiated directly from the AWS Marketplace, rather than from BlueXP.

- [Download and manually install the software on your own Linux host](#)

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

Create a Connector in AWS from BlueXP

You can create a Connector in AWS directly from BlueXP. To create a Connector in AWS from BlueXP, you need to set up your networking, prepare AWS permissions, and then create the Connector.

Before you begin

- You should have an [understanding of Connectors](#).
- You should review [Connector limitations](#).

Step 1: Set up networking

Ensure that the network location where you plan to install the Connector supports the following requirements. Meeting these requirements enables the Connector to manage resources and processes within your hybrid cloud environment.

VPC and subnet

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

Connections to target networks

A Connector requires a network connection to the location where you're planning to create and manage working environments. For example, the network where you plan to create Cloud Volumes ONTAP systems or a storage system in your on-premises environment.

Outbound internet access

The network location where you deploy the Connector must have an outbound internet connection to contact specific endpoints.

Endpoints contacted from the Connector

The Connector requires outbound internet access to contact the following endpoints in order to manage resources and processes within your public cloud environment for day-to-day operations.

Note that the endpoints listed below are all CNAME entries.

Endpoints	Purpose
AWS services (amazonaws.com): <ul style="list-style-type: none">• CloudFormation• Elastic Compute Cloud (EC2)• Identity and Access Management (IAM)• Key Management Service (KMS)• Security Token Service (STS)• Simple Storage Service (S3)	To manage resources in AWS. The exact endpoint depends on the AWS region that you're using. Refer to AWS documentation for details
https://support.netapp.com https://mysupport.netapp.com	To obtain licensing information and to send AutoSupport messages to NetApp support.
https://*.api.blueexp.netapp.com https://api.blueexp.netapp.com https://*.cloudmanager.cloud.netapp.com https://cloudmanager.cloud.netapp.com https://netapp-cloud-account.auth0.com	To provide SaaS features and services within BlueXP.
Choose between two sets of endpoints: <ul style="list-style-type: none">• Option 1 (recommended) ¹ https://bluexpinfraprod.eastus2.data.azurecr.io https://bluexpinfraprod.azurecr.io• Option 2 https://*.blob.core.windows.net https://cloudmanagerinfraprod.azurecr.io	To obtain images for Connector upgrades.

¹ The endpoints listed in option 1 are recommended because they are more secure. We recommend that you set up your firewall to allow the endpoints listed in option 1, while disallowing the endpoints listed in option 2. Note the following about these endpoints:

- The endpoints listed in option 1 are supported starting with the 3.9.47 release of the Connector. There is no backwards compatibility with previous releases of the Connector.
- The Connector contacts the endpoints listed in option 2 first. If those endpoints aren't accessible, the Connector automatically contacts the endpoints listed in option 1.
- The endpoints in option 1 are not supported if you use the Connector with BlueXP backup and recovery or BlueXP ransomware protection. In this case, you can disallow the endpoints listed in option 1, while

allowing the endpoints listed in option 2.

Endpoints contacted from the BlueXP console

As you use the BlueXP web-based console that's provided through the SaaS layer, it contacts several endpoints to complete data management tasks. This includes endpoints that are contacted to deploy the Connector from the BlueXP console.

[View the list of endpoints contacted from the BlueXP console.](#)

Proxy server

NetApp supports both explicit and transparent proxy configurations. If you are using a transparent proxy, you only need to provide the certificate for the proxy server. If you are using an explicit proxy, you'll also need the IP address and credentials.

- IP address
- Credentials
- HTTPS certificate

Ports

There's no incoming traffic to the Connector, unless you initiate it or if the Connector is used as a proxy to send AutoSupport messages from Cloud Volumes ONTAP to NetApp Support.

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

If Cloud Volumes ONTAP systems don't have an outbound internet connection to send AutoSupport messages, BlueXP automatically configures those 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 NTP

If you're planning to use BlueXP classification to scan your corporate data sources, you should enable a Network Time Protocol (NTP) service on both the BlueXP Connector system and the BlueXP classification system so that the time is synchronized between the systems. [Learn more about BlueXP classification](#)

You'll need to implement this networking requirement after you create the Connector.

Step 2: Set up AWS permissions

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

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

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

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

Steps

1. Go to the AWS IAM console.
2. Select **Policies > Create policy**.
3. Select **JSON**.
4. Copy and paste the following policy:

This policy contains only the permissions needed to launch the Connector instance in AWS from BlueXP. When BlueXP creates the Connector, it applies a new set of permissions to the Connector instance that enables the Connector to manage AWS resources. [View permissions required for the Connector instance itself](#).

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

```

        "ec2:DescribeInstances",
        "ec2:CreateTags",
        "ec2:DescribeImages",
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeLaunchTemplates",
        "ec2:CreateLaunchTemplate",
        "cloudformation:CreateStack",
        "cloudformation>DeleteStack",
        "cloudformation:DescribeStacks",
        "cloudformation:DescribeStackEvents",
        "cloudformation:ValidateTemplate",
        "ec2:AssociateIamInstanceProfile",
        "ec2:DescribeIamInstanceProfileAssociations",
        "ec2:DisassociateIamInstanceProfile",
        "iam:GetRole",
        "iam:TagRole",
        "kms:ListAliases",
        "cloudformation:ListStacks"
    ],
    "Resource": "*"
},
{
    "Effect": "Allow",
    "Action": [
        "ec2:TerminateInstances"
    ],
    "Condition": {
        "StringLike": {
            "ec2:ResourceTag/OCCMInstance": "*"
        }
    },
    "Resource": [
        "arn:aws:ec2:*:*:instance/*"
    ]
}
]
}

```

5. Select **Next** and add tags, if needed.
6. Select **Next** and enter a name and description.
7. Select **Create policy**.
8. Either attach the policy to an IAM role that BlueXP can assume or to an IAM user so that you can provide BlueXP with access keys:
 - (Option 1) Set up an IAM role that BlueXP can assume:
 - a. Go to the AWS IAM console in the target account.

- b. Under Access Management, select **Roles > Create Role** and follow the steps to create the role.
- c. Under **Trusted entity type**, select **AWS account**.
- d. Select **Another AWS account** and enter the ID of the BlueXP SaaS account: 952013314444
- e. Select the policy that you created in the previous section.
- f. After you create the role, copy the Role ARN so that you can paste it in BlueXP when you create the Connector.
- (Option 2) Set up permissions for an IAM user so that you can provide BlueXP with access keys:
 - a. From the AWS IAM console, select **Users** and then select the user name.
 - b. Select **Add permissions > Attach existing policies directly**.
 - c. Select the policy that you created.
 - d. Select **Next** and then select **Add permissions**.
 - e. Ensure that you have the access key and secret key for the IAM user.

Result

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

Step 3: Create the Connector

Create the Connector directly from the BlueXP web-based console.

About this task

- Creating the Connector from BlueXP deploys an EC2 instance in AWS using a default configuration. After you create the Connector, you should not change to a smaller EC2 instance type that has less CPU or RAM. [Learn about the default configuration for the Connector](#).
- When BlueXP creates the Connector, it creates an IAM role and an instance profile for the instance. This role includes permissions that enables the Connector to manage AWS resources. You need to ensure that the role is kept up to date as new permissions are added in subsequent releases. [Learn more about the IAM policy for the Connector](#).

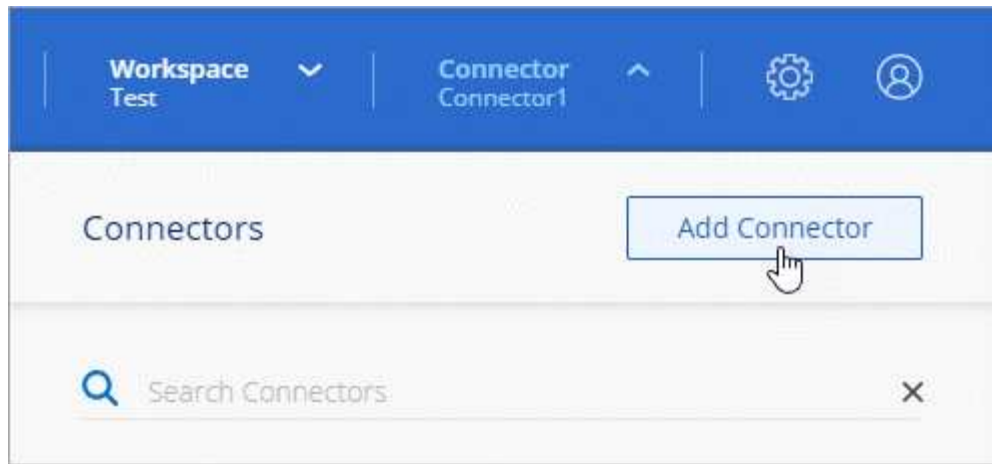
Before you begin

You should have the following:

- An AWS authentication method: either an IAM role or access keys for an IAM user with the required permissions.
- A VPC and subnet that meets networking requirements.
- A key pair for the EC2 instance.
- Details about a proxy server, if a proxy is required for internet access from the Connector.

Steps

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



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



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

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

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

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

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

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

5. Select **Add**.

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

Result

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

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 BlueXP canvas automatically. [Learn how to manage S3 buckets from BlueXP](#)

Create a Connector from the AWS Marketplace

You create a Connector in AWS directly from the AWS Marketplace. To create a Connector from the AWS Marketplace, you need to set up your networking, prepare AWS permissions, review instance requirements, and then create the Connector.

Before you begin

- You should have an [understanding of Connectors](#).
- You should review [Connector limitations](#).

Step 1: Set up networking

Ensure that the network location where you plan to install the Connector supports the following requirements. Meeting these requirements enables the Connector to manage resources and processes within your hybrid cloud environment.

VPC and subnet

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

Connections to target networks

A Connector requires a network connection to the location where you're planning to create and manage working environments. For example, the network where you plan to create Cloud Volumes ONTAP systems or a storage system in your on-premises environment.

Outbound internet access

The network location where you deploy the Connector must have an outbound internet connection to contact specific endpoints.

Endpoints contacted from the Connector

The Connector requires outbound internet access to contact the following endpoints in order to manage resources and processes within your public cloud environment for day-to-day operations.

Note that the endpoints listed below are all CNAME entries.

Endpoints	Purpose
AWS services (amazonaws.com): <ul style="list-style-type: none"> • CloudFormation • Elastic Compute Cloud (EC2) • Identity and Access Management (IAM) • Key Management Service (KMS) • Security Token Service (STS) • Simple Storage Service (S3) 	To manage resources in AWS. The exact endpoint depends on the AWS region that you're using. Refer to AWS documentation for details
https://support.netapp.com https://mysupport.netapp.com	To obtain licensing information and to send AutoSupport messages to NetApp support.
https://*.api.bluexp.netapp.com https://api.bluexp.netapp.com https://*.cloudmanager.cloud.netapp.com https://cloudmanager.cloud.netapp.com https://netapp-cloud-account.auth0.com	To provide SaaS features and services within BlueXP.
Choose between two sets of endpoints: <ul style="list-style-type: none"> • Option 1 (recommended) ¹ https://bluexpinfraprod.eastus2.data.azurecr.io https://bluexpinfraprod.azurecr.io • Option 2 https://*.blob.core.windows.net https://cloudmanagerinfraprod.azurecr.io 	To obtain images for Connector upgrades.

¹ The endpoints listed in option 1 are recommended because they are more secure. We recommend that you set up your firewall to allow the endpoints listed in option 1, while disallowing the endpoints listed in option 2. Note the following about these endpoints:

- The endpoints listed in option 1 are supported starting with the 3.9.47 release of the Connector. There is no backwards compatibility with previous releases of the Connector.
- The Connector contacts the endpoints listed in option 2 first. If those endpoints aren't accessible, the Connector automatically contacts the endpoints listed in option 1.
- The endpoints in option 1 are not supported if you use the Connector with BlueXP backup and recovery or BlueXP ransomware protection. In this case, you can disallow the endpoints listed in option 1, while allowing the endpoints listed in option 2.

Proxy server

NetApp supports both explicit and transparent proxy configurations. If you are using a transparent proxy, you only need to provide the certificate for the proxy server. If you are using an explicit proxy, you'll also need the IP address and credentials.

- IP address
- Credentials
- HTTPS certificate

Ports

There's no incoming traffic to the Connector, unless you initiate it or if the Connector is used as a proxy to send AutoSupport messages from Cloud Volumes ONTAP to NetApp Support.

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

If Cloud Volumes ONTAP systems don't have an outbound internet connection to send AutoSupport messages, BlueXP automatically configures those 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 NTP

If you're planning to use BlueXP classification to scan your corporate data sources, you should enable a Network Time Protocol (NTP) service on both the BlueXP Connector system and the BlueXP classification system so that the time is synchronized between the systems. [Learn more about BlueXP classification](#)

You'll need to implement this networking requirement after you create the Connector.

Step 2: Set up AWS permissions

To prepare for a marketplace deployment, create IAM policies in AWS and attach them to an IAM role. When you create the Connector from the AWS Marketplace, you'll be prompted to select that IAM role.

Steps

1. Log in to the AWS console and navigate to the IAM service.
2. Create a policy:
 - a. Select **Policies > Create policy**.
 - b. Select **JSON** and copy and paste the contents of the [IAM policy for the Connector](#).
 - c. Finish the remaining steps to create the policy.

Depending on the BlueXP services that you're planning to use, you might need to create a second policy. For standard regions, the permissions are spread across two policies. Two policies are required due to a maximum character size limit for managed policies in AWS. [Learn more about IAM policies for the Connector](#).

3. Create an IAM role:
 - a. Select **Roles > Create role**.
 - b. Select **AWS service > EC2**.
 - c. Add permissions by attaching the policy that you just created.
 - d. Finish the remaining steps to create the role.

Result

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

Step 3: Review instance requirements

When you create the Connector, you need to choose an EC2 instance type that meets the following requirements.

CPU

8 cores or 8 vCPUs

RAM

32 GB

AWS EC2 instance type

An instance type that meets the CPU and RAM requirements above. We recommend t3.2xlarge.

Step 4: Create the Connector

Create the Connector directly from the AWS Marketplace.

About this task

Creating the Connector from the AWS Marketplace deploys an EC2 instance in AWS using a default configuration. [Learn about the default configuration for the Connector.](#)

Before you begin

You should have the following:

- A VPC and subnet that meets networking requirements.
- An IAM role with an attached policy that includes the required permissions for the Connector.
- Permissions to subscribe and unsubscribe from the AWS Marketplace for your IAM user.
- An understanding of CPU and RAM requirements for the instance.
- A key pair for the EC2 instance.

Steps

1. Go to the [BlueXP Connector listing on the AWS Marketplace](#)
2. On the Marketplace page, select **Continue to Subscribe**.

NetApp BlueXP Connector - Manual installation

By: [NetApp, Inc.](#) Latest Version: 3.9.43

Learn how to install the BlueXP Connector from the AWS Marketplace.

Linux/Unix

Continue to Subscribe

Save to List

Typical Total Price
\$0.333/hr

Total pricing per instance for services hosted on t3.2xlarge in US East (N. Virginia). [View Details](#)

Overview Pricing Usage Support Reviews

Product Overview

NetApp BlueXP offers unified control, powerful AIOps capabilities, integrated data services, and flexible resource consumption to support an intelligent data infrastructure across hybrid multicloud environments.

This listing enables you to manually launch the BlueXP Connector instance in AWS. A Connector is NetApp software that enables the management of resources and processes across your on-premises and cloud environments.

Manually launching the Connector from the AWS Marketplace is an alternative to launching the Connector directly from BlueXP.

Highlights

- See Product Overview for instructions on how to deploy NetApp BlueXP.

3. To subscribe to the software, select **Accept Terms**.

The subscription process can take a few minutes.

4. After the subscription process is complete, select **Continue to Configuration**.

NetApp BlueXP Connector - Manual installation

[< Product Detail](#) [Subscribe](#)

Subscribe to this software

You're subscribed to this software. Please see the terms and pricing details below or click the button above to configure your software.

Terms and Conditions

NetApp, Inc. Offer

You have subscribed to this software and agreed that your use of this software is subject to the pricing terms and the seller's [End User License Agreement \(EULA\)](#). You agreed that AWS may share information about this transaction (including your payment terms) with the respective seller, reseller or underlying provider, as applicable, in accordance with the [AWS Privacy Notice](#). AWS will issue invoices and collect payments from you on behalf of the seller through your AWS account. Your use of AWS services remains subject to the [AWS Customer Agreement](#) or other agreement with AWS governing your use of such services.

Product	Effective date	Expiration date	Action
BlueXP Connector - Manual installation	N/A	N/A	Show Details

Continue to Configuration

5. On the **Configure this software** page, ensure that you've selected the correct region and then select

Continue to Launch.

6. On the **Launch this software** page, under **Choose Action**, select **Launch through EC2** and then select **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.

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

- **Name and tags:** Enter a name and tags for the instance.
- **Application and OS Images:** Skip this section. The Connector AMI is already selected.
- **Instance type:** Depending on region availability, choose an instance type that meets RAM and CPU requirements (t3.2xlarge is preselected and recommended).
- **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 security group settings that enable the required connection methods for the Connector instance: SSH, HTTP, and HTTPS.

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

- **Configure storage:** Keep the default size and disk type for the root volume.

If you want to enable Amazon EBS encryption on the root volume, select **Advanced**, expand **Volume 1**, select **Encrypted**, and then choose a KMS key.

- **Advanced details:** Under **IAM instance profile**, choose the IAM role that includes the required permissions for the Connector.
- **Summary:** Review the summary and select **Launch instance**.

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

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

`https://ipaddress`

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

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

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

Result

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

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

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 BlueXP canvas automatically. [Learn how to manage S3 buckets from BlueXP](#)

Manually install the Connector in AWS

You can manually install a Connector on a Linux host running in AWS. To manually install the Connector on your own Linux host, you need to review host requirements, set up your networking, prepare AWS permissions, install the Connector, and then provide the permissions that you prepared.

Before you begin

- You should have an [understanding of Connectors](#).
- You should review [Connector limitations](#).

Step 1: Review host requirements

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



The Connector reserves the UID and GID range of 19000 to 19200. This range is fixed and cannot be modified. If any third-party software on your host is using UIDs or GIDs within this range, the Connector installation will fail. NetApp recommends using a host that is free of third-party software to avoid conflicts.

Dedicated host

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

Host can be of any architecture that meets the following size requirements:

- CPU: 8 cores or 8 vCPUs
- RAM: 32 GB

Hypervisor

A bare metal or hosted hypervisor that is certified to run a supported operating system is required.

Operating system and container requirements

BlueXP supports the Connector with the following operating systems when using BlueXP in standard mode or restricted mode. A container orchestration tool is required before you install the Connector.

Operating system	Supported OS versions	Supported Connector versions	Required container tool	SELinux
Red Hat Enterprise Linux	9.1 to 9.4 8.6 to 8.10 7.9	3.9.40 or later with BlueXP in standard mode or restricted mode	Podman version 4.6.1 or 4.9.4 View Podman configuration requirements.	Supported in enforcing mode or permissive mode ¹
Ubuntu	24.04 LTS	3.9.45 or later with BlueXP in standard mode or restricted mode	Docker Engine 23.06 to 28.0.0.	Not supported
	22.04 LTS	3.9.29 or later	Docker Engine 23.0.6 to 28.0.0.	Not supported

Notes:

1. Management of Cloud Volumes ONTAP systems is not supported by Connectors that have SELinux enabled on the operating system.
2. The Connector is supported on English-language versions of these operating systems.
3. For RHEL, the host must be registered with Red Hat Subscription Management. If it's not registered, the host can't access repositories to update required 3rd-party software during Connector installation.

AWS EC2 instance type

An instance type that meets the CPU and RAM requirements above. We recommend t3.2xlarge.

Key pair

When you create the Connector, you'll need to select an EC2 key pair to use with the instance.

PUT response hop limit when using IMDSv2

If IMDSv2 is enabled on the EC2 instance (this is the default setting for new EC2 instances), you must change the PUT response hop limit on the instance to 3. If you don't change the limit on the EC2 instance, you'll receive a UI initialization error when you try to set up the Connector.

- [Require the use of IMDSv2 on Amazon EC2 instances](#)
- [AWS documentation: Change the PUT response hop limit](#)

Disk space in /opt

100 GiB of space must be available

BlueXP uses /opt to install the /opt/application/netapp directory and its contents.

Disk space in /var

20 GiB of space must be available

BlueXP requires this space in /var because Docker or Podman are architected to create the containers

within this directory. Specifically, they will create containers in the `/var/lib/containers/storage` directory. External mounts or symlinks do not work for this space.

Step 2: Install Podman or Docker Engine

Depending on your operating system, either Podman or Docker Engine is required before you install the Connector.

- Podman is required for Red Hat Enterprise Linux 8 and 9.

[View the Podman versions that BlueXP supports.](#)

- Docker Engine is required for Ubuntu.

[View the Docker Engine versions that BlueXP supports.](#)

Example 1. Steps

Podman

Follow these steps to install Podman and configure it to meet the following requirements:

- Enable and start the podman.socket service
- Install python3
- Install the podman-compose package version 1.0.6
- Add podman-compose to the PATH environment variable



When using Podman, adjust the aardvark-dns service port (default: 53) after installing the Connector to avoid conflicts with the DNS port on the host. Follow the instructions to configure the port.

Steps

1. Remove the podman-docker package if it's installed on the host.

```
dnf remove podman-docker
rm /var/run/docker.sock
```

2. Install Podman.

Podman is available from official Red Hat Enterprise Linux repositories.

For Red Hat Enterprise Linux 9:

```
sudo dnf install podman-2:<version>
```

Where <version> is the supported version of Podman that you're installing. [View the Podman versions that BlueXP supports.](#)

For Red Hat Enterprise Linux 8:

```
sudo dnf install podman-3:<version>
```

Where <version> is the supported version of Podman that you're installing. [View the Podman versions that BlueXP supports.](#)

3. Enable and start the podman.socket service.

```
sudo systemctl enable --now podman.socket
```

4. Install python3.

```
sudo dnf install python3
```

5. Install the EPEL repository package if it's not already available on your system.

This step is required because podman-compose is available from the Extra Packages for Enterprise Linux (EPEL) repository.

For Red Hat Enterprise Linux 9:

```
sudo dnf install https://dl.fedoraproject.org/pub/epel/epel-release-latest-9.noarch.rpm
```

For Red Hat Enterprise Linux 8:

```
sudo dnf install https://dl.fedoraproject.org/pub/epel/epel-release-latest-8.noarch.rpm
```

6. Install podman-compose package 1.0.6.

```
sudo dnf install podman-compose-1.0.6
```



Using the `dnf install` command meets the requirement for adding podman-compose to the PATH environment variable. The installation command adds podman-compose to `/usr/bin`, which is already included in the `secure_path` option on the host.

Docker Engine

Follow the documentation from Docker to install Docker Engine.

Steps

1. [View installation instructions from Docker](#)

Be sure to follow the steps to install a specific version of Docker Engine. Installing the latest version will install a version of Docker that BlueXP doesn't support.

2. Verify that Docker is enabled and running.

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

Step 3: Set up networking

Ensure that the network location where you plan to install the Connector supports the following requirements. Meeting these requirements enables the Connector to manage resources and processes within your hybrid

cloud environment.

Connections to target networks

A Connector requires a network connection to the location where you're planning to create and manage working environments. For example, the network where you plan to create Cloud Volumes ONTAP systems or a storage system in your on-premises environment.

Outbound internet access

The network location where you deploy the Connector must have an outbound internet connection to contact specific endpoints.

Endpoints contacted from computers when using the BlueXP web-based console

Computers that access the BlueXP console from a web browser must have the ability to contact several endpoints. You'll need to use the BlueXP console to set up the Connector and for day-to-day use of BlueXP.

[Prepare networking for the BlueXP console.](#)

Endpoints contacted during manual installation

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

- <https://mysupport.netapp.com>
- <https://signin.b2c.netapp.com> (this endpoint is the CNAME URL for <https://mysupport.netapp.com>)
- <https://cloudmanager.cloud.netapp.com/tenancy>
- <https://stream.cloudmanager.cloud.netapp.com>
- <https://production-artifacts.cloudmanager.cloud.netapp.com>
- To obtain images, the installer needs access to one of these two sets of endpoints:
 - Option 1 (recommended):
 - <https://bluexpinfraprod.eastus2.data.azurecr.io>
 - <https://bluexpinfraprod.azurecr.io>
 - Option 2:
 - https://*.blob.core.windows.net
 - <https://cloudmanagerinfraprod.azurecr.io>

The endpoints listed in option 1 are recommended because they are more secure. We recommend that you set up your firewall to allow the endpoints listed in option 1, while disallowing the endpoints listed in option 2. Note the following about these endpoints:

- The endpoints listed in option 1 are supported starting with the 3.9.47 release of the Connector. There is no backwards compatibility with previous releases of the Connector.
- The Connector contacts the endpoints listed in option 2 first. If those endpoints aren't accessible, the Connector automatically contacts the endpoints listed in option 1.
- The endpoints in option 1 are not supported if you use the Connector with BlueXP backup and recovery or BlueXP ransomware protection. In this case, you can disallow the endpoints listed in option 1, while allowing the endpoints listed in option 2.

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

Endpoints contacted from the Connector

The Connector requires outbound internet access to contact the following endpoints in order to manage resources and processes within your public cloud environment for day-to-day operations.

Note that the endpoints listed below are all CNAME entries.

Endpoints	Purpose
AWS services (amazonaws.com): <ul style="list-style-type: none">• CloudFormation• Elastic Compute Cloud (EC2)• Identity and Access Management (IAM)• Key Management Service (KMS)• Security Token Service (STS)• Simple Storage Service (S3)	To manage resources in AWS. The exact endpoint depends on the AWS region that you're using. Refer to AWS documentation for details
https://support.netapp.com https://mysupport.netapp.com	To obtain licensing information and to send AutoSupport messages to NetApp support.
https://*.api.blueexp.netapp.com https://api.blueexp.netapp.com https://*.cloudmanager.cloud.netapp.com https://cloudmanager.cloud.netapp.com https://netapp-cloud-account.auth0.com	To provide SaaS features and services within BlueXP.
Choose between two sets of endpoints: <ul style="list-style-type: none">• Option 1 (recommended) ¹ https://bluexpinfraprod.eastus2.data.azurecr.io https://bluexpinfraprod.azurecr.io• Option 2 https://*.blob.core.windows.net https://cloudmanagerinfraprod.azurecr.io	To obtain images for Connector upgrades.

¹ The endpoints listed in option 1 are recommended because they are more secure. We recommend that you set up your firewall to allow the endpoints listed in option 1, while disallowing the endpoints listed in option 2. Note the following about these endpoints:

- The endpoints listed in option 1 are supported starting with the 3.9.47 release of the Connector. There is no backwards compatibility with previous releases of the Connector.
- The Connector contacts the endpoints listed in option 2 first. If those endpoints aren't accessible, the Connector automatically contacts the endpoints listed in option 1.
- The endpoints in option 1 are not supported if you use the Connector with BlueXP backup and recovery or BlueXP ransomware protection. In this case, you can disallow the endpoints listed in option 1, while

allowing the endpoints listed in option 2.

Proxy server

NetApp supports both explicit and transparent proxy configurations. If you are using a transparent proxy, you only need to provide the certificate for the proxy server. If you are using an explicit proxy, you'll also need the IP address and credentials.

- IP address
- Credentials
- HTTPS certificate

Ports

There's no incoming traffic to the Connector, unless you initiate it or if the Connector is used as a proxy to send AutoSupport messages from Cloud Volumes ONTAP to NetApp Support.

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

If Cloud Volumes ONTAP systems don't have an outbound internet connection to send AutoSupport messages, BlueXP automatically configures those 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 NTP

If you're planning to use BlueXP classification to scan your corporate data sources, you should enable a Network Time Protocol (NTP) service on both the BlueXP Connector system and the BlueXP classification system so that the time is synchronized between the systems. [Learn more about BlueXP classification](#)

Step 4: Set up permissions

You need to provide AWS permissions to BlueXP by using one of the following options:

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

Follow the steps to prepare permissions for BlueXP.

IAM role

Steps

1. Log in to the AWS console and navigate to the IAM service.
2. Create a policy:
 - a. Select **Policies > Create policy**.
 - b. Select **JSON** and copy and paste the contents of the [IAM policy for the Connector](#).
 - c. Finish the remaining steps to create the policy.

Depending on the BlueXP services that you're planning to use, you might need to create a second policy. For standard regions, the permissions are spread across two policies. Two policies are required due to a maximum character size limit for managed policies in AWS. [Learn more about IAM policies for the Connector](#).

3. Create an IAM role:
 - a. Select **Roles > Create role**.
 - b. Select **AWS service > EC2**.
 - c. Add permissions by attaching the policy that you just created.
 - d. Finish the remaining steps to create the role.

Result

You now have an IAM role that you can associate with the EC2 instance after you install the Connector.

AWS access key

Steps

1. Log in to the AWS console and navigate to the IAM service.
2. Create a policy:
 - a. Select **Policies > Create policy**.
 - b. Select **JSON** and copy and paste the contents of the [IAM policy for the Connector](#).
 - c. Finish the remaining steps to create the policy.

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

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

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

Result

You now have an IAM user that has the required permissions and an access key that you can provide to BlueXP.

Step 5: Install the Connector

After the pre-requisites are complete, you can manually install the software on your own Linux host.

Before you begin

You should have the following:

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

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

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



You cannot set a certificate for a transparent proxy server when manually installing the Connector. If you need to set a certificate for a transparent proxy server, you must use the Maintenance Console after installation. Learn more about the [Connector Maintenance Console](#).

About this task

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

Steps

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

```
unset http_proxy
unset https_proxy
```

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

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

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

3. Assign permissions to run the script.

```
chmod +x BlueXP-Connector-Cloud-<version>
```

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

4. Run the installation script.

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

You'll need to add proxy information if your network requires a proxy for internet access. You can add either a transparent or explicit proxy. The `--proxy` and `--cacert` parameters are optional and you won't be prompted to add them. If you have a proxy server, you will need to enter the parameters as shown.

Here is an example configuring an explicit proxy server with a CA-signed certificate:

```
./BlueXP-Connector-Cloud-v3.9.40--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://user-name:password@address:port`
- `http://domain-name%92user-name:password@address:port`
- `https://address:port`
- `https://user-name:password@address:port`
- `https://domain-name%92user-name:password@address:port`

Note the following:

- The user can be a local user or domain user.
- For a domain user, you must use the ASCII code for a \ as shown above.
- BlueXP doesn't support user names or passwords that include the @ character.
- If the password includes any of the following special characters, you must escape that special character by prepending it with a backslash: & or !

For example:

```
http://bxpproxyuser:netapp1\!@address:3128
```

`--cacert` specifies a CA-signed certificate to use for HTTPS access between the Connector and the proxy server. This parameter is required for HTTPS proxy servers, intercepting proxy servers, and transparent proxy servers.

Here is an example configuring a transparent proxy server. When you configure a transparent proxy, you don't need to define the proxy server. You only add a CA-signed certificate to your Connector host:

```
./BlueXP-Connector-Cloud-v3.9.40 --cacert /tmp/cacert/certificate.cer
```

5. If you used Podman, you'll need to adjust the aardvark-dns port.
 - a. SSH to the BlueXP Connector virtual machine.
 - b. Open `podman /usr/share/containers/containers.conf` file and modify the chosen port for Aardvark DNS service. For example, change it to 54.

```
vi /usr/share/containers/containers.conf
...
# Port to use for dns forwarding daemon with netavark in rootful
bridge
# mode and dns enabled.
# Using an alternate port might be useful if other DNS services
should
# run on the machine.
#
dns_bind_port = 54
...
Esc:wq
```

c. Reboot the Connector virtual machine.

6. Wait for the installation to complete.

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

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

`https://ipaddress`

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

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

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

d. Select **Let's start**.

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 BlueXP canvas automatically. [Learn how to manage S3 buckets from BlueXP](#)

Step 6: Provide permissions to BlueXP

Now that you've installed the Connector, you need to provide BlueXP with the AWS permissions that you previously set up. Providing the permissions enables BlueXP to manage your data and storage infrastructure in AWS.

IAM role

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

Steps

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

Result

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

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

AWS access key

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

Steps

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



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

Result

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

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

Azure

Connector installation options in Azure

There are a few different ways to create a Connector in Azure. Directly from BlueXP is the most common way.

The following installation options are available:

- [Create a Connector directly from BlueXP](#) (this is the standard option)

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

- [Create a Connector from the Azure Marketplace](#)

This action also launches a VM running Linux and the Connector software, but the deployment is initiated directly from the Azure Marketplace, rather than from BlueXP.

- [Download and manually install the software on your own Linux host](#)

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

Create a Connector in Azure from BlueXP

You can install a Connector in Azure directly from BlueXP. To create a Connector in Azure from BlueXP, you need to set up your networking, prepare an Azure role to use to deploy the Connector, and then deploy the Connector.

Before you begin

- You should have an [understanding of Connectors](#).
- You should review [Connector limitations](#).

Step 1: Set up networking

Ensure that the network location where you plan to install the Connector supports the following requirements. Meeting these requirements enables the Connector to manage resources and processes within your hybrid cloud environment.

Azure region

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

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

VNet and subnet

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

Connections to target networks

A Connector requires a network connection to the location where you're planning to create and manage working environments. For example, the network where you plan to create Cloud Volumes ONTAP systems or a storage system in your on-premises environment.

Outbound internet access

The network location where you deploy the Connector must have an outbound internet connection to contact specific endpoints.

Endpoints contacted from the Connector

The Connector requires outbound internet access to contact the following endpoints in order to manage resources and processes within your public cloud environment for day-to-day operations.

Note that the endpoints listed below are all CNAME entries.

Endpoints	Purpose
https://management.azure.com https://login.microsoftonline.com https://blob.core.windows.net https://core.windows.net	To manage resources in Azure public regions.
https://management.chinacloudapi.cn https://login.chinacloudapi.cn https://blob.core.chinacloudapi.cn https://core.chinacloudapi.cn	To manage resources in Azure China regions.
https://support.netapp.com https://mysupport.netapp.com	To obtain licensing information and to send AutoSupport messages to NetApp support.
https://*.api.blueexp.netapp.com https://api.blueexp.netapp.com https://*.cloudmanager.cloud.netapp.com https://cloudmanager.cloud.netapp.com https://netapp-cloud-account.auth0.com	To provide SaaS features and services within BlueXP.
Choose between two sets of endpoints: <ul style="list-style-type: none">Option 1 (recommended) ¹ https://bluexpinfraproduct.eastus2.data.azurecr.io https://bluexpinfraproduct.azurecr.ioOption 2 https://*.blob.core.windows.net https://cloudmanagerinfraproduct.azurecr.io	To obtain images for Connector upgrades.

¹ The endpoints listed in option 1 are recommended because they are more secure. We recommend that you set up your firewall to allow the endpoints listed in option 1, while disallowing the endpoints listed in option 2. Note the following about these endpoints:

- The endpoints listed in option 1 are supported starting with the 3.9.47 release of the Connector. There is no backwards compatibility with previous releases of the Connector.
- The Connector contacts the endpoints listed in option 2 first. If those endpoints aren't accessible, the Connector automatically contacts the endpoints listed in option 1.
- The endpoints in option 1 are not supported if you use the Connector with BlueXP backup and recovery or BlueXP ransomware protection. In this case, you can disallow the endpoints listed in option 1, while allowing the endpoints listed in option 2.

Endpoints contacted from the BlueXP console

As you use the BlueXP web-based console that's provided through the SaaS layer, it contacts several endpoints to complete data management tasks. This includes endpoints that are contacted to deploy the Connector from the BlueXP console.

[View the list of endpoints contacted from the BlueXP console.](#)

Proxy server

NetApp supports both explicit and transparent proxy configurations. If you are using a transparent proxy, you only need to provide the certificate for the proxy server. If you are using an explicit proxy, you'll also need the IP address and credentials.

- IP address
- Credentials
- HTTPS certificate

Ports

There's no incoming traffic to the Connector, unless you initiate it or if the Connector is used as a proxy to send AutoSupport messages from Cloud Volumes ONTAP to NetApp Support.

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

If Cloud Volumes ONTAP systems don't have an outbound internet connection to send AutoSupport messages, BlueXP automatically configures those 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 NTP

If you're planning to use BlueXP classification to scan your corporate data sources, you should enable a Network Time Protocol (NTP) service on both the BlueXP Connector system and the BlueXP classification system so that the time is synchronized between the systems. [Learn more about BlueXP classification](#)

You'll need to implement this networking requirement after you create the Connector.

Step 2: Create a Connector deployment policy (custom role)

You need to create a custom role that has permissions to deploy the Connector in Azure.

Create an Azure custom role that you can assign to your Azure account or to a Microsoft Entra service principal. BlueXP authenticates with Azure and uses these permissions to create the Connector instance on your behalf.

After BlueXP deploys the Connector virtual machine in Azure, it enables a [system-assigned managed identity](#) on the virtual machine, automatically creates the role it needs, and assigns it to the virtual machine. The automatically created role provides BlueXP with the permissions required to manage resources and processes within that Azure subscription. [Review how BlueXP uses the permissions.](#)

Note that you can create an Azure custom role using the Azure portal, Azure PowerShell, Azure CLI, or REST API. The following steps show how to create the role using the Azure CLI. If you would prefer to use a different

method, refer to [Azure documentation](#)

Steps

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



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

```
{
  "Name": "Azure SetupAsService",
  "Actions": [
    "Microsoft.Compute/disks/delete",
    "Microsoft.Compute/disks/read",
    "Microsoft.Compute/disks/write",
    "Microsoft.Compute/locations/operations/read",
    "Microsoft.Compute/operations/read",
    "Microsoft.Compute/virtualMachines/instanceView/read",
    "Microsoft.Compute/virtualMachines/read",
    "Microsoft.Compute/virtualMachines/write",
    "Microsoft.Compute/virtualMachines/delete",
    "Microsoft.Compute/virtualMachines/extensions/write",
    "Microsoft.Compute/virtualMachines/extensions/read",
    "Microsoft.Compute/availabilitySets/read",
    "Microsoft.Network/locations/operationResults/read",
    "Microsoft.Network/locations/operations/read",
    "Microsoft.Network/networkInterfaces/join/action",
    "Microsoft.Network/networkInterfaces/read",
    "Microsoft.Network/networkInterfaces/write",
    "Microsoft.Network/networkInterfaces/delete",
    "Microsoft.Network/networkSecurityGroups/join/action",
    "Microsoft.Network/networkSecurityGroups/read",
    "Microsoft.Network/networkSecurityGroups/write",

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

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

```

        "Microsoft.Network/networkSecurityGroups/securityRules/write",
        "Microsoft.Network/networkSecurityGroups/securityRules/delete",
        "Microsoft.Network/publicIPAddresses/join/action",

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

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

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

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

```

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

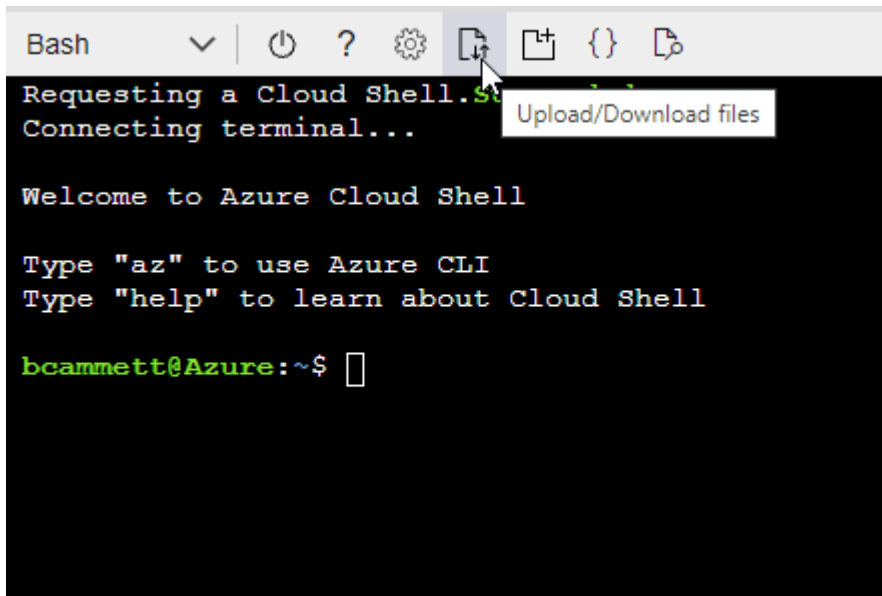
Example

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

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

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

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



- c. Enter the following Azure CLI command:

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

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

Step 3: Set up authentication

When creating the Connector from BlueXP, you need to provide a login that enables BlueXP to authenticate with Azure and deploy the VM. You have two options:

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

Follow the steps to prepare one of these authentication methods for use with BlueXP.

Azure account

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

Steps

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



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

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

Result

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

Service principal

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

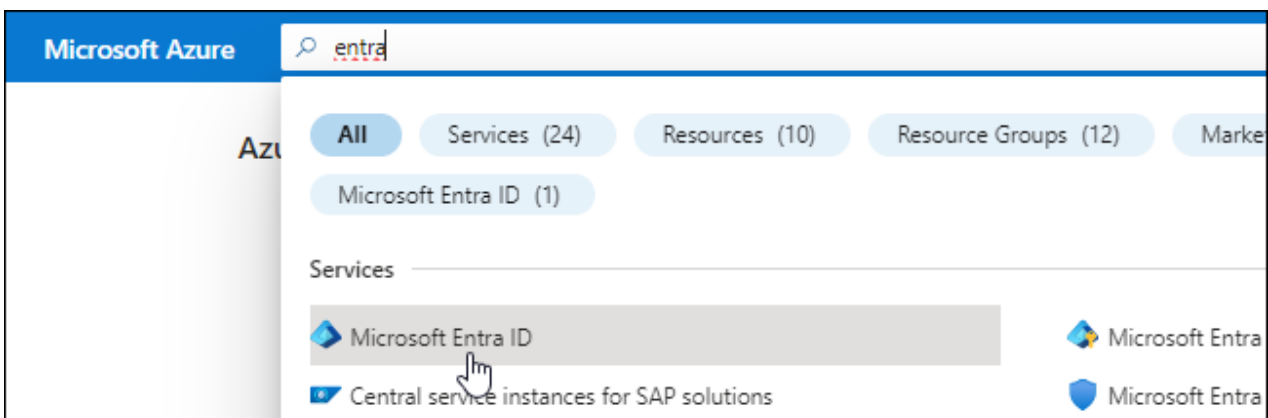
Create and set up a service principal in Microsoft Entra ID and obtain the Azure credentials that BlueXP needs.

Create a Microsoft Entra application for role-based access control

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

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

2. From the Azure portal, open the **Microsoft Entra ID** service.

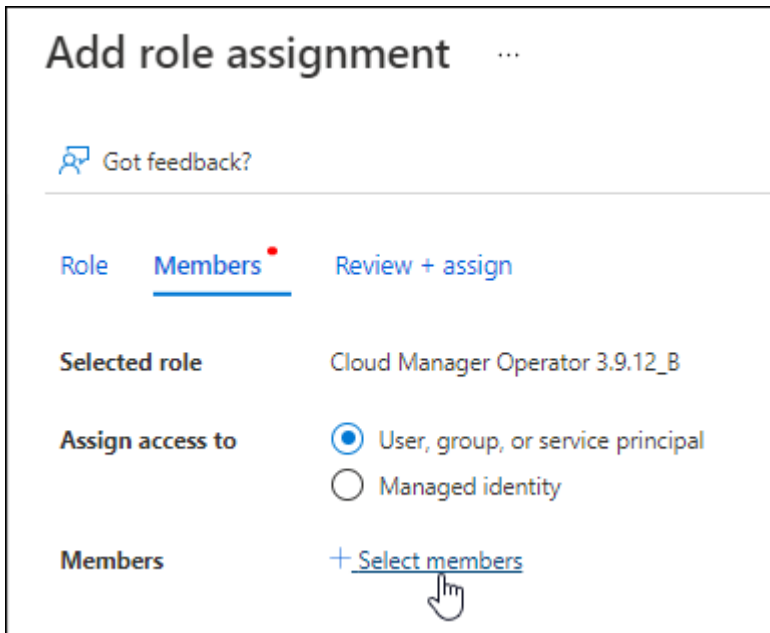


3. In the menu, select **App registrations**.
4. Select **New registration**.
5. Specify details about the application:
 - **Name**: Enter a name for the application.
 - **Account type**: Select an account type (any will work with BlueXP).
 - **Redirect URI**: You can leave this field blank.
6. Select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

You've created the AD application and service principal.

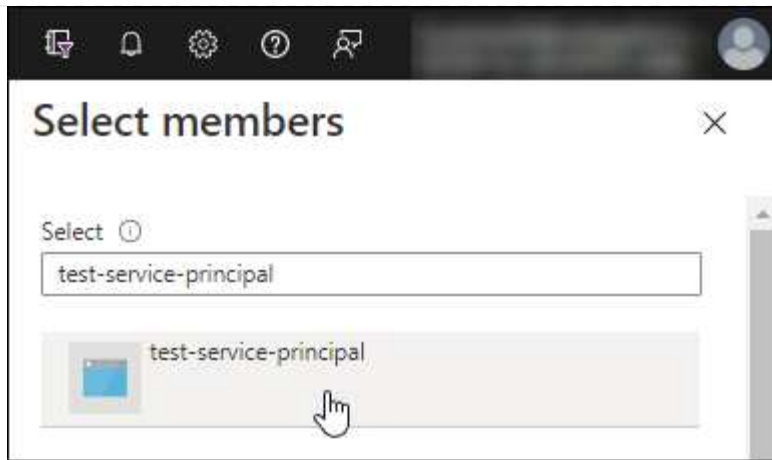
Assign the custom role to the application

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



- c. Search for the name of the application.

Here's an example:



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

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

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

Add Windows Azure Service Management API permissions

1. In the **Microsoft Entra ID** service, select **App registrations** and select the application.
2. Select **API permissions > Add a permission**.
3. Under **Microsoft APIs**, select **Azure Service Management**.

Request API permissions

Select an API

Microsoft APIs APIs my organization uses My APIs

Commonly used Microsoft APIs

Microsoft Graph

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



Azure Batch

Schedule large-scale parallel and HPC applications in the cloud

Azure Data Catalog

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

Azure Data Explorer

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

Azure Data Lake

Access to storage and compute for big data analytic scenarios

Azure DevOps

Integrate with Azure DevOps and Azure DevOps server

Azure Import/Export

Programmatic control of import/export jobs

Azure Key Vault

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

Azure Rights Management Services

Allow validated users to read and write protected content

Azure Service Management

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

Azure Storage

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

Customer Insights

Create profile and interaction models for your products

Data Export Service for Microsoft Dynamics 365

Export data from Microsoft Dynamics CRM organization to an external destination

4. Select **Access Azure Service Management as organization users** and then select **Add permissions**.

Request API permissions

[< All APIs](#)



Azure Service Management

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

What type of permissions does your application require?

Delegated permissions

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

Application permissions

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

Select permissions

[expand all](#)

Type to search

PERMISSION

ADMIN CONSENT REQUIRED

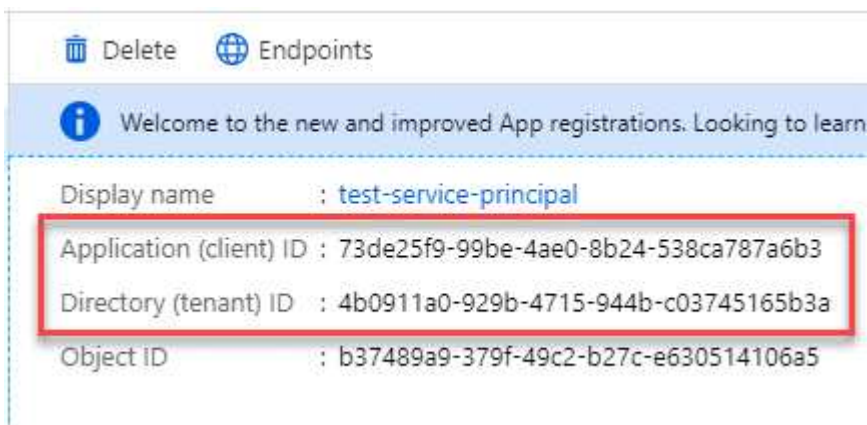


user_impersonation

Access Azure Service Management as organization users (preview) ⓘ

Get the application ID and directory ID for the application

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



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


Create a client secret

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

Client secrets

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

[+ New client secret](#)

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

You now have a client secret that BlueXP can use it to authenticate with Microsoft Entra ID.

Result

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

Step 4: Create the Connector

Create the Connector directly from the BlueXP web-based console.

About this task

- Creating the Connector from BlueXP deploys a virtual machine in Azure using a default configuration. After you create the Connector, you should not change to a smaller VM type that has less CPU or RAM. [Learn about the default configuration for the Connector.](#)
- When BlueXP deploys the Connector, it creates a custom role and assigns it to the Connector VM. This role includes permissions that enables the Connector to manage Azure resources. You need to ensure that the role is kept up to date as new permissions are added in subsequent releases. [Learn more about the custom role for the Connector.](#)

Before you begin

You should have the following:

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

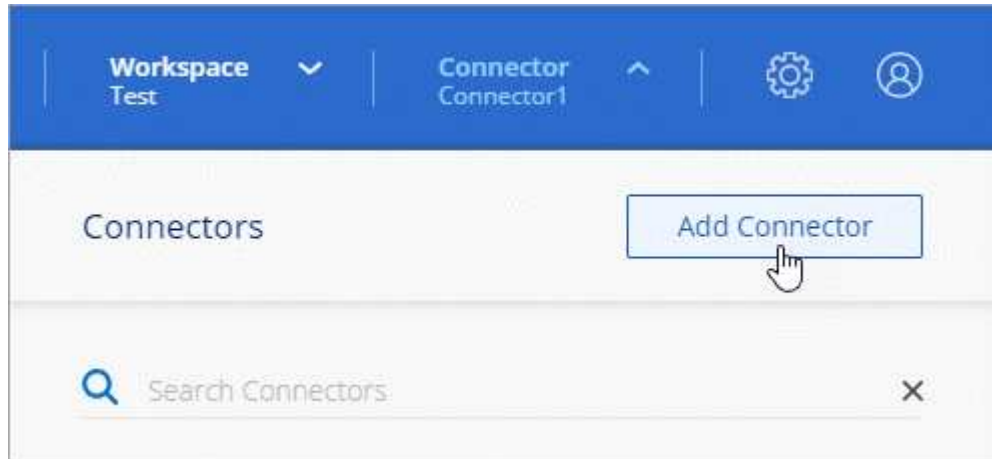
[Learn about connecting to a Linux VM in Azure](#)

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

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

Steps

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



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

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



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

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

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

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

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

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

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

Note that you can choose the Azure subscriptions associated with this role. Each subscription that you choose provides the Connector permissions to manage resources in that subscription (for example, Cloud Volumes ONTAP).

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

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

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

5. Click **Add**.

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

Result

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

If you have Azure Blob storage in the same Azure subscription where you created the Connector, you'll see an Azure Blob storage working environment appear on the BlueXP canvas automatically. [Learn how to manage Azure Blob storage from BlueXP](#)

Create a Connector from the Azure Marketplace

You can create a Connector in Azure directly from the Azure Marketplace. To create a Connector from the Azure Marketplace, you need to set up your networking, prepare Azure permissions, review instance requirements, and then create the Connector.

Before you begin

- You should have an [understanding of Connectors](#).
- Review [Connector limitations](#).

Step 1: Set up networking

Ensure that the network location where you plan to install the Connector supports the following requirements. These requirements enable the Connector to manage resources in your hybrid cloud.

Azure region

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

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

VNet and subnet

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

Connections to target networks

A Connector requires a network connection to the location where you're planning to create and manage working environments. For example, the network where you plan to create Cloud Volumes ONTAP systems or a storage system in your on-premises environment.

Outbound internet access

The network location where you deploy the Connector must have an outbound internet connection to contact specific endpoints.

Endpoints contacted from the Connector

The Connector requires outbound internet access to contact the following endpoints in order to manage resources and processes within your public cloud environment for day-to-day operations.

Note that the endpoints listed below are all CNAME entries.

Endpoints	Purpose
https://management.azure.com https://login.microsoftonline.com https://blob.core.windows.net https://core.windows.net	To manage resources in Azure public regions.
https://management.chinacloudapi.cn https://login.chinacloudapi.cn https://blob.core.chinacloudapi.cn https://core.chinacloudapi.cn	To manage resources in Azure China regions.
https://support.netapp.com https://mysupport.netapp.com	To obtain licensing information and to send AutoSupport messages to NetApp support.
https://*.api.blueexp.netapp.com https://api.blueexp.netapp.com https://*.cloudmanager.cloud.netapp.com https://cloudmanager.cloud.netapp.com https://netapp-cloud-account.auth0.com	To provide SaaS features and services within BlueXP.
Choose between two sets of endpoints: <ul style="list-style-type: none">Option 1 (recommended) ¹ https://bluexpinfraprod.eastus2.data.azurecr.io https://bluexpinfraprod.azurecr.ioOption 2 https://*.blob.core.windows.net https://cloudmanagerinfraprod.azurecr.io	To obtain images for Connector upgrades.

¹ The endpoints listed in option 1 are recommended because they are more secure. We recommend that you set up your firewall to allow the endpoints listed in option 1, while disallowing the endpoints listed in option 2. Note the following about these endpoints:

- The endpoints listed in option 1 are supported starting with the 3.9.47 release of the Connector. There is no backwards compatibility with previous releases of the Connector.
- The Connector contacts the endpoints listed in option 2 first. If those endpoints aren't accessible, the Connector automatically contacts the endpoints listed in option 1.
- The endpoints in option 1 are not supported if you use the Connector with BlueXP backup and recovery or BlueXP ransomware protection. In this case, you can disallow the endpoints listed in option 1, while allowing the endpoints listed in option 2.

Proxy server

NetApp supports both explicit and transparent proxy configurations. If you are using a transparent proxy, you only need to provide the certificate for the proxy server. If you are using an explicit proxy, you'll also need the IP address and credentials.

- IP address
- Credentials
- HTTPS certificate

Ports

There's no incoming traffic to the Connector, unless you initiate it or if the Connector is used as a proxy to send AutoSupport messages from Cloud Volumes ONTAP to NetApp Support.

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

If Cloud Volumes ONTAP systems don't have an outbound internet connection to send AutoSupport messages, BlueXP automatically configures those 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 NTP

If you're planning to use BlueXP classification to scan your corporate data sources, you should enable a Network Time Protocol (NTP) service on both the BlueXP Connector system and the BlueXP classification system so that the time is synchronized between the systems. [Learn more about BlueXP classification](#)

Implement the networking requirements after creating the Connector.

Step 2: Review VM requirements

When you create the Connector, choose a virtual machine type that meets the following requirements.

CPU

8 cores or 8 vCPUs

RAM

32 GB

Azure VM size

An instance type that meets the CPU and RAM requirements above. We recommend Standard_D8s_v3.

Step 3: Set up permissions

You can provide permissions in the following ways:

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

Follow these steps to set up permissions for BlueXP.

Custom role

Note that you can create an Azure custom role using the Azure portal, Azure PowerShell, Azure CLI, or REST API. The following steps show how to create the role using the Azure CLI. If you would prefer to use a different method, refer to [Azure documentation](#)

Steps

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

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

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

You should add the ID for each Azure subscription that you want to use with BlueXP.

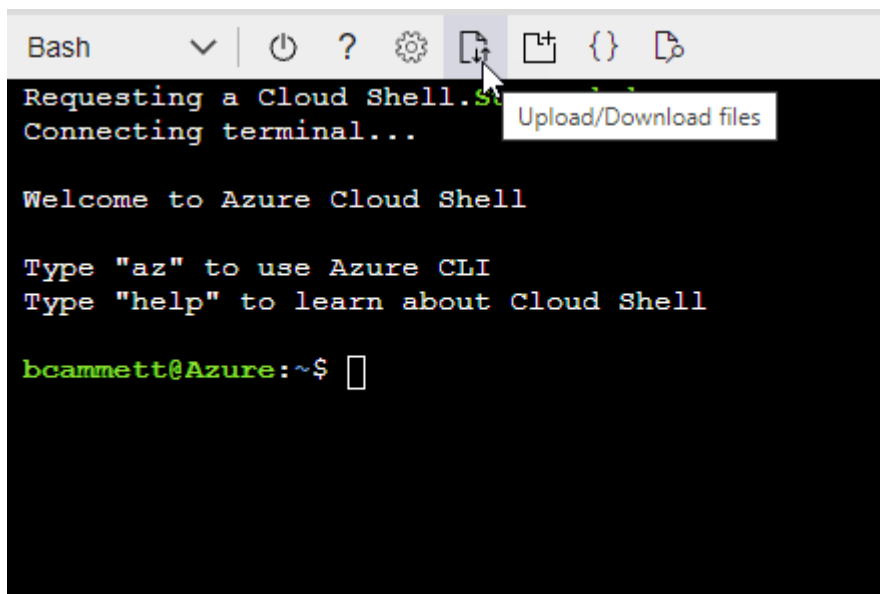
Example

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

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

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

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



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

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

Result

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

Service principal

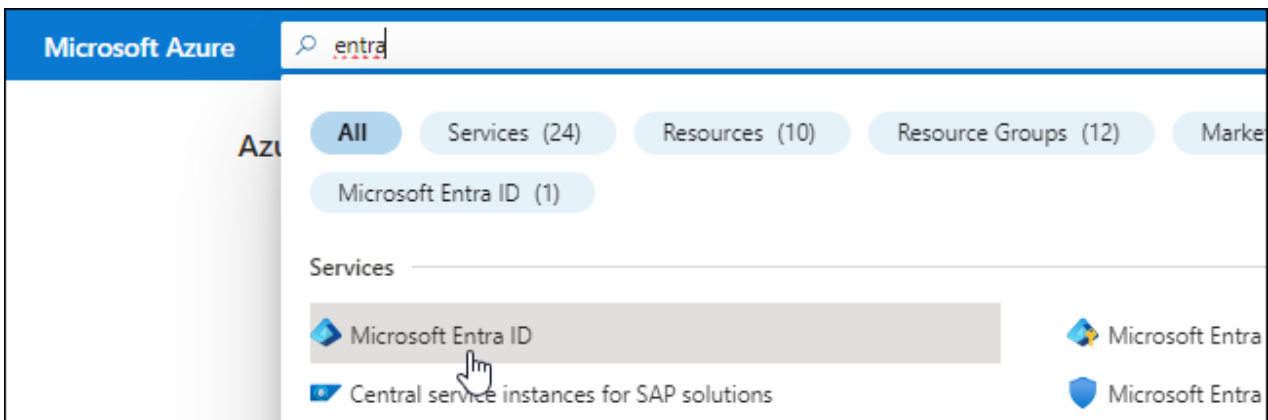
Create and set up a service principal in Microsoft Entra ID and obtain the Azure credentials that BlueXP needs.

Create a Microsoft Entra application for role-based access control

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

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

2. From the Azure portal, open the **Microsoft Entra ID** service.



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

You've created the AD application and service principal.

Assign the application to a role

1. Create a custom role:

Note that you can create an Azure custom role using the Azure portal, Azure PowerShell, Azure CLI, or REST API. The following steps show how to create the role using the Azure CLI. If you would

prefer to use a different method, refer to [Azure documentation](#)

- 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.

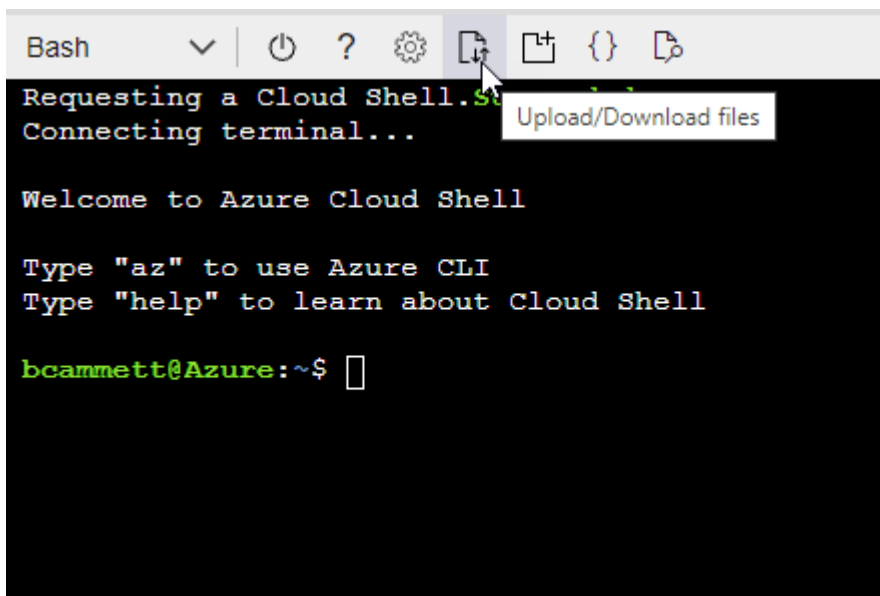
Example

```
"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.



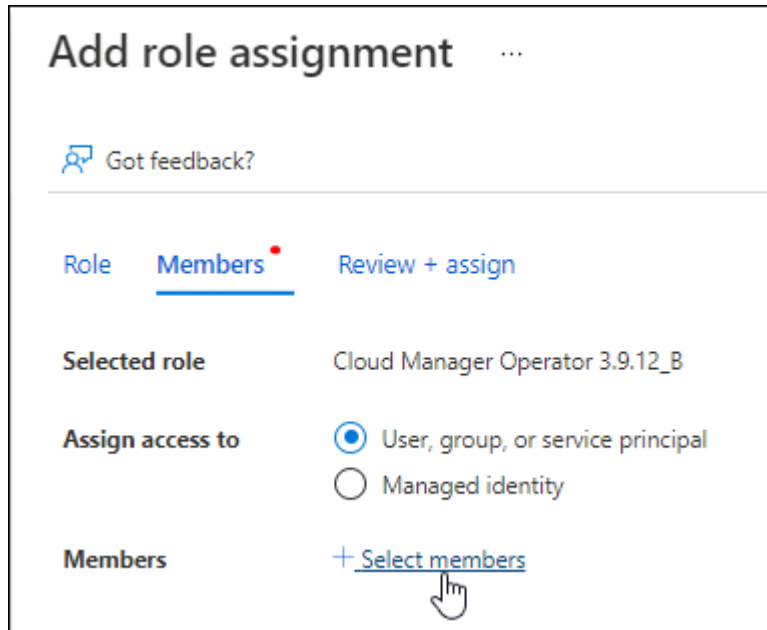
- Use the Azure CLI to create the custom role:

```
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.

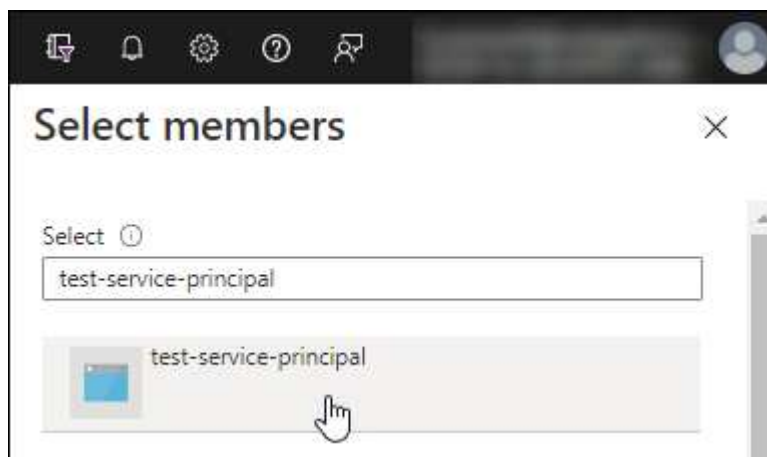
2. Assign the application to the role:

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



- Search for the name of the application.

Here's an example:



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

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

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

Add Windows Azure Service Management API permissions

1. In the **Microsoft Entra ID** service, select **App registrations** and select the application.
2. Select **API permissions > Add a permission**.
3. Under **Microsoft APIs**, select **Azure Service Management**.













Request API permissions

Select an API

Microsoft APIs APIs my organization uses My APIs

Commonly used Microsoft APIs

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

 Azure Batch Schedule large-scale parallel and HPC applications in the cloud	 Azure Data Catalog Programmatic access to Data Catalog resources to register, annotate and search data assets	 Azure Data Explorer Perform ad-hoc queries on terabytes of data to build near real-time and complex analytics solutions
 Azure Data Lake Access to storage and compute for big data analytic scenarios	 Azure DevOps Integrate with Azure DevOps and Azure DevOps server	 Azure Import/Export Programmatic control of import/export jobs
 Azure Key Vault Manage your key vaults as well as the keys, secrets, and certificates within your Key Vaults	 Azure Rights Management Services Allow validated users to read and write protected content	 Azure Service Management Programmatic access to much of the functionality available through the Azure portal
 Azure Storage Secure, massively scalable object and data lake storage for unstructured and semi-structured data	 Customer Insights Create profile and interaction models for your products	 Data Export Service for Microsoft Dynamics 365 Export data from Microsoft Dynamics CRM organization to an external destination

4. Select **Access Azure Service Management as organization users** and then select **Add permissions**.

Request API permissions

[← All APIs](#)



Azure Service Management

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

What type of permissions does your application require?

Delegated permissions

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

Application permissions

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

Select permissions

[expand all](#)

Type to search

PERMISSION

ADMIN CONSENT REQUIRED

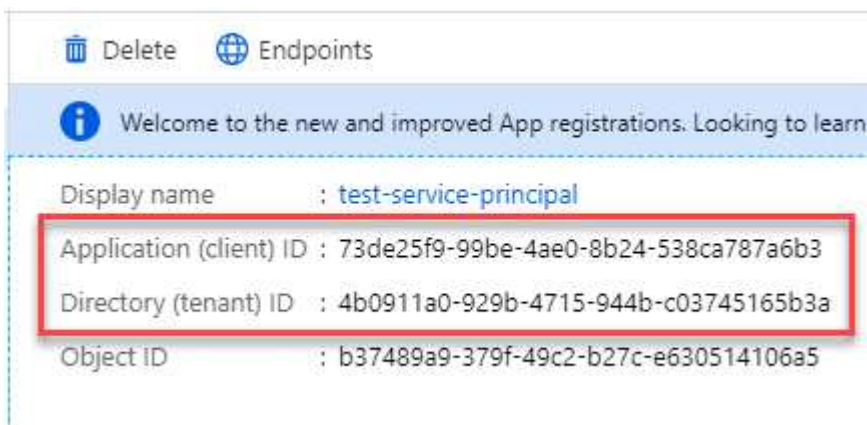


user_impersonation

Access Azure Service Management as organization users (preview) ⓘ

Get the application ID and directory ID for the application

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



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


Create a client secret

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

Client secrets

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

[+ New client secret](#)

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

You now have a client secret that BlueXP can use it to authenticate with Microsoft Entra ID.

Step 4: Create the Connector

Launch the Connector directly from the Azure Marketplace.

About this task

Creating the Connector from the Azure Marketplace sets up a virtual machine with a default configuration.

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

Before you begin

You should have the following:

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

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

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

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

Steps

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

[Azure Marketplace page for commercial regions](#)

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

Note the following as you configure the VM:

- **VM size:** Choose a VM size that meets CPU and RAM requirements. We recommend `Standard_D8s_v3`.
- **Disks:** The Connector can perform optimally with either HDD or SSD disks.
- **Network security group:** The Connector requires inbound connections using SSH, HTTP, and HTTPS.

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

- **Identity:** Under **Management**, select **Enable system assigned managed identity**.

This setting is important because a managed identity allows the Connector virtual machine to identify itself to Microsoft Entra ID without providing any credentials. [Learn more about managed identities for Azure resources.](#)

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

Azure deploys the virtual machine with the specified settings. You should see the virtual machine and Connector software running in about five minutes.

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

`https://ipaddress`

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

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

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

Result

You have now installed the Connector and set it up with your BlueXP organization.

If you have Azure Blob storage in the same Azure subscription where you created the Connector, you'll see an Azure Blob storage working environment appear on the BlueXP canvas automatically. [Learn how to manage Azure Blob storage from BlueXP](#)

Step 5: Provide permissions to BlueXP

Now that you've created the Connector, you need to provide BlueXP with the permissions that you previously set up. Providing the permissions enables BlueXP to manage your data and storage infrastructure in Azure.

Custom role

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

Steps

1. From the Azure Portal, open the **Subscriptions** service and select your subscription.

It's important to assign the role from the **Subscriptions** service because this specifies the scope of the role assignment at the subscription level. The *scope* defines the set of resources that the access applies to. If you specify a scope at a different level (for example, at the virtual machine level), your ability to complete actions from within BlueXP will be affected.

[Microsoft Azure documentation: Understand scope for Azure RBAC](#)

2. Select **Access control (IAM) > Add > Add role assignment**.
3. In the **Role** tab, select the **BlueXP Operator** role and select **Next**.



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

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

Result

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

What's next?

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

Service principal

Steps

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



2. Select **Add Credentials** and follow the steps in the wizard.
 - a. **Credentials Location**: Select **Microsoft Azure > Connector**.

- b. **Define Credentials:** Enter information about the Microsoft Entra service principal that grants the required permissions:
 - Application (client) ID
 - Directory (tenant) ID
 - Client Secret
- c. **Marketplace Subscription:** Associate a Marketplace subscription with these credentials by subscribing now or by selecting an existing subscription.
- d. **Review:** Confirm the details about the new credentials and select **Add**.

Result

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

Manually install the Connector in Azure

A Connector is NetApp software running in your cloud network or on-premises network that gives you the ability to use all BlueXP features and services. One of the available installation options is to manually install the Connector software on a Linux host running in Azure. To manually install the Connector on your own Linux host, you need to review host requirements, set up your networking, prepare Azure permissions, install the Connector, and then provide the permissions that you prepared.

Before you begin

- You should have an [understanding of Connectors](#).
- You should review [Connector limitations](#).

Step 1: Review host requirements

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



The Connector reserves the UID and GID range of 19000 to 19200. This range is fixed and cannot be modified. If any third-party software on your host is using UIDs or GIDs within this range, the Connector installation will fail. NetApp recommends using a host that is free of third-party software to avoid conflicts.

Dedicated host

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

Host can be of any architecture that meets the following size requirements:

- CPU: 8 cores or 8 vCPUs
- RAM: 32 GB

Hypervisor

A bare metal or hosted hypervisor that is certified to run a supported operating system is required.

Operating system and container requirements

BlueXP supports the Connector with the following operating systems when using BlueXP in standard mode or restricted mode. A container orchestration tool is required before you install the Connector.

Operating system	Supported OS versions	Supported Connector versions	Required container tool	SELinux
Red Hat Enterprise Linux	9.1 to 9.4 8.6 to 8.10 7.9	3.9.40 or later with BlueXP in standard mode or restricted mode	Podman version 4.6.1 or 4.9.4 View Podman configuration requirements.	Supported in enforcing mode or permissive mode ¹
Ubuntu	24.04 LTS	3.9.45 or later with BlueXP in standard mode or restricted mode	Docker Engine 23.06 to 28.0.0.	Not supported
	22.04 LTS	3.9.29 or later	Docker Engine 23.0.6 to 28.0.0.	Not supported

Notes:

1. Management of Cloud Volumes ONTAP systems is not supported by Connectors that have SELinux enabled on the operating system.
2. The Connector is supported on English-language versions of these operating systems.
3. For RHEL, the host must be registered with Red Hat Subscription Management. If it's not registered, the host can't access repositories to update required 3rd-party software during Connector installation.

Azure VM size

An instance type that meets the CPU and RAM requirements above. We recommend Standard_D8s_v3.

Disk space in /opt

100 GiB of space must be available

BlueXP uses /opt to install the /opt/application/netapp directory and its contents.

Disk space in /var

20 GiB of space must be available

BlueXP requires this space in /var because Docker or Podman are architected to create the containers within this directory. Specifically, they will create containers in the /var/lib/containers/storage directory. External mounts or symlinks do not work for this space.

Step 2: Install Podman or Docker Engine

Depending on your operating system, either Podman or Docker Engine is required before you install the Connector.

- Podman is required for Red Hat Enterprise Linux 8 and 9.

[View the Podman versions that BlueXP supports.](#)

- Docker Engine is required for Ubuntu.

[View the Docker Engine versions that BlueXP supports.](#)

Example 2. Steps

Podman

Follow these steps to install Podman and configure it to meet the following requirements:

- Enable and start the podman.socket service
- Install python3
- Install the podman-compose package version 1.0.6
- Add podman-compose to the PATH environment variable



When using Podman, adjust the aardvark-dns service port (default: 53) after installing the Connector to avoid conflicts with the DNS port on the host. Follow the instructions to configure the port.

Steps

1. Remove the podman-docker package if it's installed on the host.

```
dnf remove podman-docker
rm /var/run/docker.sock
```

2. Install Podman.

Podman is available from official Red Hat Enterprise Linux repositories.

For Red Hat Enterprise Linux 9:

```
sudo dnf install podman-2:<version>
```

Where <version> is the supported version of Podman that you're installing. [View the Podman versions that BlueXP supports.](#)

For Red Hat Enterprise Linux 8:

```
sudo dnf install podman-3:<version>
```

Where <version> is the supported version of Podman that you're installing. [View the Podman versions that BlueXP supports.](#)

3. Enable and start the podman.socket service.

```
sudo systemctl enable --now podman.socket
```

4. Install python3.

```
sudo dnf install python3
```

5. Install the EPEL repository package if it's not already available on your system.

This step is required because podman-compose is available from the Extra Packages for Enterprise Linux (EPEL) repository.

For Red Hat Enterprise Linux 9:

```
sudo dnf install https://dl.fedoraproject.org/pub/epel/epel-release-latest-9.noarch.rpm
```

For Red Hat Enterprise Linux 8:

```
sudo dnf install https://dl.fedoraproject.org/pub/epel/epel-release-latest-8.noarch.rpm
```

6. Install podman-compose package 1.0.6.

```
sudo dnf install podman-compose-1.0.6
```



Using the `dnf install` command meets the requirement for adding podman-compose to the PATH environment variable. The installation command adds podman-compose to `/usr/bin`, which is already included in the `secure_path` option on the host.

Docker Engine

Follow the documentation from Docker to install Docker Engine.

Steps

1. [View installation instructions from Docker](#)

Be sure to follow the steps to install a specific version of Docker Engine. Installing the latest version will install a version of Docker that BlueXP doesn't support.

2. Verify that Docker is enabled and running.

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

Step 3: Set up networking

Ensure that the network location where you plan to install the Connector supports the following requirements. Meeting these requirements enables the Connector to manage resources and processes within your hybrid

cloud environment.

Azure region

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

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

Connections to target networks

A Connector requires a network connection to the location where you're planning to create and manage working environments. For example, the network where you plan to create Cloud Volumes ONTAP systems or a storage system in your on-premises environment.

Outbound internet access

The network location where you deploy the Connector must have an outbound internet connection to contact specific endpoints.

Endpoints contacted from computers when using the BlueXP web-based console

Computers that access the BlueXP console from a web browser must have the ability to contact several endpoints. You'll need to use the BlueXP console to set up the Connector and for day-to-day use of BlueXP.

[Prepare networking for the BlueXP console.](#)

Endpoints contacted during manual installation

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

- <https://mysupport.netapp.com>
- <https://signin.b2c.netapp.com> (this endpoint is the CNAME URL for <https://mysupport.netapp.com>)
- <https://cloudmanager.cloud.netapp.com/tenancy>
- <https://stream.cloudmanager.cloud.netapp.com>
- <https://production-artifacts.cloudmanager.cloud.netapp.com>
- To obtain images, the installer needs access to one of these two sets of endpoints:
 - Option 1 (recommended):
 - <https://bluexpinfraprod.eastus2.data.azurecr.io>
 - <https://bluexpinfraprod.azurecr.io>
 - Option 2:
 - https://*.blob.core.windows.net
 - <https://cloudmanagerinfraprod.azurecr.io>

The endpoints listed in option 1 are recommended because they are more secure. We recommend that you set up your firewall to allow the endpoints listed in option 1, while disallowing the endpoints listed in option 2. Note the following about these endpoints:

- The endpoints listed in option 1 are supported starting with the 3.9.47 release of the Connector. There is no backwards compatibility with previous releases of the Connector.

- The Connector contacts the endpoints listed in option 2 first. If those endpoints aren't accessible, the Connector automatically contacts the endpoints listed in option 1.
- The endpoints in option 1 are not supported if you use the Connector with BlueXP backup and recovery or BlueXP ransomware protection. In this case, you can disallow the endpoints listed in option 1, while allowing the endpoints listed in option 2.

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

Endpoints contacted from the Connector

The Connector requires outbound internet access to contact the following endpoints in order to manage resources and processes within your public cloud environment for day-to-day operations.

Note that the endpoints listed below are all CNAME entries.

Endpoints	Purpose
https://management.azure.com https://login.microsoftonline.com https://blob.core.windows.net https://core.windows.net	To manage resources in Azure public regions.
https://management.chinacloudapi.cn https://login.chinacloudapi.cn https://blob.core.chinacloudapi.cn https://core.chinacloudapi.cn	To manage resources in Azure China regions.
https://support.netapp.com https://mysupport.netapp.com	To obtain licensing information and to send AutoSupport messages to NetApp support.
https://*.api.bluexp.netapp.com https://api.bluexp.netapp.com https://*.cloudmanager.cloud.netapp.com https://cloudmanager.cloud.netapp.com https://netapp-cloud-account.auth0.com	To provide SaaS features and services within BlueXP.
<p>Choose between two sets of endpoints:</p> <ul style="list-style-type: none"> • Option 1 (recommended) ¹ https://bluexpinfraprod.eastus2.data.azurecr.io https://bluexpinfraprod.azurecr.io • Option 2 https://*.blob.core.windows.net https://cloudmanagerinfraprod.azurecr.io 	To obtain images for Connector upgrades.

¹ The endpoints listed in option 1 are recommended because they are more secure. We recommend that you set up your firewall to allow the endpoints listed in option 1, while disallowing the endpoints listed in option 2. Note the following about these endpoints:

- The endpoints listed in option 1 are supported starting with the 3.9.47 release of the Connector. There is no backwards compatibility with previous releases of the Connector.
- The Connector contacts the endpoints listed in option 2 first. If those endpoints aren't accessible, the Connector automatically contacts the endpoints listed in option 1.
- The endpoints in option 1 are not supported if you use the Connector with BlueXP backup and recovery or BlueXP ransomware protection. In this case, you can disallow the endpoints listed in option 1, while allowing the endpoints listed in option 2.

Proxy server

NetApp supports both explicit and transparent proxy configurations. If you are using a transparent proxy, you only need to provide the certificate for the proxy server. If you are using an explicit proxy, you'll also need the IP address and credentials.

- IP address
- Credentials
- HTTPS certificate

Ports

There's no incoming traffic to the Connector, unless you initiate it or if the Connector is used as a proxy to send AutoSupport messages from Cloud Volumes ONTAP to NetApp Support.

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

If Cloud Volumes ONTAP systems don't have an outbound internet connection to send AutoSupport messages, BlueXP automatically configures those 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 NTP

If you're planning to use BlueXP classification to scan your corporate data sources, you should enable a Network Time Protocol (NTP) service on both the BlueXP Connector system and the BlueXP classification system so that the time is synchronized between the systems. [Learn more about BlueXP classification](#)

Step 4: Set up Connector deployment permissions

You need to provide Azure permissions to BlueXP by using one of the following options:

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

Follow the steps to prepare permissions for BlueXP.

Create a custom role for Connector deployment

Note that you can create an Azure custom role using the Azure portal, Azure PowerShell, Azure CLI, or REST API. The following steps show how to create the role using the Azure CLI. If you would prefer to use a different method, refer to [Azure documentation](#)

Steps

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

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

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

You should add the ID for each Azure subscription that you want to use with BlueXP.

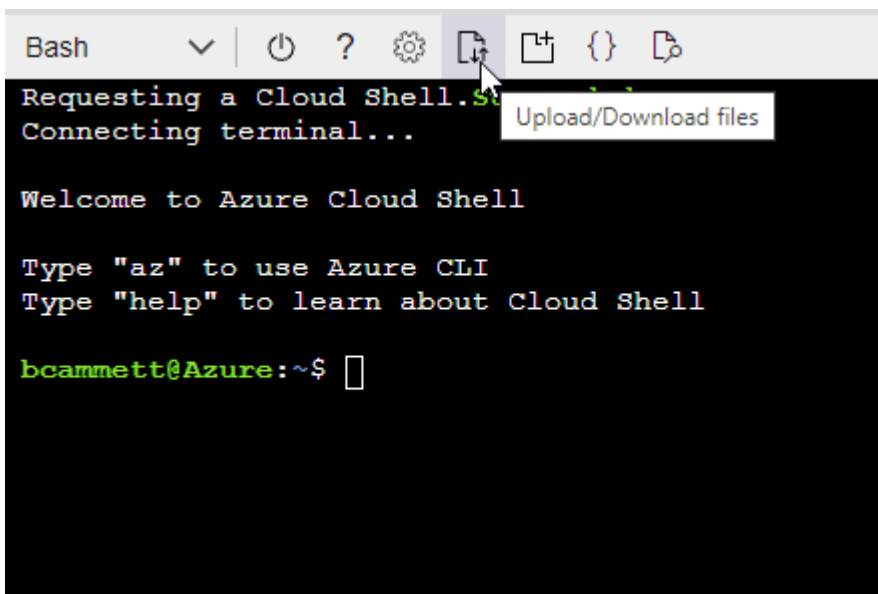
Example

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

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

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

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



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

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

Result

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

Service principal

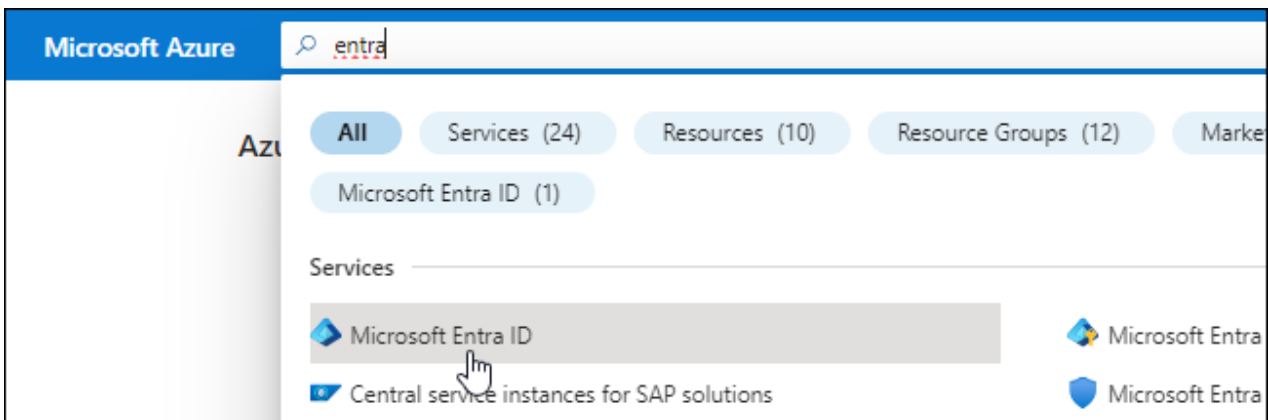
Create and set up a service principal in Microsoft Entra ID and obtain the Azure credentials that BlueXP needs.

Create a Microsoft Entra application for role-based access control

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

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

2. From the Azure portal, open the **Microsoft Entra ID** service.



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

You've created the AD application and service principal.

Assign the application to a role

1. Create a custom role:

Note that you can create an Azure custom role using the Azure portal, Azure PowerShell, Azure CLI, or REST API. The following steps show how to create the role using the Azure CLI. If you would

prefer to use a different method, refer to [Azure documentation](#)

- 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.

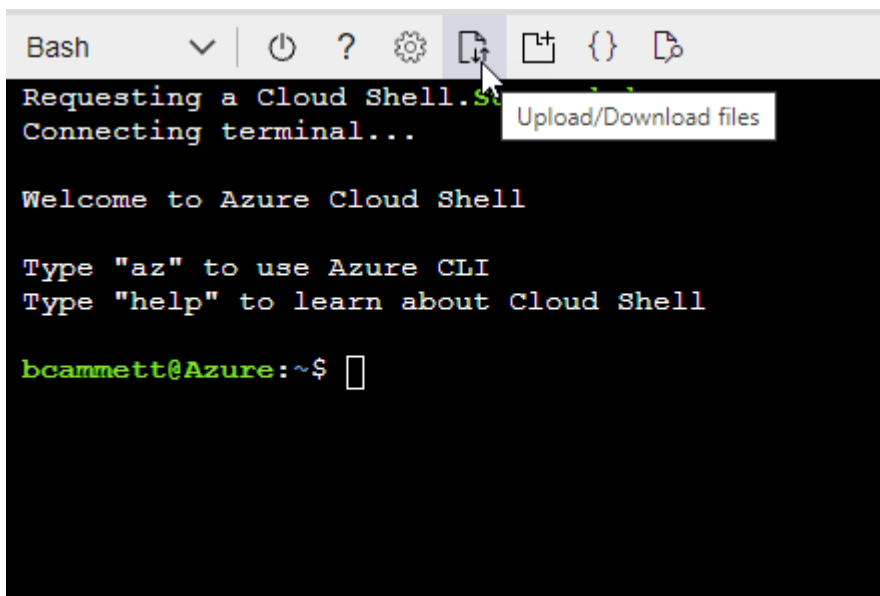
Example

```
"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.



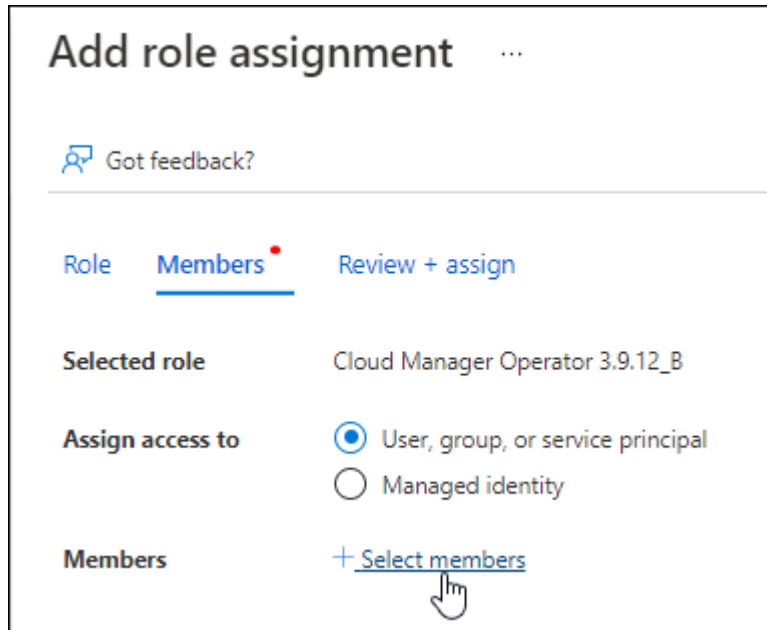
- Use the Azure CLI to create the custom role:

```
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.

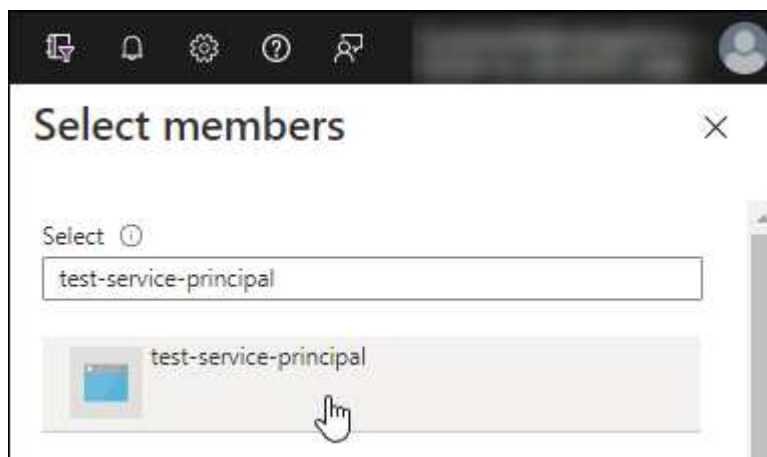
2. Assign the application to the role:

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



- Search for the name of the application.

Here's an example:



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

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

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

Add Windows Azure Service Management API permissions

1. In the **Microsoft Entra ID** service, select **App registrations** and select the application.
2. Select **API permissions > Add a permission**.
3. Under **Microsoft APIs**, select **Azure Service Management**.













Request API permissions

Select an API

Microsoft APIs APIs my organization uses My APIs

Commonly used Microsoft APIs

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

 Azure Batch Schedule large-scale parallel and HPC applications in the cloud	 Azure Data Catalog Programmatic access to Data Catalog resources to register, annotate and search data assets	 Azure Data Explorer Perform ad-hoc queries on terabytes of data to build near real-time and complex analytics solutions
 Azure Data Lake Access to storage and compute for big data analytic scenarios	 Azure DevOps Integrate with Azure DevOps and Azure DevOps server	 Azure Import/Export Programmatic control of import/export jobs
 Azure Key Vault Manage your key vaults as well as the keys, secrets, and certificates within your Key Vaults	 Azure Rights Management Services Allow validated users to read and write protected content	 Azure Service Management Programmatic access to much of the functionality available through the Azure portal
 Azure Storage Secure, massively scalable object and data lake storage for unstructured and semi-structured data	 Customer Insights Create profile and interaction models for your products	 Data Export Service for Microsoft Dynamics 365 Export data from Microsoft Dynamics CRM organization to an external destination

4. Select **Access Azure Service Management as organization users** and then select **Add permissions**.

Request API permissions

[< All APIs](#)



Azure Service Management

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

What type of permissions does your application require?

Delegated permissions

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

Application permissions

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

Select permissions

[expand all](#)

Type to search

PERMISSION

ADMIN CONSENT REQUIRED

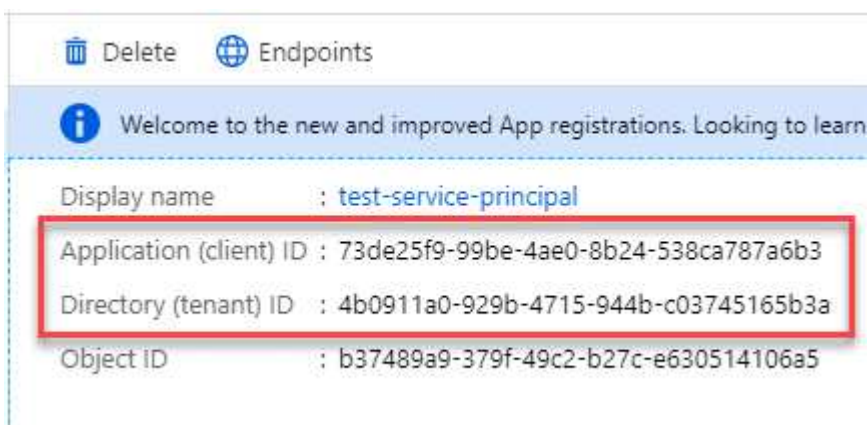


user_impersonation

Access Azure Service Management as organization users (preview) ⓘ

Get the application ID and directory ID for the application

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



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

Create a client secret

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

Client secrets

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

[+ New client secret](#)

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

You now have a client secret that BlueXP can use it to authenticate with Microsoft Entra ID.

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.

Step 5: Install the Connector

After the pre-requisites are complete, you can manually install the software on your own Linux host.

Before you begin

You should have the following:

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

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

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



You cannot set a certificate for a transparent proxy server when manually installing the Connector. If you need to set a certificate for a transparent proxy server, you must use the Maintenance Console after installation. Learn more about the [Connector Maintenance Console](#).

- A managed identity enabled on the VM in Azure so that you can provide the required Azure permissions through a custom role.

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

About this task

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

```
unset http_proxy
unset https_proxy
```

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

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

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

3. Assign permissions to run the script.

```
chmod +x BlueXP-Connector-Cloud-<version>
```

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

4. Run the installation script.

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

You'll need to add proxy information if your network requires a proxy for internet access. You can add either a transparent or explicit proxy. The `--proxy` and `--cacert` parameters are optional and you won't be prompted to add them. If you have a proxy server, you will need to enter the parameters as shown.

Here is an example configuring an explicit proxy server with a CA-signed certificate:

```
./BlueXP-Connector-Cloud-v3.9.40--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://user-name:password@address:port`
- `http://domain-name%92user-name:password@address:port`
- `https://address:port`
- `https://user-name:password@address:port`
- `https://domain-name%92user-name:password@address:port`

Note the following:

- The user can be a local user or domain user.

- For a domain user, you must use the ASCII code for a \ as shown above.
- BlueXP doesn't support user names or passwords that include the @ character.
- If the password includes any of the following special characters, you must escape that special character by prepending it with a backslash: & or !

For example:

`http://bxpproxyuser:netapp1\!@address:3128`

--cacert specifies a CA-signed certificate to use for HTTPS access between the Connector and the proxy server. This parameter is required for HTTPS proxy servers, intercepting proxy servers, and transparent proxy servers.

Here is an example configuring a transparent proxy server. When you configure a transparent proxy, you don't need to define the proxy server. You only add a CA-signed certificate to your Connector host:

```
./BlueXP-Connector-Cloud-v3.9.40 --cacert /tmp/cacert/certificate.cer
```

5. If you used Podman, you'll need to adjust the aardvark-dns port.
 - a. SSH to the BlueXP Connector virtual machine.
 - b. Open `podman /usr/share/containers/containers.conf` file and modify the chosen port for Aardvark DNS service. For example, change it to 54.

```
vi /usr/share/containers/containers.conf
...
# Port to use for dns forwarding daemon with netavark in rootful
bridge
# mode and dns enabled.
# Using an alternate port might be useful if other DNS services
should
# run on the machine.
#
dns_bind_port = 54
...
Esc:wq
```

- c. Reboot the Connector virtual machine.
6. Wait for the installation to complete.

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

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

`https://ipaddress`

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

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

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

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

If you have Azure Blob storage in the same Azure subscription where you created the Connector, you'll see an Azure Blob storage working environment appear on the BlueXP canvas automatically. [Learn how to manage Azure Blob storage from BlueXP](#)

Step 6: Provide permissions to BlueXP

Now that you've installed the Connector, you need to provide BlueXP with the Azure permissions that you previously set up. Providing the permissions enables BlueXP to manage your data and storage infrastructure in Azure.

Custom role

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

Steps

1. From the Azure Portal, open the **Subscriptions** service and select your subscription.

It's important to assign the role from the **Subscriptions** service because this specifies the scope of the role assignment at the subscription level. The *scope* defines the set of resources that the access applies to. If you specify a scope at a different level (for example, at the virtual machine level), your ability to complete actions from within BlueXP will be affected.

[Microsoft Azure documentation: Understand scope for Azure RBAC](#)

2. Select **Access control (IAM) > Add > Add role assignment**.
3. In the **Role** tab, select the **BlueXP Operator** role and select **Next**.



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

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

Result

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

What's next?

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

Service principal

Steps

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



2. Select **Add Credentials** and follow the steps in the wizard.
 - a. **Credentials Location**: Select **Microsoft Azure > Connector**.

- b. **Define Credentials:** Enter information about the Microsoft Entra service principal that grants the required permissions:
 - Application (client) ID
 - Directory (tenant) ID
 - Client Secret
- c. **Marketplace Subscription:** Associate a Marketplace subscription with these credentials by subscribing now or by selecting an existing subscription.
- d. **Review:** Confirm the details about the new credentials and select **Add**.

Result

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

Google Cloud

Connector installation options in Google Cloud

There are a few different ways to create a Connector in Google Cloud. Directly from BlueXP is the most common way.

The following installation options are available:

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

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

- [Create the Connector using gcloud](#)

This action also launches a VM instance running Linux and the Connector software, but the deployment is initiated directly from Google Cloud, rather than from BlueXP.

- [Download and manually install the software on your own Linux host](#)

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

Create a Connector in Google Cloud from BlueXP or gcloud

You can create a Connector in Google Cloud from BlueXP or by using Google Cloud. You need to set up your networking, prepare Google Cloud permissions, enable Google Cloud APIs, and then create the Connector.

Before you begin

- You should have an [understanding of Connectors](#).
- You should review [Connector limitations](#).

Step 1: Set up networking

Set up networking to ensure the Connector can manage resources, with connections to target networks and outbound internet access.

VPC and subnet

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

Connections to target networks

A Connector requires a network connection to the location where you're planning to create and manage working environments. For example, the network where you plan to create Cloud Volumes ONTAP systems or a storage system in your on-premises environment.

Outbound internet access

The network location where you deploy the Connector must have an outbound internet connection to contact specific endpoints.

Endpoints contacted from the Connector

The Connector requires outbound internet access to contact the following endpoints in order to manage resources and processes within your public cloud environment for day-to-day operations.

Note that the endpoints listed below are all CNAME entries.

Endpoints	Purpose
https://www.googleapis.com/compute/v1/ https://compute.googleapis.com/compute/v1 https://cloudresourcemanager.googleapis.com/v1/projects https://www.googleapis.com/compute/beta https://storage.googleapis.com/storage/v1 https://www.googleapis.com/storage/v1 https://iam.googleapis.com/v1 https://cloudkms.googleapis.com/v1 https://www.googleapis.com/deploymentmanager/v2/projects	To manage resources in Google Cloud.
https://support.netapp.com https://mysupport.netapp.com	To obtain licensing information and to send AutoSupport messages to NetApp support.
https://*.api.bluexp.netapp.com https://api.bluexp.netapp.com https://*.cloudmanager.cloud.netapp.com https://cloudmanager.cloud.netapp.com https://netapp-cloud-account.auth0.com	To provide SaaS features and services within BlueXP.

Endpoints	Purpose
<p>Choose between two sets of endpoints:</p> <ul style="list-style-type: none"> Option 1 (recommended) ¹ <p>https://bluexpinfraprod.eastus2.data.azurecr.io https://bluexpinfraprod.azurecr.io</p> <ul style="list-style-type: none"> Option 2 <p>https://*.blob.core.windows.net https://cloudmanagerinfraprod.azurecr.io</p>	To obtain images for Connector upgrades.

¹ The endpoints listed in option 1 are recommended because they are more secure. We recommend that you set up your firewall to allow the endpoints listed in option 1, while disallowing the endpoints listed in option 2. Note the following about these endpoints:

- The endpoints listed in option 1 are supported starting with the 3.9.47 release of the Connector. There is no backwards compatibility with previous releases of the Connector.
- The Connector contacts the endpoints listed in option 2 first. If those endpoints aren't accessible, the Connector automatically contacts the endpoints listed in option 1.
- The endpoints in option 1 are not supported if you use the Connector with BlueXP backup and recovery or BlueXP ransomware protection. In this case, you can disallow the endpoints listed in option 1, while allowing the endpoints listed in option 2.

Endpoints contacted from the BlueXP console

As you use the BlueXP web-based console that's provided through the SaaS layer, it contacts several endpoints to complete data management tasks. This includes endpoints that are contacted to deploy the Connector from the BlueXP console.

[View the list of endpoints contacted from the BlueXP console.](#)

Proxy server

NetApp supports both explicit and transparent proxy configurations. If you are using a transparent proxy, you only need to provide the certificate for the proxy server. If you are using an explicit proxy, you'll also need the IP address and credentials.

- IP address
- Credentials
- HTTPS certificate

Ports

There's no incoming traffic to the Connector, unless you initiate it or if the Connector is used as a proxy to send AutoSupport messages from Cloud Volumes ONTAP to NetApp Support.

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

If Cloud Volumes ONTAP systems don't have an outbound internet connection to send AutoSupport messages, BlueXP automatically configures those 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 NTP

If you're planning to use BlueXP classification to scan your corporate data sources, you should enable a Network Time Protocol (NTP) service on both the BlueXP Connector system and the BlueXP classification system so that the time is synchronized between the systems. [Learn more about BlueXP classification](#)

Implement this networking requirement after creating the Connector.

Step 2: Set up permissions to create the Connector

Before you can deploy a Connector from BlueXP or by using gcloud, you need to set up permissions for the Google Cloud user who will deploy the Connector VM.

Steps

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

```
title: Connector deployment policy
description: Permissions for the user who deploys the Connector from
BlueXP
stage: GA
includedPermissions:
- compute.disks.create
- compute.disks.get
- compute.disks.list
- compute.disks.setLabels
- compute.disks.use
- compute.firewalls.create
- compute.firewalls.delete
- compute.firewalls.get
- compute.firewalls.list
- compute.globalOperations.get
- compute.images.get
- compute.images.getFromFamily
- compute.images.list
- compute.images.useReadOnly
- compute.instances.attachDisk
- compute.instances.create
- compute.instances.get
- compute.instances.list
- compute.instances.setDeletionProtection
- compute.instances.setLabels
- compute.instances.setMachineType
- compute.instances.setMetadata
```

```

- compute.instances.setTags
- compute.instances.start
- compute.instances.updateDisplayDevice
- compute.machineTypes.get
- compute.networks.get
- compute.networks.list
- compute.networks.updatePolicy
- compute.projects.get
- compute.regions.get
- compute.regions.list
- compute.subnetworks.get
- compute.subnetworks.list
- compute.zoneOperations.get
- compute.zones.get
- compute.zones.list
- deploymentmanager.compositeTypes.get
- deploymentmanager.compositeTypes.list
- deploymentmanager.deployments.create
- deploymentmanager.deployments.delete
- deploymentmanager.deployments.get
- deploymentmanager.deployments.list
- deploymentmanager.manifests.get
- deploymentmanager.manifests.list
- deploymentmanager.operations.get
- deploymentmanager.operations.list
- deploymentmanager.resources.get
- deploymentmanager.resources.list
- deploymentmanager.typeProviders.get
- deploymentmanager.typeProviders.list
- deploymentmanager.types.get
- deploymentmanager.types.list
- resourcemanager.projects.get
- compute.instances.setServiceAccount
- iam.serviceAccounts.list

```

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

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

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

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

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

Step 3: Set up permissions for the Connector

A Google Cloud service account is required to provide the Connector with the permissions that BlueXP needs to manage resources in Google Cloud. When you create the Connector, you'll need to associate this service account with the Connector VM.

It's your responsibility to update the custom role as new permissions are added in subsequent releases. If new permissions are required, they will be listed in the release notes.

Steps

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

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

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

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

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

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

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

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

- a. From the IAM & Admin service, select the Google Cloud project where you want to create Cloud Volumes ONTAP systems.
- b. On the **IAM** page, select **Grant Access** and provide the required details.
 - Enter the email of the Connector's service account.
 - Select the Connector's custom role.
 - Select **Save**.

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

Result

The service account for the Connector VM is set up.

Step 4: Set up shared VPC permissions

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

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

View shared VPC permissions

Identity	Creator	Hosted in	Service project permissions	Host project permissions	Purpose
Google account to deploy the Connector	Custom	Service Project	Connector deployment policy	compute.network User	Deploying the Connector in the service project
Connector or service account	Custom	Service project	Connector service account policy	compute.network User deploymentmanager.editor	Deploying and maintaining Cloud Volumes ONTAP and services in the service project
Cloud Volumes ONTAP service account	Custom	Service project	storage.admin member: BlueXP service account as serviceAccount.user	N/A	(Optional) For data tiering and BlueXP backup and recovery
Google APIs service agent	Google Cloud	Service project	(Default) Editor	compute.network User	Interacts with Google Cloud APIs on behalf of deployment. Allows BlueXP to use the shared network.
Google Compute Engine default service account	Google Cloud	Service project	(Default) Editor	compute.network User	Deploys Google Cloud instances and compute infrastructure on behalf of deployment. Allows BlueXP to use the shared network.

Notes:

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

Step 5: Enable Google Cloud APIs

You must enable several Google Cloud APIs before deploying the Connector and Cloud Volumes ONTAP.

Step

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

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

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

[Google Cloud documentation: Enabling APIs](#)

Step 6: Create the Connector

Create a Connector directly from the BlueXP web-based console or by using gcloud.

About this task

Creating the Connector deploys a virtual machine instance in Google Cloud using a default configuration. Do not change the Connector to a smaller VM instance with less CPU or RAM after creation. [Learn about the default configuration for the Connector.](#)

BlueXP

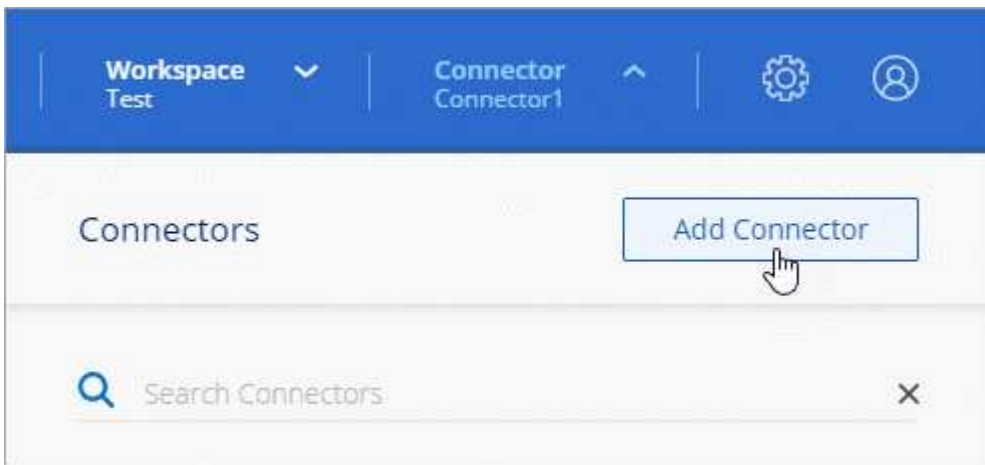
Before you begin

You should have the following:

- The required Google Cloud permissions to create the Connector and a service account for the Connector VM.
- A VPC and subnet that meets networking requirements.
- Details about a proxy server, if a proxy is required for internet access from the Connector.

Steps

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



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

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

- **Details:** Enter a name for the virtual machine instance, specify tags, select a project, and then select the service account that has the required permissions (refer to the section above for details).
- **Location:** Specify a region, zone, VPC, and subnet for the instance.
- **Network:** Choose whether to enable a public IP address and optionally specify a proxy configuration.
- **Network tags:** Add a network tag to the Connector instance if using a transparent proxy. Network tags must start with a lowercase letter and can contain lowercase letters, numbers, and hyphens. Tags must end with a lowercase letter or number. For example, you might use the tag "connector-proxy".

- **Firewall Policy:** Choose whether to create a new firewall policy or whether to select an existing firewall policy that allows the required inbound and outbound rules.

[Firewall rules in Google Cloud](#)

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

5. Select **Add**.

The instance is ready in approximately 7 minutes; stay on the page until the process completes.

Result

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

If you have Google Cloud Storage buckets in the same Google Cloud account where you created the Connector, you'll see a Google Cloud Storage working environment appear on the BlueXP canvas automatically. [Learn how to manage Google Cloud Storage from BlueXP](#)

gcloud

Before you begin

You should have the following:

- The required Google Cloud permissions to create the Connector and a service account for the Connector VM.
- A VPC and subnet that meets networking requirements.
- An understanding of VM instance requirements.
 - **CPU:** 8 cores or 8 vCPUs
 - **RAM:** 32 GB
 - **Machine type:** We recommend n2-standard-8.

The Connector is supported in Google Cloud on a VM instance with an OS that supports Shielded VM features.

Steps

1. Log in to the gcloud SDK using your preferred method.

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

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

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

```
gcloud auth list
```

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

Credentialed Accounts

ACTIVE ACCOUNT

some_user_account@domain.com

* desired_user_account@domain.com

To set the active account, run:

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

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

please run:

```
$ gcloud components update
```

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

```
gcloud compute instances create <instance-name>
  --machine-type=n2-standard-8
  --image-project=netapp-cloudmanager
  --image-family=cloudmanager
  --scopes=cloud-platform
  --project=<project>
  --service-account=<service-account>
  --zone=<zone>
  --no-address
  --tags <network-tag>
  --network <network-path>
  --subnet <subnet-path>
  --boot-disk-kms-key <kms-key-path>
```

instance-name

The desired instance name for the VM instance.

project

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

service-account

The service account specified in the output from step 2.

zone

The zone where you want to deploy the VM

no-address

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

network-tag

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

network-path

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

subnet-path

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

kms-key-path

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

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

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

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

`https://ipaddress`

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

[Learn about BlueXP identity and access management](#).

- b. Enter a name for the system.

Result

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

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

Manually install the Connector in Google Cloud

You can manually install the Connector on a Linux host running in Google Cloud. To manually install the Connector on your own Linux host, you need to review host requirements, set up your networking, prepare Google Cloud permissions, enable APIs, install the Connector, and then provide the permissions that you prepared.

Before you begin

- You should have an [understanding of Connectors](#).
- You should review [Connector limitations](#).

Step 1: Review host requirements

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



The Connector reserves the UID and GID range of 19000 to 19200. This range is fixed and cannot be modified. If any third-party software on your host is using UIDs or GIDs within this range, the Connector installation will fail. NetApp recommends using a host that is free of third-party software to avoid conflicts.

Dedicated host

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

Host can be of any architecture that meets the following size requirements:

- CPU: 8 cores or 8 vCPUs
- RAM: 32 GB

Hypervisor

A bare metal or hosted hypervisor that is certified to run a supported operating system is required.

Operating system and container requirements

BlueXP supports the Connector with the following operating systems when using BlueXP in standard mode or restricted mode. A container orchestration tool is required before you install the Connector.

Operating system	Supported OS versions	Supported Connector versions	Required container tool	SELinux
Red Hat Enterprise Linux	9.1 to 9.4 8.6 to 8.10 7.9	3.9.40 or later with BlueXP in standard mode or restricted mode	Podman version 4.6.1 or 4.9.4 View Podman configuration requirements.	Supported in enforcing mode or permissive mode ¹
Ubuntu	24.04 LTS	3.9.45 or later with BlueXP in standard mode or restricted mode	Docker Engine 23.06 to 28.0.0.	Not supported
	22.04 LTS	3.9.29 or later	Docker Engine 23.0.6 to 28.0.0.	Not supported

Notes:

1. Management of Cloud Volumes ONTAP systems is not supported by Connectors that have SELinux enabled on the operating system.
2. The Connector is supported on English-language versions of these operating systems.
3. For RHEL, the host must be registered with Red Hat Subscription Management. If it's not registered, the host can't access repositories to update required 3rd-party software during Connector installation.

Google Cloud machine type

An instance type that meets the CPU and RAM requirements above. We recommend n2-standard-8.

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

Disk space in /opt

100 GiB of space must be available

BlueXP uses /opt to install the /opt/application/netapp directory and its contents.

Disk space in /var

20 GiB of space must be available

BlueXP requires this space in /var because Docker or Podman are architected to create the containers within this directory. Specifically, they will create containers in the /var/lib/containers/storage directory. External mounts or symlinks do not work for this space.

Step 2: Install Podman or Docker Engine

Depending on your operating system, either Podman or Docker Engine is required before you install the Connector.

- Podman is required for Red Hat Enterprise Linux 8 and 9.

[View the Podman versions that BlueXP supports.](#)

- Docker Engine is required for Ubuntu.

[View the Docker Engine versions that BlueXP supports.](#)

Example 3. Steps

Podman

Follow these steps to install Podman and configure it to meet the following requirements:

- Enable and start the podman.socket service
- Install python3
- Install the podman-compose package version 1.0.6
- Add podman-compose to the PATH environment variable



When using Podman, adjust the aardvark-dns service port (default: 53) after installing the Connector to avoid conflicts with the DNS port on the host. Follow the instructions to configure the port.

Steps

1. Remove the podman-docker package if it's installed on the host.

```
dnf remove podman-docker
rm /var/run/docker.sock
```

2. Install Podman.

Podman is available from official Red Hat Enterprise Linux repositories.

For Red Hat Enterprise Linux 9:

```
sudo dnf install podman-2:<version>
```

Where <version> is the supported version of Podman that you're installing. [View the Podman versions that BlueXP supports.](#)

For Red Hat Enterprise Linux 8:

```
sudo dnf install podman-3:<version>
```

Where <version> is the supported version of Podman that you're installing. [View the Podman versions that BlueXP supports.](#)

3. Enable and start the podman.socket service.

```
sudo systemctl enable --now podman.socket
```

4. Install python3.

```
sudo dnf install python3
```

5. Install the EPEL repository package if it's not already available on your system.

This step is required because podman-compose is available from the Extra Packages for Enterprise Linux (EPEL) repository.

For Red Hat Enterprise Linux 9:

```
sudo dnf install https://dl.fedoraproject.org/pub/epel/epel-release-latest-9.noarch.rpm
```

For Red Hat Enterprise Linux 8:

```
sudo dnf install https://dl.fedoraproject.org/pub/epel/epel-release-latest-8.noarch.rpm
```

6. Install podman-compose package 1.0.6.

```
sudo dnf install podman-compose-1.0.6
```



Using the `dnf install` command meets the requirement for adding podman-compose to the PATH environment variable. The installation command adds podman-compose to `/usr/bin`, which is already included in the `secure_path` option on the host.

Docker Engine

Follow the documentation from Docker to install Docker Engine.

Steps

1. [View installation instructions from Docker](#)

Be sure to follow the steps to install a specific version of Docker Engine. Installing the latest version will install a version of Docker that BlueXP doesn't support.

2. Verify that Docker is enabled and running.

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

Step 3: Set up networking

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

outbound internet access is available.

Connections to target networks

A Connector requires a network connection to the location where you're planning to create and manage working environments. For example, the network where you plan to create Cloud Volumes ONTAP systems or a storage system in your on-premises environment.

Outbound internet access

The network location where you deploy the Connector must have an outbound internet connection to contact specific endpoints.

Endpoints contacted from computers when using the BlueXP web-based console

Computers that access the BlueXP console from a web browser must have the ability to contact several endpoints. You'll need to use the BlueXP console to set up the Connector and for day-to-day use of BlueXP.

[Prepare networking for the BlueXP console.](#)

Endpoints contacted during manual installation

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

- <https://mysupport.netapp.com>
- <https://signin.b2c.netapp.com> (this endpoint is the CNAME URL for <https://mysupport.netapp.com>)
- <https://cloudmanager.cloud.netapp.com/tenancy>
- <https://stream.cloudmanager.cloud.netapp.com>
- <https://production-artifacts.cloudmanager.cloud.netapp.com>
- To obtain images, the installer needs access to one of these two sets of endpoints:
 - Option 1 (recommended):
 - <https://bluexpinfraprod.eastus2.data.azurecr.io>
 - <https://bluexpinfraprod.azurecr.io>
 - Option 2:
 - https://*.blob.core.windows.net
 - <https://cloudmanagerinfraprod.azurecr.io>

The endpoints listed in option 1 are recommended because they are more secure. We recommend that you set up your firewall to allow the endpoints listed in option 1, while disallowing the endpoints listed in option 2. Note the following about these endpoints:

- The endpoints listed in option 1 are supported starting with the 3.9.47 release of the Connector. There is no backwards compatibility with previous releases of the Connector.
- The Connector contacts the endpoints listed in option 2 first. If those endpoints aren't accessible, the Connector automatically contacts the endpoints listed in option 1.
- The endpoints in option 1 are not supported if you use the Connector with BlueXP backup and recovery or BlueXP ransomware protection. In this case, you can disallow the endpoints listed in option 1, while allowing the endpoints listed in option 2.

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

Endpoints contacted from the Connector

The Connector requires outbound internet access to contact the following endpoints in order to manage resources and processes within your public cloud environment for day-to-day operations.

Note that the endpoints listed below are all CNAME entries.

Endpoints	Purpose
https://www.googleapis.com/compute/v1/ https://compute.googleapis.com/compute/v1 https://cloudresourcemanager.googleapis.com/v1/projects https://www.googleapis.com/compute/beta https://storage.googleapis.com/storage/v1 https://www.googleapis.com/storage/v1 https://iam.googleapis.com/v1 https://cloudkms.googleapis.com/v1 https://www.googleapis.com/deploymentmanager/v2/projects	To manage resources in Google Cloud.
https://support.netapp.com https://mysupport.netapp.com	To obtain licensing information and to send AutoSupport messages to NetApp support.
https://*.api.blueexp.netapp.com https://api.blueexp.netapp.com https://*.cloudmanager.cloud.netapp.com https://cloudmanager.cloud.netapp.com https://netapp-cloud-account.auth0.com	To provide SaaS features and services within BlueXP.
Choose between two sets of endpoints: • Option 1 (recommended) ¹ https://bluexpinfraprod.eastus2.data.azurecr.io https://bluexpinfraprod.azurecr.io • Option 2 https://*.blob.core.windows.net https://cloudmanagerinfraprod.azurecr.io	To obtain images for Connector upgrades.

¹ The endpoints listed in option 1 are recommended because they are more secure. We recommend that you set up your firewall to allow the endpoints listed in option 1, while disallowing the endpoints listed in option 2. Note the following about these endpoints:

- The endpoints listed in option 1 are supported starting with the 3.9.47 release of the Connector. There is no backwards compatibility with previous releases of the Connector.
- The Connector contacts the endpoints listed in option 2 first. If those endpoints aren't accessible, the Connector automatically contacts the endpoints listed in option 1.
- The endpoints in option 1 are not supported if you use the Connector with BlueXP backup and recovery or BlueXP ransomware protection. In this case, you can disallow the endpoints listed in option 1, while

allowing the endpoints listed in option 2.

Proxy server

NetApp supports both explicit and transparent proxy configurations. If you are using a transparent proxy, you only need to provide the certificate for the proxy server. If you are using an explicit proxy, you'll also need the IP address and credentials.

- IP address
- Credentials
- HTTPS certificate

Ports

There's no incoming traffic to the Connector, unless you initiate it or if the Connector is used as a proxy to send AutoSupport messages from Cloud Volumes ONTAP to NetApp Support.

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

If Cloud Volumes ONTAP systems don't have an outbound internet connection to send AutoSupport messages, BlueXP automatically configures those 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 NTP

If you're planning to use BlueXP classification to scan your corporate data sources, you should enable a Network Time Protocol (NTP) service on both the BlueXP Connector system and the BlueXP classification system so that the time is synchronized between the systems. [Learn more about BlueXP classification](#)

Step 4: Set up permissions for the Connector

A Google Cloud service account is required to provide the Connector with the permissions that BlueXP needs to manage resources in Google Cloud. When you create the Connector, you'll need to associate this service account with the Connector VM.

It's your responsibility to update the custom role as new permissions are added in subsequent releases. If new permissions are required, they will be listed in the release notes.

Steps

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

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

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

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

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

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

- a. From the IAM & Admin service, select the Google Cloud project where you want to create Cloud Volumes ONTAP systems.
- b. On the **IAM** page, select **Grant Access** and provide the required details.
 - Enter the email of the Connector's service account.
 - Select the Connector's custom role.
 - Select **Save**.

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

Result

The service account for the Connector VM is set up.

Step 5: Set up shared VPC permissions

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

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

View shared VPC permissions

Identity	Creator	Hosted in	Service project permissions	Host project permissions	Purpose
Google account to deploy the Connector	Custom	Service Project	Connector deployment policy	compute.network User	Deploying the Connector in the service project
Connector or service account	Custom	Service project	Connector service account policy	compute.network User deploymentmanager.editor	Deploying and maintaining Cloud Volumes ONTAP and services in the service project
Cloud Volumes ONTAP service account	Custom	Service project	storage.admin member: BlueXP service account as serviceAccount.user	N/A	(Optional) For data tiering and BlueXP backup and recovery
Google APIs service agent	Google Cloud	Service project	(Default) Editor	compute.network User	Interacts with Google Cloud APIs on behalf of deployment. Allows BlueXP to use the shared network.
Google Compute Engine default service account	Google Cloud	Service project	(Default) Editor	compute.network User	Deploys Google Cloud instances and compute infrastructure on behalf of deployment. Allows BlueXP to use the shared network.

Notes:

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

Step 6: Enable Google Cloud APIs

Several Google Cloud APIs must be enabled before you can deploy Cloud Volumes ONTAP systems in Google Cloud.

Step

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

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

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

[Google Cloud documentation: Enabling APIs](#)

Step 7: Install the Connector

After the pre-requisites are complete, you can manually install the software on your own Linux host.

Before you begin

You should have the following:

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

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

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



You cannot set a certificate for a transparent proxy server when manually installing the Connector. If you need to set a certificate for a transparent proxy server, you must use the Maintenance Console after installation. Learn more about the [Connector Maintenance Console](#).

About this task

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

Steps

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

```
unset http_proxy
unset https_proxy
```

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

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

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

3. Assign permissions to run the script.

```
chmod +x BlueXP-Connector-Cloud-<version>
```

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

4. Run the installation script.

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

You'll need to add proxy information if your network requires a proxy for internet access. You can add either a transparent or explicit proxy. The --proxy and --cacert parameters are optional and you won't be prompted to add them. If you have a proxy server, you will need to enter the parameters as shown.

Here is an example configuring an explicit proxy server with a CA-signed certificate:

```
./BlueXP-Connector-Cloud-v3.9.40--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://user-name:password@address:port
- http://domain-name%92user-name:password@address:port
- https://address:port
- https://user-name:password@address:port
- https://domain-name%92user-name:password@address:port

Note the following:

- The user can be a local user or domain user.
- For a domain user, you must use the ASCII code for a \ as shown above.
- BlueXP doesn't support user names or passwords that include the @ character.
- If the password includes any of the following special characters, you must escape that special character by prepending it with a backslash: & or !

For example:

`http://bxpproxyuser:netapp1!@address:3128`

`--cacert` specifies a CA-signed certificate to use for HTTPS access between the Connector and the proxy server. This parameter is required for HTTPS proxy servers, intercepting proxy servers, and transparent proxy servers.

Here is an example configuring a transparent proxy server. When you configure a transparent proxy, you don't need to define the proxy server. You only add a CA-signed certificate to your Connector host:

```
./BlueXP-Connector-Cloud-v3.9.40 --cacert /tmp/cacert/certificate.cer
```

5. If you used Podman, you'll need to adjust the aardvark-dns port.
 - a. SSH to the BlueXP Connector virtual machine.
 - b. Open podman `/usr/share/containers/containers.conf` file and modify the chosen port for Aardvark DNS service. For example, change it to 54.

```
vi /usr/share/containers/containers.conf
...
# Port to use for dns forwarding daemon with netavark in rootful
bridge
# mode and dns enabled.
# Using an alternate port might be useful if other DNS services
should
# run on the machine.
#
dns_bind_port = 54
...
Esc:wq
```

- c. Reboot the Connector virtual machine.

6. Wait for the installation to complete.

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

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

`https://ipaddress`

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

You should keep restricted mode disabled because these steps describe how to use BlueXP in

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

d. Select **Let's start**.

If you have Google Cloud Storage buckets in the same Google Cloud account where you created the Connector, you'll see a Google Cloud Storage working environment appear on the BlueXP canvas automatically. [Learn how to manage Google Cloud Storage from BlueXP](#)

Step 8: Provide permissions to BlueXP

You need to provide BlueXP with the Google Cloud permissions that you previously set up. Providing the permissions enables BlueXP to manage your data and storage infrastructure in Google Cloud.

Steps

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

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

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

Result

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

Install and set up a Connector on-premises

You can install a Connector on one of your on-premises machines. To run the Connector on-premises, you need to review host requirements, set up your networking, prepare cloud permissions, install the Connector, set up the Connector, and then provide the permissions that you prepared.

Before you begin

- Review information about [Connectors](#).
- You should review [Connector limitations](#).

Step 1: Review host requirements

Run the Connector software on a host that meets operating system, RAM, and port requirements. Ensure that your host meets these requirements before you install the Connector.



The Connector reserves the UID and GID range of 19000 to 19200. This range is fixed and cannot be modified. If any third-party software on your host is using UIDs or GIDs within this range, the Connector installation will fail. NetApp recommends using a host that is free of third-party software to avoid conflicts.

Dedicated host

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

Host can be of any architecture that meets the following size requirements:

- CPU: 8 cores or 8 vCPUs
- RAM: 32 GB

Hypervisor

A bare metal or hosted hypervisor that is certified to run a supported operating system is required.

Operating system and container requirements

BlueXP supports the Connector with the following operating systems when using BlueXP in standard mode or restricted mode. A container orchestration tool is required before you install the Connector.

Operating system	Supported OS versions	Supported Connector versions	Required container tool	SELinux
Red Hat Enterprise Linux	9.1 to 9.4 8.6 to 8.10 7.9	3.9.40 or later with BlueXP in standard mode or restricted mode	Podman version 4.6.1 or 4.9.4 View Podman configuration requirements.	Supported in enforcing mode or permissive mode ¹
Ubuntu	24.04 LTS	3.9.45 or later with BlueXP in standard mode or restricted mode	Docker Engine 23.06 to 28.0.0.	Not supported
	22.04 LTS	3.9.29 or later	Docker Engine 23.0.6 to 28.0.0.	Not supported

Notes:

1. Management of Cloud Volumes ONTAP systems is not supported by Connectors that have SELinux enabled on the operating system.
2. The Connector is supported on English-language versions of these operating systems.
3. For RHEL, the host must be registered with Red Hat Subscription Management. If it's not registered, the host can't access repositories to update required 3rd-party software during Connector installation.

Disk space in /opt

100 GiB of space must be available

BlueXP uses /opt to install the /opt/application/netapp directory and its contents.

Disk space in /var

20 GiB of space must be available

BlueXP requires this space in /var because Docker or Podman are architected to create the containers within this directory. Specifically, they will create containers in the /var/lib/containers/storage directory. External mounts or symlinks do not work for this space.

Step 2: Install Podman or Docker Engine

Depending on your operating system, either Podman or Docker Engine is required before you install the Connector.

- Podman is required for Red Hat Enterprise Linux 8 and 9.

[View the Podman versions that BlueXP supports.](#)

- Docker Engine is required for Ubuntu.

[View the Docker Engine versions that BlueXP supports.](#)

Example 4. Steps

Podman

Follow these steps to install Podman and configure it to meet the following requirements:

- Enable and start the podman.socket service
- Install python3
- Install the podman-compose package version 1.0.6
- Add podman-compose to the PATH environment variable



When using Podman, adjust the aardvark-dns service port (default: 53) after installing the Connector to avoid conflicts with the DNS port on the host. Follow the instructions to configure the port.

Steps

1. Remove the podman-docker package if it's installed on the host.

```
dnf remove podman-docker
rm /var/run/docker.sock
```

2. Install Podman.

Podman is available from official Red Hat Enterprise Linux repositories.

For Red Hat Enterprise Linux 9:

```
sudo dnf install podman-2:<version>
```

Where <version> is the supported version of Podman that you're installing. [View the Podman versions that BlueXP supports.](#)

For Red Hat Enterprise Linux 8:

```
sudo dnf install podman-3:<version>
```

Where <version> is the supported version of Podman that you're installing. [View the Podman versions that BlueXP supports.](#)

3. Enable and start the podman.socket service.

```
sudo systemctl enable --now podman.socket
```

4. Install python3.

```
sudo dnf install python3
```

5. Install the EPEL repository package if it's not already available on your system.

This step is required because podman-compose is available from the Extra Packages for Enterprise Linux (EPEL) repository.

For Red Hat Enterprise Linux 9:

```
sudo dnf install https://dl.fedoraproject.org/pub/epel/epel-release-latest-9.noarch.rpm
```

For Red Hat Enterprise Linux 8:

```
sudo dnf install https://dl.fedoraproject.org/pub/epel/epel-release-latest-8.noarch.rpm
```

6. Install podman-compose package 1.0.6.

```
sudo dnf install podman-compose-1.0.6
```



Using the `dnf install` command meets the requirement for adding podman-compose to the PATH environment variable. The installation command adds podman-compose to `/usr/bin`, which is already included in the `secure_path` option on the host.

Docker Engine

Follow the documentation from Docker to install Docker Engine.

Steps

1. [View installation instructions from Docker](#)

Be sure to follow the steps to install a specific version of Docker Engine. Installing the latest version will install a version of Docker that BlueXP doesn't support.

2. Verify that Docker is enabled and running.

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

Step 3: Set up networking

Set up networking to ensure the Connector can manage resources, with connections to target networks and outbound internet access.

Connections to target networks

A Connector requires a network connection to the location where you're planning to create and manage working environments. For example, the network where you plan to create Cloud Volumes ONTAP systems or a storage system in your on-premises environment.

Outbound internet access

The network location where you deploy the Connector must have an outbound internet connection to contact specific endpoints.

Endpoints contacted from computers when using the BlueXP web-based console

Computers that access the BlueXP console from a web browser must have the ability to contact several endpoints. You'll need to use the BlueXP console to set up the Connector and for day-to-day use of BlueXP.

[Prepare networking for the BlueXP console.](#)

Endpoints contacted during manual installation

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

- <https://mysupport.netapp.com>
- <https://signin.b2c.netapp.com> (this endpoint is the CNAME URL for <https://mysupport.netapp.com>)
- <https://cloudmanager.cloud.netapp.com/tenancy>
- <https://stream.cloudmanager.cloud.netapp.com>
- <https://production-artifacts.cloudmanager.cloud.netapp.com>
- To obtain images, the installer needs access to one of these two sets of endpoints:
 - Option 1 (recommended):
 - <https://bluexpinfraprod.eastus2.data.azurecr.io>
 - <https://bluexpinfraprod.azurecr.io>
 - Option 2:
 - https://*.blob.core.windows.net
 - <https://cloudmanagerinfraprod.azurecr.io>

The endpoints listed in option 1 are recommended because they are more secure. We recommend that you set up your firewall to allow the endpoints listed in option 1, while disallowing the endpoints listed in option 2. Note the following about these endpoints:

- The endpoints listed in option 1 are supported starting with the 3.9.47 release of the Connector. There is no backwards compatibility with previous releases of the Connector.
- The Connector contacts the endpoints listed in option 2 first. If those endpoints aren't accessible, the Connector automatically contacts the endpoints listed in option 1.
- The endpoints in option 1 are not supported if you use the Connector with BlueXP backup and recovery or BlueXP ransomware protection. In this case, you can disallow the endpoints listed in option 1, while allowing the endpoints listed in option 2.

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

Endpoints contacted from the Connector

The Connector requires outbound internet access to contact the following endpoints in order to manage resources and processes within your public cloud environment for day-to-day operations.

Note that the endpoints listed below are all CNAME entries.

Endpoints	Purpose
AWS services (amazonaws.com): <ul style="list-style-type: none">• CloudFormation• Elastic Compute Cloud (EC2)• Identity and Access Management (IAM)• Key Management Service (KMS)• Security Token Service (STS)• Simple Storage Service (S3)	To manage resources in AWS. The exact endpoint depends on the AWS region that you're using. Refer to AWS documentation for details
https://management.azure.com https://login.microsoftonline.com https://blob.core.windows.net https://core.windows.net	To manage resources in Azure public regions.
https://management.chinacloudapi.cn https://login.chinacloudapi.cn https://blob.core.chinacloudapi.cn https://core.chinacloudapi.cn	To manage resources in Azure China regions.
https://www.googleapis.com/compute/v1/ https://compute.googleapis.com/compute/v1 https://cloudresourcemanager.googleapis.com/v1/projects https://www.googleapis.com/compute/beta https://storage.googleapis.com/storage/v1 https://www.googleapis.com/storage/v1 https://iam.googleapis.com/v1 https://cloudkms.googleapis.com/v1 https://www.googleapis.com/deploymentmanager/v2/projects	To manage resources in Google Cloud.
https://support.netapp.com https://mysupport.netapp.com	To obtain licensing information and to send AutoSupport messages to NetApp support.
https://*.api.bluexp.netapp.com https://api.bluexp.netapp.com https://*.cloudmanager.cloud.netapp.com https://cloudmanager.cloud.netapp.com https://netapp-cloud-account.auth0.com	To provide SaaS features and services within BlueXP.

Endpoints	Purpose
<p>Choose between two sets of endpoints:</p> <ul style="list-style-type: none"> Option 1 (recommended) ¹ <p>https://bluexpinfraprod.eastus2.data.azurecr.io https://bluexpinfraprod.azurecr.io</p> <ul style="list-style-type: none"> Option 2 <p>https://*.blob.core.windows.net https://cloudmanagerinfraprod.azurecr.io</p>	To obtain images for Connector upgrades.

¹ The endpoints listed in option 1 are recommended because they are more secure. We recommend that you set up your firewall to allow the endpoints listed in option 1, while disallowing the endpoints listed in option 2. Note the following about these endpoints:

- The endpoints listed in option 1 are supported starting with the 3.9.47 release of the Connector. There is no backwards compatibility with previous releases of the Connector.
- The Connector contacts the endpoints listed in option 2 first. If those endpoints aren't accessible, the Connector automatically contacts the endpoints listed in option 1.
- The endpoints in option 1 are not supported if you use the Connector with BlueXP backup and recovery or BlueXP ransomware protection. In this case, you can disallow the endpoints listed in option 1, while allowing the endpoints listed in option 2.

Proxy server

NetApp supports both explicit and transparent proxy configurations. If you are using a transparent proxy, you only need to provide the certificate for the proxy server. If you are using an explicit proxy, you'll also need the IP address and credentials.

- IP address
- Credentials
- HTTPS certificate

Ports

There's no incoming traffic to the Connector, unless you initiate it or if the Connector is used as a proxy to send AutoSupport messages from Cloud Volumes ONTAP to NetApp Support.

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

If Cloud Volumes ONTAP systems don't have an outbound internet connection to send AutoSupport messages, BlueXP automatically configures those 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 NTP

If you're planning to use BlueXP classification to scan your corporate data sources, you should enable a Network Time Protocol (NTP) service on both the BlueXP Connector system and the BlueXP classification system so that the time is synchronized between the systems. [Learn more about BlueXP classification](#)

Step 4: Set up cloud permissions

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



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

AWS

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

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

Steps

1. Log in to the AWS console and navigate to the IAM service.
2. Create a policy:
 - a. Select **Policies > Create policy**.
 - b. Select **JSON** and copy and paste the contents of the [IAM policy for the Connector](#).
 - c. Finish the remaining steps to create the policy.

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

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

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

Result

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

Azure

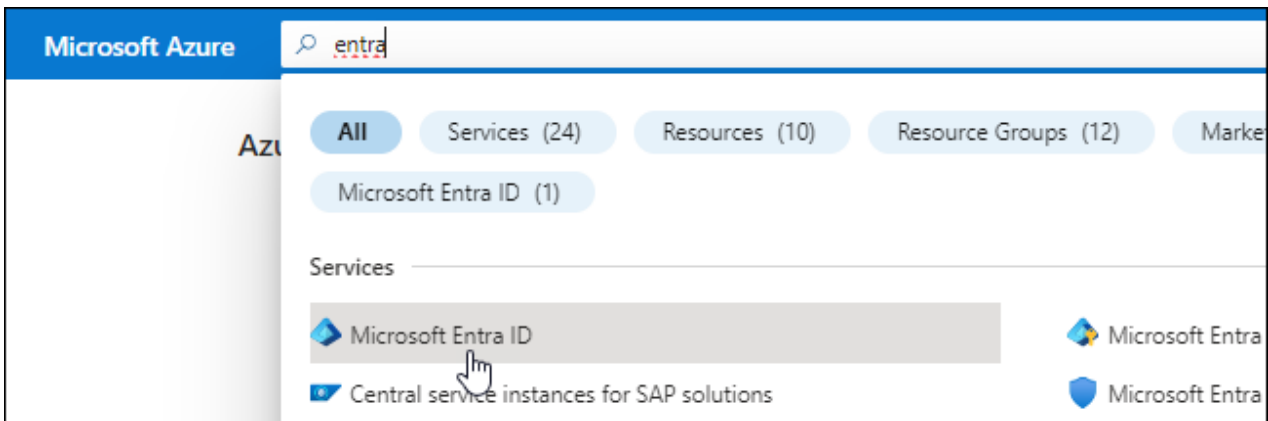
When the Connector is installed on-premises, you need to provide BlueXP with Azure permissions by setting up a service principal in Microsoft Entra ID and obtaining the Azure credentials that BlueXP needs.

Create a Microsoft Entra application for role-based access control

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

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

2. From the Azure portal, open the **Microsoft Entra ID** service.



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

You've created the AD application and service principal.

Assign the application to a role

1. Create a custom role:

Note that you can create an Azure custom role using the Azure portal, Azure PowerShell, Azure CLI, or REST API. The following steps show how to create the role using the Azure CLI. If you would prefer to use a different method, refer to [Azure documentation](#)

- 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

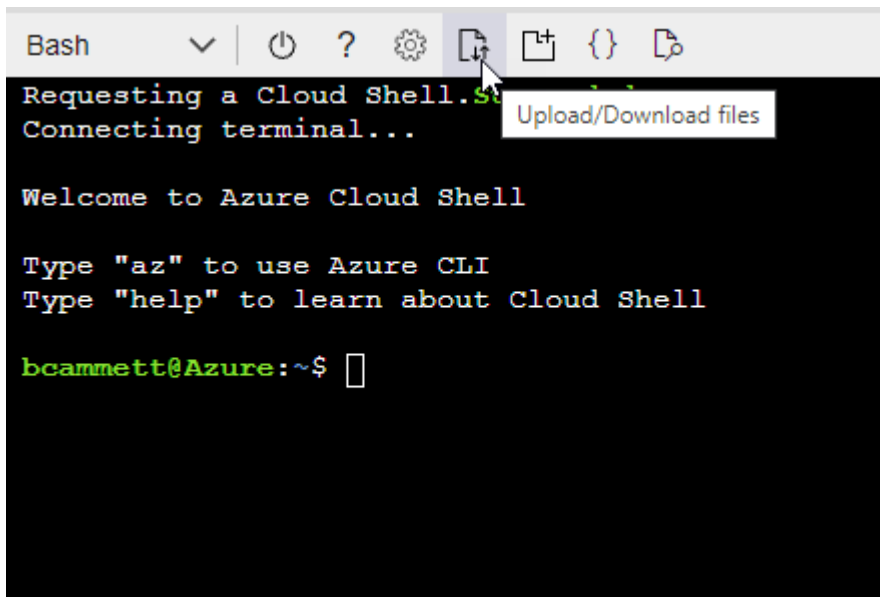
```
"AssignableScopes": [
  "/subscriptions/d333af45-0d07-4154-943d-c25fbzzzzzzz",
  "/subscriptions/54b91999-b3e6-4599-908e-416e0zzzzzzz",
  "/subscriptions/398e471c-3b42-4ae7-9b59-ce5bbzzzzzzz"
```

- 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:

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

Add role assignment ...

Got feedback?

Role **Members** Review + assign

Selected role Cloud Manager Operator 3.9.12_B

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

Members + [Select members](#)

- Search for the name of the application.

Here's an example:

Select members ✕

Select ⓘ

test-service-principal

test-service-principal

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

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

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

Add Windows Azure Service Management API permissions

1. In the **Microsoft Entra ID** service, select **App registrations** and select the application.
2. Select **API permissions > Add a permission**.
3. Under **Microsoft APIs**, select **Azure Service Management**.

Request API permissions

Select an API

Microsoft APIs APIs my organization uses My APIs

Commonly used Microsoft APIs

Microsoft Graph

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



Azure Batch

Schedule large-scale parallel and HPC applications in the cloud

Azure Data Catalog

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

Azure Data Explorer

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

Azure Data Lake

Access to storage and compute for big data analytic scenarios

Azure DevOps

Integrate with Azure DevOps and Azure DevOps server

Azure Import/Export

Programmatic control of import/export jobs

Azure Key Vault

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

Azure Rights Management Services

Allow validated users to read and write protected content

Azure Service Management

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

Azure Storage

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

Customer Insights

Create profile and interaction models for your products

Data Export Service for Microsoft Dynamics 365

Export data from Microsoft Dynamics CRM organization to an external destination

4. Select **Access Azure Service Management as organization users** and then select **Add permissions**.

Request API permissions

[< All APIs](#)



Azure Service Management

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

What type of permissions does your application require?

Delegated permissions

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

Application permissions

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

Select permissions

[expand all](#)

Type to search

PERMISSION

ADMIN CONSENT REQUIRED

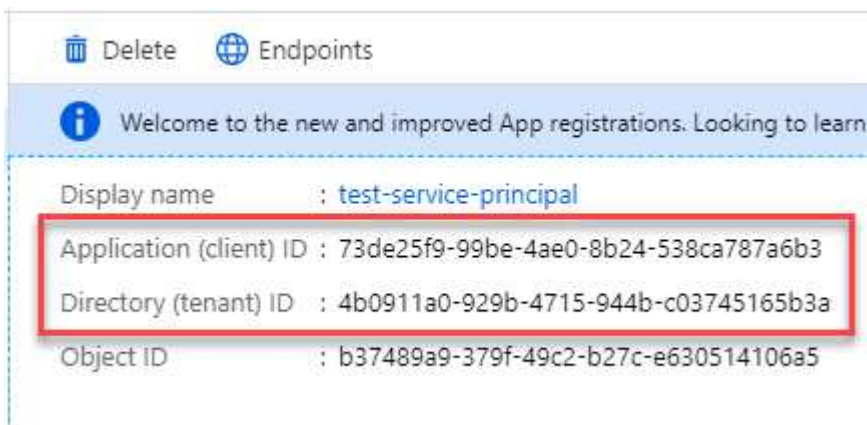


user_impersonation

Access Azure Service Management as organization users (preview) ⓘ

Get the application ID and directory ID for the application

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



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

Create a client secret

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

Client secrets

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

[+ New client secret](#)

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

You now have a client secret that BlueXP can use it to authenticate with Microsoft Entra ID.

Step 5: Install the Connector

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

Before you begin

You should have the following:

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

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

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



You cannot set a certificate for a transparent proxy server when manually installing the Connector. If you need to set a certificate for a transparent proxy server, you must use the Maintenance Console after installation. Learn more about the [Connector Maintenance Console](#).

About this task

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

Steps

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

```
unset http_proxy
unset https_proxy
```

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

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

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

3. Assign permissions to run the script.

```
chmod +x BlueXP-Connector-Cloud-<version>
```

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

4. Run the installation script.

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

You'll need to add proxy information if your network requires a proxy for internet access. You can add either a transparent or explicit proxy. The --proxy and --cacert parameters are optional and you won't be prompted to add them. If you have a proxy server, you will need to enter the parameters as shown.

Here is an example configuring an explicit proxy server with a CA-signed certificate:

```
./BlueXP-Connector-Cloud-v3.9.40--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://user-name:password@address:port
- http://domain-name%92user-name:password@address:port
- https://address:port
- https://user-name:password@address:port
- https://domain-name%92user-name:password@address:port

Note the following:

- The user can be a local user or domain user.
- For a domain user, you must use the ASCII code for a \ as shown above.
- BlueXP doesn't support user names or passwords that include the @ character.
- If the password includes any of the following special characters, you must escape that special character by prepending it with a backslash: & or !

For example:

```
http://bxpproxyuser:netapp1\!@address:3128
```

--cacert specifies a CA-signed certificate to use for HTTPS access between the Connector and the proxy server. This parameter is required for HTTPS proxy servers, intercepting proxy servers, and transparent proxy servers.

Here is an example configuring a transparent proxy server. When you configure a transparent proxy, you don't need to define the proxy server. You only add a CA-signed certificate to your Connector host:

```
./BlueXP-Connector-Cloud-v3.9.40 --cacert /tmp/cacert/certificate.cer
```

5. If you used Podman, you'll need to adjust the aardvark-dns port.
 - a. SSH to the BlueXP Connector virtual machine.
 - b. Open podman `/usr/share/containers/containers.conf` file and modify the chosen port for Aardvark DNS service. For example, change it to 54.

```
vi /usr/share/containers/containers.conf
...
# Port to use for dns forwarding daemon with netavark in rootful
bridge
# mode and dns enabled.
# Using an alternate port might be useful if other DNS services
should
# run on the machine.
#
dns_bind_port = 54
...
Esc:wq
```

- c. Reboot the Connector virtual machine.

Result

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

Step 6: Register the Connector with BlueXP

Log into BlueXP and associate the Connector with your organization. How you log in depends on the mode in which you are using BlueXP. If you are using BlueXP in standard mode, you log in through the SaaS website. If you are using BlueXP in restricted or private mode, you log in locally from the Connector host.

Steps

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

`https://ipaddress`

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

2. Sign up or log in.
3. After you log in, set up BlueXP:
 - a. Specify the BlueXP organization to associate with the Connector.

- b. Enter a name for the system.
- c. Under **Are you running in a secured environment?** keep restricted mode disabled.

Keep restricted mode disabled because these steps use BlueXP in standard mode. (In addition, restricted mode isn't supported when the Connector is installed on-premises.)

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

Step 7: Provide permissions to BlueXP

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

AWS

Before you begin

If you just created these AWS credentials, they may take a few minutes to become available. Wait a few minutes before you add the credentials to BlueXP.

Steps

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



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

Result

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

You can now go to the [BlueXP console](#) to start using the Connector with BlueXP.

Azure

Before you begin

If you just created these Azure credentials, they may take a few minutes to become available. Wait a few minutes before you add the credentials to BlueXP.

Steps

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



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

Result

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

Subscribe to NetApp Intelligent Services (standard mode)

Subscribe to NetApp Intelligent Services from your cloud provider's marketplace to pay for data services at an hourly rate (PAYGO) or through an annual contract. If you purchased a license from NetApp (BYOL), you also need to subscribe to the marketplace offering. Your license is always charged first, but you'll be charged at the hourly rate if you exceed your licensed capacity or if the license's term expires.

A marketplace subscription enables charging for the following NetApp data services:

- Backup and recovery
- Cloud Volumes ONTAP
- Tiering
- Ransomware protection
- Disaster recovery

Classification is enabled through your subscription, but there is no charge for using classification.

Before you begin

Subscribing to data services involves associating a marketplace subscription with the cloud credentials that are associated with a Connector. If you followed the "Get started with standard mode" workflow, then you should already have a Connector. To learn more, view the [Quick start for BlueXP in standard mode](#).

AWS

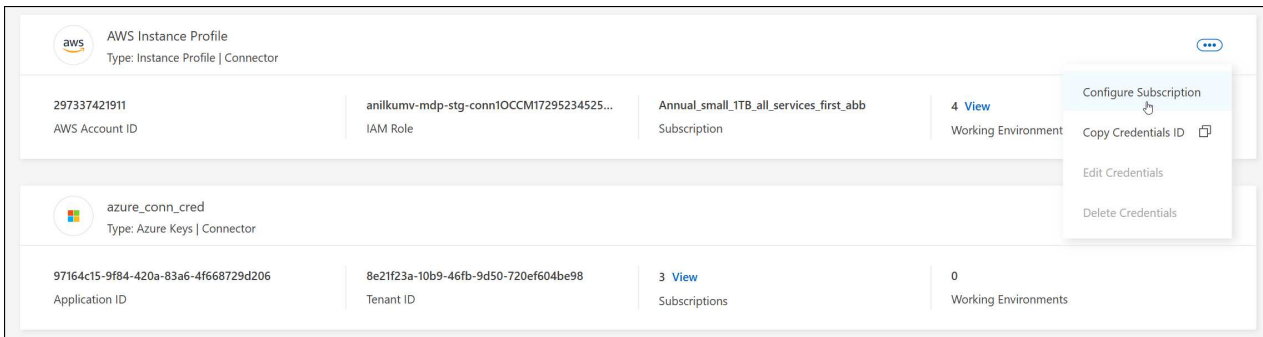
The following video shows the steps to subscribe to NetApp Intelligent Services from the AWS Marketplace:

Subscribe to NetApp Intelligent Services from the AWS Marketplace

Steps

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

You must select credentials that are associated with a Connector. You can't associate a marketplace subscription with credentials that are associated with BlueXP.



3. To associate the credentials with an existing subscription, select the subscription from the down-down list and select **Configure**.
4. To associate the credentials with a new subscription, select **Add Subscription > Continue** and follow the steps in the AWS Marketplace:
 - a. Select **View purchase options**.
 - b. Select **Subscribe**.
 - c. Select **Set up your account**.

You'll be redirected to the BlueXP website.

- d. From the **Subscription Assignment** page:
 - Select the BlueXP organizations or accounts that you'd like to associate this subscription with.
 - In the **Replace existing subscription** field, choose whether you'd like to automatically replace the existing subscription for one organization or account with this new subscription.

BlueXP replaces the existing subscription for all credentials in the organization or account with this new subscription. If a set of credentials wasn't ever associated with a subscription, then this new subscription won't be associated with those credentials.

For all other organizations or accounts, you'll need to manually associate the subscription by repeating these steps.

- Select **Save**.

Azure

Steps

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

You must select credentials that are associated with a Connector. You can't associate a marketplace subscription with credentials that are associated with BlueXP.

3. To associate the credentials with an existing subscription, select the subscription from the down-down list and select **Configure**.
4. To associate the credentials with a new subscription, select **Add Subscription > Continue** and follow the steps in the Azure Marketplace:
 - a. If prompted, log in to your Azure account.
 - b. Select **Subscribe**.
 - c. Fill out the form and select **Subscribe**.
 - d. After the subscription process is complete, select **Configure account now**.

You'll be redirected to BlueXP.

- e. From the **Subscription Assignment** page:
 - Select the BlueXP organizations or accounts that you'd like to associate this subscription with.
 - In the **Replace existing subscription** field, choose whether you'd like to automatically replace the existing subscription for one organization or account with this new subscription.

BlueXP replaces the existing subscription for all credentials in the organization or account with this new subscription. If a set of credentials wasn't ever associated with a subscription, then this new subscription won't be associated with those credentials.

For all other organizations or accounts, you'll need to manually associate the subscription by repeating these steps.

- Select **Save**.

The following video shows the steps to subscribe from the Azure Marketplace:

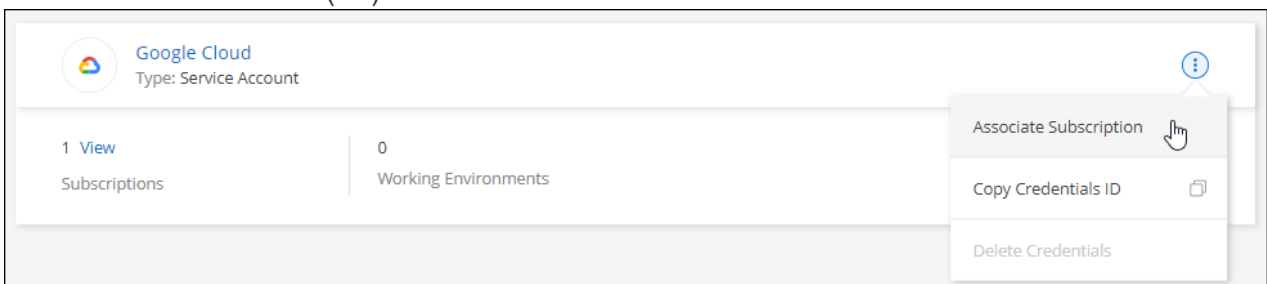
[Subscribe to NetApp Intelligent Services from the Azure Marketplace](#)

Google Cloud

Steps

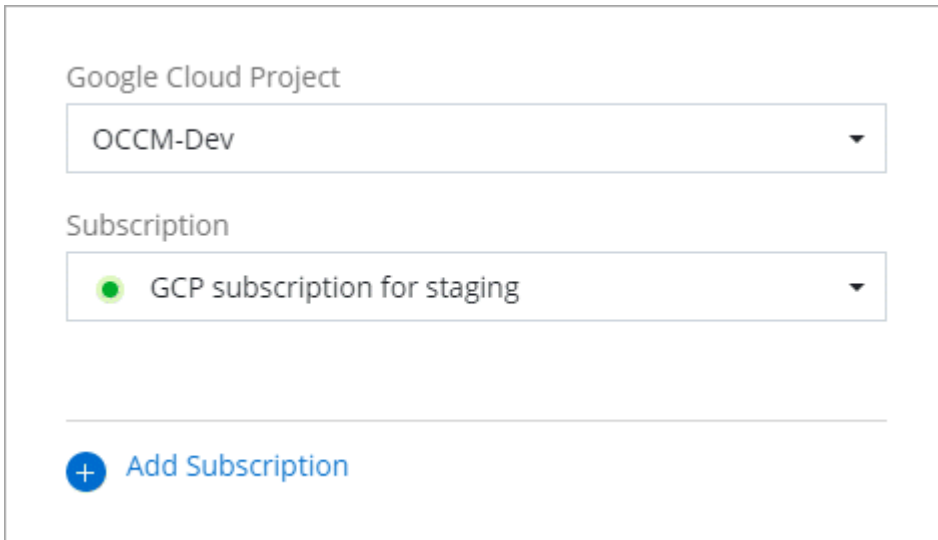
1. In the upper right of the console, select the Settings icon, and select **Credentials**.
2. Select the action menu for a set of credentials and then select **Configure Subscription**.

+new screenshot needed (TS)



3. To configure an existing subscription with the selected credentials, select a Google Cloud project and

subscription from the drop-down list, and then select **Configure**.



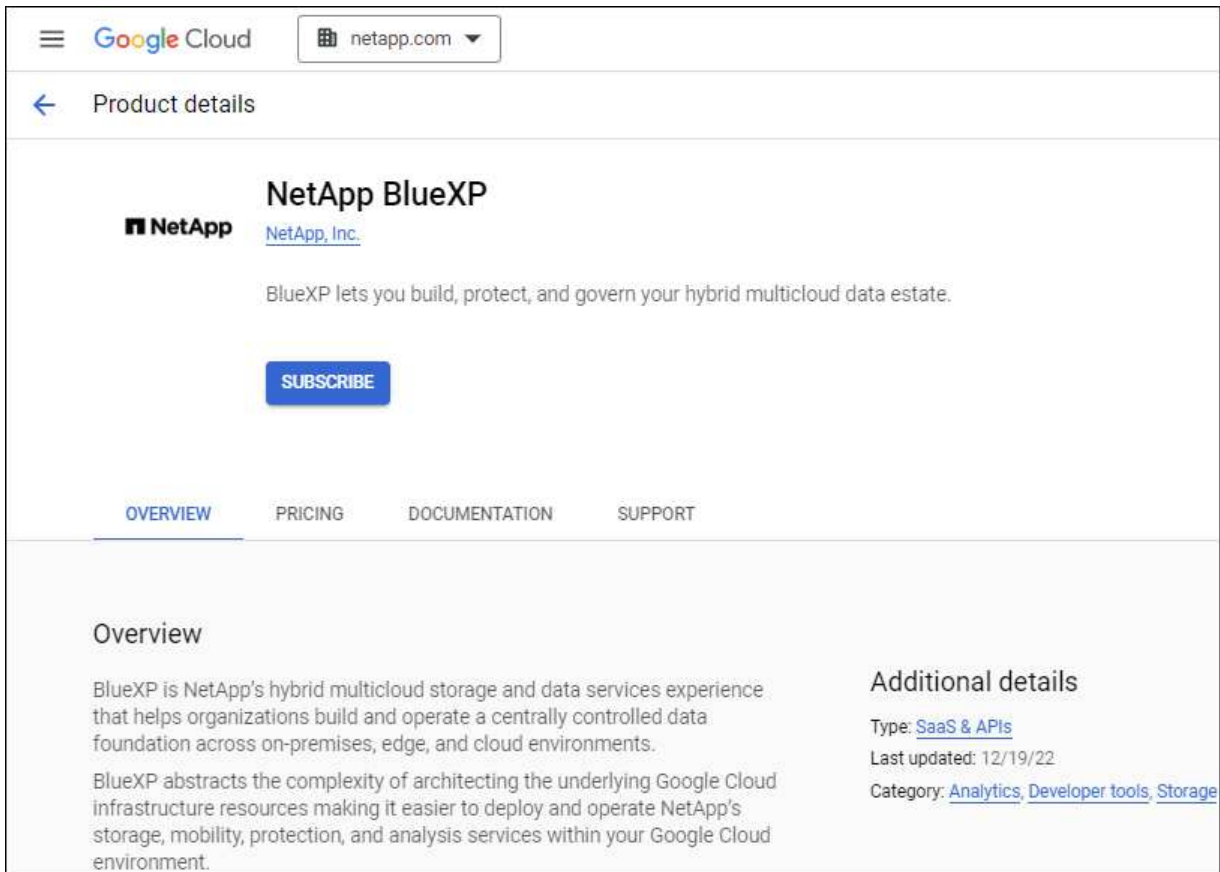
The screenshot shows a configuration interface for Google Cloud. At the top, there's a section labeled "Google Cloud Project" with a dropdown menu currently showing "OCCM-Dev". Below this is a section labeled "Subscription" with a dropdown menu showing "GCP subscription for staging" next to a green dot icon. At the bottom of the section is a blue button with a plus icon and the text "Add Subscription".

4. If you don't already have a subscription, select **Add Subscription > Continue** and follow the steps in the Google Cloud Marketplace.



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.

- a. After you're redirected to the [NetApp Intelligent Services page on the Google Cloud Marketplace](#), ensure that the correct project is selected at the top navigation menu.



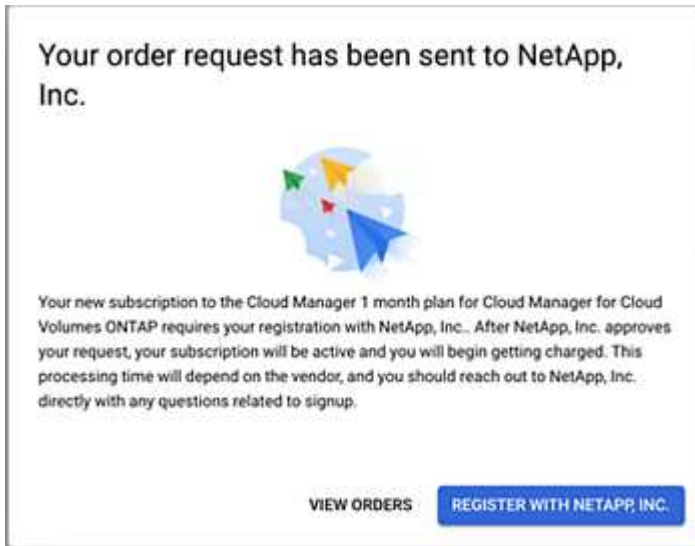
The screenshot shows the "Product details" page for NetApp BlueXP on the Google Cloud Marketplace. The top navigation bar includes the Google Cloud logo and a dropdown menu showing "netapp.com". Below the navigation bar is a back arrow and the text "Product details". The main content area features the NetApp logo, the product name "NetApp BlueXP", and a link to "NetApp, Inc.". A description states: "BlueXP lets you build, protect, and govern your hybrid multicloud data estate." Below this is a blue "SUBSCRIBE" button. A horizontal menu contains links for "OVERVIEW", "PRICING", "DOCUMENTATION", and "SUPPORT". The "OVERVIEW" section is active, showing a detailed description of BlueXP as a hybrid multicloud storage and data services experience. To the right, under "Additional details", it lists the type as "SaaS & APIs", the last updated date as "12/19/22", and the category as "Analytics, Developer tools, Storage".

- b. Select **Subscribe**.
- c. Select the appropriate billing account and agree to the terms and conditions.
- d. Select **Subscribe**.

This step sends your transfer request to NetApp.

- e. On the pop-up dialog box, select **Register with NetApp, Inc.**

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



- f. Complete the steps on the **Subscription Assignment** page:



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.

- Select the BlueXP organizations or accounts that you'd like to associate this subscription with.
- In the **Replace existing subscription** field, choose whether you'd like to automatically replace the existing subscription for one organization or account with this new subscription.

BlueXP replaces the existing subscription for all credentials in the organization or account with this new subscription. If a set of credentials wasn't ever associated with a subscription, then this new subscription won't be associated with those credentials.

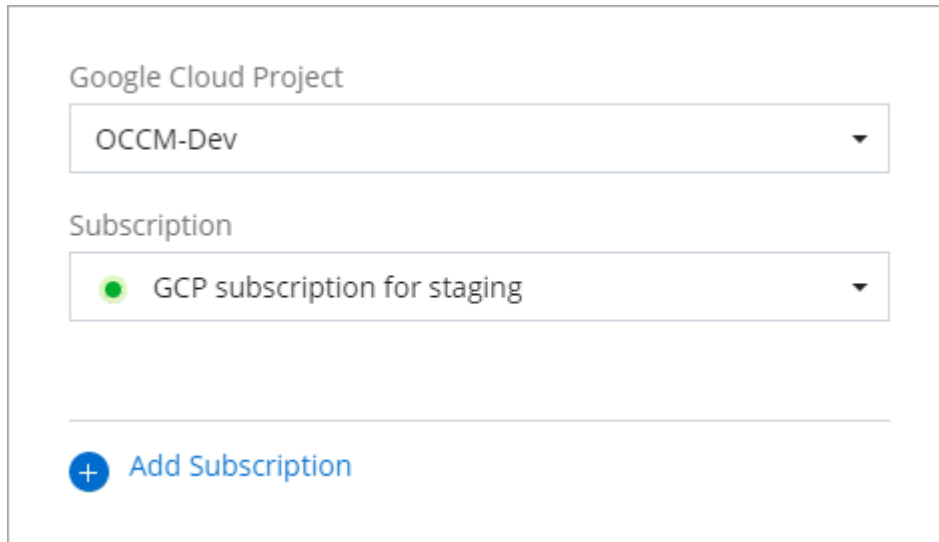
For all other organizations or accounts, you'll need to manually associate the subscription by repeating these steps.

- Select **Save**.

The following video shows the steps to subscribe from the Google Cloud Marketplace:

[Subscribe to BlueXP from the Google Cloud Marketplace](#)

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



The screenshot shows a form with two dropdown menus. The first dropdown is labeled "Google Cloud Project" and has "OCCM-Dev" selected. The second dropdown is labeled "Subscription" and has "GCP subscription for staging" selected, which is preceded by a green circular icon. Below these dropdowns is a horizontal line, and then a blue button with a plus sign and the text "Add Subscription".

Related information

- [Manage BYOL capacity-based licenses for Cloud Volumes ONTAP](#)
- [Manage BYOL licenses for data services](#)
- [Manage AWS credentials and subscriptions](#)
- [Manage Azure credentials and subscriptions](#)
- [Manage Google Cloud credentials and subscriptions](#)

What you can do next (standard mode)

Now that you've logged in and set up BlueXP in standard mode, users can create and discover working environments and use BlueXP data services.



If you installed a Connector in AWS, Microsoft Azure, or Google Cloud, then BlueXP automatically discovers information about the Amazon S3 buckets, Azure Blob storage, or Google Cloud Storage buckets in the location where the Connector is installed. A working environment is automatically added to the BlueXP canvas.

For help, go to the [home page for the BlueXP documentation](#) to view the docs for all BlueXP services.

Related information

[BlueXP deployment modes](#)

Get started with restricted mode

Getting started workflow (restricted mode)

Get started with BlueXP in restricted mode by preparing your environment and deploying the Connector.

Restricted mode is typically used by state and local governments and regulated companies, including deployments in AWS GovCloud and Azure Government regions. Before getting started, ensure you have an understanding of [Connectors](#) and [deployment modes](#).

1

Prepare for deployment

- a. Prepare a dedicated Linux host that meets requirements for CPU, RAM, disk space, container orchestration tool, and more.
- b. Set up networking that provides access to the target networks, outbound internet access for manual installations, and outbound internet for day-to-day access.
- c. Set up permissions in your cloud provider so that you can associate those permissions with the Connector instance after you deploy it.

2

Deploy the Connector

- a. Install the Connector from your cloud provider's marketplace or by manually installing the software on your own Linux host.
- b. Set up BlueXP by opening a web browser and entering the Linux host's IP address.
- c. Provide BlueXP with the permissions that you previously set up.

3

Subscribe to NetApp Intelligent Services (optional)

Optional: Subscribe to NetApp Intelligent Services from your cloud provider's marketplace to pay for data services at an hourly rate (PAYGO) or through an annual contract. NetApp Intelligent Services include Backup and recovery, Cloud Volumes ONTAP, Tiering, Ransomware protection, and Disaster recovery. Classification is included with your subscription at no additional cost.

Prepare for deployment in restricted mode

Prepare your environment before you deploy BlueXP in restricted mode. For example, you need to review host requirements, prepare networking, set up permissions, and more.

Step 1: Understand how restricted mode works

Before you get started, you should have an understanding of how BlueXP works in restricted mode.

For example, you should understand that you need to use the browser-based interface that is available locally from the BlueXP Connector that you need to install. You can't access BlueXP from the web-based console that's provided through the SaaS layer.

In addition, not all BlueXP services are available.

[Learn how restricted mode works.](#)

Step 2: Review installation options

In restricted mode, you can only install the Connector in the cloud. The following installation options are available:

- From the AWS Marketplace
- From the Azure Marketplace
- Manually installing the Connector on your own Linux host that's running in AWS, Azure, or Google Cloud

Step 3: Review host requirements

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

When you deploy the Connector from the AWS or Azure Marketplace, the image includes the required OS and software components. You simply need to choose an instance type that meets CPU and RAM requirements.

Dedicated host

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

Host can be of any architecture that meets the following size requirements:

- CPU: 8 cores or 8 vCPUs
- RAM: 32 GB

Hypervisor

A bare metal or hosted hypervisor that is certified to run a supported operating system is required.

Operating system and container requirements

BlueXP supports the Connector with the following operating systems when using BlueXP in standard mode or restricted mode. A container orchestration tool is required before you install the Connector.

Operating system	Supported OS versions	Supported Connector versions	Required container tool	SELinux
Red Hat Enterprise Linux	9.1 to 9.4 8.6 to 8.10 7.9	3.9.40 or later with BlueXP in standard mode or restricted mode	Podman version 4.6.1 or 4.9.4 View Podman configuration requirements.	Supported in enforcing mode or permissive mode ¹
Ubuntu	24.04 LTS	3.9.45 or later with BlueXP in standard mode or restricted mode	Docker Engine 23.06 to 28.0.0.	Not supported
	22.04 LTS	3.9.29 or later	Docker Engine 23.0.6 to 28.0.0.	Not supported

Notes:

1. Management of Cloud Volumes ONTAP systems is not supported by Connectors that have SELinux enabled on the operating system.

2. The Connector is supported on English-language versions of these operating systems.
3. For RHEL, the host must be registered with Red Hat Subscription Management. If it's not registered, the host can't access repositories to update required 3rd-party software during Connector installation.

AWS EC2 instance type

An instance type that meets the CPU and RAM requirements above. We recommend t3.2xlarge.

Azure VM size

An instance type that meets the CPU and RAM requirements above. We recommend Standard_D8s_v3.

Google Cloud machine type

An instance type that meets the CPU and RAM requirements above. We recommend n2-standard-8.

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

Disk space in /opt

100 GiB of space must be available

BlueXP uses /opt to install the /opt/application/netapp directory and its contents.

Disk space in /var

20 GiB of space must be available

BlueXP requires this space in /var because Docker or Podman are architected to create the containers within this directory. Specifically, they will create containers in the /var/lib/containers/storage directory. External mounts or symlinks do not work for this space.

Step 4: Install Podman or Docker Engine

If you're planning to manually install the Connector software, you need to prepare the host by installing Podman or Docker Engine.

Depending on your operating system, either Podman or Docker Engine is required before you install the Connector.

- Podman is required for Red Hat Enterprise Linux 8 and 9.

[View the Podman versions that BlueXP supports.](#)

- Docker Engine is required for Ubuntu.

[View the Docker Engine versions that BlueXP supports.](#)

Example 5. Steps

Podman

Follow these steps to install Podman and configure it to meet the following requirements:

- Enable and start the podman.socket service
- Install python3
- Install the podman-compose package version 1.0.6
- Add podman-compose to the PATH environment variable



When using Podman, adjust the aardvark-dns service port (default: 53) after installing the Connector to avoid conflicts with the DNS port on the host. Follow the instructions to configure the port.

Steps

1. Remove the podman-docker package if it's installed on the host.

```
dnf remove podman-docker
rm /var/run/docker.sock
```

2. Install Podman.

Podman is available from official Red Hat Enterprise Linux repositories.

For Red Hat Enterprise Linux 9:

```
sudo dnf install podman-2:<version>
```

Where <version> is the supported version of Podman that you're installing. [View the Podman versions that BlueXP supports.](#)

For Red Hat Enterprise Linux 8:

```
sudo dnf install podman-3:<version>
```

Where <version> is the supported version of Podman that you're installing. [View the Podman versions that BlueXP supports.](#)

3. Enable and start the podman.socket service.

```
sudo systemctl enable --now podman.socket
```

4. Install python3.

```
sudo dnf install python3
```

5. Install the EPEL repository package if it's not already available on your system.

This step is required because podman-compose is available from the Extra Packages for Enterprise Linux (EPEL) repository.

For Red Hat Enterprise Linux 9:

```
sudo dnf install https://dl.fedoraproject.org/pub/epel/epel-release-latest-9.noarch.rpm
```

For Red Hat Enterprise Linux 8:

```
sudo dnf install https://dl.fedoraproject.org/pub/epel/epel-release-latest-8.noarch.rpm
```

6. Install podman-compose package 1.0.6.

```
sudo dnf install podman-compose-1.0.6
```



Using the `dnf install` command meets the requirement for adding podman-compose to the PATH environment variable. The installation command adds podman-compose to `/usr/bin`, which is already included in the `secure_path` option on the host.

Docker Engine

Follow the documentation from Docker to install Docker Engine.

Steps

1. [View installation instructions from Docker](#)

Be sure to follow the steps to install a specific version of Docker Engine. Installing the latest version will install a version of Docker that BlueXP doesn't support.

2. Verify that Docker is enabled and running.

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

Step 5: Prepare networking

Set up your networking so the Connector can manage resources and processes within your public cloud environment. Other than having a virtual network and subnet for the Connector, you'll need to ensure that the

following requirements are met.

Connections to target networks

The Connector must have a network connection to the location where you plan to manage storage. For example, the VPC or VNet where you plan to deploy Cloud Volumes ONTAP, or the data center where your on-premises ONTAP clusters reside.

Prepare networking for user access to BlueXP console

In restricted mode, the BlueXP user interface is accessible from the Connector. As you use the BlueXP user interface, it contacts a few endpoints to complete data management tasks. These endpoints are contacted from a user's computer when completing specific actions from the BlueXP console.

Endpoints	Purpose
https://api.blueexp.netapp.com	The BlueXP web-based console contacts this endpoint to interact with the BlueXP API for actions related to authorization, licensing, subscriptions, credentials, notifications, and more.
https://signin.b2c.netapp.com	Required to update NetApp Support Site (NSS) credentials or to add new NSS credentials to BlueXP.
https://netapp-cloud-account.auth0.com https://cdn.auth0.com https://services.cloud.netapp.com	Your web browser connects to these endpoints for centralized user authentication through BlueXP.
https://widget.intercom.io	For in-product chat that enables you to talk to NetApp cloud experts.

Endpoints contacted during manual installation

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

- The following endpoints are always contacted no matter where you install the Connector:
 - <https://mysupport.netapp.com>
 - <https://signin.b2c.netapp.com> (this endpoint is the CNAME URL for <https://mysupport.netapp.com>)
 - <https://cloudmanager.cloud.netapp.com/tenancy>
 - <https://stream.cloudmanager.cloud.netapp.com>
 - <https://production-artifacts.cloudmanager.cloud.netapp.com>
- If you install the Connector in an AWS Government region, the installer also needs access to these endpoints:
 - https://*.blob.core.windows.net
 - <https://cloudmanagerinfraprod.azurecr.io>
- If you install the Connector in an Azure Government region, the installer also needs access to these endpoints:
 - https://*.blob.core.windows.net
 - <https://occmclientinfragov.azurecr.us>

- If you install the Connector in a commercial region or sovereign region, you can choose between two sets of endpoints:
 - Option 1 (recommended):
 - <https://bluexpinfraprod.eastus2.data.azurecr.io>
 - <https://bluexpinfraprod.azurecr.io>
 - Option 2:
 - https://*.blob.core.windows.net
 - <https://cloudmanagerinfraprod.azurecr.io>

The endpoints listed in option 1 are recommended because they are more secure. We recommend that you set up your firewall to allow the endpoints listed in option 1, while disallowing the endpoints listed in option 2. Note the following about these endpoints:

- The endpoints listed in option 1 are supported starting with the 3.9.47 release of the Connector. There is no backwards compatibility with previous releases of the Connector.
- The Connector contacts the endpoints listed in option 2 first. If those endpoints aren't accessible, the Connector automatically contacts the endpoints listed in option 1.
- The endpoints in option 1 are not supported if you use the Connector with BlueXP backup and recovery or BlueXP ransomware protection. In this case, you can disallow the endpoints listed in option 1, while allowing the endpoints listed in option 2.

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

Outbound internet access for day-to-day operations

The network location where you deploy the Connector must have an outbound internet connection. The Connector requires outbound internet access to contact the following endpoints in order to manage resources and processes within your public cloud environment.

Endpoints	Purpose
AWS services (amazonaws.com): <ul style="list-style-type: none"> • CloudFormation • Elastic Compute Cloud (EC2) • Identity and Access Management (IAM) • Key Management Service (KMS) • Security Token Service (STS) • Simple Storage Service (S3) 	To manage resources in AWS. The exact endpoint depends on the AWS region that you're using. Refer to AWS documentation for details
https://management.azure.com https://login.microsoftonline.com https://blob.core.windows.net https://core.windows.net	To manage resources in Azure public regions.

Endpoints	Purpose
https://management.usgovcloudapi.net https://login.microsoftonline.us https://blob.core.usgovcloudapi.net https://core.usgovcloudapi.net	To manage resources in Azure Government regions.
https://management.chinacloudapi.cn https://login.chinacloudapi.cn https://blob.core.chinacloudapi.cn https://core.chinacloudapi.cn	To manage resources in Azure China regions.
https://www.googleapis.com/compute/v1/ https://compute.googleapis.com/compute/v1 https://cloudresourcemanager.googleapis.com/v1/projects https://www.googleapis.com/compute/beta https://storage.googleapis.com/storage/v1 https://www.googleapis.com/storage/v1 https://iam.googleapis.com/v1 https://cloudkms.googleapis.com/v1 https://www.googleapis.com/deploymentmanager/v2/projects	To manage resources in Google Cloud.
https://support.netapp.com https://mysupport.netapp.com	To obtain licensing information and to send AutoSupport messages to NetApp support.
https://*.api.bluexp.netapp.com https://api.bluexp.netapp.com https://*.cloudmanager.cloud.netapp.com https://cloudmanager.cloud.netapp.com https://netapp-cloud-account.auth0.com	To provide SaaS features and services within BlueXP.
If the Connector is in an AWS Government region: https://*.blob.core.windows.net https://cloudmanagerinfragov.azurecr.io	To obtain images for Connector upgrades when the Connector is installed in an AWS Government region.
If the Connector is in an Azure Government region: https://*.blob.core.windows.net https://occmclientinfragov.azurecr.us	To obtain images for Connector upgrades when the Connector is installed in an Azure Government region.

Endpoints	Purpose
<p>If the Connector is in a commercial region or sovereign region, you can choose between two sets of endpoints:</p> <ul style="list-style-type: none"> Option 1 (recommended) ¹ <p>https://bluexpinfraprod.eastus2.data.azurecr.io https://bluexpinfraprod.azurecr.io</p> <ul style="list-style-type: none"> Option 2 <p>https://*.blob.core.windows.net https://cloudmanagerinfraprod.azurecr.io</p>	<p>To obtain images for Connector upgrades when the Connector is installed in a commercial region or sovereign region.</p>

¹ The endpoints listed in option 1 are recommended because they are more secure. We recommend that you set up your firewall to allow the endpoints listed in option 1, while disallowing the endpoints listed in option 2. Note the following about these endpoints:

- The endpoints listed in option 1 are supported starting with the 3.9.47 release of the Connector. There is no backwards compatibility with previous releases of the Connector.
- The Connector contacts the endpoints listed in option 2 first. If those endpoints aren't accessible, the Connector automatically contacts the endpoints listed in option 1.
- The endpoints in option 1 are not supported if you use the Connector with BlueXP backup and recovery or BlueXP ransomware protection. In this case, you can disallow the endpoints listed in option 1, while allowing the endpoints listed in option 2.

Public IP address in Azure

If you want to use a public IP address with the Connector VM in Azure, the IP address must use a Basic SKU to ensure that BlueXP uses this public IP address.

Create public IP address ✕

Name *
newIP ✓

SKU * ⓘ
☒ Basic ☐ Standard

Assignment
☐ Dynamic ☒ Static

If you use a Standard SKU IP address instead, then BlueXP uses the *private* IP address of the Connector, instead of the public IP. If the machine that you're using to access the BlueXP Console doesn't have access to that private IP address, then actions from the BlueXP Console will fail.

[Azure documentation: Public IP SKU](#)

Proxy server

NetApp supports both explicit and transparent proxy configurations. If you are using a transparent proxy, you only need to provide the certificate for the proxy server. If you are using an explicit proxy, you'll also need the IP address and credentials.

- IP address
- Credentials
- HTTPS certificate

Ports

There's no incoming traffic to the Connector, unless you initiate it or if the Connector is used as a proxy to send AutoSupport messages from Cloud Volumes ONTAP to NetApp Support.

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

If Cloud Volumes ONTAP systems don't have an outbound internet connection to send AutoSupport messages, BlueXP automatically configures those 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 NTP

If you're planning to use BlueXP classification to scan your corporate data sources, you should enable a Network Time Protocol (NTP) service on both the BlueXP Connector system and the BlueXP classification system so that the time is synchronized between the systems. [Learn more about BlueXP classification](#)

If you're planning to create the Connector from your cloud provider's marketplace, then you'll need to implement this networking requirement after you create the Connector.

Step 6: Prepare cloud permissions

BlueXP requires permissions from your cloud provider to deploy Cloud Volumes ONTAP in a virtual network and to use BlueXP data services. You need to set up permissions in your cloud provider and then associate those permissions with the Connector.

To view the required steps, select the authentication option that you'd like to use for your cloud provider.

AWS IAM role

Use an IAM role to provide the Connector with permissions.

If you're creating the Connector from the AWS Marketplace, you'll be prompted to select that IAM role when you launch the EC2 instance.

If you're manually installing the Connector on your own Linux host, you'll need to attach the role to the EC2 instance.

Steps

1. Log in to the AWS console and navigate to the IAM service.
2. Create a policy:
 - a. Select **Policies > Create policy**.
 - b. Select **JSON** and copy and paste the contents of the [IAM policy for the Connector](#).
 - c. Finish the remaining steps to create the policy.
3. Create an IAM role:
 - a. Select **Roles > Create role**.
 - b. Select **AWS service > EC2**.
 - c. Add permissions by attaching the policy that you just created.
 - d. Finish the remaining steps to create the role.

Result

You now have an IAM role for the Connector EC2 instance.

AWS access key

Set up permissions and an access key for an IAM user. You'll need to provide BlueXP with the AWS access key after you install the Connector and set up BlueXP.

Steps

1. Log in to the AWS console and navigate to the IAM service.
2. Create a policy:
 - a. Select **Policies > Create policy**.
 - b. Select **JSON** and copy and paste the contents of the [IAM policy for the Connector](#).
 - c. Finish the remaining steps to create the policy.

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

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

3. Attach the policies to an IAM user.
 - [AWS Documentation: Creating IAM Roles](#)
 - [AWS Documentation: Adding and Removing IAM Policies](#)

4. Ensure that the user has an access key that you can add to BlueXP after you install the Connector.

Result

The account now has the required permissions.

Azure role

Create an Azure custom role with the required permissions. You'll assign this role to the Connector VM.

Note that you can create an Azure custom role using the Azure portal, Azure PowerShell, Azure CLI, or REST API. The following steps show how to create the role using the Azure CLI. If you would prefer to use a different method, refer to [Azure documentation](#)

Steps

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

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

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

You should add the ID for each Azure subscription that you want to use with BlueXP.

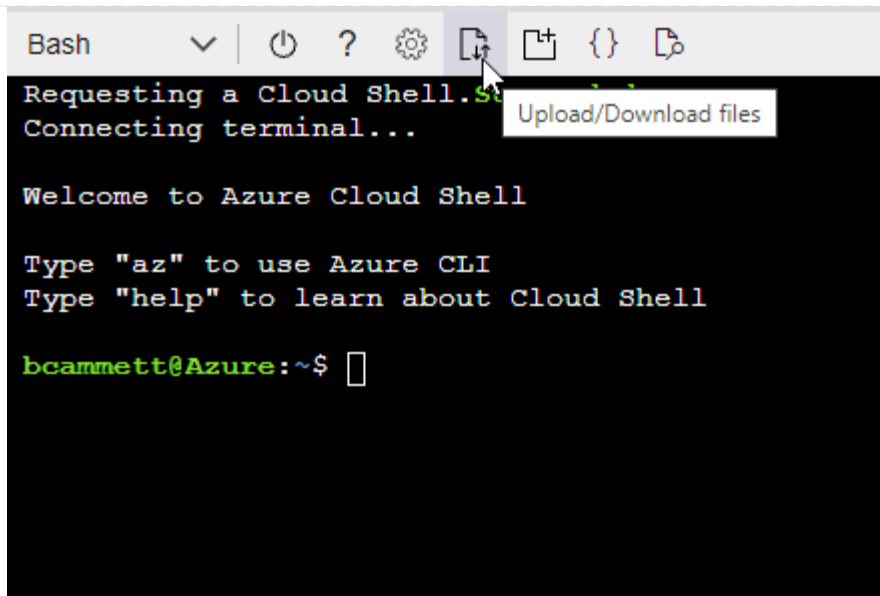
Example

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

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

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

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



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

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

Result

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

Azure service principal

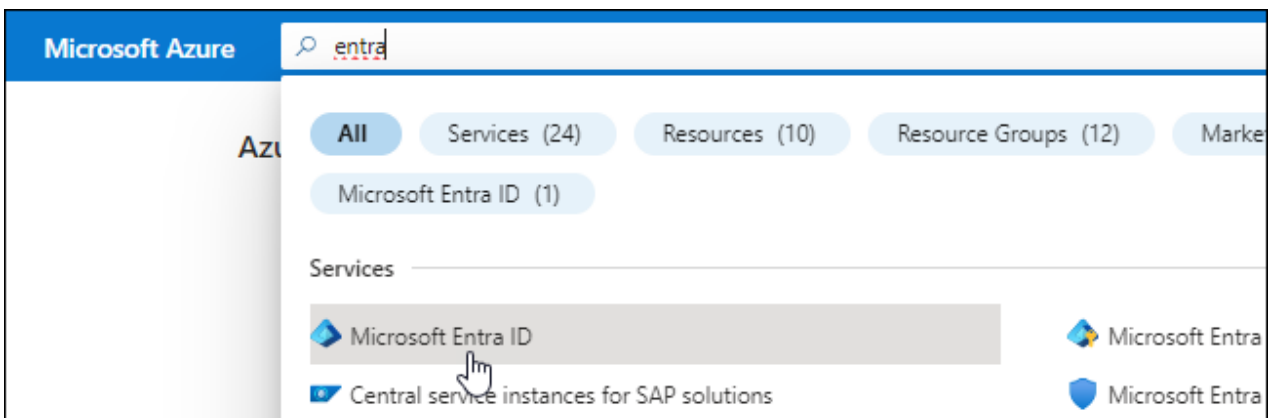
Create and set up a service principal in Microsoft Entra ID and obtain the Azure credentials that BlueXP needs. You'll need to provide BlueXP with these credentials after you install the Connector and set up BlueXP.

Create a Microsoft Entra application for role-based access control

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

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

2. From the Azure portal, open the **Microsoft Entra ID** service.



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

You've created the AD application and service principal.

Assign the application to a role

1. Create a custom role:

Note that you can create an Azure custom role using the Azure portal, Azure PowerShell, Azure CLI, or REST API. The following steps show how to create the role using the Azure CLI. If you would prefer to use a different method, refer to [Azure documentation](#)

- 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.

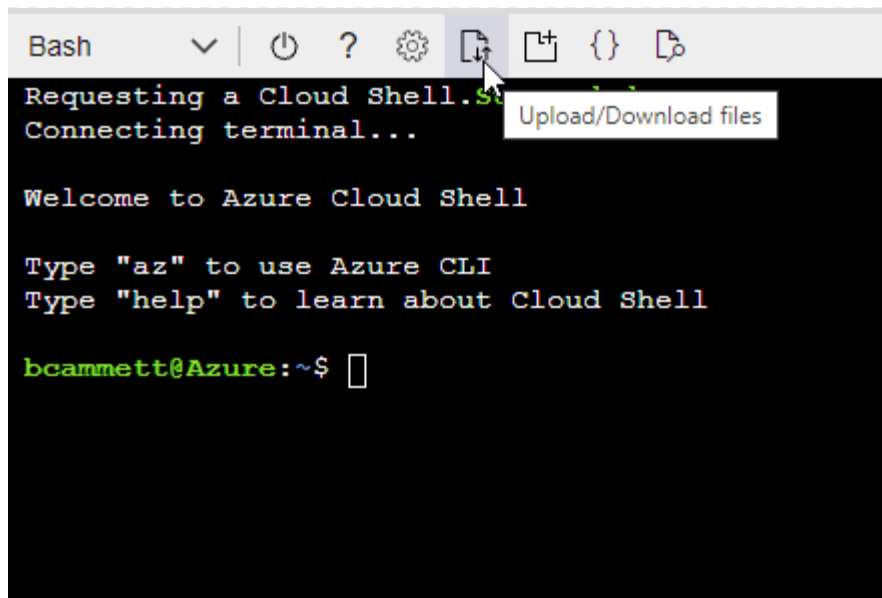
Example

```
"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. Select **Access control (IAM) > Add > Add role assignment**.
 - d. In the **Role** tab, select the **BlueXP Operator** role and select **Next**.
 - e. In the **Members** tab, complete the following steps:
 - Keep **User, group, or service principal** selected.
 - Select **Select members**.

Add role assignment ...

[Got feedback?](#)

Role **Members** Review + assign

Selected role Cloud Manager Operator 3.9.12_B

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

Members [+ Select members](#)

- Search for the name of the application.

Here's an example:

Select members ✕

Select ⓘ

test-service-principal

test-service-principal

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

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

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

Add Windows Azure Service Management API permissions

1. In the **Microsoft Entra ID** service, select **App registrations** and select the application.
2. Select **API permissions > Add a permission**.
3. Under **Microsoft APIs**, select **Azure Service Management**.

Request API permissions

Select an API

Microsoft APIs APIs my organization uses My APIs

Commonly used Microsoft APIs

Microsoft Graph

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



Azure Batch

Schedule large-scale parallel and HPC applications in the cloud

Azure Data Catalog

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

Azure Data Explorer

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

Azure Data Lake

Access to storage and compute for big data analytic scenarios

Azure DevOps

Integrate with Azure DevOps and Azure DevOps server

Azure Import/Export

Programmatic control of import/export jobs

Azure Key Vault

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

Azure Rights Management Services

Allow validated users to read and write protected content

Azure Service Management

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

Azure Storage

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

Customer Insights

Create profile and interaction models for your products

Data Export Service for Microsoft Dynamics 365

Export data from Microsoft Dynamics CRM organization to an external destination

4. Select **Access Azure Service Management as organization users** and then select **Add permissions**.

Request API permissions

[< All APIs](#)



Azure Service Management

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

What type of permissions does your application require?

Delegated permissions

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

Application permissions

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

Select permissions

[expand all](#)

Type to search

PERMISSION

ADMIN CONSENT REQUIRED

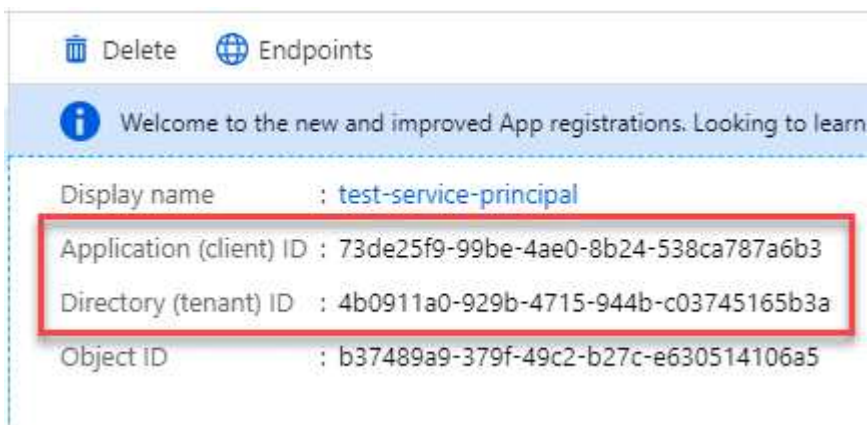


user_impersonation

Access Azure Service Management as organization users (preview) ⓘ

Get the application ID and directory ID for the application

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



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

Create a client secret

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

Client secrets

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

+ New client secret		
DESCRIPTION	EXPIRES	VALUE
test secret	8/16/2020	*sZ1jSe2By:D*-ZRoV4NLfdAcY7:+0vA

Copy to clipboard

You now have a client secret that BlueXP can use it to authenticate with Microsoft Entra ID.

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.

Google Cloud service account

Create a role and apply it to a service account that you'll use for the Connector VM instance.

Steps

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

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

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

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

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

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

Result

You now have a service account that you can assign to the Connector VM instance.

Step 7: Enable Google Cloud APIs

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

Step

1. [Enable the following Google Cloud APIs in your project](#)

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

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

Deploy the Connector in restricted mode

Deploy the Connector in restricted mode so that you can use BlueXP with limited outbound connectivity. To get started, install the Connector, set up BlueXP by accessing the user interface that's running on the Connector, and then provide the cloud permissions that you previously set up.

Step 1: Install the Connector

Install the Connector from your cloud provider's marketplace or by manually installing the software on your own Linux host.

AWS Commercial Marketplace

Before you begin

You should have the following:

- A VPC and subnet that meets networking requirements.

[Learn about networking requirements](#)

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

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

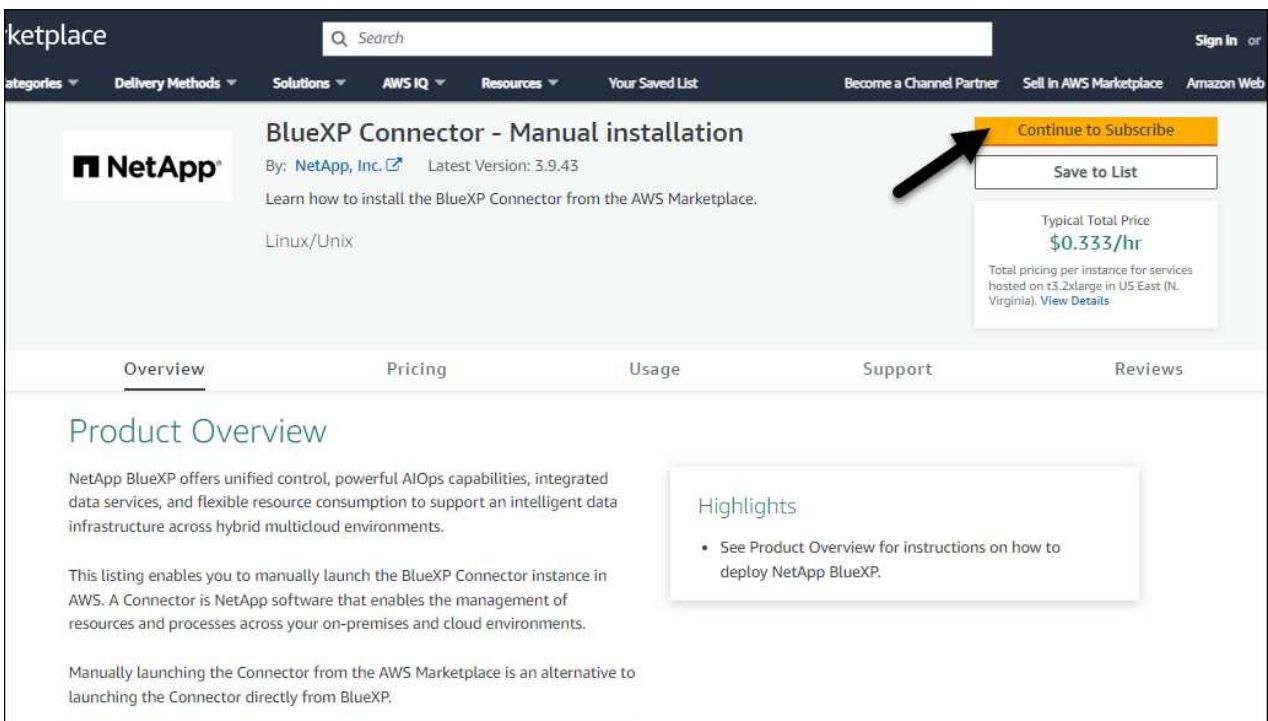
- Permissions to subscribe and unsubscribe from the AWS Marketplace for your IAM user.
- An understanding of CPU and RAM requirements for the instance.

[Review instance requirements.](#)

- A key pair for the EC2 instance.

Steps

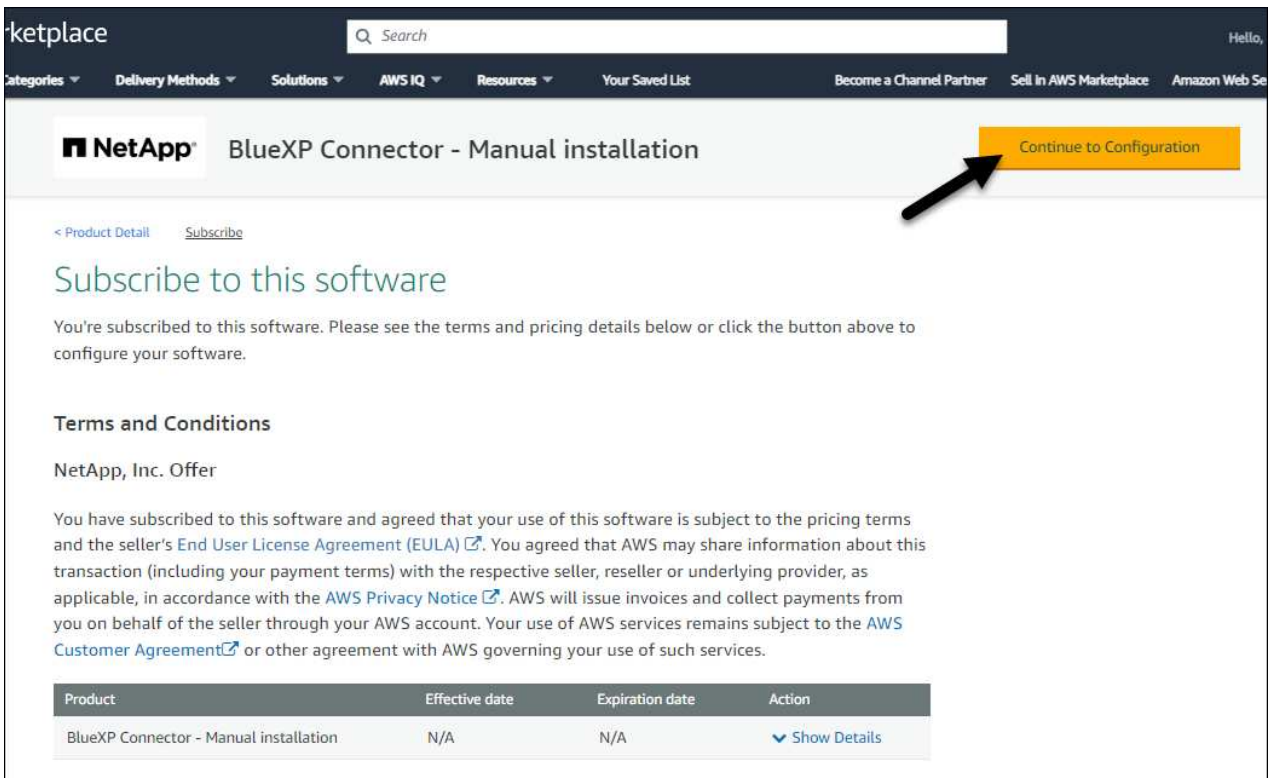
1. Go to the [BlueXP Connector listing on the AWS Marketplace](#)
2. On the Marketplace page, select **Continue to Subscribe**.



3. To subscribe to the software, select **Accept Terms**.

The subscription process can take a few minutes.

4. After the subscription process is complete, select **Continue to Configuration**.



5. On the **Configure this software** page, ensure that you've selected the correct region and then select **Continue to Launch**.
6. On the **Launch this software** page, under **Choose Action**, select **Launch through EC2** and then select **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.

7. Follow the prompts to configure and deploy the instance:
 - **Name and tags**: Enter a name and tags for the instance.
 - **Application and OS Images**: Skip this section. The Connector AMI is already selected.
 - **Instance type**: Depending on region availability, choose an instance type that meets RAM and CPU requirements (t3.2xlarge is preselected and recommended).
 - **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 security group settings that enable the required connection methods for the Connector instance: SSH, HTTP, and HTTPS.
 - [View security group rules for AWS.](#)
 - **Configure storage**: Keep the default size and disk type for the root volume.

If you want to enable Amazon EBS encryption on the root volume, select **Advanced**, expand **Volume 1**, select **Encrypted**, and then choose a KMS key.

- **Advanced details:** Under **IAM instance profile**, choose the IAM role that includes the required permissions for the Connector.
- **Summary:** Review the summary and select **Launch instance**.

Result

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

What's next?

Set up BlueXP.

AWS Gov Marketplace

Before you begin

You should have the following:

- A VPC and subnet that meets networking requirements.

[Learn about networking requirements](#)

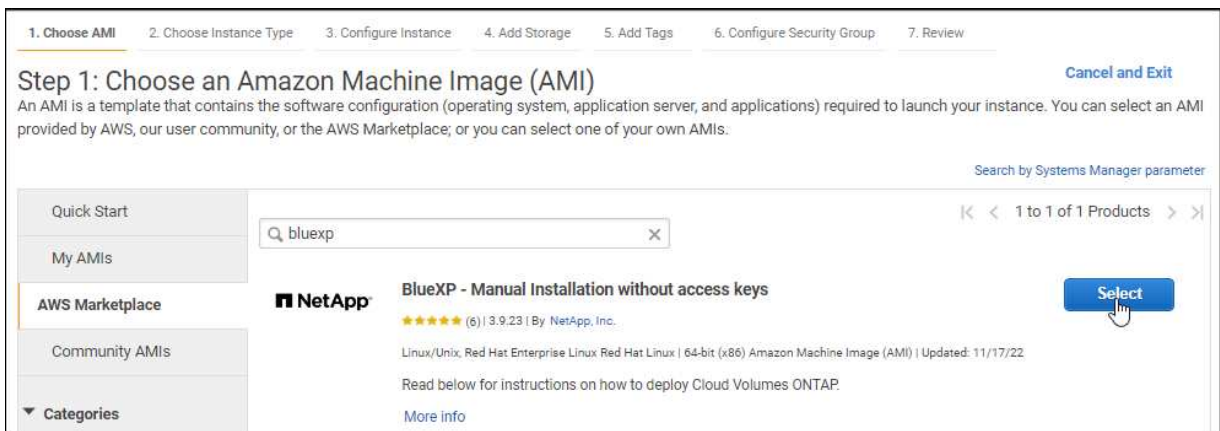
- An IAM role with an attached policy that includes the required permissions for the Connector.

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

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

Steps

1. Go to the BlueXP offering in the AWS Marketplace.
 - a. Open the EC2 service and select **Launch instance**.
 - b. Select **AWS Marketplace**.
 - c. Search for BlueXP and select the offering.



- d. Select **Continue**.
2. Follow the prompts to configure and deploy the instance:
 - **Choose an Instance Type:** Depending on region availability, choose one of the supported instance types (t3.2xlarge 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.

Number of instances	<input type="text" value="1"/>	Launch into Auto Scaling Group
Purchasing option	<input type="checkbox"/> Request Spot instances	
Network	<input type="text" value="vpc-a76d91c2 VPC4QA (default)"/>	Create new VPC
Subnet	<input type="text" value="subnet-39536c13 QASubnet1 us-east-1b"/> 155 IP Addresses available	Create new subnet
Auto-assign Public IP	<input type="text" value="Enable"/>	
Placement group	<input type="checkbox"/> Add instance to placement group	
Capacity Reservation	<input type="text" value="Open"/>	Create new Capacity Reservation
IAM role	<input type="text" value="Cloud_Manager"/>	Create new IAM role
CPU options	<input type="checkbox"/> Specify CPU options	
Shutdown behavior	<input type="text" value="Stop"/>	
Enable termination protection	<input checked="" type="checkbox"/> Protect against accidental termination	
Monitoring	<input type="checkbox"/> Enable CloudWatch detailed monitoring Additional charges apply.	

- **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 select **Launch**.

Result

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

What's next?

Set up BlueXP.

Azure Marketplace

Before you begin

You should have the following:

- A VNet and subnet that meets networking requirements.

[Learn about networking requirements](#)

- An Azure custom role that includes the required permissions for the Connector.

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

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

Note the following as you configure the VM:

- **VM size:** Choose a VM size that meets CPU and RAM requirements. We recommend Standard_D8s_v3.
- **Disks:** The Connector can perform optimally with either HDD or SSD disks.
- **Public IP:** If you want to use a public IP address with the Connector VM, the IP address must use a Basic SKU to ensure that BlueXP uses this public IP address.

If you use a Standard SKU IP address instead, then BlueXP uses the *private* IP address of the Connector, instead of the public IP. If the machine that you're using to access the BlueXP Console doesn't have access to that private IP address, then actions from the BlueXP Console will fail.

[Azure documentation: Public IP SKU](#)

- **Network security group:** The Connector requires inbound connections using SSH, HTTP, and HTTPS.

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

- **Identity:** Under **Management**, select **Enable system assigned managed identity**.

This setting is important because a managed identity allows the Connector virtual machine to identify itself to Microsoft Entra ID without providing any credentials. [Learn more about managed identities for Azure resources.](#)

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

Result

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

What's next?

Set up BlueXP.

Manual install

Before you begin

You should have the following:

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

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

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



You cannot set a certificate for a transparent proxy server when manually installing the Connector. If you need to set a certificate for a transparent proxy server, you must use the Maintenance Console after installation. Learn more about the [Connector Maintenance Console](#).

- Depending on your operating system, either Podman or Docker Engine is required before you install the Connector.

About this task

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

Steps

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

```
unset http_proxy
unset https_proxy
```

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

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

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

3. Assign permissions to run the script.

```
chmod +x BlueXP-Connector-Cloud-<version>
```

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

4. Run the installation script.

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

You'll need to add proxy information if your network requires a proxy for internet access. You can add either a transparent or explicit proxy. The `--proxy` and `--cacert` parameters are optional and you won't be prompted to add them. If you have a proxy server, you will need to enter the parameters as shown.

Here is an example configuring an explicit proxy server with a CA-signed certificate:

```
./BlueXP-Connector-Cloud-v3.9.40--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://user-name:password@address:port`
- `http://domain-name%92user-name:password@address:port`
- `https://address:port`
- `https://user-name:password@address:port`
- `https://domain-name%92user-name:password@address:port`

Note the following:

- The user can be a local user or domain user.
- For a domain user, you must use the ASCII code for a \ as shown above.
- BlueXP doesn't support user names or passwords that include the @ character.
- If the password includes any of the following special characters, you must escape that special character by prepending it with a backslash: & or !

For example:

```
http://bxpproxyuser:netapp1\!@address:3128
```

`--cacert` specifies a CA-signed certificate to use for HTTPS access between the Connector and the proxy server. This parameter is required for HTTPS proxy servers, intercepting proxy servers, and transparent proxy servers.

Here is an example configuring a transparent proxy server. When you configure a transparent proxy, you don't need to define the proxy server. You only add a CA-signed certificate to your Connector host:

```
./BlueXP-Connector-Cloud-v3.9.40 --cacert  
/tmp/cacert/certificate.cer
```

5. If you used Podman, you'll need to adjust the aardvark-dns port.
 - a. SSH to the BlueXP Connector virtual machine.
 - b. Open podman `/usr/share/containers/containers.conf` file and modify the chosen port for Aardvark DNS service. For example, change it to 54.

```
vi /usr/share/containers/containers.conf
...
# Port to use for dns forwarding daemon with netavark in rootful
bridge
# mode and dns enabled.
# Using an alternate port might be useful if other DNS services
should
# run on the machine.
#
dns_bind_port = 54
...
Esc:wq
```

- c. Reboot the Connector virtual machine.

Result

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

What's next?

Set up BlueXP.

Step 2: Set up BlueXP

When you access the BlueXP console for the first time, you'll be prompted to choose an account to associate the Connector with and you'll need to enable restricted mode.

Before you begin

The person who sets up the BlueXP Connector must log in to BlueXP using a login that doesn't belong to a BlueXP account or organization.

If your BlueXP login is associated with another account or organization, you'll need to sign up with a new BlueXP login. Otherwise, you won't see the option to enable restricted mode on the setup screen.

Steps

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

`https://ipaddress`
2. Sign up or log in to BlueXP.
3. After you're logged in, set up BlueXP:

- a. Enter a name for the Connector.
- b. Enter a name for a new BlueXP account.
- c. Select **Are you running in a secured environment?**
- d. Select **Enable restricted mode on this account.**

Note that you can't change this setting after BlueXP creates the account. You can't enable restricted mode later and you can't disable it later.

If you deployed the Connector in a Government region, the checkbox is already enabled and can't be changed. This is because restricted mode is the only mode supported in Government regions.

Hi Tami,
Welcome to NetApp BlueXP

Let's get started by creating an account for your organization.

If your organization already has an existing account, it's best to ask the account admin to add you to it. [Learn how to add user](#)

Connector name: BlueXP1

Account name: MyCompany

Are you running in a secured environment?

Use restricted deployment mode to disconnect this account from the BlueXP backend services. Restricted deployments are often required in extremely secure or regulated environments. Note: Use this option only if you're sure you need it as some BlueXP functionality is not available in restricted deployments.

[Learn more about BlueXP deployment modes](#)

☒ Enable restricted mode on this account

Let's start

- e. Select **Let's start.**

Result

The Connector is now installed and set up with your BlueXP account. All users need to access BlueXP using the IP address of the Connector instance.

What's next?

Provide BlueXP with the permissions that you previously set up.

Step 3: Provide permissions to BlueXP

If you deployed the Connector from the Azure Marketplace or if you manually installed the Connector software, you need to provide the permissions that you previously set up so that you can use BlueXP services.

These steps don't apply if you deployed the Connector from the AWS Marketplace because you chose the required IAM role during deployment.

[Learn how to prepare cloud permissions.](#)

AWS IAM role

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

These steps apply only if you manually installed the Connector in AWS. For AWS Marketplace deployments, you already associated the Connector instance with an IAM role that includes the required permissions.

Steps

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

Result

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

AWS access key

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

Steps

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



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

Result

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

Azure role

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

Steps

1. From the Azure Portal, open the **Subscriptions** service and select your subscription.

It's important to assign the role from the **Subscriptions** service because this specifies the scope of the role assignment at the subscription level. The *scope* defines the set of resources that the access applies to. If you specify a scope at a different level (for example, at the virtual machine level), your ability to complete actions from within BlueXP will be affected.

2. Select **Access control (IAM) > Add > Add role assignment**.
3. In the **Role** tab, select the **BlueXP Operator** role and select **Next**.



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

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

Result

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

Azure service principal

Provide BlueXP with the credentials for the Azure service principal that you previously setup.

Steps

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



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

Result

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

Google Cloud service account

Associate the service account with the Connector VM.

Steps

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

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

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

Result

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

Subscribe to NetApp Intelligent Services (restricted mode)

Subscribe to NetApp Intelligent Services from your cloud provider's marketplace to pay for data services at an hourly rate (PAYGO) or through an annual contract. If you purchased a license from NetApp (BYOL), you also need to subscribe to the marketplace offering. Your license is always charged first, but you'll be charged at the hourly rate if you exceed your licensed capacity or if the license's term expires.

A marketplace subscription enables charging for the following data services with restricted mode:

- Backup and recovery
- Cloud Volumes ONTAP
- Tiering
- Ransomware protection
- Disaster recovery

Classification is enabled through your subscription, but there is no charge for using classification.

Before you begin

Subscribing to data services involves associating a marketplace subscription with the cloud credentials that are associated with a Connector. If you followed the "Get started with restricted mode" workflow, then you should already have a Connector. To learn more, view the [Quick start for BlueXP in restricted mode](#).

AWS

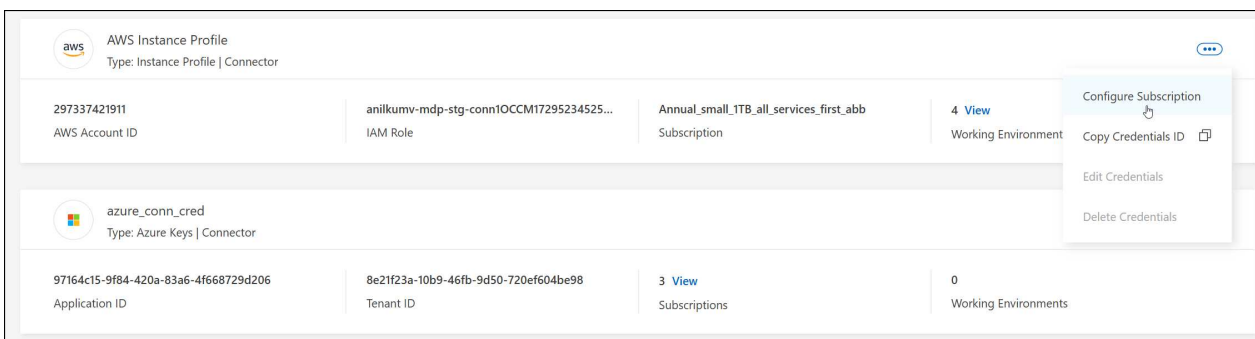
The following video shows the steps to subscribe to NetApp Intelligent Services from the AWS Marketplace:

Subscribe to NetApp Intelligent Services from the AWS Marketplace

Steps

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

You must select credentials that are associated with a Connector. You can't associate a marketplace subscription with credentials that are associated with BlueXP.



3. To associate the credentials with an existing subscription, select the subscription from the down-down list and select **Configure**.
4. To associate the credentials with a new subscription, select **Add Subscription > Continue** and follow the steps in the AWS Marketplace:
 - a. Select **View purchase options**.
 - b. Select **Subscribe**.
 - c. Select **Set up your account**.

You'll be redirected to the BlueXP website.

- d. From the **Subscription Assignment** page:
 - Select the BlueXP organizations or accounts that you'd like to associate this subscription with.
 - In the **Replace existing subscription** field, choose whether you'd like to automatically replace the existing subscription for one organization or account with this new subscription.

BlueXP replaces the existing subscription for all credentials in the organization or account with this new subscription. If a set of credentials wasn't ever associated with a subscription, then this new subscription won't be associated with those credentials.

For all other organizations or accounts, you'll need to manually associate the subscription by repeating these steps.

- Select **Save**.

Azure Steps

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

You must select credentials that are associated with a Connector. You can't associate a marketplace subscription with credentials that are associated with BlueXP.

3. To associate the credentials with an existing subscription, select the subscription from the down-down list and select **Configure**.
4. To associate the credentials with a new subscription, select **Add Subscription > Continue** and follow the steps in the Azure Marketplace:
 - a. If prompted, log in to your Azure account.
 - b. Select **Subscribe**.
 - c. Fill out the form and select **Subscribe**.
 - d. After the subscription process is complete, select **Configure account now**.

You'll be redirected to BlueXP.

- e. From the **Subscription Assignment** page:
 - Select the BlueXP organizations or accounts that you'd like to associate this subscription with.
 - In the **Replace existing subscription** field, choose whether you'd like to automatically replace the existing subscription for one organization or account with this new subscription.

BlueXP replaces the existing subscription for all credentials in the organization or account with this new subscription. If a set of credentials wasn't ever associated with a subscription, then this new subscription won't be associated with those credentials.

For all other organizations or accounts, you'll need to manually associate the subscription by repeating these steps.

- Select **Save**.

The following video shows the steps to subscribe from the Azure Marketplace:

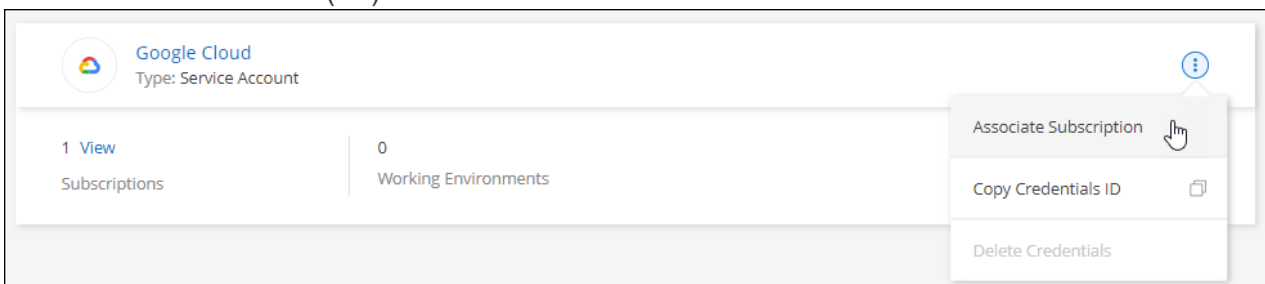
[Subscribe to NetApp Intelligent Services from the Azure Marketplace](#)

Google Cloud

Steps

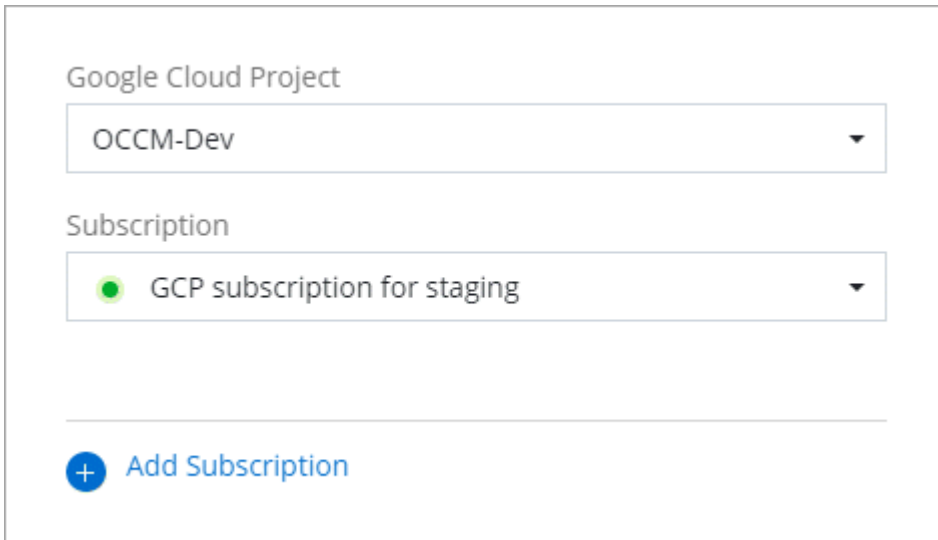
1. In the upper right of the console, select the Settings icon, and select **Credentials**.
2. Select the action menu for a set of credentials and then select **Configure Subscription**.

+new screenshot needed (TS)



3. To configure an existing subscription with the selected credentials, select a Google Cloud project and

subscription from the drop-down list, and then select **Configure**.



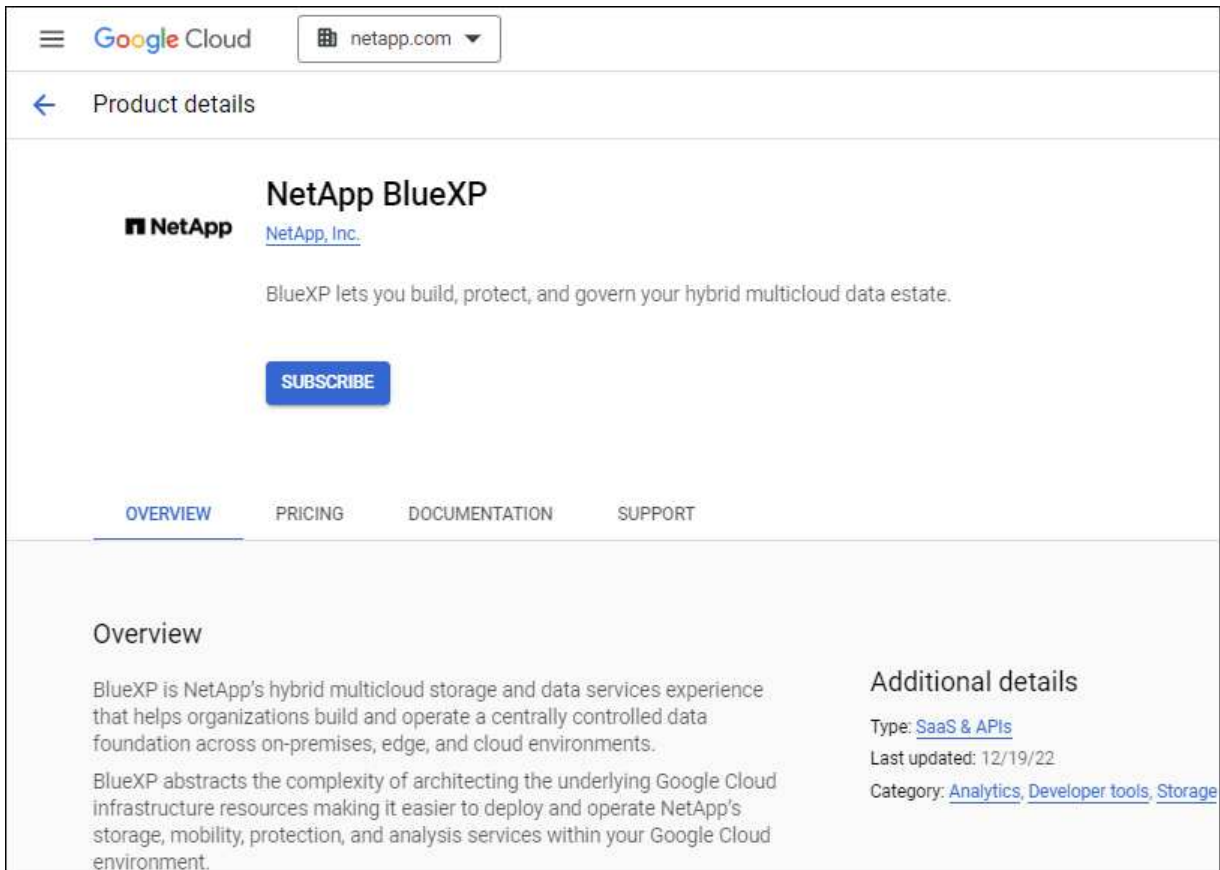
The screenshot shows a configuration interface for Google Cloud. At the top, under the heading "Google Cloud Project", there is a dropdown menu with "OCCM-Dev" selected. Below this, under the heading "Subscription", there is another dropdown menu with "GCP subscription for staging" selected, preceded by a green circular icon. At the bottom of the interface, there is a blue button with a plus sign and the text "Add Subscription".

4. If you don't already have a subscription, select **Add Subscription > Continue** and follow the steps in the Google Cloud Marketplace.



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.

- a. After you're redirected to the [NetApp Intelligent Services page on the Google Cloud Marketplace](#), ensure that the correct project is selected at the top navigation menu.



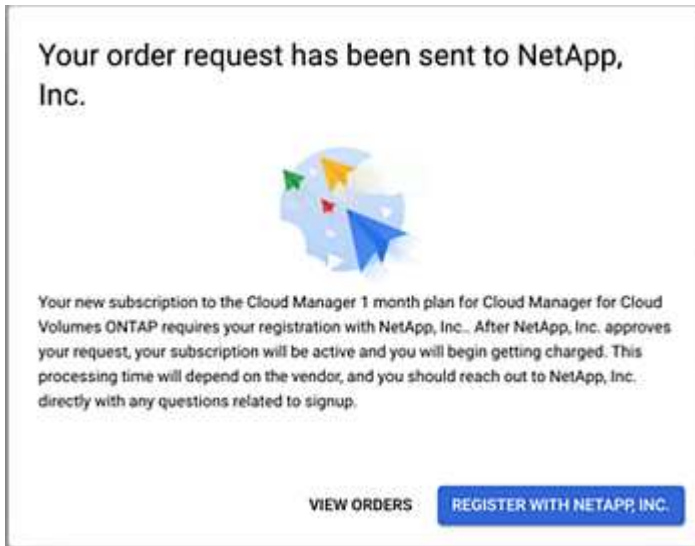
The screenshot displays the "Product details" page for NetApp BlueXP on the Google Cloud Marketplace. The top navigation bar includes the Google Cloud logo and a dropdown menu showing "netapp.com". Below the navigation bar, the page title "Product details" is followed by the NetApp logo and the product name "NetApp BlueXP". A link to "NetApp, Inc." is provided. A description states: "BlueXP lets you build, protect, and govern your hybrid multicloud data estate." A prominent blue "SUBSCRIBE" button is visible. Below this, there are tabs for "OVERVIEW", "PRICING", "DOCUMENTATION", and "SUPPORT", with "OVERVIEW" currently selected. The "Overview" section contains two paragraphs: "BlueXP is NetApp's hybrid multicloud storage and data services experience that helps organizations build and operate a centrally controlled data foundation across on-premises, edge, and cloud environments." and "BlueXP abstracts the complexity of architecting the underlying Google Cloud infrastructure resources making it easier to deploy and operate NetApp's storage, mobility, protection, and analysis services within your Google Cloud environment." To the right, under "Additional details", it lists the type as "SaaS & APIs", the last updated date as "12/19/22", and the category as "Analytics, Developer tools, Storage".

- b. Select **Subscribe**.
- c. Select the appropriate billing account and agree to the terms and conditions.
- d. Select **Subscribe**.

This step sends your transfer request to NetApp.

- e. On the pop-up dialog box, select **Register with NetApp, Inc.**

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



- f. Complete the steps on the **Subscription Assignment** page:



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.

- Select the BlueXP organizations or accounts that you'd like to associate this subscription with.
- In the **Replace existing subscription** field, choose whether you'd like to automatically replace the existing subscription for one organization or account with this new subscription.

BlueXP replaces the existing subscription for all credentials in the organization or account with this new subscription. If a set of credentials wasn't ever associated with a subscription, then this new subscription won't be associated with those credentials.

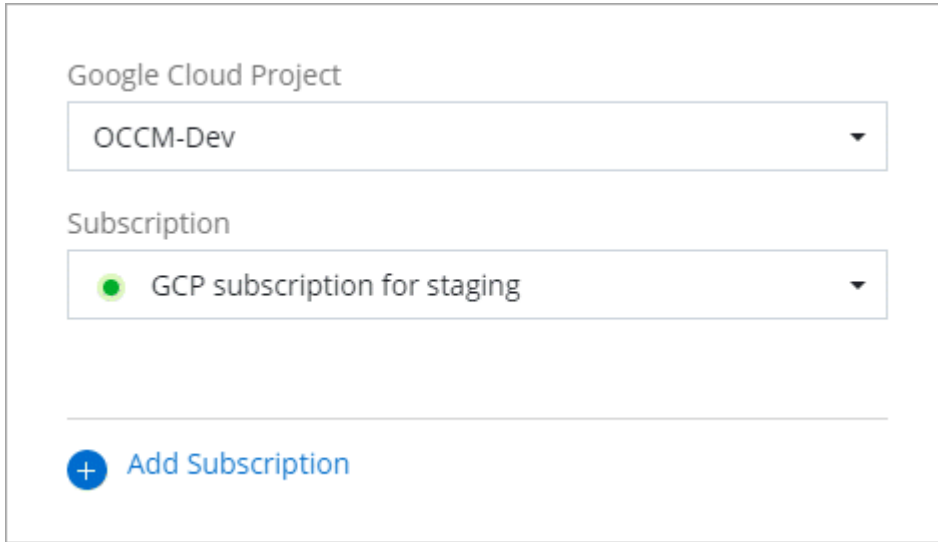
For all other organizations or accounts, you'll need to manually associate the subscription by repeating these steps.

- Select **Save**.

The following video shows the steps to subscribe from the Google Cloud Marketplace:

[Subscribe to BlueXP from the Google Cloud Marketplace](#)

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



The screenshot shows a web interface for selecting Google Cloud credentials. It features two dropdown menus. The first, labeled 'Google Cloud Project', has 'OCCM-Dev' selected. The second, labeled 'Subscription', has 'GCP subscription for staging' selected, which is preceded by a small green circle icon. Below these menus is a horizontal line and a button with a blue plus icon and the text 'Add Subscription'.

Related information

- [Manage BYOL capacity-based licenses for Cloud Volumes ONTAP](#)
- [Manage BYOL licenses for data services](#)
- [Manage AWS credentials and subscriptions](#)
- [Manage Azure credentials and subscriptions](#)
- [Manage Google Cloud credentials and subscriptions](#)

What you can do next (restricted mode)

After you get up and running with BlueXP in restricted mode, you can start using the BlueXP services that are supported with restricted mode.

For help, refer to the documentation for these services:

- [Azure NetApp Files docs](#)
- [Backup and recovery docs](#)
- [Classification docs](#)
- [Cloud Volumes ONTAP docs](#)
- [Digital wallet docs](#)
- [On-premises ONTAP cluster docs](#)
- [Replication docs](#)

Related information

[BlueXP deployment modes](#)

Get started with private mode

Getting started workflow (private mode)

Get started with BlueXP in private mode by preparing your environment and deploying the Connector.

Private mode is typically used with on-premises environments that have no internet connection and with secure cloud regions, which includes [AWS Secret Cloud](#), [AWS Top Secret Cloud](#), and [Azure IL6](#)

Before you get started, you should have an understanding of [Connectors](#) and [deployment modes](#).

1

Prepare for deployment

- a. Prepare a dedicated Linux host that meets requirements for CPU, RAM, disk space, container orchestration tool, and more.
- b. Set up networking that provides access to the target networks.
- c. For cloud deployments, set up permissions in your cloud provider so that you can associate those permissions with the Connector after you install the software.

2

Deploy the Connector

- a. Install the Connector software on your own Linux host.
- b. Set up BlueXP by opening a web browser and entering the Linux host's IP address.
- c. For cloud deployments, provide BlueXP with the permissions that you previously set up.

Prepare for deployment in private mode

Prepare your environment before you deploy BlueXP in private mode. For example, you need to review host requirements, prepare networking, set up permissions, and more.



To use BlueXP in the [AWS Secret Cloud](#) or the [AWS Top Secret Cloud](#), follow the specific instructions for those environments. [Learn how to get started with Cloud Volumes ONTAP in the AWS Secret Cloud or Top Secret Cloud](#)

Step 1: Understand how private mode works

Before you get started, you should understand private mode.

For example, you need to use the browser-based interface that is available locally from the Connector that you install. You can't access BlueXP from the web-based console that's provided through the SaaS layer.

In addition, not all features and services are available.

[Learn how private mode works.](#)

Step 2: Review installation options

In private mode, you can install the Connector on-premises or in the cloud by manually installing the Connector on your own Linux host.

Where you install the Connector determines which BlueXP services and features are available when using private mode. For example, the Connector must be installed in the cloud if you want to deploy and manage Cloud Volumes ONTAP. [Learn more about private mode.](#)

Step 3: Review host requirements

The host must meet specific operating system requirements, RAM requirements, port requirements, and so on to run the Connector software.

Dedicated host

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

Host can be of any architecture that meets the following size requirements:

- CPU: 8 cores or 8 vCPUs
- RAM: 32 GB

Operating system and container requirements

BlueXP supports the Connector with the following operating systems when using BlueXP in private mode. A container orchestration tool is required before you install the Connector.

Operating system	Supported OS versions	Supported Connector versions	Required container tool	SELinux
Red Hat Enterprise Linux	9.1 to 9.4 8.6 to 8.10	3.9.42 or later with BlueXP in private mode	Podman version 4.6.1 or 4.9.4 View Podman configuration requirements.	Supported in enforcing mode or permissive mode ¹
Ubuntu	22.04 LTS	3.9.29 or later	Docker Engine 23.0.6 to 26.0.0 26.0.0 is supported with <i>new</i> Connector 3.9.44 or later installations	Not supported

Notes:

1. Management of Cloud Volumes ONTAP systems is not supported by Connectors that have SELinux enabled on the operating system.
2. The Connector is supported on English-language versions of these operating systems.
3. For RHEL, the host must be registered with Red Hat Subscription Management. If it's not registered, the

host can't access repositories to update required 3rd-party software during Connector installation.

Hypervisor

A bare metal or hosted hypervisor that is certified to run a supported operating system is required.

CPU

8 cores or 8 vCPUs

RAM

32 GB

AWS EC2 instance type

An instance type that meets the CPU and RAM requirements above. We recommend t3.2xlarge.

Azure VM size

An instance type that meets the CPU and RAM requirements above. We recommend Standard_D8s_v3.

Google Cloud machine type

An instance type that meets the CPU and RAM requirements above. We recommend n2-standard-8.

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

Disk space in /opt

100 GiB of space must be available

BlueXP uses /opt to install the /opt/application/netapp directory and its contents.

Disk space in /var

20 GiB of space must be available

BlueXP requires this space in /var because Docker or Podman are architected to create the containers within this directory. Specifically, they will create containers in the /var/lib/containers/storage directory. External mounts or symlinks do not work for this space.

Step 4: Install Podman or Docker Engine

You need to prepare the host for the Connector by installing Podman or Docker Engine.

Depending on your operating system, either Podman or Docker Engine is required before you install the Connector.

- Podman is required for Red Hat Enterprise Linux 8 and 9.

[View the Podman versions that BlueXP supports.](#)

- Docker Engine is required for Ubuntu.

[View the Docker Engine versions that BlueXP supports.](#)

Example 6. Steps

Podman

Follow these steps to install Podman and configure it to meet the following requirements:

- Enable and start the podman.socket service
- Install python3
- Install the podman-compose package version 1.0.6
- Add podman-compose to the PATH environment variable



When using Podman, adjust the aardvark-dns service port (default: 53) after installing the Connector to avoid conflicts with the DNS port on the host. Follow the instructions to configure the port.

Steps

1. Remove the podman-docker package if it's installed on the host.

```
dnf remove podman-docker
rm /var/run/docker.sock
```

2. Install Podman.

Podman is available from official Red Hat Enterprise Linux repositories.

For Red Hat Enterprise Linux 9:

```
sudo dnf install podman-2:<version>
```

Where <version> is the supported version of Podman that you're installing. [View the Podman versions that BlueXP supports.](#)

For Red Hat Enterprise Linux 8:

```
sudo dnf install podman-3:<version>
```

Where <version> is the supported version of Podman that you're installing. [View the Podman versions that BlueXP supports.](#)

3. Enable and start the podman.socket service.

```
sudo systemctl enable --now podman.socket
```

4. Install python3.

```
sudo dnf install python3
```

5. Install the EPEL repository package if it's not already available on your system.

This step is required because podman-compose is available from the Extra Packages for Enterprise Linux (EPEL) repository.

For Red Hat Enterprise Linux 9:

```
sudo dnf install https://dl.fedoraproject.org/pub/epel/epel-release-latest-9.noarch.rpm
```

For Red Hat Enterprise Linux 8:

```
sudo dnf install https://dl.fedoraproject.org/pub/epel/epel-release-latest-8.noarch.rpm
```

6. Install podman-compose package 1.0.6.

```
sudo dnf install podman-compose-1.0.6
```



Using the `dnf install` command meets the requirement for adding podman-compose to the PATH environment variable. The installation command adds podman-compose to `/usr/bin`, which is already included in the `secure_path` option on the host.

Docker Engine

Follow the documentation from Docker to install Docker Engine.

Steps

1. [View installation instructions from Docker](#)

Be sure to follow the steps to install a specific version of Docker Engine. Installing the latest version will install a version of Docker that BlueXP doesn't support.

2. Verify that Docker is enabled and running.

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

Step 5: Prepare networking

Set up networking for the Connector to manage resources in your public cloud. Other than having a virtual network and subnet for the Connector, ensure that the following requirements are met.

Connections to target networks::

The Connector must have a network connection to the location where you plan to manage storage. For example, the VPC or VNet where you plan to deploy Cloud Volumes ONTAP, or the data center where your on-premises ONTAP clusters reside.

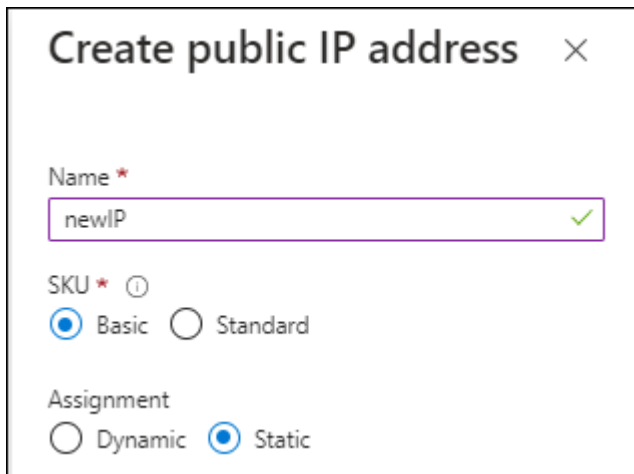
Endpoints for day-to-day operations

If you are planning to create Cloud Volumes ONTAP systems, the Connector needs connectivity to endpoints in your cloud provider's publicly available resources.

Endpoints	Purpose
AWS services (amazonaws.com): <ul style="list-style-type: none">• CloudFormation• Elastic Compute Cloud (EC2)• Identity and Access Management (IAM)• Key Management Service (KMS)• Security Token Service (STS)• Simple Storage Service (S3)	To manage resources in AWS. The exact endpoint depends on the AWS region that you're using. Refer to AWS documentation for details
https://management.azure.com https://login.microsoftonline.com https://blob.core.windows.net https://core.windows.net	To manage resources in Azure public regions.
https://management.azure.microsoft.scloud https://login.microsoftonline.microsoft.scloud https://blob.core.microsoft.scloud https://core.microsoft.scloud	To manage resources in the Azure IL6 region.
https://management.chinacloudapi.cn https://login.chinacloudapi.cn https://blob.core.chinacloudapi.cn https://core.chinacloudapi.cn	To manage resources in Azure China regions.
https://www.googleapis.com/compute/v1/ https://compute.googleapis.com/compute/v1 https://cloudresourcemanager.googleapis.com/v1/projects https://www.googleapis.com/compute/beta https://storage.googleapis.com/storage/v1 https://www.googleapis.com/storage/v1 https://iam.googleapis.com/v1 https://cloudkms.googleapis.com/v1 https://www.googleapis.com/deploymentmanager/v2/projects	To manage resources in Google Cloud.

Public IP address in Azure

If you want to use a public IP address with the Connector VM in Azure, the IP address must use a Basic SKU to ensure that BlueXP uses this public IP address.



Create public IP address ✕

Name *
newIP ✓

SKU * ⓘ
☒ Basic ☐ Standard

Assignment
☐ Dynamic ☒ Static

If you use a Standard SKU IP address instead, then BlueXP uses the *private* IP address of the Connector, instead of the public IP. If the machine that you're using to access the BlueXP Console doesn't have access to that private IP address, then actions from the BlueXP Console will fail.

[Azure documentation: Public IP SKU](#)

Proxy server

NetApp supports both explicit and transparent proxy configurations. If you are using a transparent proxy, you only need to provide the certificate for the proxy server. If you are using an explicit proxy, you'll also need the IP address and credentials.

- IP address
- Credentials
- HTTPS certificate

With private mode, the only time that BlueXP sends outbound traffic is to your cloud provider in order to create a Cloud Volumes ONTAP system.

Ports

There's no incoming traffic to the Connector, unless you initiate it.

HTTP (80) and HTTPS (443) provide access to the BlueXP console. SSH (22) is only needed if you need to connect to the host for troubleshooting.

Enable NTP

If you're planning to use BlueXP classification to scan your corporate data sources, you should enable a Network Time Protocol (NTP) service on both the BlueXP Connector system and the BlueXP classification system so that the time is synchronized between the systems. [Learn more about BlueXP classification](#)

Step 6: Prepare cloud permissions

If the Connector is installed in the cloud and you plan to create Cloud Volumes ONTAP systems, BlueXP requires cloud provider permissions. You need to set up permissions in your cloud provider and then associate those permission with the Connector instance after you install it.

To view the required steps, select the authentication option that you'd like to use for your cloud provider.

AWS IAM role

Use an IAM role to provide the Connector with permissions. You'll need to manually attach the role to the EC2 instance for the Connector.

Steps

1. Log in to the AWS console and navigate to the IAM service.
2. Create a policy:
 - a. Select **Policies > Create policy**.
 - b. Select **JSON** and copy and paste the contents of the [IAM policy for the Connector](#).
 - c. Finish the remaining steps to create the policy.
3. Create an IAM role:
 - a. Select **Roles > Create role**.
 - b. Select **AWS service > EC2**.
 - c. Add permissions by attaching the policy that you just created.
 - d. Finish the remaining steps to create the role.

Result

You now have an IAM role for the Connector EC2 instance.

AWS access key

Set up permissions and an access key for an IAM user. Provide BlueXP with the AWS access key after you install the Connector and set up BlueXP.

Steps

1. Log in to the AWS console and navigate to the IAM service.
2. Create a policy:
 - a. Select **Policies > Create policy**.
 - b. Select **JSON** and copy and paste the contents of the [IAM policy for the Connector](#).
 - c. Finish the remaining steps to create the policy.

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

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

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

Result

The account now has the required permissions.

Azure role

Create an Azure custom role with the required permissions. Assign this role to the Connector VM.

Note that you can create an Azure custom role using the Azure portal, Azure PowerShell, Azure CLI, or REST API. The following steps show how to create the role using the Azure CLI. If you would prefer to use a different method, refer to [Azure documentation](#)

Steps

1. Enable a system-assigned managed identity on the VM where you plan to install the Connector so that you can provide the required Azure permissions through a custom role.

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

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

You should add the ID for each Azure subscription that you want to use with BlueXP.

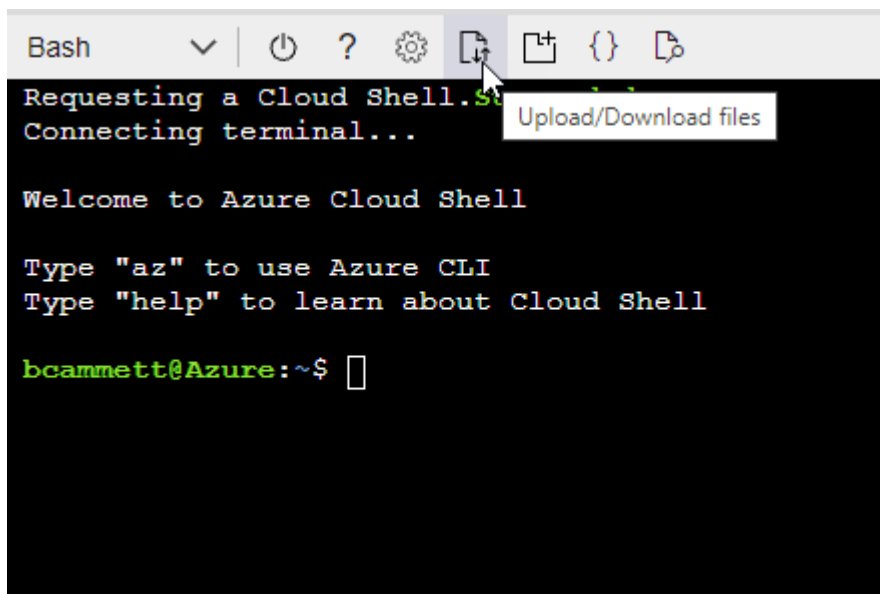
Example

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

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

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

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



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

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

Result

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

Azure service principal

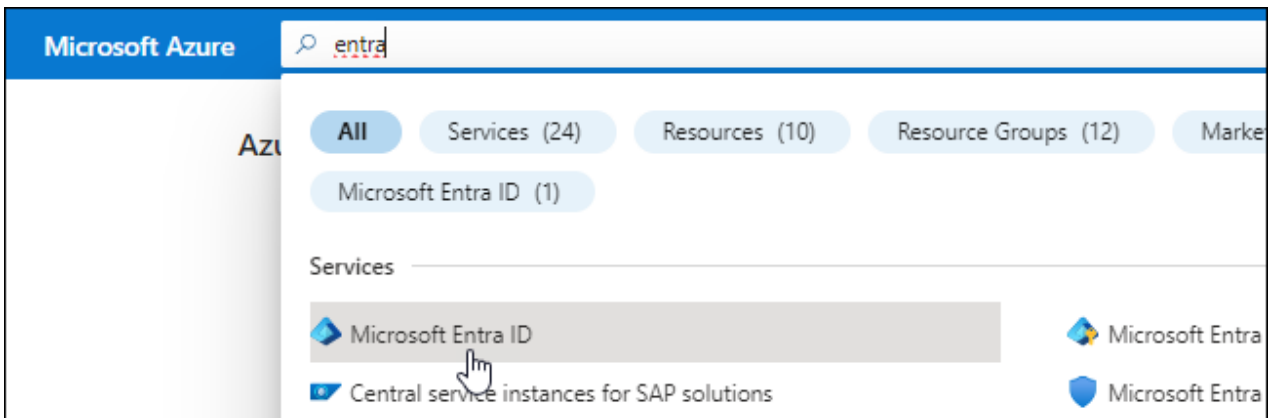
Create and set up a service principal in Microsoft Entra ID and obtain the Azure credentials that BlueXP needs. You'll need to provide BlueXP with these credentials after you install the Connector and set up BlueXP.

Create a Microsoft Entra application for role-based access control

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

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

2. From the Azure portal, open the **Microsoft Entra ID** service.



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

You've created the AD application and service principal.

Assign the application to a role

1. Create a custom role:

Note that you can create an Azure custom role using the Azure portal, Azure PowerShell, Azure CLI,

or REST API. The following steps show how to create the role using the Azure CLI. If you would prefer to use a different method, refer to [Azure documentation](#)

- 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.

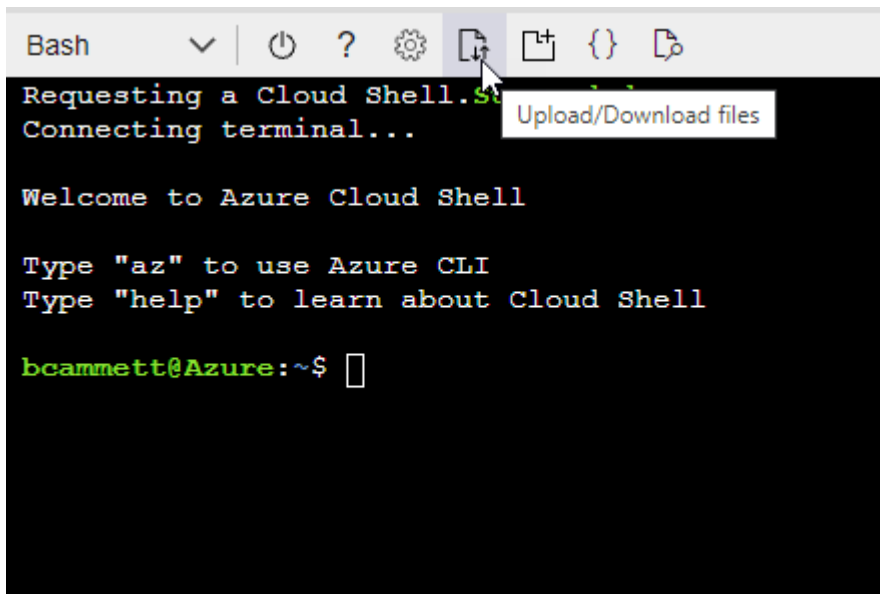
Example

```
"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.

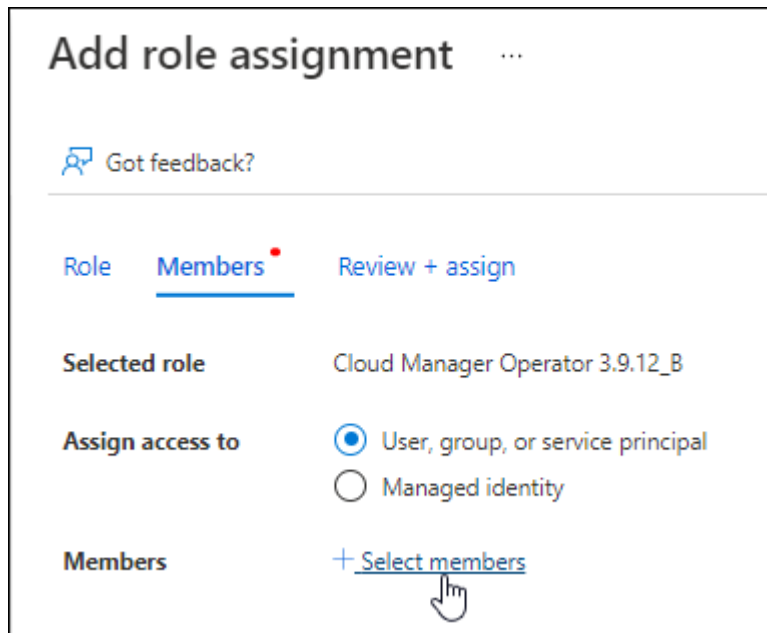


- Use the Azure CLI to create the custom role:

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

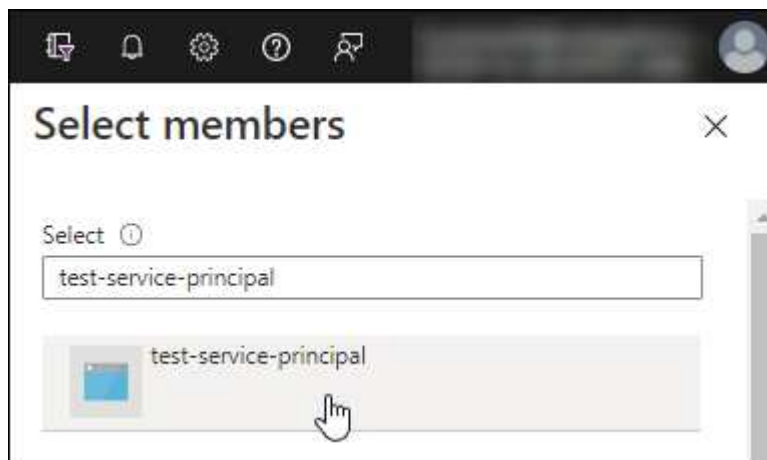
You should now have a custom role called BlueXP Operator that you can assign to the Connector virtual machine.

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



- Search for the name of the application.

Here's an example:



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

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

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

Add Windows Azure Service Management API permissions

1. In the **Microsoft Entra ID** service, select **App registrations** and select the application.
2. Select **API permissions > Add a permission**.
3. Under **Microsoft APIs**, select **Azure Service Management**.


Request API permissions


Select an API


Microsoft APIs [APIs my organization uses](#) [My APIs](#)


Commonly used Microsoft APIs


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





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


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


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


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


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


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


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

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

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

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

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

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

4. Select **Access Azure Service Management as organization users** and then select **Add permissions**.

Request API permissions

[< All APIs](#)



Azure Service Management

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

What type of permissions does your application require?

Delegated permissions

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

Application permissions

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

Select permissions

[expand all](#)

Type to search

PERMISSION

ADMIN CONSENT REQUIRED

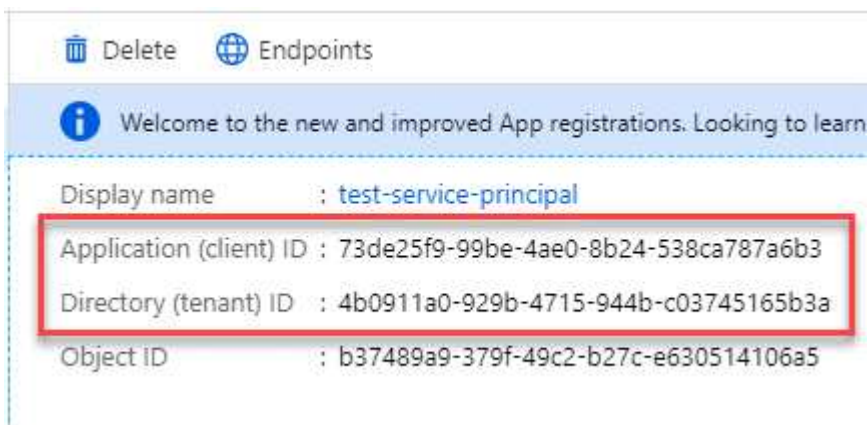


user_impersonation

Access Azure Service Management as organization users (preview) ⓘ

Get the application ID and directory ID for the application

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



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

Create a client secret

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

Client secrets

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

+ New client secret		
DESCRIPTION	EXPIRES	VALUE
test secret	8/16/2020	*sZ1jSe2By:D*-ZRoV4NLfdAcY7:+0vA

Copy to clipboard

You now have a client secret that BlueXP can use it to authenticate with Microsoft Entra ID.

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. Enter this information in BlueXP when you add an Azure account.

Google Cloud service account

Create a role and apply it to a service account that you'll use for the Connector VM instance.

Steps

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

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

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

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

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

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

Result

You now have a service account that you can assign to the Connector VM instance.

Step 7: Enable Google Cloud APIs

You need to enable several APIs to deploy Cloud Volumes ONTAP in Google Cloud.

Step

1. [Enable the following Google Cloud APIs in your project](#)

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

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

Deploy the Connector in private mode

Deploy the Connector in private mode so that you can use BlueXP with no outbound connectivity to the BlueXP software as a service (SaaS) layer. To get started, install the Connector, set up BlueXP by accessing the user interface that's running on the Connector, and then provide the cloud permissions that you previously set up.

Step 1: Install the Connector

Download the product installer from the [NetApp Support Site](#) and then manually install the Connector on your own Linux host.

If you want to use BlueXP in the [AWS Secret Cloud](#) or the [AWS Top Secret Cloud](#), then you should follow separate instructions to get started in those environments. [Learn how to get started with Cloud Volumes ONTAP in the AWS Secret Cloud or Top Secret Cloud](#)

Before you begin

- Root privileges are required to install the Connector.
- Depending on your operating system, either Podman or Docker Engine is required before you install the Connector.

Steps

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

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

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

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

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

4. Run the installation script:

```
sudo /path/BlueXP-Connector-offline-<version>
```

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

Result

The Connector software is installed. You can now set up BlueXP.

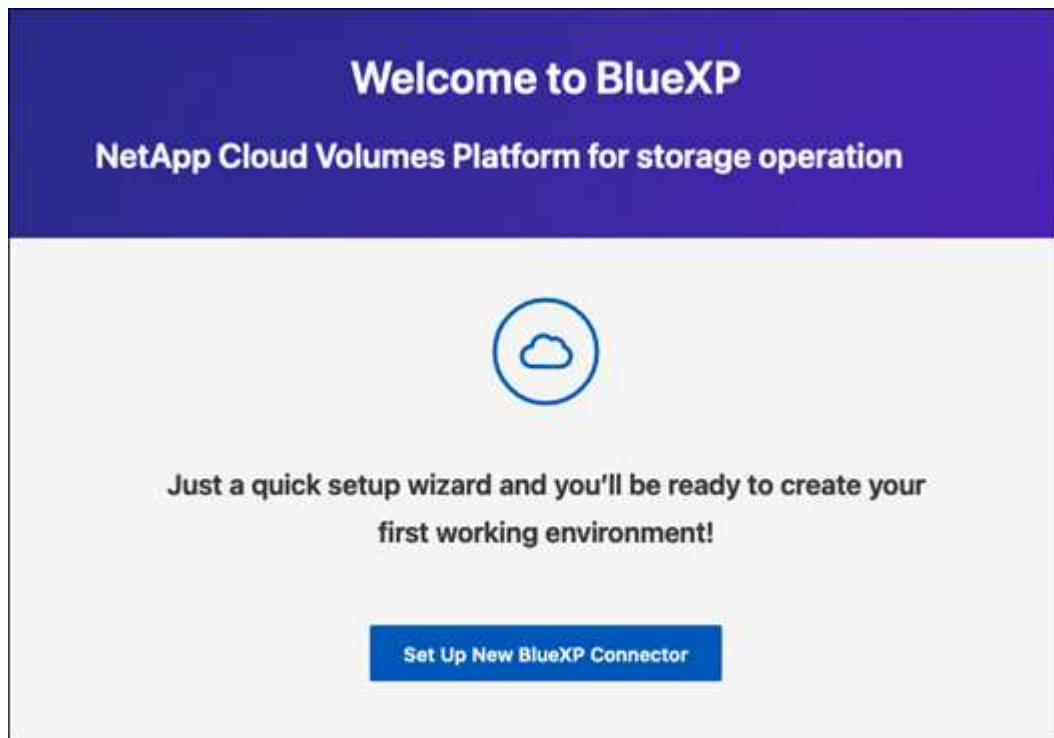
Step 2: Set up BlueXP

When you access the BlueXP console for the first time, you'll be prompted to set up BlueXP.

Steps

1. Open a web browser and enter `https://ipaddress` where *ipaddress* is the IP address of the Linux host where you installed the Connector.

You should see the following screen.



2. Select **Set Up New BlueXP Connector** and follow the prompts to set up the system.
 - **System Details:** Enter a name for the Connector and your company name.

The screenshot shows a web interface for the BlueXP Connector setup. At the top, there are three steps: 1 System Details (active), 2 Create Admin User, and 3 Review. The main heading is "System Details". Below it, a message says: "To help us provide better support, enter a name for BlueXP Connector and your company name." There are two input fields: "BlueXP Connector Name" with the value "aug27-dark-site-karana" and "Company Name" with the value "netapp".

- **Create an 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 select **Set Up**.

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

Result

The Connector is now installed and set up.

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

What's next?

Provide BlueXP with the permissions that you previously set up.

Step 3: Provide permissions to BlueXP

If you want to create Cloud Volumes ONTAP working environments, you'll need to provide BlueXP with the cloud permissions that you previously set up.

[Learn how to prepare cloud permissions.](#)

AWS IAM role

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

Steps

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

Result

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

AWS access key

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

Steps

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



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

Result

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

Azure role

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

Steps

1. From the Azure Portal, open the **Subscriptions** service and select your subscription.

It's important to assign the role from the **Subscriptions** service because this specifies the scope of the role assignment at the subscription level. The *scope* defines the set of resources that the access applies to. If you specify a scope at a different level (for example, at the virtual machine level), your ability to complete actions from within BlueXP will be affected.

[Microsoft Azure documentation: Understand scope for Azure RBAC](#)

2. Select **Access control (IAM) > Add > Add role assignment**.

3. In the **Role** tab, select the **BlueXP Operator** role and select **Next**.



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

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

Result

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

Azure service principal

Provide BlueXP with the credentials for the Azure service principal that you previously setup.

Steps

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



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

Result

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

Google Cloud service account

Associate the service account with the Connector VM.

Steps

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

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

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

Result

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

What you can do next (private mode)

After you get up and running with BlueXP in private mode, you can start using the BlueXP services that are supported with private mode.

For help, refer to the following documentation:

- [Discover on-premises ONTAP clusters](#)
- [Manage software updates](#)
- [Scan on-premises ONTAP volume data using BlueXP classification](#)
- [Monitor license usage with digital wallet](#)
- [View storage health information with digital advisor](#)

Use BlueXP

Log in to BlueXP

How you log in to BlueXP depends on the BlueXP deployment mode that you're using for your account.

[Learn about BlueXP deployment modes.](#)

Standard mode

After you sign up to BlueXP, you can log in from the web-based console to start managing your data and storage infrastructure.

About this task

You can log in to the BlueXP web-based console using one of the following options:

- Your existing NetApp Support Site (NSS) credentials
- A NetApp cloud login using your email address and a password
- A federated connection

You can use single sign-on to log in using credentials from your corporate directory (federated identity). [Learn how to use identity federation with BlueXP.](#)

Steps

1. Open a web browser and go to the [BlueXP console](#)
2. On the **Log in** page, enter the email address that's associated with your login.
3. Depending on the authentication method associated with your login, you'll be prompted to enter your credentials:
 - NetApp cloud credentials: Enter your password
 - Federated user: Enter your federated identity credentials
 - NetApp Support Site account: Enter your NetApp Support Site credentials

Result

You're now logged in and can start using BlueXP to manage your hybrid multi-cloud infrastructure.

Restricted mode

When you use BlueXP in restricted mode, you need to log in to the BlueXP console from the user interface that runs locally on the Connector.

About this task

BlueXP supports logging in with one of the following options when your account is set up in restricted mode:

- A NetApp cloud login using your email address and a password
- A federated connection

You can use single sign-on to log in using credentials from your corporate directory (federated identity). [Learn how to use identity federation with BlueXP.](#)

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 where you installed the Connector. For example, you might need to 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.

Result

You're now logged in and can start using BlueXP to manage your hybrid multi-cloud infrastructure.

Private mode

When you use BlueXP in private mode, you need to log in to the BlueXP console from the user interface that runs locally on the Connector.

About this task

Private mode supports local user management and access. Authentication is not provided through BlueXP's cloud service.

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 where you installed the Connector. For example, you might need to 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.

Result

You're now logged in and can start using BlueXP to manage your hybrid multi-cloud infrastructure.

Manage your BlueXP user settings

You can modify your BlueXP profile including change your password, enable multi-factor authentication (MFA), and see who your BlueXP administrator is.

Within BlueXP, each user has a profile that contains information about the user and their settings. You can view and edit your profile settings.

Change your display name

You can change your display name. The display name is used to identify you in the BlueXP console and is visible to other users. Your display name is not the same as your username or email address, which cannot be changed.

Steps

1. Select the profile icon in the upper right corner of the BlueXP console to view the User settings panel.
2. Select the **Edit** icon next to your name.
3. Enter your new display name in the **Name** field.

Configure multi-factor authentication

Configure multi-factor authentication (MFA) to enhance account security by requiring a second verification method with your password.

Users using single-sign on with an external identity provider or the NetApp Support Site cannot enable MFA. If either of these are true for you, you won't see the option to enable MFA in your profile settings.

Do not enable MFA if your user account is for BlueXP API access. Multi-factor authentication stops API access when enabled for a user account. Use service accounts for all API access.

Before you begin

- You must have already downloaded an authentication app, such as Google Authenticator or Microsoft Authenticator, to your device.
- You'll need your password to set up MFA.



If you do not have access to your authentication app or lose your recovery code, contact your BlueXP administrator for help.

Steps

1. Select the profile icon in the upper right corner of the BlueXP console to view the User settings panel.
2. Select **Configure** next to the **Multi-Factor Authentication** header.
3. Follow the prompts to set up MFA for your account.
4. When you finish, you'll be prompted to save your recovery code. Choose to either copy the code or download a text file containing the code. Keep this code somewhere safe. You need the recovery code if you lose access to your authentication app.

After you set up MFA, you are prompted to enter a one-time code from your authentication app each time you log in to BlueXP.

Regenerate your MFA recovery code

You can only use recovery codes once. If you use or lose yours, create a new one.

Steps

1. Select the profile icon in the upper right corner of the BlueXP console to view the User settings panel.
2. Select **...** next to the **Multi-Factor Authentication** header.
3. Select **Regenerate recovery code**.
4. Copy the generated recovery code and save it in a secure location.

Delete your MFA configuration

To stop using multi-factor authentication (MFA) for your BlueXP account, delete your MFA configuration. This removes the need to enter a one-time code from your authentication app when you log in.



If you are unable to access your authentication app or recovery code, you will need to contact your BlueXP administrator to reset your MFA configuration.

Steps

1. Select the profile icon in the upper right corner of the BlueXP console to view the User settings panel.
2. Select **...** next to the **Multi-Factor Authentication** header.
3. Select **Delete**.

Contact your Organization administrator

If you need to contact your organization administrator, you can send an email to them directly from BlueXP. The administrator manages user accounts and permissions within your organization.



You must have a default email application configured for your browser to use the **Contact admins** feature.

Steps

1. Select the profile icon in the upper right corner of the BlueXP console to view the User settings panel.
2. Select **Contact admins** to send an email to your organization administrator.
3. Select the email application to use.
4. Finish the email and select **Send**.

Configure dark mode (dark theme)

You can set BlueXP to display in dark mode.

Steps

1. Select the profile icon in the upper right corner of the BlueXP console to view the User settings panel.
2. Move the **Dark theme** slider to enable it.

Administer BlueXP

Identity and access management

Learn about BlueXP identity and access management

BlueXP identity and access management (IAM) enables you to organize and control access to your NetApp resources. You can organize your resources according to your organization's hierarchy. For example, you can organize resources by geographical location, site, or business unit. You can then assign IAM roles to members at specific parts of the hierarchy, which prevents access to resources in other parts of the hierarchy.

- [Learn about BlueXP deployment modes](#)

How BlueXP IAM works

BlueXP IAM lets you grant resource access by assigning users access roles to specific parts of the hierarchy. For example, a member can be assigned the Folder or project admin role for a project with five resources.

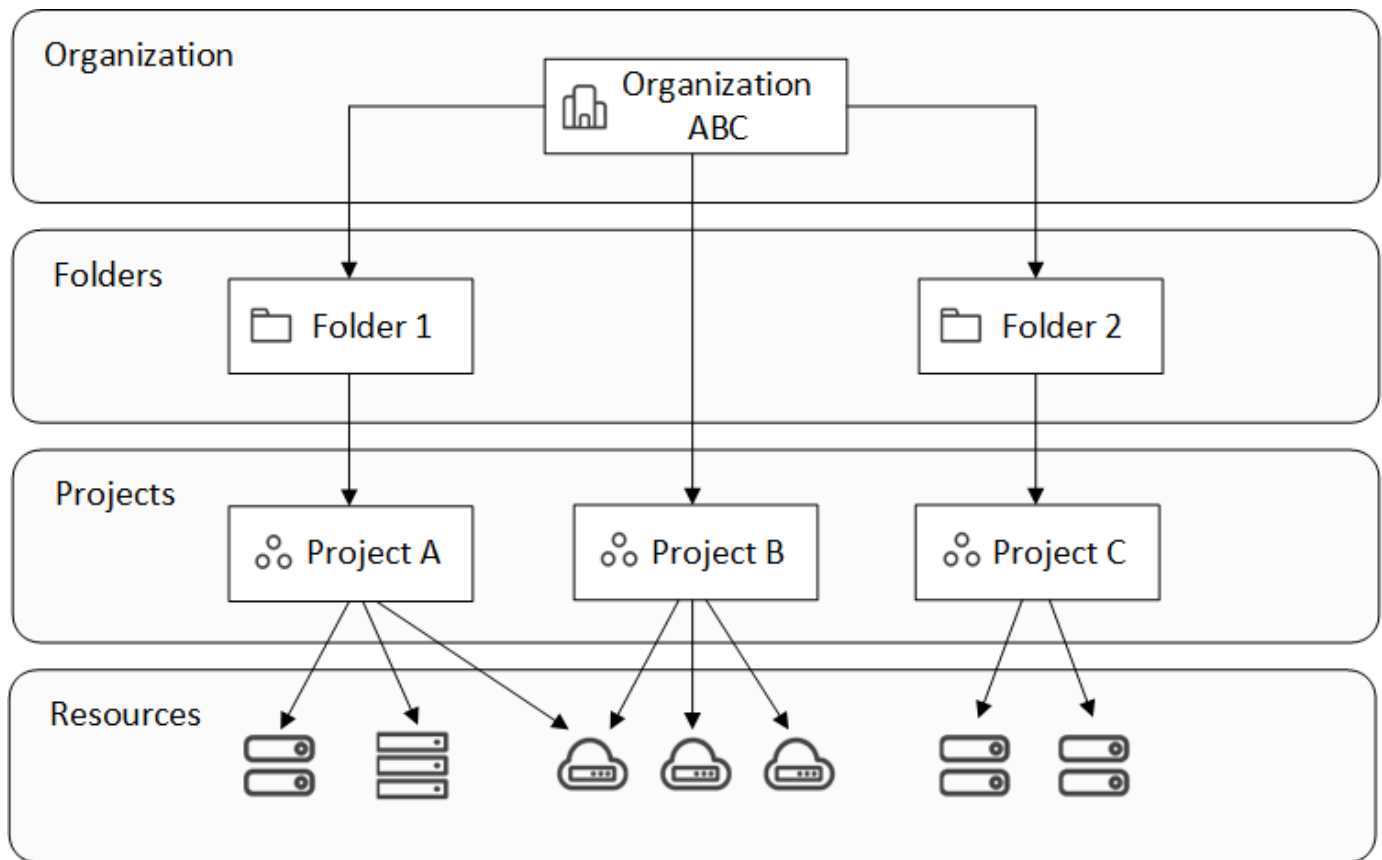
When using BlueXP IAM, you'll manage the following components:

- The organization
- Folders
- Projects
- Resources
- Members
- Roles and permissions
- Connectors

BlueXP resources are organized hierarchically:

- The organization is the top of the hierarchy.
- Folders are children of the organization or of another folder.
- Projects are children of the organization or of a folder.
- Resources are associated with one or more folders or projects.

The following image illustrates this hierarchy at a basic level.



Organization

An *organization* is the top level of BlueXP's IAM system and typically represents your company. Your organization consists of folders, projects, members, roles, and resources. Connectors are associated with specific projects in the organization.

Folders

A *folder* enables you to group related projects together and separate them from other projects in your organization. For example, a folder might represent a geographical location (EU or US East), a site (London or Toronto), or a business unit (engineering or marketing).

olders can contain projects, other folders, or both. Creating folders is optional.

Projects

A *project* represents a workspace in BlueXP that organization members access from the BlueXP canvas in order to manage resources. For example, a project can include a Cloud Volumes ONTAP system, an on-premises ONTAP cluster, or an FSx for ONTAP file system.

An organization can have one or many projects. A project can reside directly underneath the organization or within a folder.

Resources

A *resource* is a working environment that you created or discovered in BlueXP.

When you create or discover a resource, the resource is associated with the currently selected project. That might be the only project that you want to associate this resource with. But you can choose to associate the

resource with additional projects in your organization.

For example, you might associate a Cloud Volumes ONTAP system with one additional project or with all projects in your organization. How you associate a resource depends on your organization's needs.



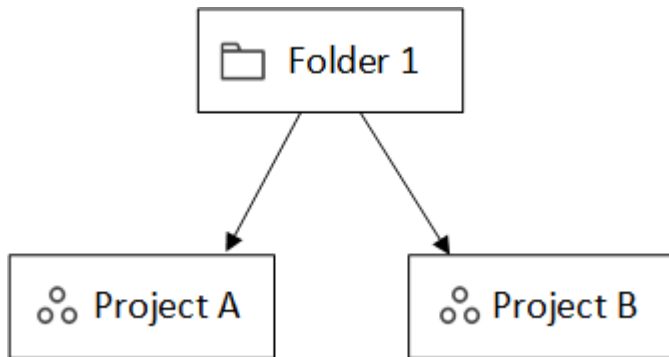
You can also associate a Connector with another folder or project in your organization. [Learn more about using Connectors with BlueXP IAM.](#)

When to associate a resource with a folder

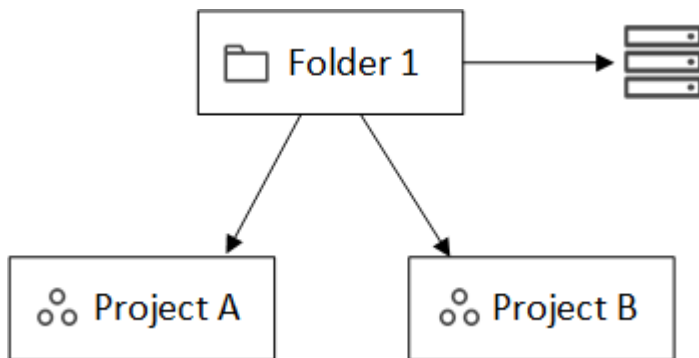
You also have the option to associate a resource with a folder, but this is optional and meets the needs of a specific use case.

An *Organization administrator* might associate a resource with a folder to allow a *Folder or project administrator* to link that resource to the appropriate projects in the folder.

For example, let's say you have a folder that contains two projects:

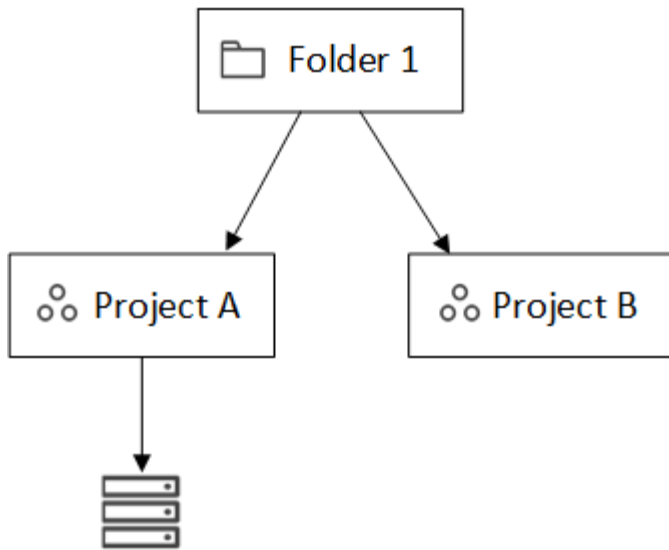


The *Organization admin* can associate a resource with the folder:



Associating a resource with a folder doesn't make it accessible to all projects; only the *Folder or project admin* can see it. The *Folder or project admin* decides which projects can access it and associates the resource with the appropriate projects.

In this example, the admin associates the resource with Project A:



Members who have permissions for project A can now access the resource.

Members

Members of your organization are user accounts or service accounts. A service account is typically used by an application to complete specified tasks without human intervention.

Each organization includes at least one user with the *Organization admin* role (BlueXP automatically assigns this role to the user who creates the organization). You can add other members to the organization and assign different permissions across different levels of the resource hierarchy.

Roles and permissions

In BlueXP IAM, you don't grant permissions directly to organization members. Instead, you grant each member a role. A role contains a set of permissions that enables a member to perform specific actions at a specific level of the resource hierarchy.

Granting permissions at a specific hierarchy level restricts access to the resources a member needs and the services that they can use with those resources.

Where you can assign roles in the hierarchy

When you associate a member with a role, you need to select the entire organization, a specific folder, or a specific project. The role that you select gives a member permissions to the resources in the selected part of the hierarchy.

Role inheritance

When you assign a role, the role is inherited down the organization hierarchy:

Organization

Granting a member an access role at the organization level gives them permissions to all folders, projects, and resources.

Folders

When you grant an access role at the folder level, all folders, projects, and resources in the folder inherit that role.

For example, if you assign a role at the folder level and that folder has three projects, the member will have permissions to those three projects and any associated resources.

Projects

When you grant an access role at the project level, all resources associated with that project inherit that role.

Multiple roles

You can assign each organization member a role at different levels of the organization hierarchy. It can be the same role or a different role. For example, you can assign a member role A for project 1 and project 2. Or you can assign a member role A for project 1 and role B for project 2.

Access roles

BlueXP supports several predefined roles that you can assign to the members of your organization.

[Learn about access roles.](#)

Connectors

When an *Organization admin* creates a Connector, BlueXP automatically associates that Connector with the organization and the currently selected project. The *Organization admin* automatically has access to that Connector from anywhere in the organization. But if you have other members in your organization with different roles, those members can only access that Connector from the project in which it was created, unless you associate that Connector with other projects.

You make a Connector available for another project in these cases:

- You want to allow members in your organization to use an existing Connector to create or discover additional working environments in another project
- You associated an existing resource with another project and that resource is managed by a Connector

If a resource that you associate with an additional project is discovered using a BlueXP Connector, then you also need to associate the Connector with the project that the resource is now associated with. Otherwise, the Connector and its associated resource aren't accessible from the BlueXP canvas by members who don't have the *Organization admin* role.

You can create an association from the **Connectors** page in BlueXP IAM:

- Associate a Connector with a project

When you associate a Connector with a project, that Connector is accessible from the BlueXP canvas when viewing the project.

- Associate a Connector with a folder

Associating a Connector with a folder doesn't automatically make that Connector accessible from all projects in the folder. Organization members can't access a Connector from a project until you associate the Connector with that specific project.

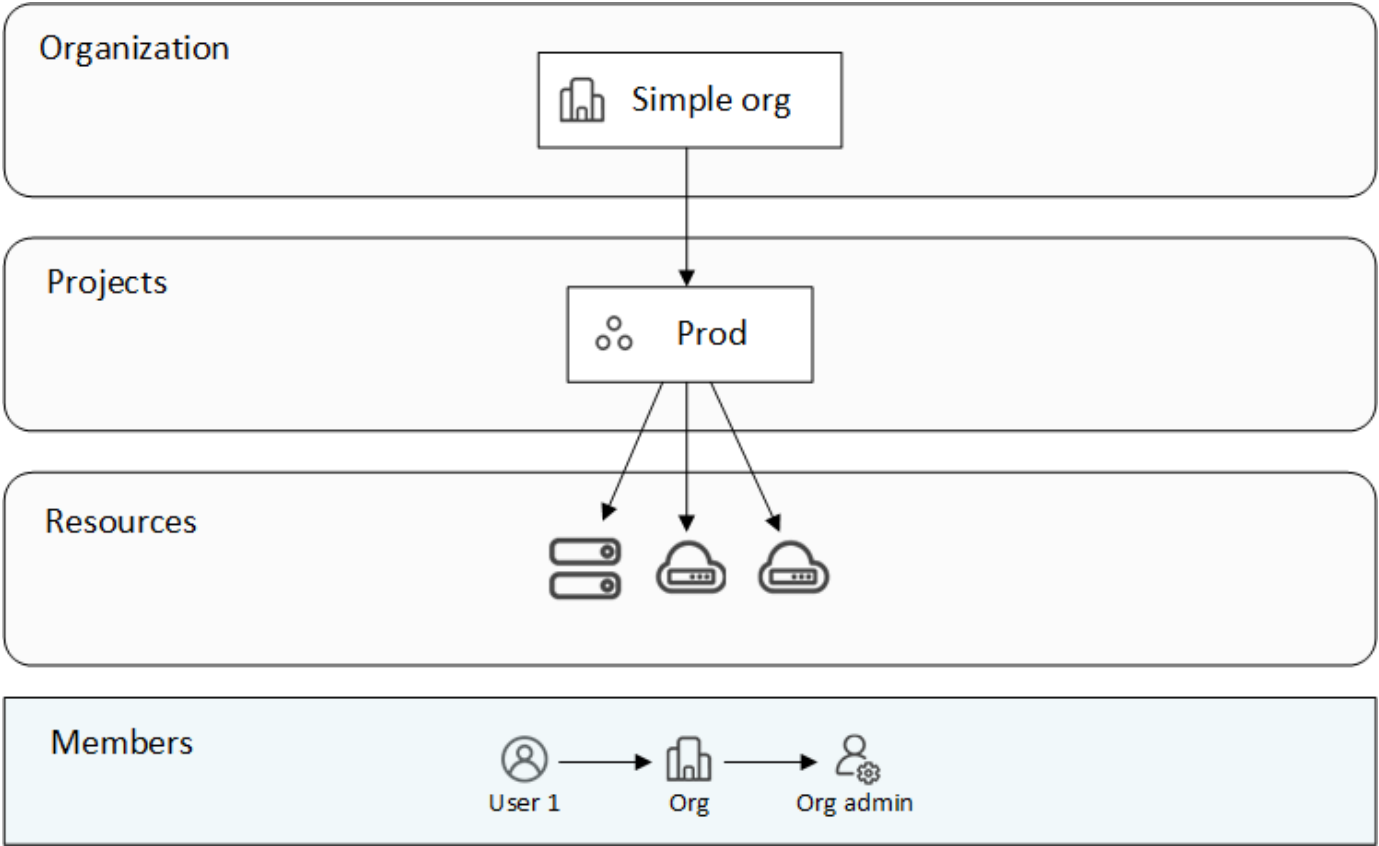
An *Organization admin* might associate a Connector with a folder so that the *Folder or project admin* can make the decision to associate that Connector with the appropriate projects that reside in the folder.

IAM examples

These examples demonstrate how you might set up your organization.

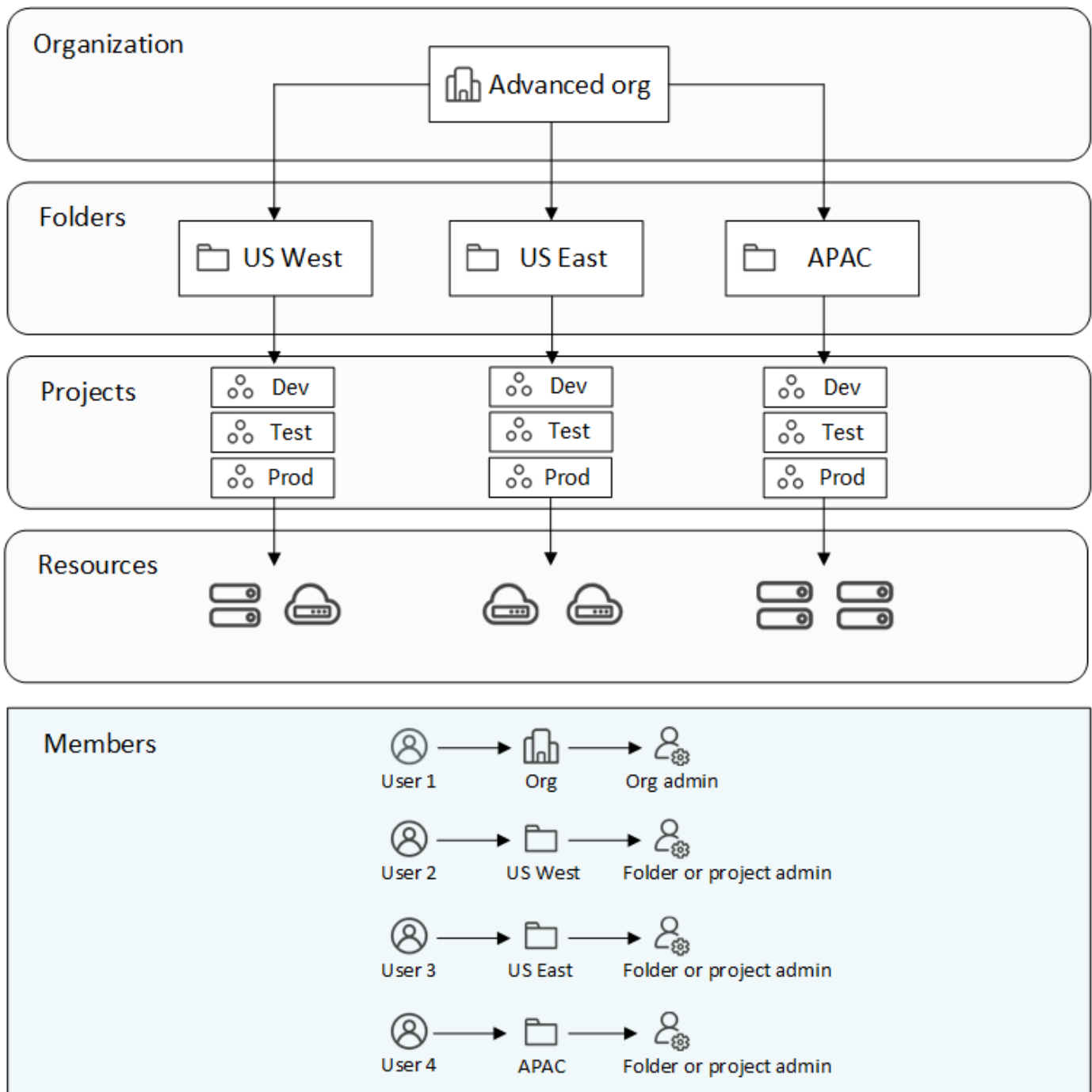
Simple organization

The following diagram shows a simple example of an organization that uses the default project and no folders. A single member manages the entire organization.



Advanced organization

The following diagram shows an organization that uses folders to organize the projects for each geographic location in the business. Each project has its own set of associated resources. The members include an organization admin and an admin for each folder in the organization.



What you can do with BlueXP IAM

The following examples describe how you might use IAM to manage your BlueXP organization:

- Grant specific roles to specific members so that they can only complete the required tasks.
- Modify member permissions because they moved departments or because they have additional responsibilities.
- Remove a user who left the company.
- Add folders or projects to your hierarchy because a new business unit has added NetApp storage.
- Associate a resource with another project because that resource has capacity that another team can utilize.

- View the resources that a member can access.
- View the members and resources associated with a specific project.

Where to go next

- [Get started with BlueXP IAM](#)
- [Organize your resources in BlueXP with folders and projects](#)
- [Manage BlueXP members and their permissions](#)
- [Manage the resource hierarchy in your BlueXP organization](#)
- [Associate Connectors with folders and projects](#)
- [Switch between BlueXP projects and organizations](#)
- [Rename your BlueXP organization](#)
- [Monitor or audit IAM activity](#)
- [BlueXP access roles](#)
- [Learn about the API for BlueXP IAM](#)

Get started with BlueXP identity and access management

When you sign up to BlueXP, you're prompted to create a new organization. The organization includes one member (an Organization admin) and one default project. To set up BlueXP identity and access management (IAM) to meet your business needs, you'll need to customize your organization's hierarchy, add additional members, add or discover resources, and associate those resources across your hierarchy.

You must have **Organization admin** permissions to administer the entire organization from BlueXP IAM. If you have **Folder or project admin** permissions, you can only administer the folders and projects for which you have permissions.

Follow these steps to set up a new BlueXP organization. The order in which you complete these steps might be different, depending on your organization's needs.

1

Edit the default project or add to your organization's hierarchy

Use the default project or create additional projects and folders matching your business hierarchy.

[Learn how to organize your resources with folders and projects.](#)

2

Associate members with your organization

If multiple people in your business need access to BlueXP, associate their user accounts with your organization and assign the necessary permissions. You also have the option to add service accounts to your organization.

[Learn how to manage members and their permissions.](#)

3

Add or discover resources

Add or discover resources in BlueXP as *the working environments*. Organization members manage a working environment, which represents a storage system, from within a project.

Learn how to create or discover resources:

- [Amazon FSx for NetApp ONTAP](#)
- [Azure NetApp Files](#)
- [Cloud Volumes ONTAP](#)
- [E-Series systems](#)
- [On-premises ONTAP clusters](#)
- [StorageGRID](#)



Associate resources with additional projects

When you create or discover a resource in BlueXP, that resource is automatically associated with the project that was selected when you created or discovered the working environment. If you want to make that resource available to another project in your organization, then you'll need to create an association between them. If a Connector manages the resource, associate the Connector with the respective project.S

- [Learn how to manage your organization's resource hierarchy.](#)
- [Learn how to associate a Connector with a folder or project.](#)

Related information

- [Learn about BlueXP identity and access management](#)
- [Learn about the API for BlueXP IAM](#)

Organize your resources in BlueXP IAM with folders and projects

BlueXP identity and access management (IAM) enables you to organize your NetApp resources using projects and folders. A *project* represents a workspace in BlueXP that organization members access to manage *resources* (for example, a Cloud Volumes ONTAP system). A *folder* groups related projects together. After you organize your resources into folders and projects, you can grant granular access to resources by providing organization members with permissions to specific folders and projects.

Add a folder or project


When you create your BlueXP organization, it includes a single project. You can create additional projects to manage your organization's resources. You can optionally create folders to group related projects together.

About this task

Your organization's resource hierarchy can have up to 7 levels, with nested folders down to 6 levels and projects at the seventh level.

The following image illustrates the maximum depth of your organization's resource hierarchy:

Steps

1. In the upper right of the BlueXP console, select  > **Identity & Access Management**.
2. From the **Organization** page, select **Add folder or project**.
3. Select **Folder** or **Project**.
4. Provide details about the folder or project:
 - **Name and location:** Enter a name and choose a location in the hierarchy for the folder or project. A folder or project can reside directly underneath the organization or within a folder.
 - **Resources:** Select the resources that you want to associate with this folder or project.

You can select resources associated with the parent folder or project: all resources for an organization parent, or folder-specific resources for a folder parent.

[Learn when you might associate a resource with a folder.](#)
 - **Access:** View the members who will have access to the folder or project based on the existing permissions already defined in your resource hierarchy.


If needed, select **Add a member** to specify additional organization members who should have access to the folder or project and then select a role. A role defines the permissions that members have for the folder or project.

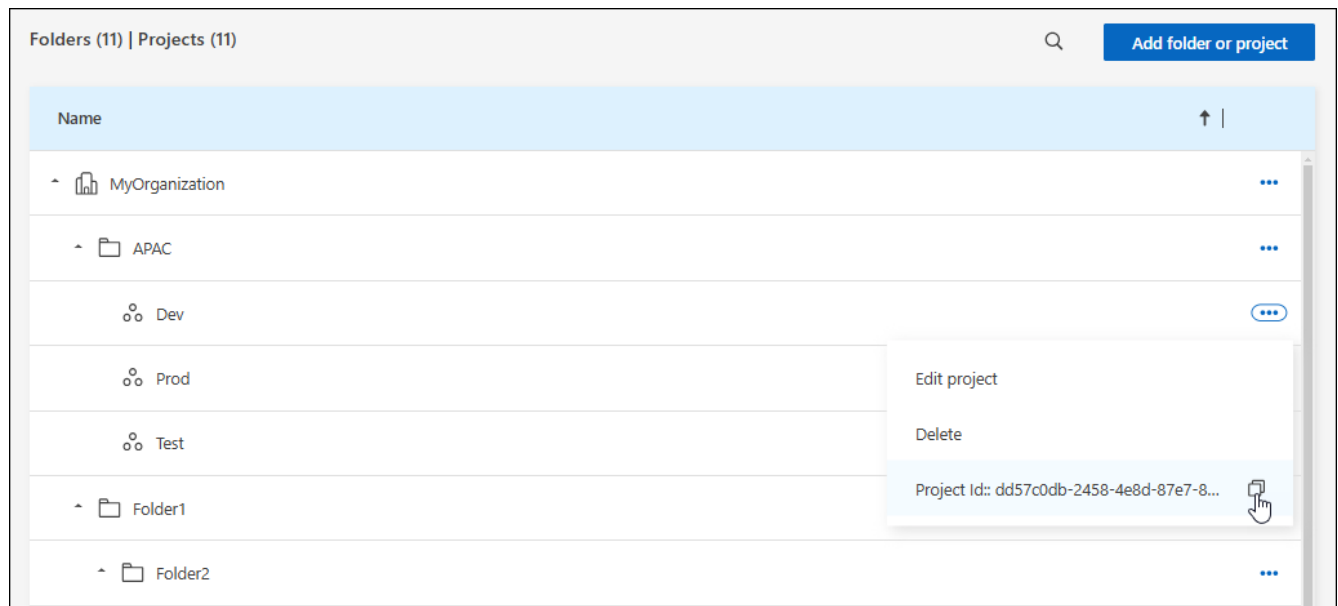
[Learn about predefined IAM roles.](#)
5. Select **Add**.

Obtain the ID for a project

If you're using the BlueXP API, you might need to obtain the ID for a project. For example, when creating a Cloud Volumes ONTAP working environment.

Steps

1. From the **Organization** page, navigate to a project in the table and select 
 - The system displays the project ID.
2. To copy the ID, select the copy button.



Rename a folder or project

If needed, you can change the name of your folders and projects.

Steps

1. From the **Organization** page, navigate to a project or folder in the table, select **...** and then select **Edit folder** or **Edit project**.
2. On the **Edit** page, enter a new name and select **Apply**.

Delete a folder or project

You can delete the folders and projects that you no longer need.

Before you begin

- The folder or project must not have any associated resources. [Learn how to disassociate resources](#).
- A folder must not contain any subfolders or projects. You need to delete those folders and projects first.

Steps

1. From the **Organization** page, navigate to a project or folder in the table, select **...** and then select **Delete**.
2. Confirm that you want to delete the folder or project.

View the resources associated with a folder or project

To verify that your resources are organized appropriately and accessible to the right members in your organization, you can view which resources and members are associated with a folder or project.

Steps

1. From the **Organization** page, navigate to a project or folder in the table, select **...** and then select **Edit folder** or **Edit project**.



2. On the **Edit** page, you can view details about the selected folder or project by expanding the **Resources** or **Access** sections.

- Select **Resources** to view the associated resources. In the table, the **Status** column identifies the resources that are associated with the folder or project.

Available resources (45) 🔍

<input type="checkbox"/>	Platform Type	Resource Type	Resource Name	Status
<input type="checkbox"/>	AWS	Cloud Volumes ONTAP HA	Keystonecvo2	Associated
<input type="checkbox"/>	AWS	Cloud Volumes ONTAP HA	kfuKeystone1vadim	Associated
<input type="checkbox"/>	AWS	Cloud Volumes ONTAP	cvo1Vadim	Associated
<input type="checkbox"/>	AWS	Cloud Volumes ONTAP HA	cvoparts11test	Associated

Modify the resources associated with a folder or project

Members with permissions for a folder or project can access its associated resources.

Before you begin

[Learn when you might associate a resource with a folder.](#)

Steps

1. From the **Organization** page, navigate to a project or folder in the table, select **...** and then select **Edit folder** or **Edit project**.
2. On the **Edit** page, select **Resources**.

In the table, the **Status** column identifies the resources that are associated with the folder or project.

3. Select the resources that you'd like to associate or disassociate.
4. Depending on the resources that you selected, select either **Associate with the project** or **Disassociate from the project**.

Available resources (45) | Selected (3)

Actions:

Associate with the project

Disassociate from the project

<input type="checkbox"/>	Platform Type	Resource Type	Resource Name	Status
<input checked="" type="checkbox"/>		Cloud Volumes ONTAP HA	Keystonecvo2	Associated
<input checked="" type="checkbox"/>		Cloud Volumes ONTAP HA	kfuKeystone1vadim	Associated
<input checked="" type="checkbox"/>		Cloud Volumes ONTAP	cvo1Vadim	Associated
<input type="checkbox"/>		Cloud Volumes ONTAP HA	cvoparts11test	Associated
<input type="checkbox"/>		Cloud Volumes ONTAP	cvosecondaryparts11	Associated
<input type="checkbox"/>		Cloud Volumes ONTAP HA	keystonetest	Associated
<input type="checkbox"/>		Cloud Volumes ONTAP HA	keystonetesting55	Associated

5. Select **Apply**

View members associated with a folder or project

- Select **Access** to view the members who have access to the folder or project.

Access

Members (2)

Load users which inherits access

<input type="checkbox"/>	Type	Name	Role
<input type="checkbox"/>		Gabriel	Folder or project admin
<input type="checkbox"/>		Ben	Organization admin

Modify member access to a folder or project

Modify member access to ensure the right members can access the associated resources.

Member access provided at a higher hierarchy level cannot be changed at lower levels. You need to switch to that part of the hierarchy and update the member's permissions there. Alternatively, you can [manage permissions from the Members page](#).

[Learn more about role inheritance](#).

Steps

1. From the **Organization** page, navigate to a project or folder in the table, select **...** and then select **Edit folder** or **Edit project**.
2. On the **Edit** page, select **Access** to view the list of members who have access to the selected folder or project.
3. Modify member access:
 - **Add a member**: Select the member that you'd like to add to the folder or project and assign them a role.
 - **Change a member's role**: For any members with a role other than Organization Admin, select their existing role and then choose a new role.
 - **Remove member access**: For members who have a role defined at the folder or project for which you're viewing, you can remove their access.
4. Select **Apply**.

Related information

- [Learn about BlueXP identity and access management](#)
- [Get started with BlueXP IAM](#)
- [Learn about the API for BlueXP IAM](#)

Add BlueXP members and service accounts

BlueXP identity and access management (IAM) enables you to add members to your organization and assign them one or more roles across your resource hierarchy. A *role* contains a set of permissions that enables a member to perform specific actions at a specific level of the resource hierarchy. You can associate new user accounts and service accounts, manage member roles, and more.



Ensure two members have the Organization admin role to avoid losing access to your BlueXP organization.

To manage users and their permissions, you must be assigned one of the following roles:

- Organization admin

Users with this role can manage all members

- Folder or project admin

Users with this role can manage members only of a designated folder or project

`_Folder or project admin_ can view all members on the *Members* page but manage permissions only for folders and projects they have access to. xref:{relative_path}reference-iam-predefined-roles.html[Learn more about the actions that a _Folder or project admin_ can complete].`

Add members to your organization

You can add two types of members to your organization: a user account and a service account. A service account is used by applications to perform tasks via the BlueXP API without human intervention. A user account is typically used by a person to log in to BlueXP and manage resources.

Users must sign up for BlueXP before being added to an organization or assigned a role. However, you can create service accounts directly from BlueXP.

To manage users and their permissions, you must have the **Organization admin** role or the **Folder or project admin** role. Remember that users with the **Folder or project admin** role can only manage members for the folder or projects of which they have admin permissions.


User account

Steps

1. Direct the user to visit [NetApp BlueXP website](#) to sign up.

Once users sign up, they complete the **Sign up** page, check their email, and log in. If BlueXP prompts users to create an organization, they close it and notify you of their account creation. You can then add the user to your existing BlueXP organization.

[Learn how to sign up to BlueXP.](#)

2. In the upper right of the BlueXP console, select  > **Identity & Access Management**.
3. Select **Members**.
4. Select **Add a member**.
5. To add the member, complete the steps in the dialog box:
 - **Entity Type**: Keep **User** selected.
 - **User's email**: Enter the user's email address that is associated with the BlueXP login that they created.
 - **Select an organization, folder, or project**: Choose the level of your resource hierarchy that the member should have permissions for.

Note the following:

- You can only select from the folders and projects for which you have admin permissions.
- Selecting an organization or folder grants the member permissions to all its contents.
- **Select a category** and then select a **Role** that provides the member with permissions for the resources that are associated with the organization, folder, or project that you selected.
 - If you selected a folder or project, you can choose from any role other than **Organization admin**.


[Learn about access roles.](#)

- **Add role**: If you want to provide access to additional folders or projects within your organization or grant the user further permissions in the selected area, select **Add role**, specify another folder or project or a different role category and then choose a role.
6. Select **Add**.

NetApp BlueXP sends the user an email with information on how to access BlueXP.

Service account

Steps

1. In the upper right of the BlueXP console, select  > **Identity & Access Management**.
2. Select **Members**.
3. Select **Add a member**.
4. To add the member, complete the steps in the dialog box:
 - **Entity Type**: Select **Service account**.

- **Service account name:** Enter a name for the service account.
- **Select an organization, folder, or project:** Choose the level of your resource hierarchy that the member should have permissions for.

Note the following:

- You can only select from the folders and projects for which you have admin permissions.
- Selecting an organization or folder grants the member permissions to all its contents.
- **Select a category** then select a **Role** that provides the member with permissions for the resources that are associated with the organization, folder, or project that you selected.
 - If you selected a folder or project, you can choose from any role other than **Organization admin**.

[Learn about predefined IAM roles.](#)

- **Add role:** If you want to provide access to additional folders or projects within your organization or grant the user further permissions in the selected area, select **Add role**, specify another folder or project or a different role category and then choose a role.

5. Download or copy the client ID and client secret.

BlueXP displays the client secret only once. Copy or download it and store it securely. Note that you can recreate the client ID and client secret later on as needed.

6. Select **Close**.

View organization members

You can view a list of all members in your BlueXP organization. To understand which resources and permissions are available to a member, you can view the roles assigned to the member at different levels of your organization's resource hierarchy. [Learn how to use roles to control access to BlueXP resources.](#)

You can view both user accounts and service accounts from the **Members** page.



You can also view all of the members associated with a specific folder or project. [Learn more.](#)

Steps

1. In the upper right of the BlueXP console, select > **Identity & Access Management**.
2. Select **Members**.

The **Members** table lists the members of your organization.


3. From the **Members** page, navigate to a member in the table, select and then select **View details**.

Remove a member from your organization

You might need to remove a member from your organization—for example, if they leave your company.

Removing a member removes their permissions but keeps their BlueXP and NetApp Support Site accounts.

Steps

1. From the **Members** page, navigate to a member in the table, select  then select **Delete user**.
2. Confirm that you want to remove the member from your organization.



Recreate the credentials for a service account

Create new credentials if lost or when updating security credentials becomes necessary.

About this task

When you recreate the credentials, you delete the existing credentials for the service account and create new ones. You cannot use the previous credentials.

Steps

1. In the upper right of the BlueXP console, select  > **Identity & Access Management**.
2. Select **Members**.
3. In the **Members** table, navigate to a service account, select  and then select **Recreate secrets**.
4. Select **Recreate**.
5. Download or copy the client ID and client secret.

BlueXP displays the client secret only once. Copy or download it and store it securely.

Manage a user's multi-factor authentication (MFA)

If a user has loses access to their MFA device, you can either remove or disable their MFA configuration.

If you remove their MFA configuration, the user needs to set up MFA again when they log in to BlueXP. If the user has only lost access to their MFA device temporarily, they can use the recovery code that they saved when they set up MFA to log in to BlueXP.

If they do not have their recovery code, temporarily disable MFA to allow login. When you disable MFA for a user, it is disabled for only eight hours and then re-enabled automatically. The user is allowed one login during that time without MFA. After the eight hours, the user must use MFA to log in to BlueXP.




You must have an email address in the same domain as the affected user to manage that user's multi-factor authentication.

Steps

1. In the upper right of the console, select  > **Identity & Access Management**.
2. Select **Members**.

The members of your organization appear in the **Members** table.

3. From the **Members** page, navigate to a member in the table, select  and then select **Manage multi-factor authentication**.
4. Choose whether to remove or to disable the user's MFA configuration.

Related information

- [Learn about BlueXP identity and access management](#)

- [Get started with BlueXP IAM](#)
- [Predefined BlueXP IAM roles](#)
- [Learn about the API for BlueXP IAM](#)

Use roles to manage user access to resources

Within BlueXP, you can assign roles to users based on what they need to do and where.

Users with the **Organization admin** or **Folder or project admin** role have the responsibility of assigning roles to other users. You can assign access roles on a project or folder basis. For example, you can assign a user the Ransomware protection admin role for one project and the SnapCenter admin role for a different project. Alternatively, if a user needs the Classification admin role for all projects within a specific folder, you can give them this role at the folder level.

Use access roles to assign access to storage resources based on the specific tasks that users need to perform. For example, if a user needs to interact with ransomware protection services, they must be given an access role that includes either viewing or administrative permissions for the ransomware protection service for the project for which the access role is granted.

Assign roles to users based on your IAM strategy for enhanced security. IAM roles ensure users have only the access they need.



Remember that you can't directly grant access to resources. Assign resources to projects first. Consider setting up your resource hierarchy before assigning users access. [Learn how to organize your resources in BlueXP IAM with folders and projects.](#)

View roles(s) assigned to a member

When you add a member to your organization, you are prompted to assign them a role. You can members to verify which roles they are currently assigned.

If you have the *Folder or project admin* role, the page displays all members in the organization. However, you can only view and manage member permissions for the folders and projects for which you have permissions. [Learn more about the actions that a *Folder or project admin* can complete.](#)

1. From the **Members** page, navigate to a member in the table, select **...** and then select **View details**.
2. In the table, expand the respective row for organization, folder, or project where you want to view the member's assigned role and select **View** in the **Role** column.

Add an access role to a member

You typically assign a role when adding a member to your organization, but you can update it at any time by removing or adding roles.

You can assign a user an access role for your organization, folder, or project.

Members can have multiple roles within the same project and in different projects. For example, smaller organizations may assign all available access roles to the same user, while larger organizations may have users do more specialized tasks. Alternatively, you could also assign one user the Ransomware protection admin role for an organization. In that example, the user would be able to perform ransomware protection tasks on all projects within your organization.

Your access role strategy should align with the way you have organized your NetApp resources.



A member who is assigned the Organization admin role can't be assigned any additional roles. They already have permissions across the entire organization. A member with the Folder or project role can't be assigned any other roles within the folder or project where they have that role already. Both of these roles provide access to all services within the scope that they are assigned.

Steps

1. From the **Members** page, navigate to a member in the table, select **...** and then select **Add a role**.
2. To add a role, complete the steps in the dialog box:

- **Select an organization, folder, or project:** Choose the level of your resource hierarchy that the member should have permissions for.

If you select the organization or a folder, the member will have permissions to everything that resides within the organization or folder.

- **Select a category:** Choose a role category. [Learn about access roles](#).
- **Select a Role:** Choose a role that provides the member with permissions for the resources that are associated with the organization, folder, or project that you selected.

[Learn about access roles](#).

* **Add role:** If you want to provide access to additional folders or projects within your organization, select **Add role**, specify another folder or project or role category, and then select a role category and a corresponding role.

1. Select **Add new roles**.


Change a member's assigned role

You can change the assigned roles for a member should you need to adjust the access for a user.



Users must have at least one role assigned to them. You can't remove all roles from a user. If you need to remove all roles, you must delete the user from your organization.

Steps

1. From the **Members** page, navigate to a member in the table, select **...** and then select **View details**.
2. In the table, expand the respective row for organization, folder, or project where you want to change the member's assigned role and select **View** in the **Role** column to view the roles assigned to this member.
3. You can change an existing role for a member or remove a role.
 - a. To change a member's role, select **Change** next to the role you want to change. You can only change this role to a role within the same role category. For example, you can change from one data service role to another. Confirm the change.
 - b. To unassign a member's role, select  next to the role to unassign the member the respective role. You'll be asked to confirm the removal.

Manage the resource hierarchy in your BlueXP organization

When you use associate a member with your organization, you provide permissions at

the organization, folder, or project level. To ensure that those members have permissions to access the right resources, you'll need to manage the resource hierarchy of your organization by associating resources with specific projects and folders. A *resource* is a storage resource that BlueXP already manages or is aware of.


View the resources in your organization

You can view both discovered and undiscovered resources associated with your organization. Undiscovered resources are storage resources identified by digital advisor but not added as working environments.



The IAM resources page excludes Amazon FSx for NetApp ONTAP resources because you cannot associate them with an IAM role. View these resources on their respective canvas or from workloads.

Steps

1. In the upper right of the BlueXP console, select  > **Identity & Access Management**.
2. Select **Resources** to view the Resources page.
3. Select **Advanced Search & Filtering**.
4. Use any of the available options to find the resource that you're looking for:
 - **Search by resource name:** Enter a text string and select **Add**.
 - **Platform:** Select one or more platforms, such as Amazon Web Services.
 - **Resources:** Select one or more resources, such as Cloud Volumes ONTAP.
 - **Organization, folder, or project:** Select the entire organization, a specific folder, or a specific project.
5. Select **Search**.


Associate a resource with folders and projects

Associate a resource to a folder or project to make it available.

Before you begin

You should understand how resource association works. [Learn about resources, including when to associate a resource with a folder.](#)

Steps

1. From the **Resources** page, navigate to a resource in the table, select  and then select **Associate to folders or projects**.
2. Select a folder or project and then select **Accept**.
3. To associate an additional folder or project, select **Add folder or project** and then select the folder or project.

Note that you can only select from the folders and projects for which you have admin permissions.

4. Select **Associate resources**.
 - If you associated the resource with projects, members who have permissions for those projects now have the ability to access the resource in BlueXP.
 - If you associated the resource with a folder, a *Folder or project admin* can now access the resource

from within BlueXP IAM. [Learn about associating a resource with a folder.](#)

After you finish

If you discover a resource using a BlueXP Connector associate the Connector with the project to grant them access. Otherwise, the Connector and its associated resource are not accessible from the BlueXP canvas by members without the *Organization admin* role.

[Learn how to associate a Connector with a folder or project.](#)

View the folders and projects associated with a resource

To identify where a resource is available in your organization's hierarchy, you can view the folders and projects that are associated with that resource.






If you need to determine which organization members have access to the resource, you can [view the members who have access to the folders and projects that are associated with the resource.](#)

Steps

1. From the **Resources** page, navigate to a resource in the table, select **...** and then select **View details**.

The following example shows a resource that is associated with one project.

Folders (0) Project (1)		Associate to folder or project
Type	Associated folders or projects	
	MyOrganization	
	MyOrganization > Project1	



If you need to determine which organization members have access to the resource, you can [view the members who have access to the folders and projects that are associated with the resource.](#)


Remove a resource from a folder or project

To remove a resource from a folder or project, you need to remove the association between the folder or project and the resource. Removing the association prevents members from managing the resource in the folder or project.



If you want to remove a discovered resource from the entire organization, you need to remove the working environment from the BlueXP canvas.

Steps

1. From the **Resources** page, navigate to a resource in the table, select **...** and then select **View details**.
2. For the folder or project for which you want to remove the resource, select .
3. Confirm that you want to remove the association by selecting **Delete**.

Related information

- [Learn about BlueXP identity and access management](#)
- [Get started with BlueXP IAM](#)
- [Learn about the API for BlueXP IAM](#)

Associate a BlueXP Connector with other folders and projects

When an `_Organization admin_` creates a Connector, it is automatically associated with currently selected project within the organization. Although someone with the `_Organization admin_` can access to that Connector from anywhere in the organization. Other members in your organization can only access that Connector from the project in which it was created, unless you associate that Connector with other projects.


Before you begin

You should understand how Connector association works. [Learn about using Connectors with BlueXP IAM.](#)

About this task

- When a *Folder or project admin* views the **Connectors** page, the page displays all Connectors in the organization. However, a member with this role can only view and associate Connectors with the folders and projects for which they have permissions. [Learn more about the actions that a *Folder or project admin* can complete.](#)

Steps

1. In the upper right of the BlueXP console, select  > **Identity & Access Management**.
2. Select **Connectors**.
3. From the table, find the Connector that you want to associate.

Use the search above the table to find a specific Connector or filter the table by resource hierarchy.

4. To view the folders and projects linked to the Connector, select  and then select **View details**.

BlueXP displays details about the folders and projects that the Connector is associated with.

5. Select **Associate to folder or project**.
6. Select a folder or project and then select **Accept**.
7. To associate the Connector with an additional folder or project, select **Add a folder or project** and then select the folder or project.
8. Select **Associate Connector**.

After you finish

If you want to associate the resources that the Connector manages with the same folders and projects, you can do so from the Resources page.

[Learn how to associate a resource with folders and projects.](#)

Related information

- [Learn about BlueXP Connectors](#)
- [Learn about BlueXP identity and access management](#)
- [Get started with BlueXP IAM](#)
- [Learn about the API for BlueXP IAM](#)

Switch between BlueXP organizations, projects, and Connectors

You might belong to multiple BlueXP organizations or have permissions to access multiple projects or Connectors within a BlueXP organization. When needed, you can easily switch between organizations, projects, and Connectors to access the resources associated with that organization, project, or Connector.



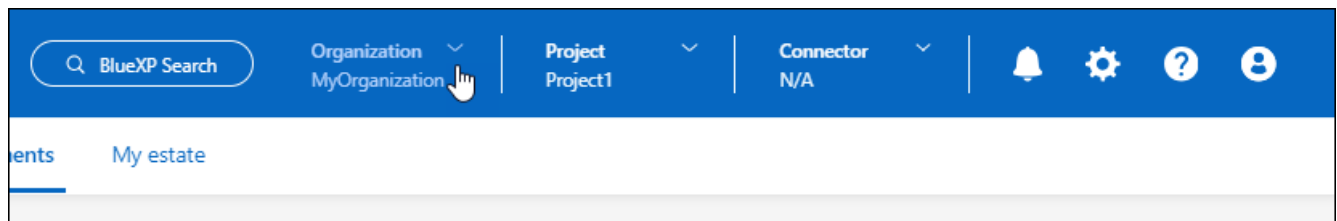
You might belong to multiple organizations if you were invited to join another organization or if you created an additional organization yourself. You can create an additional organization by using the API. [Learn how to create a new organization](#)

Switch between organizations

If you are a member of multiple organizations, you can switch between them at any time.

Steps

1. At the top of BlueXP, select **Organization**.



2. Select another organization and then select **Switch**.

Result

BlueXP switches to the selected organization and displays the resources associated with that organization.

Switch between projects

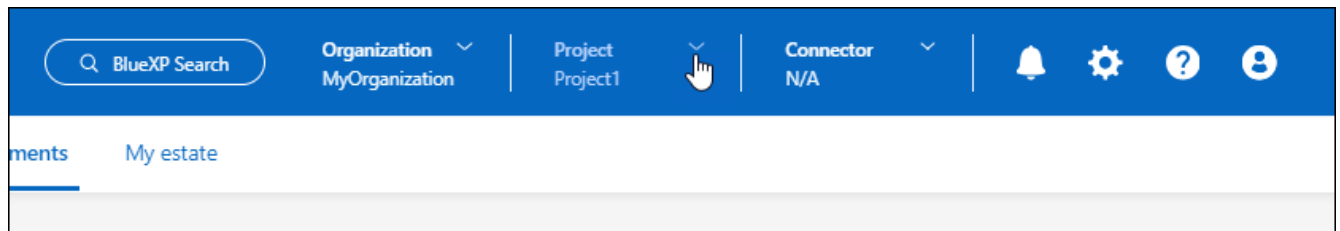
If your organization includes multiple projects and you have access to those projects, you can switch between them at any time.

Before you begin

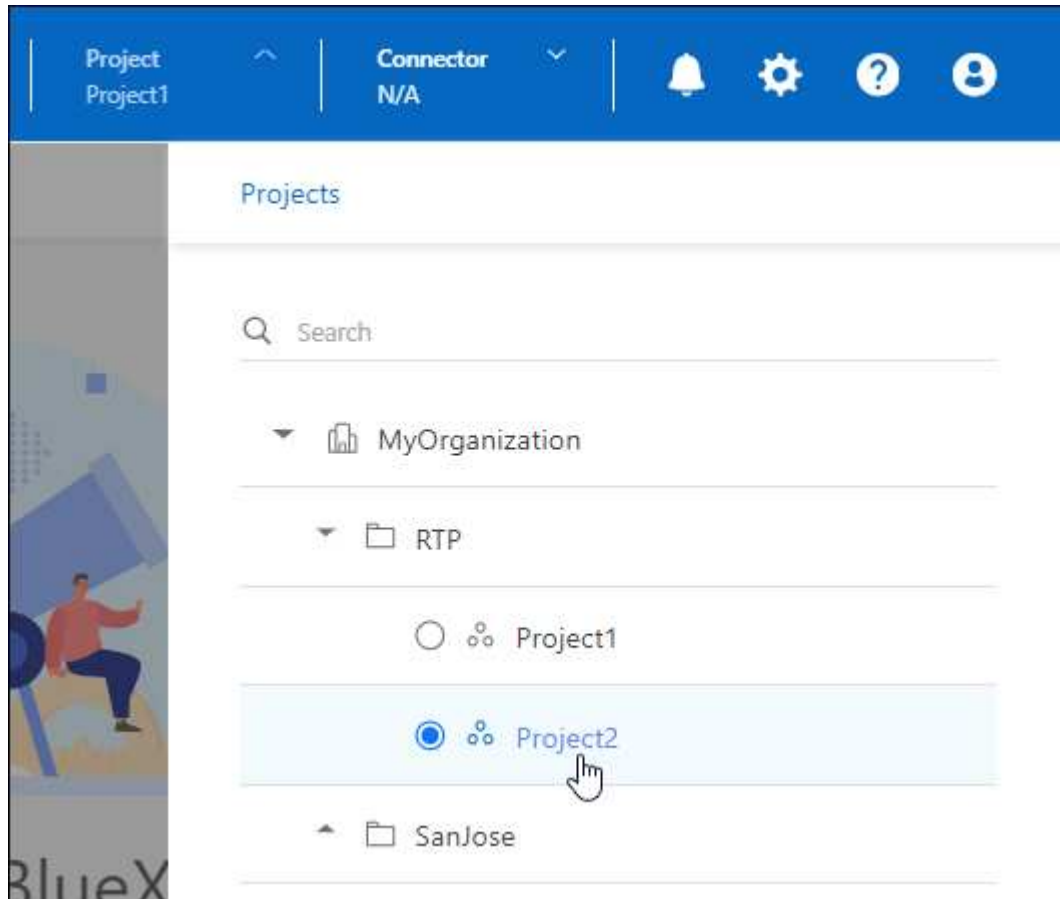
You must be on any page in the BlueXP console other than the BlueXP identity and access management (IAM) pages. You can't switch to another project when viewing any of the IAM pages.

Steps

1. At the top of BlueXP, select **Project**.



2. Browse through the folders and projects in your organization, select the project that you want, and then select **Switch**.



Result

BlueXP switches to the selected project and displays the resources associated with that project.

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.

Steps

1. At the top of BlueXP, select **Connector**.
2. Select another Connector and then select **Switch**.

Result

BlueXP refreshes and shows the working environments associated with the selected Connector.

Related information

[Associate Connectors with folders and projects.](#)

Related information

- [Learn about BlueXP identity and access management](#)
- [Get started with BlueXP IAM](#)
- [Learn about the API for BlueXP IAM](#)



Organization and project IDs

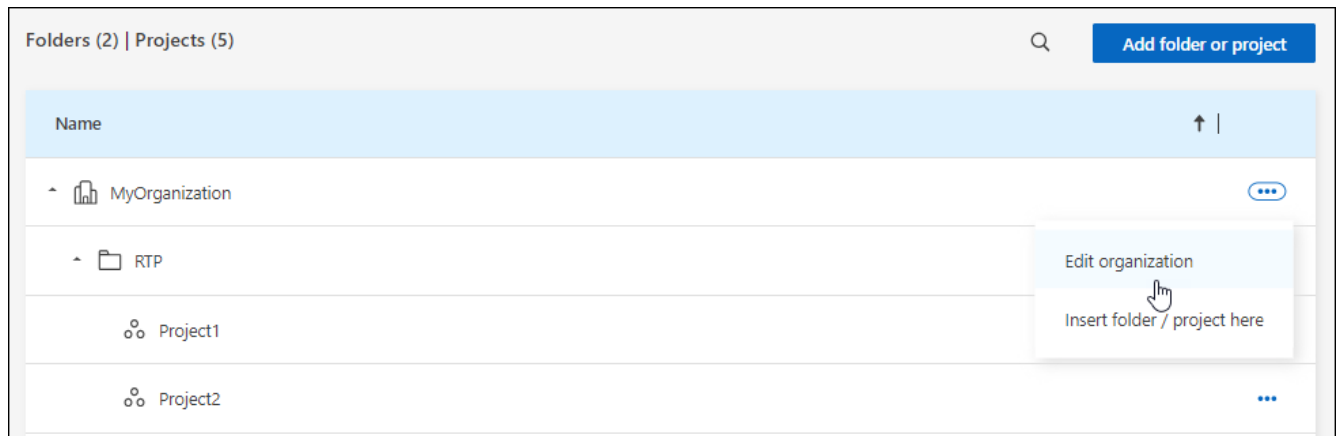
Your BlueXP organization has a name and an ID. You can choose a name for your organization to help identify it in your BlueXP deployment. You may also need to retrieve the organization ID for certain integrations.

Rename your organization

You can rename your organization within BlueXP. This is helpful if you support more than organization within your BlueXP deployment.

Steps

1. In the upper right of the BlueXP console, select  > **Identity & Access Management**.
2. From the **Organization** page, navigate to the first row in the table, select  and then select **Edit organization**.




3. Enter a new organization name and select **Apply**.

Get the organization ID

The organization ID is used for certain integrations with BlueXP.

You can view the organization ID from the Organizations page and copy it to the clipboard for your needs.

Steps

1. In the upper right of the BlueXP console, select  > **Identity & Access Management**.
2. Select the **Organization** tab to view the **Organization** page.

3. On the **Organization** page, look for your organization ID in the summary bar and copy it to the clipboard. You can save this for use later or copy it directly to where you need to use it.

Obtain the ID for a project

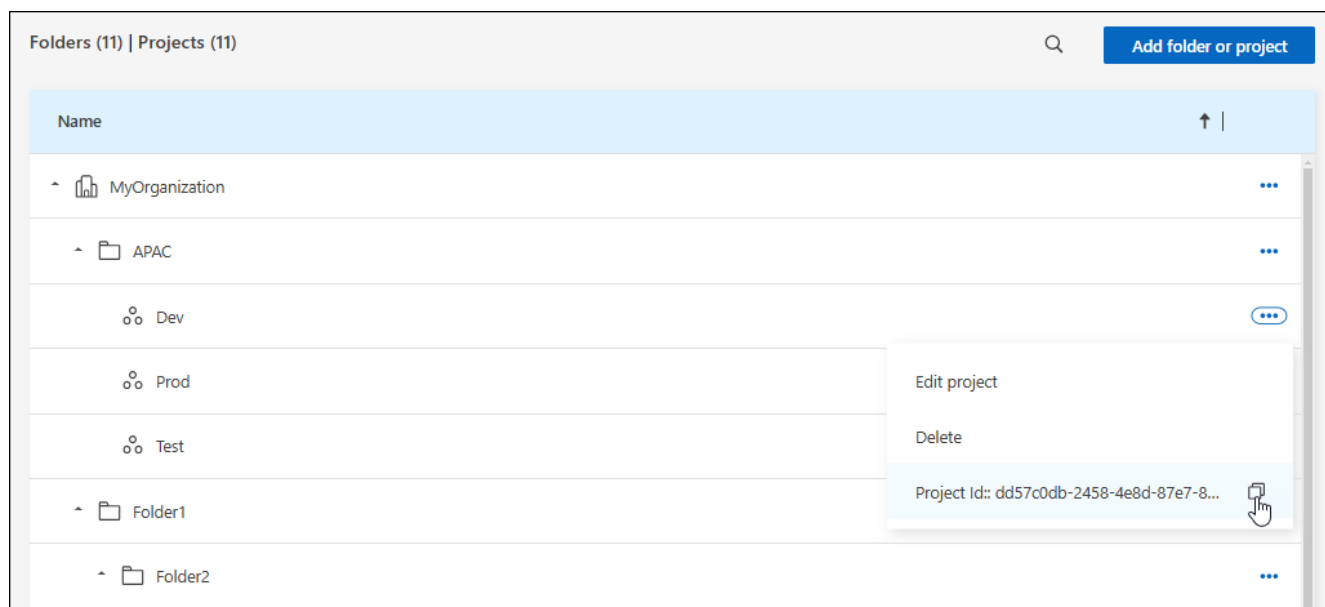
If you're using the BlueXP API, you might need to obtain the ID for a project. For example, when creating a Cloud Volumes ONTAP working environment.

Steps

1. From the **Organization** page, navigate to a project in the table and select **...**

The project ID displays.

2. To copy the ID, select the copy button.




Related information

- [Learn about BlueXP identity and access management](#)
- [Get started with BlueXP IAM](#)
- [Learn about the API for BlueXP IAM](#)

Monitor or audit IAM activity from the BlueXP timeline

If you need to monitor or audit an action that was completed from BlueXP identity and access management (IAM), you can view details from the BlueXP Timeline. For example, you might want to verify who added a member to an organization or that a project was deleted successfully.

Steps

1. In the upper right of the BlueXP console, select  > **Timeline**.
2. From the filters, select **Service** and then select **Tenancy**.
3. Use any of the other filters to change which actions display in the table.

For example, you can use the **User** filter to show actions related to a specific user account.

Result

The Timeline updates to show you completed management actions related to BlueXP IAM.

BlueXP access roles

Learn about BlueXP access roles

BlueXP identity and access management (IAM) includes predefined roles that you can assign to the members of your organization across different levels of your resource hierarchy. Before you assign these roles, you should understand the permissions that each role includes. Roles fall into the following categories: platform, application, and data service.

Platform roles

Platform roles grant all BlueXP administration permissions, including assigning roles and adding users. Platform roles provide access to all BlueXP data services and applications. BlueXP IAM includes two platform roles: Organization admin and Folder or project admin. The main difference between the two BlueXP IAM platform roles is scope.

Platform role	Responsibilities
Organization admin	<p>Allows a user unrestricted access to all projects and folders within an organization, add members to any project or folder, as well as perform any BlueXP task and use any data service that does not have an explicit role associated with it.</p> <p>Users with this role organize and manage your BlueXP organization. They create folders and projects, assign roles, add users, and can manage all working environments, if they have the credentials to do so.</p> <p>This is the only access role that can create Connectors.</p>
Folder or project admin	<p>Allows a user unrestricted access to specific projects and folders to which they are assigned. Can add members to folders or projects they manage, as well as perform any BlueXP task and use any data service or application on resources within the folder or project they are assigned.</p> <p>Folder or project admins cannot create Connectors.</p>
Federation admin	<p>Allows a user create and manage federations with BlueXP, which enables single-sign on (SSO).</p>
Federation viewer	<p>Allows a user to view existing federations with BlueXP. Cannot create or manage federations</p>

Application roles

The following is a list of roles in the application category. Each role grants specific permissions within its designated scope. Users who do not have the required application role or a platform role will be unable to access the application.

Application role	Responsibilities
Google Cloud NetApp Volumes admin	Users with the Google Cloud NetApp Volumes role can discover and manage Google Cloud NetApp Volumes.
Keystone admin	Users with the Keystone admin role can create service requests. Allows users to monitor and view consumption, assets, and administrative information within the Keystone tenant they are accessing.
Keystone viewer	Users with the Keystone viewer role CANNOT create service requests. Allows users to monitor and view consumption, assets, and administrative information within the Keystone tenant they are accessing.
ONTAP Mediator setup role	Service accounts with the ONTAP Mediator setup role can create service requests. This role is required in a service account to configure an instance of the ONTAP Cloud Mediator .
Operation support analyst	Provides access to alerts and monitoring tools and ability to enter and manage support cases.
Storage admin	Administer storage health and governance functions, discover storage resources, as well as modify and delete existing working environments.
Storage viewer	View storage health and governance functions, as well as view previously discovered storage resources. Cannot discover, modify, or delete existing storage working environments.
System health specialist	Administer storage and health and governance functions, all permissions of the Storage admin except cannot modify or delete existing working environments.

Data service roles

The following is a list of roles in the data service category. Each role grants specific permissions within its designated scope. Users who do not have the required data service role or a platform role will be unable to access the data service.

Data service role	Responsibilities
Backup and recovery super admin	Perform any actions in the Backup and recovery service.
Backup and recovery admin	Perform backups to local snapshots, replicate to secondary storage, and back up to object storage.
Backup and recovery restore admin	Restore workloads in the Backup and recovery service.
Backup and recovery clone admin	Clone applications and data in the Backup and recovery service.
Backup and recovery viewer	View Backup and recovery information.
Disaster recovery admin	Perform any actions in the Disaster recovery service.
Disaster recovery failover admin	Perform failover and migrations.

Data service role	Responsibilities
Disaster recovery application admin	Create replication plans, modify replication plans, and start test failovers.
Disaster recovery viewer	View information only.
Classification viewer	Provides the ability to view BlueXP classification scan results. Users with this role can view compliance information and generate reports for resources that they have permission to access. These users can't enable or disable scanning of volumes, buckets, or database schemas. Classification does not have a viewer role.
Ransomware protection admin	Manage actions on the Protect, Alerts, Recover, Settings, and Reports tabs of the Ransomware protection service.
Ransomware protection viewer	View workload data, view alert data, download recovery data, and download reports in the Ransomware protection service.
SnapCenter admin	Provides the ability to back up snapshots from on-premises ONTAP clusters using BlueXP backup and recovery for applications. A member who has this role can complete the following actions in BlueXP: <ul style="list-style-type: none"> * Complete any action from Backup and recovery > Applications * Manage all working environments in the projects and folders for which they have permissions * Use all BlueXP services SnapCenter does not have a viewer role.

Related links

- [Learn about BlueXP identity and access management](#)
- [Get started with BlueXP IAM](#)
- [Manage BlueXP members and their permissions](#)
- [Learn about the API for BlueXP IAM](#)

BlueXP platform access roles

Assign platform roles to users to grant permissions to perform administration tasks in BlueXP, assign roles, add users, create Connectors, and manage federations.

Example for organization roles in BlueXP for a large multi-national organization

XYZ Corporation organizes data storage access by region—North America, Europe, and Asia-Pacific—providing regional control with centralized oversight.

The **Organization admin** in XYZ Corporation's BlueXP creates an initial organization and separate folders for each region. The **Folder or project admin** for each region organizes projects (with associated resources) within the region's folder.

Regional admins with the **Folder or project admin** role actively manage their folders by adding resources and users. These regional admins can also add, remove, or rename folders and projects they manage. The **Organization admin** inherits permissions for any new resources, maintaining visibility of storage usage across

the entire organization.

Within the same organization, one user is assigned the **Federation admin** role to manage the federation of the organization with their corporate IdP. This user can add or remove federated organizations, but cannot manage users or resources within the organization. The **Organization admin** assigns a user the **Federation viewer** role to check federation status and view federated organizations.

The following tables indicate the actions that each BlueXP platform role can perform.

Organization administration roles

Task	Organization admin	Folder or project admin
Create Connectors	Yes	No
Create, modify or delete working environments (add or discover new resources using the BlueXP canvas)	Yes	Yes
Create folders and projects, including deleting	Yes	No
Rename existing folders and projects	Yes	Yes
Assign roles and add users	Yes	Yes
Associate resources with folders and projects	Yes	Yes
Associate Connectors with folders and projects	Yes	No
Remove Connectors from a folders and projects	Yes	No
Manage Connectors (edit certificates, settings, and so on)	Yes	No
Manage credentials from Settings > Credentials	Yes	Yes
Create, manage, and view federations	Yes	No
Register for support and submit cases through BlueXP	Yes	Yes
Use data services	Yes	Yes
View the BlueXP timeline and notifications	Yes	Yes

Federation roles

Task	Federation admin	Federation viewer
Create a federation	Yes	No
Verify a domain	Yes	No
Add a domain to a federation	Yes	No
Disable and delete federations	Yes	No
Test federations	Yes	No
View federations and their details	Yes	Yes

Application roles

Keystone access roles for BlueXP

Keystone roles provide access to the Keystone dashboards and allow users to view and manage their Keystone subscription. There are two Keystone roles: Keystone admin and Keystone viewer. The main difference between the two roles is the actions they can take in Keystone. The Keystone admin role is the only role that is allowed to create service requests or modify subscriptions.

Example for Keystone roles in BlueXP

XYZ Corporation has four storage engineers from different departments who view Keystone subscription information. Although all of these users need to monitor the Keystone subscription, only the team lead is allowed to make service requests. Three of the team members are given the **Keystone viewer** role, while the team lead is given the **Keystone admin** role so that there is a point of control over service requests for the company.

The following table indicates the actions that each Keystone role can perform.

Feature and action	Keystone admin	Keystone viewer
View the following tabs: Subscription, Assets, Monitor, and Administration	Yes	Yes
Keystone subscription page:		
View subscriptions	Yes	Yes
Amend or renew subscriptions	Yes	No
Keystone assets page:		
View assets	Yes	Yes
Manage assets	Yes	No
Keystone alerts page:		
View alerts	Yes	No
Manage alerts	Yes	No
Create alerts for self	Yes	Yes
Digital wallet:		
Can view digital wallet	Yes	Yes
Keystone reports page:		
Download reports	Yes	Yes

Feature and action	Keystone admin	Keystone viewer
Manage reports	Yes	Yes
Create reports for self	Yes	Yes
Service requests:		
Create service requests	Yes	No
View service requests created by any user within the Organization	Yes	Yes

Operational support analyst access role for BlueXP

You can assign the following role to users to provide them access to alerts and monitoring. Users with this role can also open support cases.

Operational support analyst

Task	Can perform
Manage own user credentials from Settings > Credentials	Yes
View discovered resources	Yes
Register for support and submit cases through BlueXP	Yes
View the BlueXP timeline and notifications	Yes
View, download, and configure alerts	Yes

Storage access roles for BlueXP

You can assign the following roles to users to provide them access to the storage management features in BlueXP that are associated with supported storage resources. You can assign users an administrative role to manage storage or a viewer role for monitoring.



These roles are not available from the BlueXP partnership API.

Administrators can assign storage roles to users for the following storage resources and features:

Storage resources:

- On-premises ONTAP clusters
- StorageGRID
- E-Series

BlueXP services and features:

- Digital advisor
- Software updates
- Economic efficiency
- Sustainability

Example for storage roles in BlueXP

XYZ Corporation, a multinational company, has a large team of storage engineers and storage administrators. They allow this team to manage storage assets for their regions while limiting access to core BlueXP tasks like user management, Connector creation, and cost tools such as the digital wallet.

Within a team of 12, two users are given the **Storage viewer** role which allows them to monitor the storage resources associated with the BlueXP projects they are assigned to. The remaining nine are given the **Storage admin** role which includes the ability to manage software updates, access ONTAP System Manager through BlueXP, as well as discover storage resources (add working environments). One person on the team is given the **System health specialist** role so they can manage the health of the storage resources in their region, but not modify or delete any working environments. This person can also perform software updates on the storage resources for projects they are assigned.

The organization has two additional users with the **Organization admin** role who can manage all aspects of BlueXP, including user management, Connector creation, and cost management tools like digital wallet, as well as several users with the **Folder or project admin** role who can perform BlueXP administration tasks for the folders and projects they are assigned to.

The following table shows the actions each BlueXP storage role performs.

Feature and action	Storage admin	System health specialist	Storage viewer
Canvas:			
Discover new resources (create new working environment)	Yes	Yes	No
View discovered resources	Yes	Yes	No
Delete working environments	Yes	No	No
Modify working environments	Yes	No	No
Create Connector	No	No	No
Digital advisor			
View all pages and functions	Yes	Yes	Yes
Digital wallet			
View all pages and functions	No	No	No
Software updates			

Feature and action	Storage admin	System health specialist	Storage viewer
View landing page and recommendations	Yes	Yes	Yes
Review potential version recommendations and key benefits	Yes	Yes	Yes
View update details for a cluster	Yes	Yes	Yes
Run pre-update checks and download upgrade plan	Yes	Yes	Yes
Install software updates	Yes	Yes	No
Economic efficiency			
Review capacity planning status	Yes	Yes	Yes
Choose next action (best practice, tier)	Yes	No	No
Tier cold data to cloud storage and free up storage	Yes	Yes	No
Set up reminders	Yes	Yes	Yes
Sustainability			
View dashboard and recommendations	Yes	Yes	Yes
Download report data	Yes	Yes	Yes
Edit carbon mitigation percentage	Yes	Yes	No
Fix recommendations	Yes	Yes	No
Defer recommendations	Yes	Yes	No
System manager access			
May enter credentials	Yes	Yes	No
Credentials			
User credentials	Yes	Yes	No

Data services roles

BlueXP backup and recovery roles

You can assign the following roles to users to provide them access to the Backup and

recovery service within BlueXP. Backup and recovery roles give you the flexibility to assign users a role specific to the tasks they need to accomplish within your organization. How you assign roles depends on your own business and storage management practices.

Backup and recovery uses the following roles:

- **Backup and recovery super admin:** Perform any actions.
- **Backup and recovery admin:** Perform backups to local snapshots, replicate to secondary storage, and back up to object storage.
- **Backup and recovery restore admin:** Restore workloads.
- **Backup and recovery clone admin:** Clone applications and data.
- **Backup and recovery viewer:** View backup and recovery information.

The following table indicates the actions that each role can perform.

Feature and action	Backup and recovery super admin	Backup admin	Restore admin	Clone admin	Viewer
Add, edit, or delete hosts	Yes	No	No	No	No
Install plugins	Yes	No	No	No	No
Add credentials (host, instance, vCenter)	Yes	No	No	No	No
View dashboard and all tabs	Yes	Yes	Yes	Yes	Yes
Start free trial	Yes	No	No	No	No
Initiate discovery of workloads	No	Yes	Yes	Yes	No
View license information	Yes	Yes	Yes	Yes	Yes
Activate license	Yes	No	No	No	No
View hosts	Yes	Yes	Yes	Yes	Yes
Schedules:					
Activate schedules	Yes	Yes	Yes	Yes	No
Suspend schedules	Yes	Yes	Yes	Yes	No
Policies and protection:					

Feature and action	Backup and recovery super admin	Backup admin	Restore admin	Clone admin	Viewer
View protection plans	Yes	Yes	Yes	Yes	Yes
Create, modify, or delete protection plans	Yes	Yes	No	No	No
Restore workloads	Yes	No	Yes	No	No
Create, split, or delete clones	Yes	No	No	Yes	No
Create, modify, or delete policy	Yes	Yes	No	No	No
Reports:					
View reports	Yes	Yes	Yes	Yes	Yes
Create reports	Yes	Yes	Yes	Yes	No
Delete reports	Yes	No	No	No	No
Import from SnapCenter and manage host:					
View imported SnapCenter data	Yes	Yes	Yes	Yes	Yes
Import data from SnapCenter	Yes	Yes	No	No	No
Manage (migrate) host	Yes	Yes	No	No	No
Configure settings:					
Configure log directory	Yes	Yes	Yes	No	No
Associate or remove instance credentials	Yes	Yes	Yes	No	No
Buckets:					
View storage buckets	Yes	Yes	Yes	Yes	Yes
Create, edit, or delete storage buckets	Yes	Yes	No	No	No

BlueXP disaster recovery roles

You can assign the following roles to users to provide them access to the Disaster

recovery within BlueXP. Disaster recovery roles give you the flexibility to assign users a role specific to the tasks they need to accomplish within your organization. How you assign roles depends on your own business and storage management practices.

Disaster recovery uses the following roles:

- **Disaster recovery admin:** Perform any actions.
- **Disaster recovery failover admin:** Perform failover and migrations.
- **Disaster recovery application admin:** Create replication plans. Modify replication plans. Start test failovers.
- **Disaster recovery viewer:** View information only.

The following table indicates the actions that each role can perform.

Feature and action	Disaster recovery admin	Disaster recovery failover admin	Disaster recovery application admin	Disaster recovery viewer
View dashboard and all tabs	Yes	Yes	Yes	Yes
Start free trial	Yes	No	No	No
Initiate discovery of workloads	Yes	No	No	No
View license information	Yes	Yes	Yes	Yes
Activate license	Yes	No	Yes	No
On the Sites tab:				
View sites	Yes	Yes	Yes	Yes
Add, modify, or delete sites	Yes	No	No	No
On the Replication plans tab:				
View replication plans	Yes	Yes	Yes	Yes
View replication plan details	Yes	Yes	Yes	Yes
Create or modify replication plans	Yes	Yes	Yes	No
Create reports	Yes	No	No	No
View snapshots	Yes	Yes	Yes	Yes
Perform failover tests	Yes	Yes	Yes	No

Feature and action	Disaster recovery admin	Disaster recovery failover admin	Disaster recovery application admin	Disaster recovery viewer
Perform failovers	Yes	Yes	No	No
Perform failbacks	Yes	Yes	No	No
Perform migrations	Yes	Yes	No	No
On the Resource groups tab:				
View resource groups	Yes	Yes	Yes	Yes
Create, modify, or delete resource groups	Yes	No	Yes	No
On the Job Monitoring tab:				
View jobs	Yes	No	Yes	Yes
Cancel jobs	Yes	Yes	Yes	No

Ransomware protection access roles for BlueXP

Ransomware roles provide users access to the Ransomware protection service. The two roles are Ransomware protection admin and Ransomware protection viewer. The main difference between the two roles is the actions they can take in Ransomware protection.

The following table shows the actions each BlueXP ransomware protection role can perform.

Feature and action	Ransomware protection admin	Ransomware protection viewer
View dashboard and all tabs	Yes	Yes
Start free trial	Yes	No
Discover workloads	Yes	No
On the Protect tab:		
Add, modify, or delete policies	Yes	No
Protect workloads	Yes	No
Identify sensitive data	Yes	No
Edit workload protection	Yes	No

Feature and action	Ransomware protection admin	Ransomware protection viewer
View workload details	Yes	Yes
Download data	Yes	Yes
On the Alerts tab:		
View alert details	Yes	Yes
Edit incident status	Yes	No
View incident details	Yes	Yes
Get full list of impacted files	Yes	No
Download alerts data	Yes	Yes
On the Recover tab:		
Download impacted files	Yes	No
Restore workload	Yes	No
Download recovery data	Yes	Yes
Download reports	Yes	Yes
On the Settings tab:		
Add or modify backup targets	Yes	No
Add or modify SIEM targets	Yes	No
On the Reports tab:		
Download reports	Yes	Yes

Identity federation

Enable single sign-on by using identity federation with BlueXP

Single-sign on (federation) simplifies the login process and enhances security by allowing users to log in to BlueXP using their corporate credentials. You can enable single sign-on (SSO) with your identity provider (IdP) or with the NetApp Support site.

Required role

Organization admin, Federation admin, Federation viewer. [Learn more about access roles.](#)

Identity federation with NetApp Support Site

When you federate with the NetApp Support Site, users can login with the same credentials to access BlueXP as you use for the NetApp Support Site, Active IQ Digital Advisor and other apps associated with your NetApp Support Site account. After you set up federation, any new users who create a NetApp Support Site accounts are also be able to access BlueXP.



If you federate with the NetApp Support Site, you can't also federate with your corporate identity management provider. Choose which one works best for your organization.

Steps

1. Download and complete the [NetApp Federation Request Form](#).
2. Submit the form to the email address specified in the form.

The NetApp support team reviews and processes your request.

Set up a federated connection with your identity provider

You can set up a federated connection with your identity provider to enable single sign-on (SSO) for BlueXP. The process involves configuring your identity provider to trust NetApp as a service provider and then creating the connection in BlueXP.



If you previously configured federation using NetApp Cloud Central (an external application to BlueXP), you'll need to import your federation using the BlueXP Federation page to be able to manage it within BlueXP. [Learn how to import your federation.](#)

Supported identity providers

NetApp supports the following protocols and identity providers for federation:

Protocols

- Security Assertion Markup Language (SAML) identity providers
- Active Directory Federation Services (AD FS)

Identity providers

- Microsoft Entra ID
- PingFederate

Federation with BlueXP workflow

NetApp supports service provider-initiated (SP-initiated) SSO only. You need to first configure the identity provider to trust NetApp as a service provider. Then, you can create a connection in BlueXP that uses the identity provider's configuration.

You can federate with your email domain or with a different domain that you own. To federate with a domain different from your email domain, first verify you own the domain.



Verify your domain (if not using your email domain)

To federate with a domain different from your email domain, verify that you own it. You can federate your email domain without any extra steps.

2

Configure your IdP to trust NetApp as a service provider

Configure your identity provider to trust NetApp by creating a new application and providing the necessary information, such as the ACS URL, Entity ID or other credential information. Service provider information varies by identity provider, so refer to the documentation for your specific identity provider for details. You'll need to work with your IdP administrator to complete this step.

3

Create the federated connection in BlueXP

To create the connection, you need to provide the necessary information from your identity provider, such as the SAML metadata URL or file. This information is used to establish the trust relationship between BlueXP and your identity provider. The information you provide depends on the IdP that you are using. For example, if you're using Microsoft Entra ID, you need to provide the client ID, secret, and domain.

4

Test your federation in BlueXP

Test your federated connection before enabling it. The Federation page in BlueXP provides a test option that allows you to verify your test user is able to authenticate successfully. If the test is successful, you can enable the connection.

5

Enable your connection in BlueXP

After you enable the connection, users can log in to BlueXP using their corporate credentials.

Review the topic for your respective protocol or IdP to get started:

- [Set up a federated connection with AD FS](#)
- [Set up a federated connection with Microsoft Entra ID](#)
- [Set up a federated connection with PingFederate](#)
- [Set up a federated connection with a SAML identity provider](#)

Domain verification

Verify the email domain for your federated connection


If you want to federate with a domain that is different than your email domain, you must first verify that you own the domain. You can only use verified domains for federation.

Required roles

Organization admin or Federation admin. [Learn more about access roles.](#)

Verifying your domain involves adding a TXT record to your domain's DNS settings. This record is used to prove that you own the domain and allows BlueXP to trust the domain for federation. You may need to coordinate with your IT or network administrator to complete this step.

Steps

1. In the upper right of the BlueXP console, select  > **Identity & Access Management**.
2. Select the **Federation** tab.
3. Select **Configure new federation**.
4. Select **Verify domain ownership**.
5. Enter the domain that you want to verify and select **Continue**.
6. Copy the TXT record that is provided.
7. Go to your domain's DNS settings and configure the TXT value that was provided as a TXT record for your domain. Work with your IT or network administrator if needed.
8. After the TXT record is added, return to BlueXP and select **Verify**.

Configure federations

Federate BlueXP with Active Directory Federation Services (AD FS)

Federate your Active Directory Federation Services (AD FS) with BlueXP to enable single sign-on (SSO) for BlueXP. This allows users to log in to BlueXP using their corporate credentials.

Required roles

Organization admin or Federation admin is required to make create and manage federations. Federation viewer can view the Federation page. [Learn more about access roles](#).



You can federate with your corporate IdP or with the NetApp Support Site. NetApp recommends choosing one or the other, but not both.


NetApp supports service provider-initiated (SP-initiated) SSO only. First, configure the identity provider to trust BlueXP as a service provider. Then, create a connection in BlueXP using your identity provider's configuration.

You can set up federation with your AD FS server to enable single sign-on (SSO) for BlueXP. The process involves configuring your AD FS to trust BlueXP as a service provider and then creating the connection in BlueXP.

Before you begin

- An IdP account with administrative privileges is required. Coordinate with your IdP administrator to complete the steps.
- Identify the domain you want to use for federation. You can use your email domain or a different domain that you own. If you want to use a domain other than your email domain, you must first verify the domain in BlueXP. You can do this by following the steps in the [Verify your domain in BlueXP](#) topic.

Steps

1. In the upper right of the BlueXP console, select  > **Identity & Access Management**.
2. Select the **Federation** tab.
3. Select **Configure new federation**.
4. Enter your domain details:
 - a. Choose whether you want to use a verified domain or your email domain. The email domain is the domain associated with the account you are logged in with.

- b. Enter the name of the federation you are configuring.
 - c. If you choose a verified domain, select the domain from the list.
5. Select **Next**.
6. For your connection method, choose **Protocol** and then select **Active Directory Federation Services (AD FS)**.
7. Select **Next**.
8. Create a Relying Party Trust in your AD FS server. You can use PowerShell or manually configure it on your AD FS server. Consult the AD FS documentation for details on how to create a relying party trust.
 - a. Create the trust using PowerShell by using following script:

```
(new-object Net.WebClient -property @{Encoding = [Text.Encoding]::UTF8}).DownloadString("https://raw.githubusercontent.com/auth0/AD-FS-auth0/master/AD-FS.ps1") | iex
AddRelyingParty "urn:auth0:netapp-cloud-account" "https://netapp-cloud-account.auth0.com/login/callback"
```

- b. Alternatively, you can create the trust manually in the AD FS management console. Use the following BlueXP values when creating the trust:
 - When creating the Relying Trust Identifier, use the **YOUR_TENANT** value: netapp-cloud-account
 - When you select **Enable support for the WS-Federation**, use the **YOUR_AUTH0_DOMAIN** value: netapp-cloud-account.auth0.com
 - c. After creating the trust, copy the metadata URL from your AD FS server or download the federation metadata file. You'll need this URL or file to complete the connection in BlueXP.
- NetApp recommends using the metadata URL to let BlueXP automatically retrieve the latest AD FS configuration. If you download the federation metadata file, you will need to update it manually in BlueXP whenever there are changes to your AD FS configuration.
9. Return to BlueXP, and select **Next** to create the connection.
 10. Create the connection with AD FS.
 - a. Enter the **AD FS URL** that you copied from your AD FS server in the previous step or upload the federation metadata file that you downloaded from your AD FS server.
 11. Select **Create connection**. Creating the connection might take a few seconds.
 12. Select **Next**.
 13. Select **Test connection** to test your connection. You are directed to a login page for your IdP server. Log in with your IdP credentials to complete the test and return to BlueXP to enable the connection.
 14. Select **Next**.
 15. On the **Enable federation** page, review the federation details and then select **Enable federation**.
 16. Select **Finish** to complete the process.

After you enable the federation, users can log in to BlueXP using their corporate credentials.

Federate BlueXP with Microsoft Entra ID

Federate with your Microsoft Entra ID IdP provider to enable single sign-on (SSO) for BlueXP. This allows users to log in using their corporate credentials.

Required roles

Organization admin or Federation admin is required to make create and manage federations. Federation viewer can view the Federation page. [Learn more about access roles.](#)



You can federate with your corporate IdP or with the NetApp Support Site. NetApp recommends choosing one or the other, but not both.


NetApp supports service provider-initiated (SP-initiated) SSO only. You need to first configure the identity provider to trust NetApp as a service provider. Then, you can create a connection in BlueXP that uses the identity provider's configuration.

You can set up a federated connection with Microsoft Entra ID to enable single sign-on (SSO) for BlueXP. The process involves configuring your Microsoft Entra ID to trust BlueXP as a service provider and then creating the connection in BlueXP.

Before you begin

- An IdP account with administrative privileges is required. Coordinate with your IdP administrator to complete the steps.
- Identify the domain you want to use for federation. You can use your email domain or a different domain that you own. If you want to use a domain other than your email domain, you must first verify the domain in BlueXP. You can do this by following the steps in the [Verify your domain in BlueXP](#) topic.

Steps

1. In the upper right of the BlueXP console, select  > **Identity & Access Management**.
2. Select the **Federation** tab.
3. Select **Configure new federation**.

Domain details

4. Enter your domain details:
 - a. Choose whether you want to use a verified domain or your email domain. The email domain is the domain associated with the account you are logged in with.
 - b. Enter the name of the federation you are configuring.
 - c. If you choose a verified domain, select the domain from the list.
5. Select **Next**.

Connection method

6. For your connection method, choose **Provider** and then select **Microsoft Entra ID**.
7. Select **Next**.

Configuration instructions

1. Configure your Microsoft Entra ID to trust NetApp as a service provider. You need to do this step on your

Microsoft Entra ID server.

- a. Use the following values when registering your Microsoft Entra ID app to trust BlueXP:
 - For the **Redirect URL**, use <https://services.cloud.netapp.com>
 - For the **Reply URL**, use <https://netapp-cloud-account.auth0.com/login/callback>
- b. Create a client secret for your Microsoft Entra ID app. You'll need to provide the client ID, the client secret, and the Entra ID domain name to complete the federation.

2. Return to BlueXP, and select **Next** to create the connection.

Create connection

1. Create the connection with Microsoft Entra ID
 - a. Enter the client ID and Client secret that you created in the previous step.
 - b. Enter the Microsoft Entra ID domain name.
2. Select **Create connection**. The system creates the connection in a few seconds.

Test and enable the connection

1. Select **Next**.
2. Select **Test connection** to test your connection. You are directed to a login page for your IdP server. Log in with your IdP credentials to complete the test and return to BlueXP to enable the connection.
3. Select **Next**.
4. On the **Enable federation** page, review the federation details and then select **Enable federation**.
5. Select **Finish** to complete the process.

After you enable the federation, users can log in to BlueXP using their corporate credentials.

Federate BlueXP with PingFederate

Federate with your PingFederate IdP provider to enable single sign-on (SSO) for BlueXP. This allows users to log in using their corporate credentials.

Required roles

Organization admin or Federation admin is required to make create and manage federations. Federation viewer can view the Federation page. [Learn more about access roles](#).



You can federate with your corporate IdP or with the NetApp Support Site. NetApp recommends choosing one or the other, but not both.


NetApp supports service provider-initiated (SP-initiated) SSO only. You need to first configure the identity provider to trust NetApp as a service provider. Then, you can create a connection in BlueXP that uses the identity provider's configuration.

You can set up a federated connection with PingFederate to enable single sign-on (SSO) for BlueXP. The process involves configuring your PingFederate server to trust BlueXP as a service provider and then creating the connection in BlueXP.

Before you begin

- An IdP account with administrative privileges is required. Coordinate with your IdP administrator to complete the steps.
- Identify the domain you want to use for federation. You can use your email domain or a different domain that you own. If you want to use a domain other than your email domain, you must first verify the domain in BlueXP. You can do this by following the steps in the [Verify your domain in BlueXP](#) topic.

Steps

1. In the upper right of the BlueXP console, select  > **Identity & Access Management**.
2. Select the **Federation** tab.
3. Select **Configure new federation**.
4. Enter your domain details:
 - a. Choose whether you want to use a verified domain or your email domain. The email domain is the domain associated with the account you are logged in with.
 - b. Enter the name of the federation you are configuring.
 - c. If you choose a verified domain, select the domain from the list.
5. Select **Next**.
6. For your connection method, choose **Provider** and then select **PingFederate**.
7. Select **Next**.
8. Configure your PingFederate server to trust NetApp as a service provider. You need to do this step on your PingFederate server.
 - a. Use the following values when configuring PingFederate to trust BlueXP:
 - For the **Reply URL** or **Assertion Consumer Service (ACS) URL**, use <https://netapp-cloud-account.auth0.com/login/callback>
 - For the **Logout URL**, use <https://netapp-cloud-account.auth0.com/logout>
 - For **Audience/Entity ID**, use `urn:auth0:netapp-cloud-account:<fed-domain-name-saml>` where `<fed-domain-name-pingfederate>` is the domain name for the federation. For example, if your domain is `example.com`, the Audience/Entity ID would be `urn:auth0:netappcloud-account:fed-example-com-pingfederate`.
 - b. Copy the PingFederate server URL. You will need this URL when creating the connection in BlueXP.
 - c. Download the X.509 certificate from your PingFederate server. It needs to be in Base64-encoded PEM format (.pem, .crt, .cer).
9. Return to BlueXP, and select **Next** to create the connection.
10. Create the connection with PingFederate
 - a. Enter the PingFederate server URL that you copied in the previous step.
 - b. Upload the X.509 signing certificate. The certificate must be in PEM, CER, or CRT format.
11. Select **Create connection**. The system creates the connection in a few seconds.
12. Select **Next**.
13. Select **Test connection** to test your connection. You are directed to a login page for your IdP server. Log in with your IdP credentials to complete the test and return to BlueXP to enable the connection.
14. Select **Next**.
15. On the **Enable federation** page, review the federation details and then select **Enable federation**.

16. Select **Finish** to complete the process.

After you enable the federation, users can log in to BlueXP using their corporate credentials.

Federate with a SAML identity provider

Federate with your SAML 2.0 IdP provider to enable single sign-on (SSO) for BlueXP. This allows users to log in using their corporate credentials.

Required role

Organization admin. [Learn more about access roles.](#)



You can federate with your corporate IdP or with the NetApp Support Site. You can't federate with both.


NetApp supports service provider-initiated (SP-initiated) SSO only. You need to first configure the identity provider to trust NetApp as a service provider. Then, you can create a connection in BlueXP that uses the identity provider's configuration.

You can set up a federated connection with your SAML 2.0 provider to enable single sign-on (SSO) for BlueXP. The process involves configuring your provider to trust NetApp as a service provider and then creating the connection in BlueXP.

Before you begin

- An IdP account with administrative privileges is required. Coordinate with your IdP administrator to complete the steps.
- Identify the domain you want to use for federation. You can use your email domain or a different domain that you own. If you want to use a domain other than your email domain, you must first verify the domain in BlueXP. You can do this by following the steps in the [Verify your domain in BlueXP](#) topic.

Steps

1. In the upper right of the BlueXP console, select  > **Identity & Access Management**.
2. Select the **Federation** tab.
3. Select **Configure new federation**.
4. Enter your domain details:
 - a. Choose whether you want to use a verified domain or your email domain. The email domain is the domain associated with the account you are logged in with.
 - b. Enter the name of the federation you are configuring.
 - c. If you choose a verified domain, select the domain from the list.
5. Select **Next**.
6. For your connection method, choose **Protocol** and then select **SAML Identity Provider**.
7. Select **Next**.
8. Configure your SAML identity provider to trust NetApp as a service provider. You need to do this step on your SAML provider server.
 - a. Ensure that your IdP has the attribute `email` set to the user's email address. This is required for BlueXP to identify users correctly:


```

<saml:AttributeStatement
  xmlns:x500="urn:oasis:names:tc:SAML:2.0:profiles:attribute:X500"
  xmlns:xs="http://www.w3.org/2001/XMLSchema"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
  <saml:Attribute Name="email"
    NameFormat="urn:oasis:names:tc:SAML:1.1:nameid-format:X509SubjectName">
    <saml:AttributeValue xsi:type="xs:string">
      email@domain.com</saml:AttributeValue>
    </saml:Attribute>
  </saml:AttributeStatement>

```

b. Use the following values when registering your SAML application with BlueXP:

- For the **Reply URL** or **Assertion Consumer Service (ACS) URL**, use <https://netapp-cloud-account.auth0.com/login/callback>
- For the **Logout URL**, use <https://netapp-cloud-account.auth0.com/logout>
- For **Audience/Entity ID**, use `urn:auth0:netapp-cloud-account:<fed-domain-name-saml>` where `<fed-domain-name-saml>` is the domain name you want to use for federation. For example, if your domain is `example.com`, the Audience/Entity ID would be `urn:auth0:netapp-cloud-account:fed-example-com-samlp`.

c. After creating the trust, copy the following values from your SAML provider server:

- Sign In URL
- Sign Out URL (optional)

d. Download the X.509 certificate from your SAML provider server. It needs to be in PEM, CER, or CRT format.

9. Return to BlueXP, and select **Next** to create the connection.

10. Create the connection with SAML.

- a. Enter the **Sign In URL** of your SAML server.
- b. Upload the X.509 certificate that you downloaded from your SAML provider server.
- c. Optionally, enter the **Sign Out URL** of your SAML server.

11. Select **Create connection**. The system creates the connection in a few seconds.

12. Select **Next**.

13. Select **Test connection** to test your connection. You are directed to a login page for your IdP server. Log in with your IdP credentials to complete the test and return to BlueXP to enable the connection.

14. Select **Next**.

15. On the **Enable federation** page, review the federation details and then select **Enable federation**.

16. Select **Finish** to complete the process.

After you enable the federation, users can log in to BlueXP using their corporate credentials.

Manage federations in BLueXP

You can manage your federation in BlueXP. You can disable it, update expired credentials, as well as disable it if you no longer need it.



If you previously configured federation using NetApp Cloud Central (an external application to BlueXP), you'll need to import your federation using the BlueXP Federation page to be able to manage it within BlueXP. [Learn how to import your federation](#)

You can also add a verified domain to an existing federation, which allows you to use multiple domains for your federated connection.



Federation management events such as enabling, disabling, and updating federations display in the Timeline. [Learn more about monitoring operations in BlueXP.](#)



Required roles

Organization admin or Federation admin is required to make create and manage federations. Federation viewer can view the Federation page. [Learn more about access roles.](#)

Enable a federation

If you have created a federation but it is not enabled, you can enable it through the Federation tab in BlueXP. Enabling a federation allows users associated with the federation to log in to BlueXP using their corporate credentials. You must have already created the federation and tested it successfully before enabling it.

Steps



1. In the upper right of the BlueXP console, select  > **Identity & Access Management**.
2. Select the **Federation** tab.
3. Select the actions menu  next to the federation that you want to enable and select **Enable**.

Add a verified domain to an existing federation

You can add a verified domain to an existing federation in BlueXP to use multiple domains with the same identity provider (IdP).

You must have already verified the domain in BlueXP before you can add it to a federation. If you haven't verified the domain yet, you can do so by following the steps in [Verify your domain in BlueXP](#).

Steps

1. In the upper right of the BlueXP console, select  > **Identity & Access Management**.
2. Select the **Federation** tab.
3. Select the actions menu  next to the federation that you want to add a verified domain to and select **Update domains**. The **Update domains** dialog box lists the domain already associated with this federation.
4. Select a verified domain from the list of available domains.
5. Select **Update**. It may take up to 30 seconds for users of the new domain to have federated access to BlueXP.


Updating an expiring federated connection

You can update the details of a federation in BlueXP. For example, you'll need to update the federation if the credentials such as a certificate or client secret expire. When needed, update the notification date to remind you to update the connection before it expires.



Update BlueXP first before updating your IdP to avoid login issues. Stay logged in to BlueXP during the process.



Steps

1. In the upper right of the BlueXP console, select  > **Identity & Access Management**.
2. Select the **Federation** tab.
3. Select the actions menu (three vertical dots) next to the federation that you want to update and select **Update federation**.
4. Update the details of the federation as needed.
5. Select **Update**.

Test an existing federation

If you are having trouble with an existing federation, you can test the connection to see if it is working properly. This can help you identify any issues with the federation and troubleshoot them.

Steps



1. In the upper right of the BlueXP console, select  > **Identity & Access Management**.
2. Select the **Federation** tab.
3. Select the actions menu  next to the federation that you want to add a verified domain to and select **Test connection**.
4. Select **Test**. You're prompted to log in with your corporate credentials. If the connection is successful, you will be redirected to the BlueXP console. If the connection fails, you will see an error message indicating the issue with the federation.
5. Select **Done** to return to the **Federation** tab.

Disable a federation

If you no longer need a federation, you can disable it. This prevents users associated with the federation from logging in to BlueXP using their corporate credentials. You can re-enable the federation later if needed.

You should disable a federation before deleting it. For example, if you are decommissioning the IdP in favor of another IdP or no longer want to use federation. This allows you to re-enable it later if needed.

Steps

1. In the upper right of the BlueXP console, select  > **Identity & Access Management**.
2. Select the **Federation** tab.
3. Select the actions menu  next to the federation that you want to add a verified domain to and select **Disable**.



Delete a federation

If you no longer need a federation, you can delete it. This removes the federation from BlueXP and prevents any users associated with the federation from logging in to BlueXP using their corporate credentials. For example, if the IdP is being decommissioned or if the federation is no longer needed. After you delete a federation, you cannot recover it. You must create a new federation.



You must disable a federation before you can delete it. You cannot undelete a federation after you delete it.

Steps

1. In the upper right of the BlueXP console, select  > **Identity & Access Management**.
2. Select the **Federation** tab.
3. Select the actions menu  next to the federation that you want to add a verified domain to and select **Delete**.

Import your federation to BlueXP

If you have previously setup federation through NetApp Cloud Central (an external application to BlueXP) the Federation page prompts you to import your existing federated connection to BlueXP to manage it in the new interface. This allows you to take advantage of the latest enhancements without having to recreate your federated connections.

Existing customers who have already set up federated connections to BlueXP can import their existing federations to the new interface. This allows you to manage your federated connections in the new Federations page without having to recreate them.




After you import your existing federation, you can manage the federation from the Federations page. [Learn more about managing federations](#).

Required role

Organization admin or Federation admin. [Learn more about access roles](#).

Steps

1. In the upper right of the BlueXP console, select  > **Identity & Access Management**.
2. Select the **Federation** tab.
3. Select **Import Federation**.

Connectors

Maintain the Connector VM and operating system

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



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

Operating system patches and the Connector

Apply OS security patches without stopping Connector host services.

VM or instance type

If you create a Connector from BlueXP, it deploys a VM instance in your cloud provider with a default configuration. After you create the Connector, don't switch to a smaller VM instance with less CPU or RAM.

The following table lists the CPU and RAM requirements:

CPU

8 cores or 8 vCPUs

RAM

32 GB

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

Monitor the Connector

BlueXP notifies you when the Connector VM is unhealthy, including disk space, RAM, and CPU issues. Monitor these notifications in the Notifications Center within BlueXP or configure email notifications. Occasional increases in disk space, memory, or CPU usage are normal, but if it happens frequently, you should take steps to resolve.

BlueXP notifies you when a Connector resource (CPU, RAM, or disk space) exceeds 90% of its total capacity for 30 consecutive minutes. Afterwards, if the resource usage drops below that threshold, the notification displays as resolved (green) in the Notifications Center.



Work with NetApp support if you have questions about modifying your Connector VM.

[Learn more.](#)

Notification	Action needed
Disk space is too high	Review the NetApp Knowledge Base article.
CPU usage is too high	Increase the CPU size of the Connector VM in your hyperscaler or on-premises, depending on where you installed it. Alternatively, create additional Connectors and distribute the workload across multiple Connectors. RAM utilization can vary based on your environment, ONTAP workloads, number of Cloud Volumes ONTAP systems, and the data services that you are using.

Notification	Action needed
RAM usage is too high	Increase the RAM of the Connector VM in your hyperscaler or on-premises, depending on where you installed it. Alternatively, create additional Connectors and distribute the workload across multiple Connectors. RAM utilization can vary based on your environment, ONTAP workloads, number of Cloud Volumes ONTAP systems, and the data services that you are using.

Stopping and starting the Connector VM

If you need to, stop and start the Connector VM using your cloud provider's console or standard on-premises procedures.

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

Connect to the Linux VM

If you need to connect to the Linux VM that the Connector runs on, use the connectivity options from your cloud provider.

AWS

When you create the Connector instance in AWS, provide an AWS access key and secret key. You can use this key pair to SSH to the instance. Use the user name 'ubuntu' for the EC2 Linux instance. For Connectors created prior to May 2023, use the user name 'ec2-user'.

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

Azure

When you create the Connector VM in Azure, you specify a user name and choose to authenticate with a password or SSH public key. Use the authentication method that you chose to connect to the VM.

[Azure Docs: SSH into your VM](#)

Google Cloud

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

[Google Cloud Docs: Connect to Linux VMs](#)

Change the IP address for a Connector

You can change the internal and public IP addresses of the Connector instance assigned by your cloud provider if needed.

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. Restart the Connector instance to register a new public 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.

Update the backup location for each Cloud Volumes ONTAP system.

- a. From the Cloud Volumes ONTAP CLI, set the privilege level to advanced:

```
set -privilege advanced
```

- b. Run the following command to display the current backup target:

```
system configuration backup settings show
```

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

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

Edit a Connector's URIs

You can add and remove the Uniform Resource Identifier (URI) for a Connector.

Steps

1. Select the **Connector** drop-down from the BlueXP header.
2. Select **Manage Connectors**.
3. Expand the **Connector URIs** bar to view connector URIs.
4. Add and remove URIs and then select **Apply**.

Install a CA-signed certificate for web-based console access

When you use BlueXP in restricted mode or private mode, the user interface is accessible from the Connector virtual machine that's deployed in your cloud region or on-premises. By default, BlueXP uses a self-signed SSL certificate to provide secure HTTPS access to the web-based console running on the Connector. If required by your business, you can install a certificate signed by a certificate authority (CA), which provides better security protection than a self-signed certificate. After you install the certificate, BlueXP uses the CA-signed certificate when users access the web-based console.

Before you begin

You need to create a Connector before you can change BlueXP settings. [Learn how to create a Connector](#).

Install an HTTPS certificate

Install a certificate signed by a CA for secure access to the web-based console running on the Connector.

About this task

You can install the certificate using one of the following options:

- Generate a certificate signing request (CSR) from BlueXP, submit the certificate request to a CA, and then install the CA-signed certificate on the Connector.

The key pair that BlueXP uses to generate the CSR is stored internally on the Connector. BlueXP automatically retrieves the same key pair (private key) when you install the certificate on the Connector.

- Install a CA-signed certificate that you already have.

With this option, the CSR is not generated through BlueXP. You generate the CSR separately and store the private key externally. You provide BlueXP with the private key when you install the certificate.

Steps

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

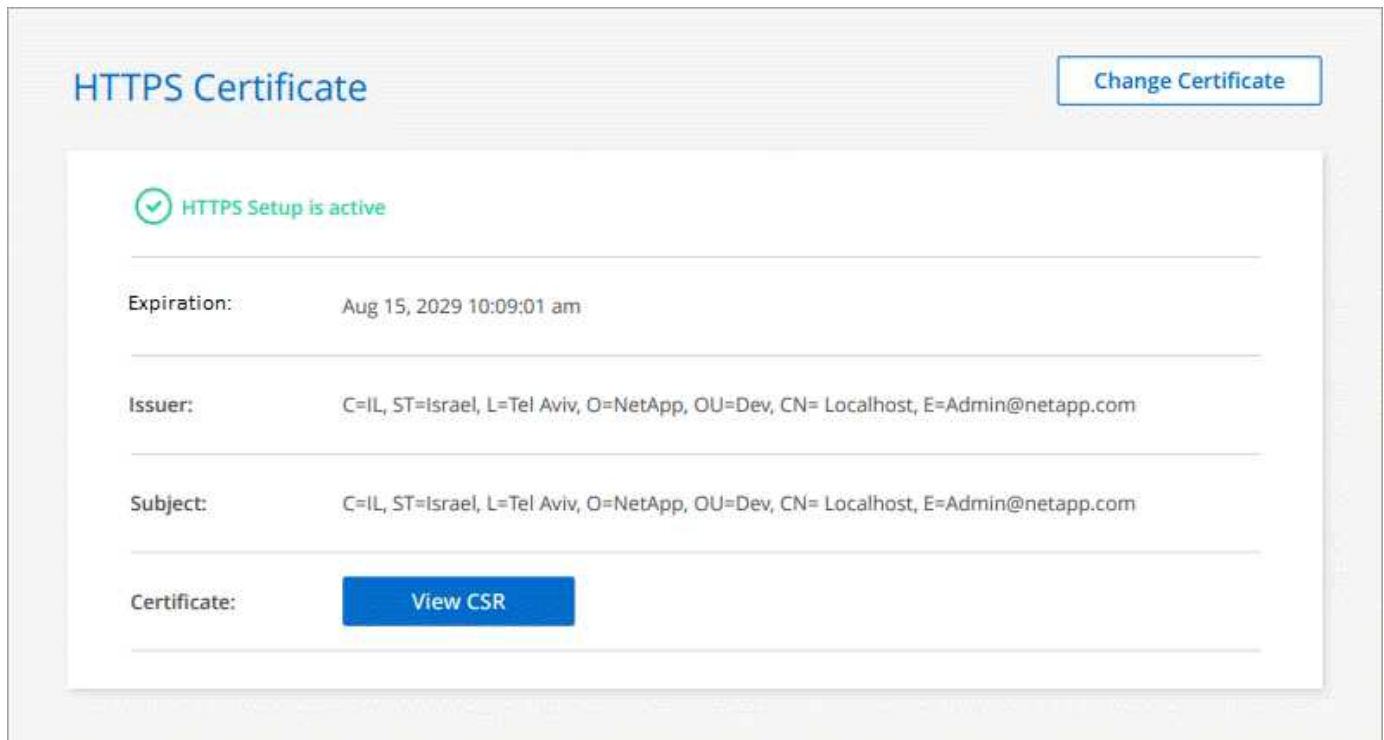


2. In the HTTPS Setup page, install a certificate by generating a certificate signing request (CSR) or by installing your own CA-signed certificate:

Option	Description
Generate a CSR	<ol style="list-style-type: none"> a. Enter the host name or DNS of the Connector host (its Common Name), and then select Generate CSR. BlueXP displays a certificate signing request. b. Use the CSR to submit an SSL certificate request to a CA. The certificate must use the Privacy Enhanced Mail (PEM) Base-64 encoded X.509 format. c. Upload the certificate file and then select Install.
Install your own CA-signed certificate	<ol style="list-style-type: none"> a. Select Install CA-signed certificate. b. Load both the certificate file and the private key and then select Install. The certificate must use the Privacy Enhanced Mail (PEM) Base-64 encoded X.509 format.

Result

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



Renew the BlueXP HTTPS certificate

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

Steps

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

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

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

Result

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

Configure a Connector to use a proxy server

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

The Connector's proxy server enables outbound internet access without a public IP or NAT gateway. The proxy server provides outbound connectivity only for the Connector, not for Cloud Volumes ONTAP systems.

If Cloud Volumes ONTAP systems lack outbound internet access, BlueXP configures them to use the Connector's proxy server. You must ensure that the Connector's security group allows inbound connections over port 3128. Open this port after deploying the Connector.

If the Connector itself doesn't have an outbound internet connection, Cloud Volumes ONTAP systems cannot use the configured proxy server.

Supported configurations

- Transparent proxy servers are supported for Connectors that serve Cloud Volumes ONTAP systems. If you use BlueXP services with Cloud Volumes ONTAP, create a dedicated Connector for Cloud Volumes ONTAP where you can use a transparent proxy server.
- Explicit proxy servers are supported with all Connectors, including those that manage Cloud Volumes ONTAP systems and those that manage BlueXP services.
- HTTP and HTTPS.
- The proxy server can reside in the cloud or in your network.



Once you have configured a proxy, you cannot change the proxy type. If you need to change the proxy type, you remove the Connector and add a new Connector with the new proxy type.

Enable an explicit 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.

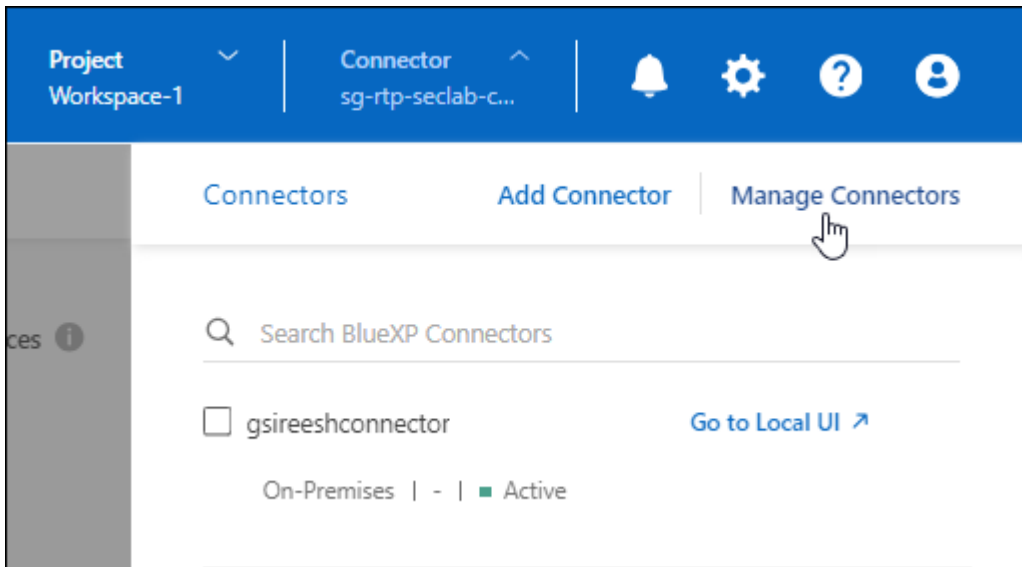
This operation restarts the Connector. Verify the Connector is idle before proceeding.

Steps

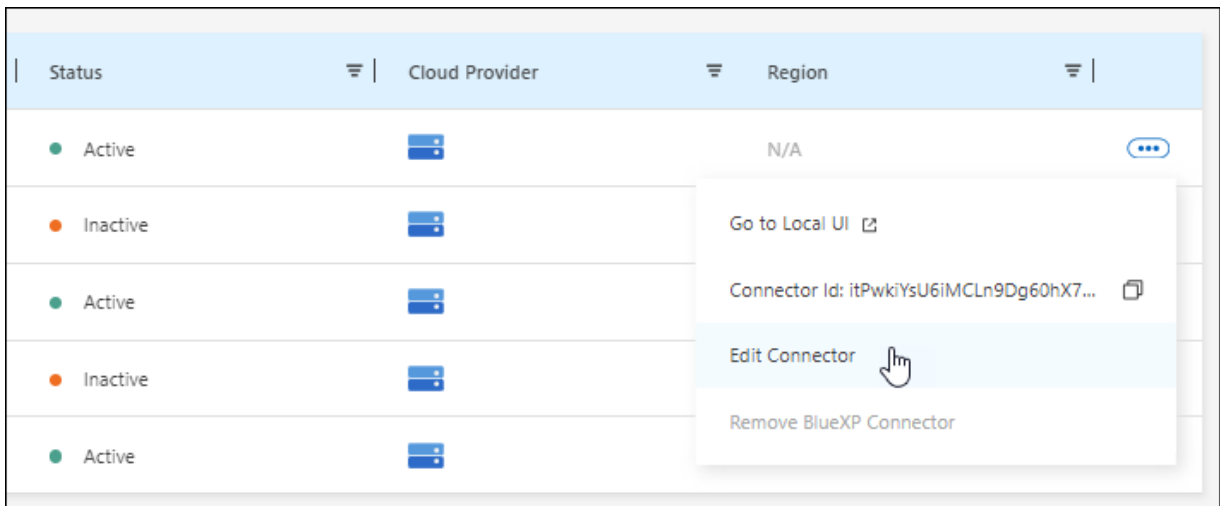
1. Navigate to the **Edit BlueXP Connector** page.

Standard mode

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

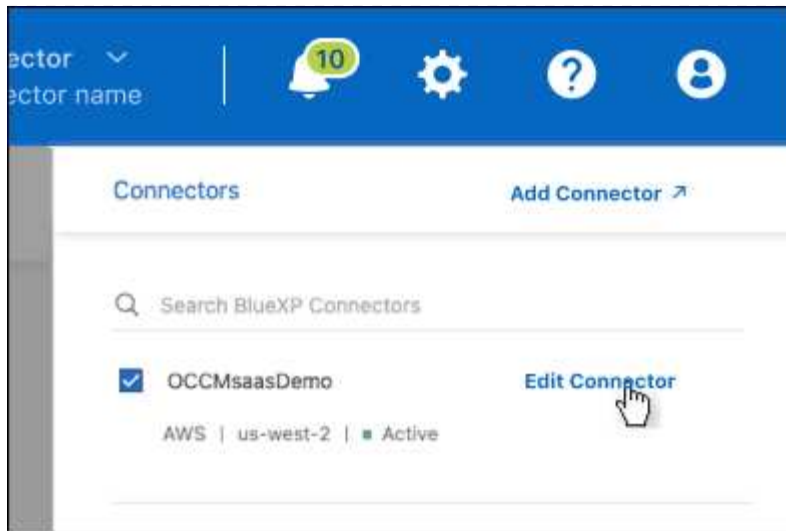


- Select the action menu for a Connector and select **Edit Connector**.



Restricted or private mode

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



2. Select **HTTP Proxy Configuration**.
3. Select **Explicit proxy** in the Configuration type field.
4. Select **Enable Proxy**.
5. Specify the server using the syntax `http://address:port` or `https://address:port`
6. Specify a user name and password if basic authentication is required for the server.

Note the following:

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

For example: `netapp%92proxy`

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

7. Select **Save**.

Enable a transparent proxy on a Connector

Only Cloud Volumes ONTAP supports using a transparent proxy on the Connector. If you use BlueXP services in addition to Cloud Volumes ONTAP, you should create a separate Connector to use for data services or to use for Cloud Volumes ONTAP.

Before enabling a transparent proxy, ensure that the following requirements are met:

- The Connector is installed on the same network as the transparent proxy server.
- TLS inspection is enabled on the proxy server.
- You have a certificate in PEM format that matches the one used on the transparent proxy server.
- You do not use the Connector for any NetApp data services other than Cloud Volumes ONTAP.

To configure an existing Connector to use a transparent proxy server, you use the Connector maintenance tool that is available through the command line on the Connector host.

When you configure a proxy server, the Connector restarts. Verify the Connector is idle before proceeding.

Steps

Ensure that you have a certificate file in PEM format for the proxy server. If you do not have a certificate, contact your network administrator to obtain one.

1. Open a command-line interface on the Connector host.
2. Navigate to the Connector maintenance tool directory: `/opt/application/netapp/service-manager-2/connector-maint-console`
3. Run the following command to enable the transparent proxy, where `/home/ubuntu/<certificate-file>.pem` is the directory and name certificate file that you have for the proxy server:

```
./connector-maint-console proxy add -c /home/ubuntu/<certificate-file>.pem
```

Ensure that the certificate file is in PEM format and resides in the same directory as the command or specify the full path to the certificate file.

```
./connector-maint-console proxy add -c /home/ubuntu/<certificate-file>.pem
```

Modify the transparent proxy for the Connector

You can update a Connector's existing transparent proxy server by using the `proxy update` command or remove the transparent proxy server by using the `proxy remove` command. For more information, review the documentation for [Connector maintenance console](#).



Once you have configured a proxy, you cannot change the proxy type. If you need to change the proxy type, you remove the Connector and add a new Connector with the new proxy type.

Update the Connector proxy if it loses access to the internet

If the proxy configuration for your network changes, your Connector might lose access to the internet. For example, if someone changes the password for the proxy server or updates the certificate. In this case, you'll need to access the UI from the Connector host directly and update the settings. Ensure you have network access to the Connector host and that you can log into the BlueXP UI.

Enable direct API traffic

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

If you disable Azure Private Links with Cloud Volumes ONTAP and use service endpoints, enable direct API traffic. Otherwise, the traffic won't be routed properly.

[Learn more about using an Azure Private Link or service endpoints with Cloud Volumes ONTAP](#)

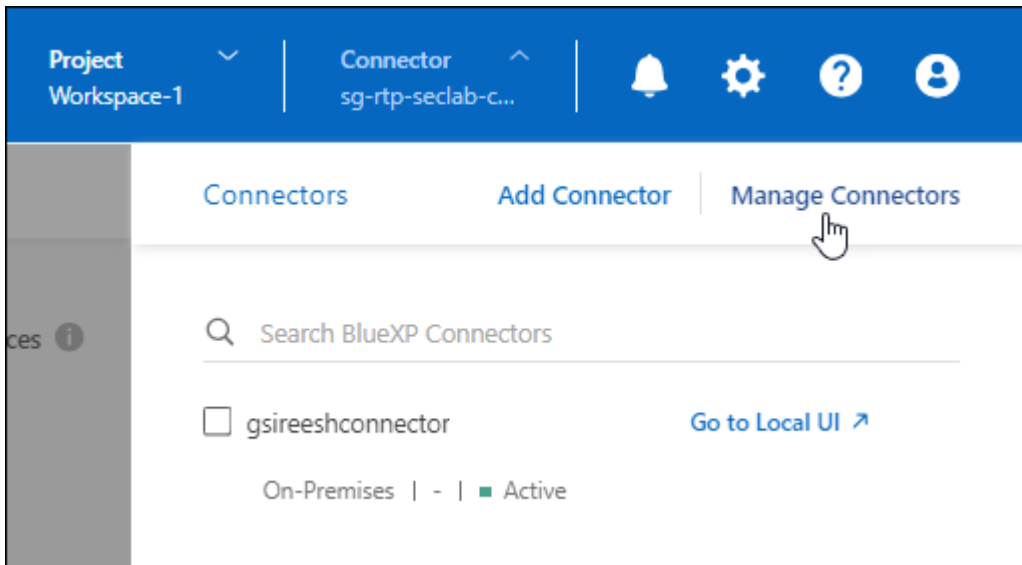
Steps

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

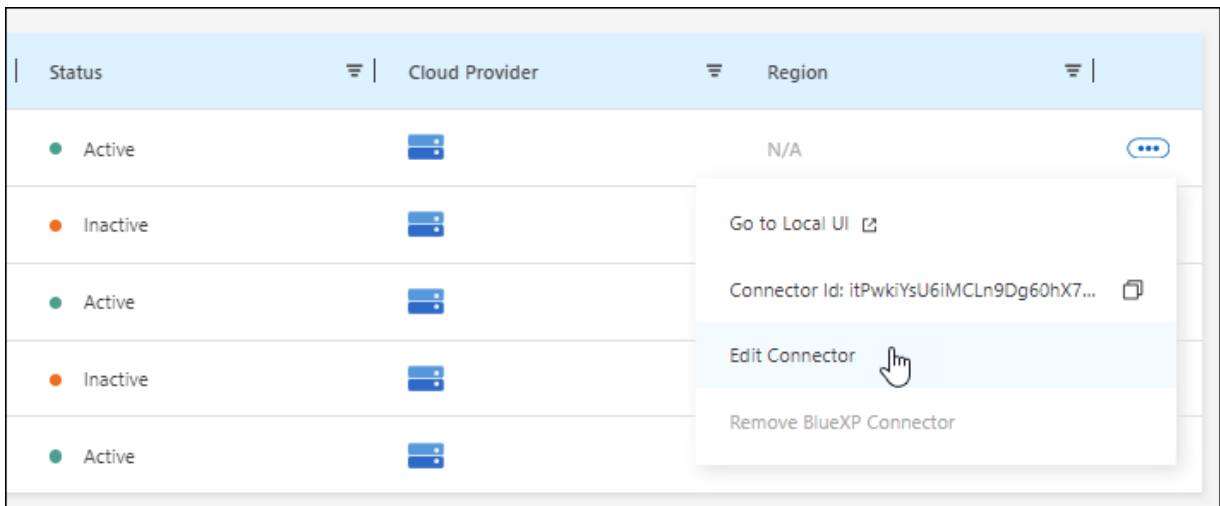
Navigation depends on your BlueXP mode. In standard mode, access the interface from the SaaS website. In restricted or private mode, access it locally from the Connector host.

Standard mode

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

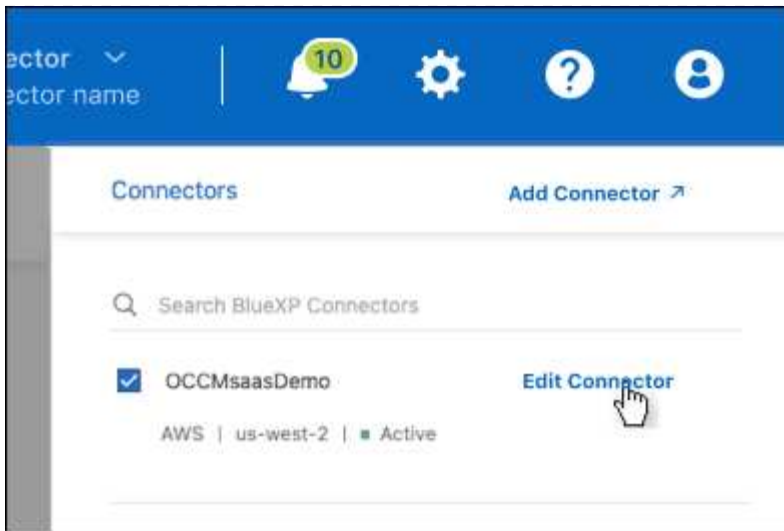


- Select the action menu for a Connector and select **Edit Connector**.



Restricted or private mode

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



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

Require the use of IMDSv2 on Amazon EC2 instances

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

Before you begin

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

About this task

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

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

- For new Connector deployments from BlueXP or using [Terraform scripts](#), IMDSv2 is enabled by default on the EC2 instance.
- If you launch a new EC2 instance in AWS and then manually install the Connector software, IMDSv2 is also enabled by default.
- If you launch the Connector from the AWS Marketplace, IMDSv1 is enabled by default. You can manually

configure IMDSv2 on the EC2 instance.

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

Steps

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

- a. Connect to the Linux VM for the Connector.

When you created the Connector instance in AWS, you provided an AWS access key and secret key. You can use this key pair to SSH to the instance. The user name for the EC2 Linux instance is ubuntu (for Connectors created prior to May 2023, the user name was ec2-user).

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

- b. Install the AWS CLI.

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

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

Example

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



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

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

- a. Go to the [Amazon EC2 console](#)
- b. From the navigation pane, select **Instances**.
- c. Select a Cloud Volumes ONTAP instance.
- d. Select **Actions > Instance settings > Modify instance metadata options**.
- e. On the **Modify instance metadata options** dialog box, select the following:
 - For **Instance metadata service**, select **Enable**.
 - For **IMDSv2**, select **Required**.
 - Select **Save**.
- f. Repeat these steps for other Cloud Volumes ONTAP instances, including the HA mediator.
- g. [Stop and start the Cloud Volumes ONTAP instances](#)

Result

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

Manage connector upgrades

When you use standard mode or restricted mode, BlueXP automatically upgrades your Connector to the latest release, as long as the Connector has outbound internet access to obtain the software update.

If you need to manually manage when the connector is upgraded, you can disable automatic upgrades for standard mode or restricted mode.



When running BlueXP in private mode, you must always upgrade the connector yourself.

Disable automatic upgrades

Disabling auto-upgrade for your connector consists of two steps. First you need to ensure that your Connector is healthy and up-to-date. Then you'll edit a configuration file to turn off the automatic upgrade feature.



You can only disable automatic upgrades if you have connector version 3.9.48 or higher.

Verify the health of your connector

You should verify that your connector is stable and all containers running on your connector VM are healthy and running. After you disable automatic upgrades, your connector VM stops checking for new services or upgrade packages.

Use one of the following commands to verify your connector. All services should have a status of *Running*. If this isn't the case, contact NetApp support before disabling auto-upgrade.

Docker

```
docker ps -a
```

Podman

```
podman ps -a
```

Disable auto-upgrade for the connector

You disable automatic upgrades by setting the *isUpgradeDisabled* flag in the *com/opt/application/netapp/service-manager-2/config.json* file. By default, this flag is set to false and your connector is automatically upgraded. You can set this flag to true to disable automatic upgrades. You should be familiar with JSON syntax before completing this step.

To re-enable auto-upgrade, use these steps and set the *isUpgradeDisabled* flag to false.

Steps

1. Ensure you have verified that your connector is up-to-date and healthy.
2. Create a backup copy of the */opt/application/netapp/service-manager-2/config.json* file to ensure you can

revert your changes.

3. Edit the `/opt/application/netapp/service-manager-2/config.json` file and change the value of the `isUpgradeDisabled` flag to true.

```
"isUpgradeDisabled": true,
```

4. Save your file.
5. Restart the service manager 2 service by running the following command:

```
systemctl restart netapp-service-manager.service
```

6. Run the following command and verify that the Connector status shows as *active(running)*:

—

```
systemctl status netapp-service-manager.service
```

Upgrade the connector

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

Steps

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

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

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

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

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

4. Run the installation script:

```
sudo /path/BlueXP-Connector-Offline-<version>
```

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

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

Work with multiple Connectors

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

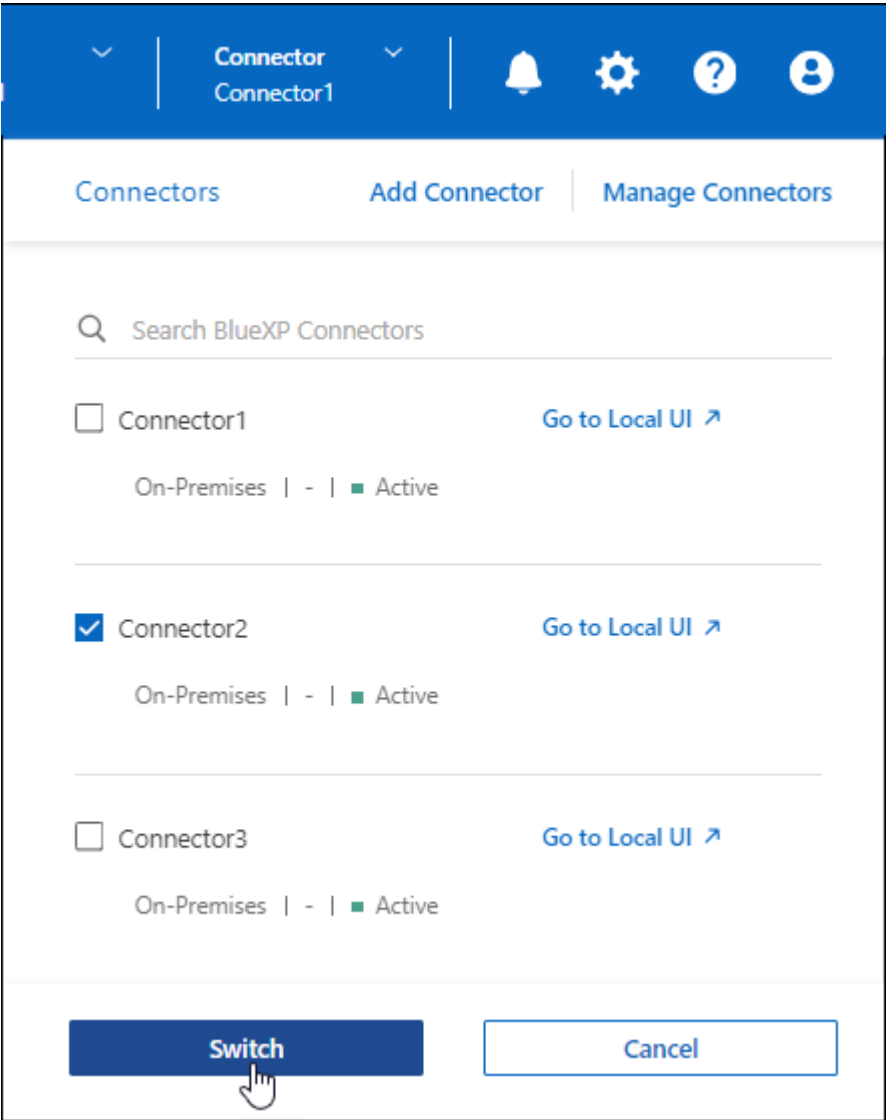
Switch between Connectors

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

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

Step

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



Result

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

Set up a disaster recovery configuration

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

Steps

1. Switch to the other Connector that you want to manage with the working environment.
2. Discover the existing working environment.
 - [Add existing Cloud Volumes ONTAP systems to BlueXP](#)
 - [Discover ONTAP clusters](#)
3. If you're managing a Cloud Volumes ONTAP working environment, select **Settings > Connector Settings** and set the Capacity Management Mode to **Manual Mode**.

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

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

Troubleshoot the Connector

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

Related information

[Get help from NetApp Support.](#)

Find the system ID for a Connector

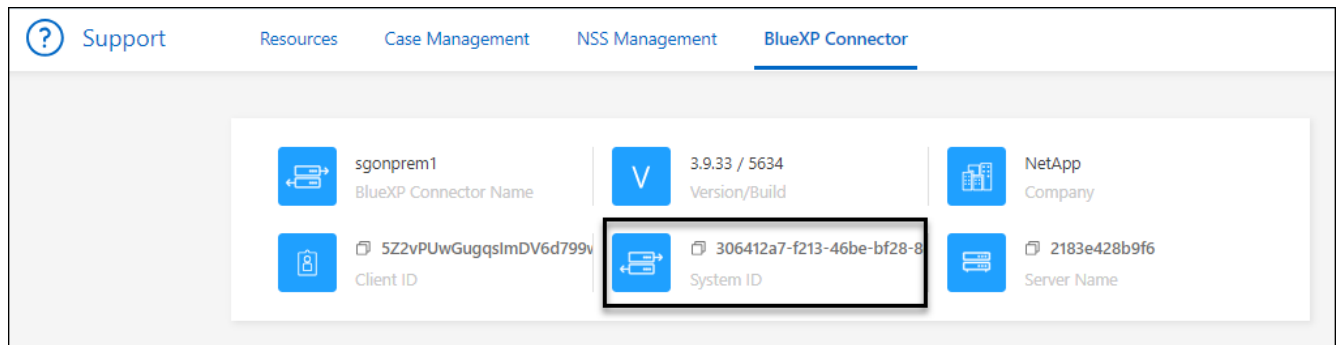
To help you get started, your NetApp representative might ask you for the system ID of your Connector. The ID is typically used for licensing and troubleshooting purposes.

Steps

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

The system ID appears at the top of the page.

Example



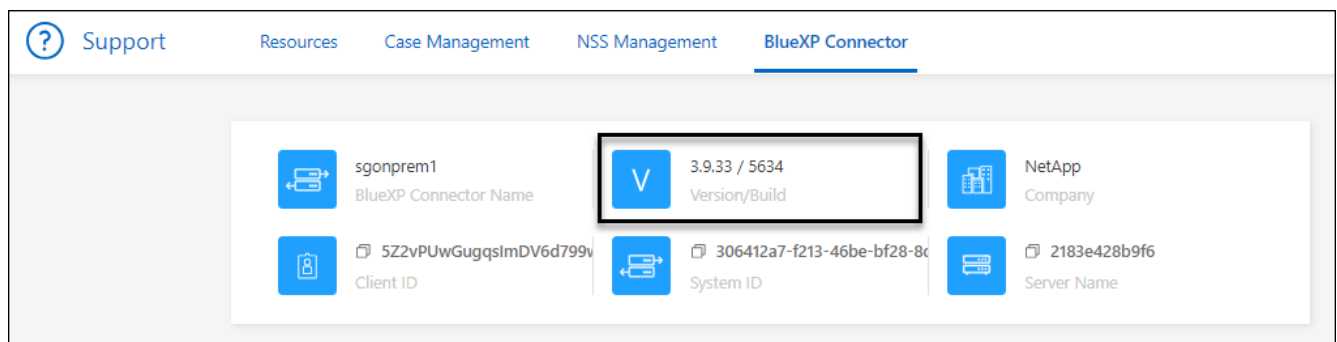
View a Connector's version

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

Steps

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

The version displays at the top of the page.

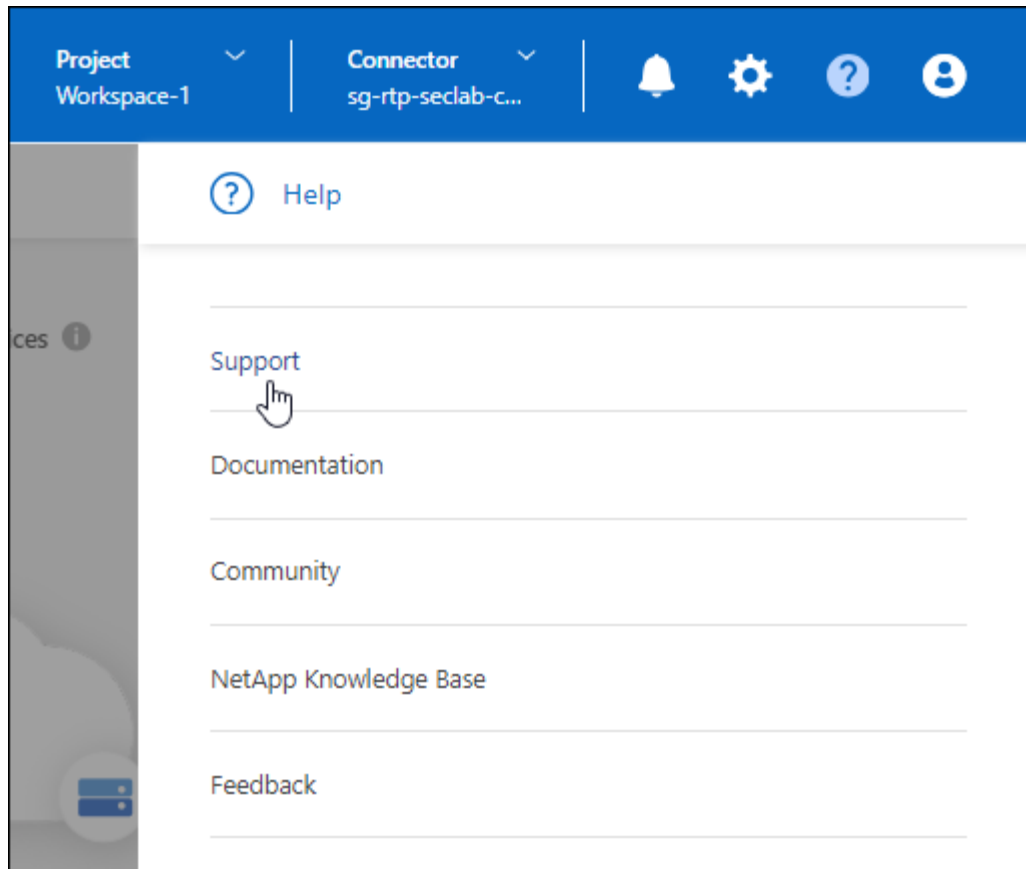


Download or send an AutoSupport message

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

Steps

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



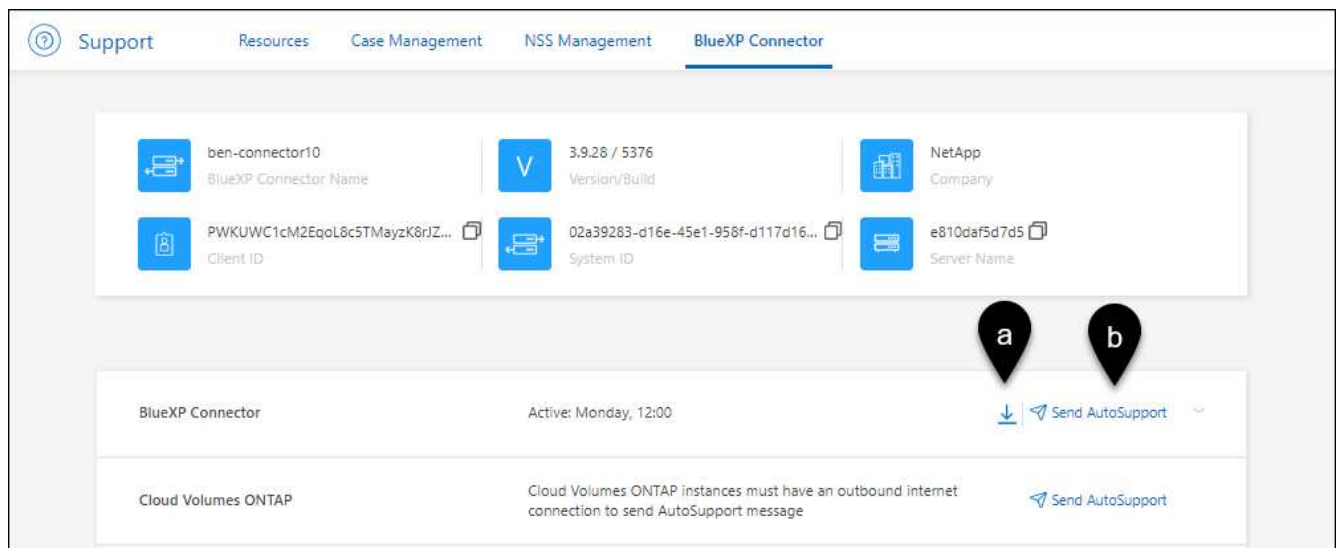
2. Select **BlueXP Connector**.

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

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



BlueXP may take up to five hours to send AutoSupport messages due to load balancing. For urgent communication, download the file and send it manually.



Fix download failures when using a Google Cloud NAT gateway

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

Step

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

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

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

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

[Learn more about the /occm/config API call](#)

Get help from the NetApp Knowledge Base

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

Uninstall and remove the Connector

Uninstall the Connector software to troubleshoot issues or to permanently remove the software from the host. The steps that you need to use depends on the deployment mode that you're using. Once a Connector has been removed from your environment, you can remove it from BlueXP.

[Learn about BlueXP deployment modes.](#)

Uninstall the Connector when using standard or restricted mode

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

Steps

1. Connect to the Linux VM for the Connector.
2. From the Linux host, run the uninstallation script:

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

silent runs the script without prompting you for confirmation.

Uninstall the Connector when using private mode

If you're using private mode (where the Connector host has *no* outbound connectivity), follow the steps below to uninstall the Connector software.

Step

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

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

3. From the Linux host, delete old, unused container image files to free space in the /var directory for re-installation.

Podman

```
podman system prune --all
```

Docker

```
docker system prune -a
```

Remove Connectors from BlueXP

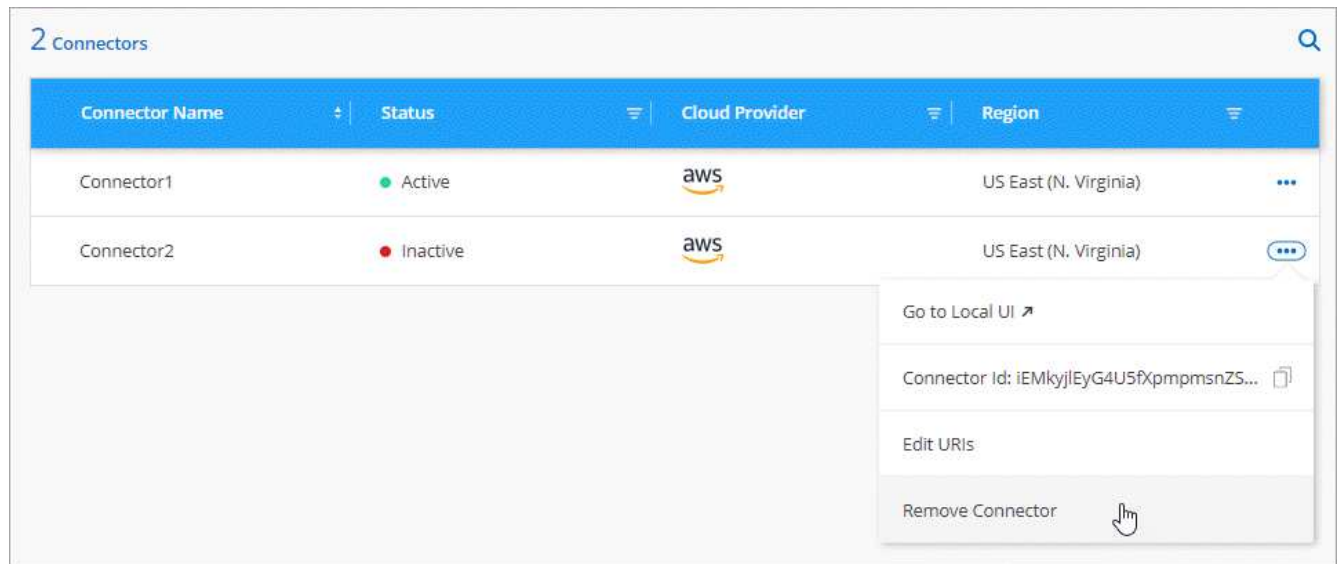
If a Connector is inactive, you can remove it from the list of Connectors in BlueXP. You might do this if you delete the Connector virtual machine or if you uninstall the Connector software.

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, you can't add it back.

Steps

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



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

Default configuration for the Connector

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

Default configuration with internet access

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

AWS details

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

- The EC2 instance type is t3.2xlarge.
- The operating system for the image is Ubuntu 22.04 LTS.

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

- The installation includes Docker Engine, which is the required container orchestration tool.
- The user name for the EC2 Linux instance is ubuntu (for Connectors created prior to May 2023, the user name was ec2-user).
- The default system disk is a 100 GiB gp2 disk.

Azure details

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

- The VM type is Standard_D8s_v3.
- The operating system for the image is Ubuntu 22.04 LTS.

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

- The installation includes Docker Engine, which is the required container orchestration tool.
- The default system disk is a 100 GiB premium SSD disk.

Google Cloud details

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

- The VM instance is n2-standard-8.
- The operating system for the image is Ubuntu 22.04 LTS.

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

- The installation includes Docker Engine, which is the required container orchestration tool.
- The default system disk is a 100 GiB SSD persistent disk.

Installation folder

The Connector installation folder resides in the following location:

`/opt/application/netapp/cloudmanager`

Log files

Log files are contained in the following folders:

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

The logs in these folders provide details about the Connector.

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

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

Connector service

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

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

Ports

The Connector uses the following ports on the Linux host:

- 80 for HTTP access
- 443 for HTTPS access

Default configuration without internet access

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

- The Connector installation folder resides in the following location:

`/opt/application/netapp/ds`

- Log files are contained in the following folders:

`/var/lib/docker/volumes/ds_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

Enforce ONTAP permissions for ONTAP Advanced View (ONTAP System Manager)

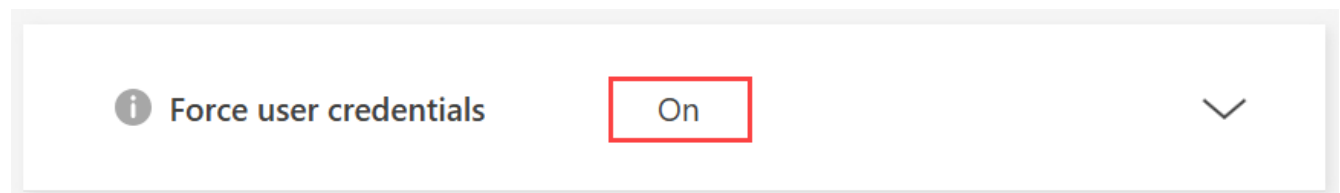
By default, the Connector credentials allow users to access the Advanced View (ONTAP System Manager). You can prompt users for their ONTAP credentials instead. This ensures that a user's ONTAP permissions are applied when they work with ONTAP clusters in both Cloud Volumes ONTAP and ONTAP on-premises clusters.



You must have the Organization admin role to edit Connector settings.

Steps

1. Select the **Connector** drop-down from the BlueXP header.
2. Select **Manage Connectors**.
3. Select the action menu in the row that corresponds to the Connector you want to edit.
4. Expand the **Force Credentials** option.
5. Select the checkbox to enable the **Force Credentials** option and then select **Save**.
6. Check if the **Force Credentials** option is enabled.



Credentials and subscriptions

AWS

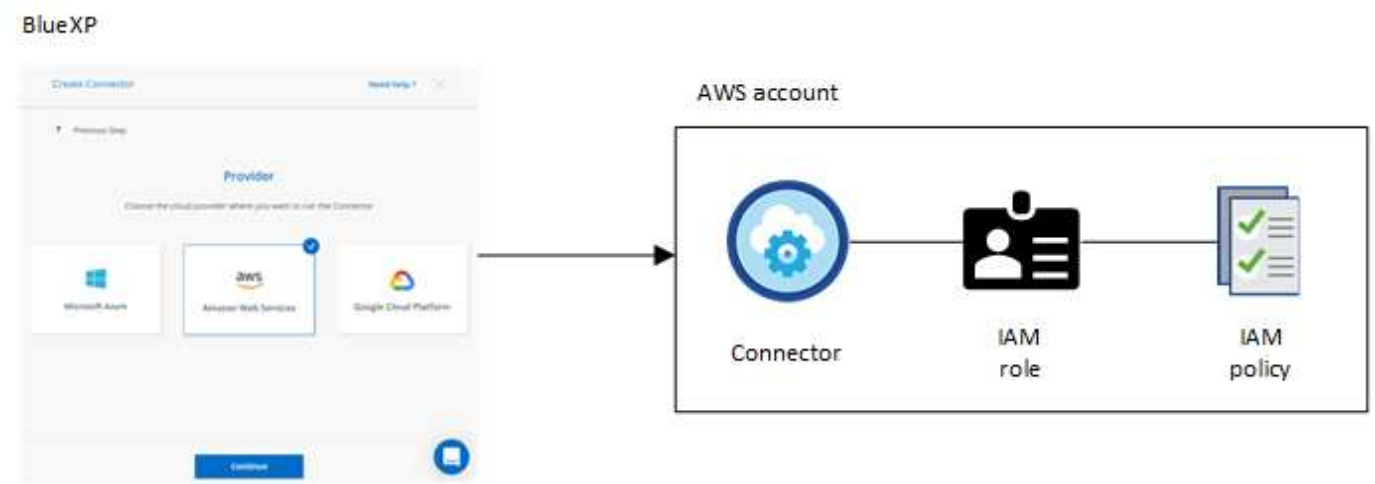
Learn about AWS credentials and permissions in BlueXP

Learn how BlueXP uses AWS credentials to perform actions on your behalf and how those credentials are associated with marketplace subscriptions. Understanding these details can be helpful as you manage the credentials for one or more AWS accounts in BlueXP. For example, you might want to learn about when to add additional AWS credentials to BlueXP.

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](#).



If you create a new working environment for Cloud Volumes ONTAP, BlueXP selects these AWS credentials by default:

Details & Credentials			
Instance Profile		QA Subscription	Edit Credentials
Credentials	Account ID	Marketplace Subscription	

You can deploy all of your Cloud Volumes ONTAP systems using the initial AWS credentials, or you can add additional credentials.

Additional AWS credentials

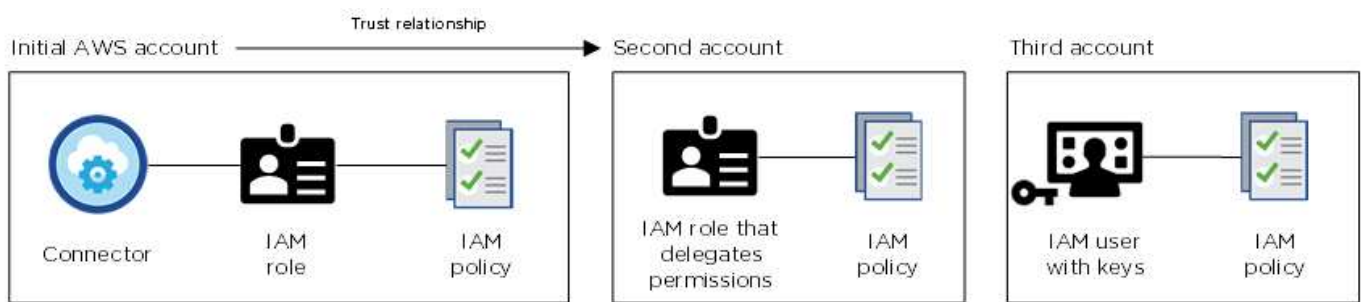
You might add additional AWS credentials to BlueXP in the following cases:

- To use your existing BlueXP Connector with an additional AWS account
- To create a new Connector in a specific AWS account
- To create and manage FSx for ONTAP file systems

Review the sections below for more details.

Add AWS credentials to use a Connector with another AWS account

If you want to use BlueXP with additional 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.

For example, you can switch between credentials when creating a new Cloud Volumes ONTAP working environment:

Edit Credentials & Add Subscription

Associate Subscription to Credentials ⓘ

Credentials

- keys | Account ID: [redacted]
- Instance Profile | Account ID: [redacted]
- casaba QA subscription

+ Add Subscription

Apply Cancel

[Learn how to add AWS credentials to an existing Connector.](#)

Add AWS credentials to create a Connector

Adding new AWS credentials to BlueXP provides the permissions needed to create a Connector.

[Learn how to add AWS credentials to BlueXP for creating a Connector](#)

Add AWS credentials for FSx for ONTAP

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

[Learn how to add AWS credentials to BlueXP for Amazon FSx for ONTAP](#)

Credentials and marketplace subscriptions

The credentials that you add to a Connector must be associated with an AWS Marketplace subscription so that you can pay for Cloud Volumes ONTAP at an hourly rate (PAYGO) or through an annual contract, and to use other BlueXP services.

[Learn how to associate an AWS subscription.](#)

Note the following about AWS credentials and marketplace subscriptions:

- You can associate only one AWS Marketplace subscription with a set of AWS credentials
- You can replace an existing marketplace subscription with a new subscription

FAQ

The following questions are related to credentials and subscriptions.

How can I securely rotate my AWS credentials?

As described in the sections 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.

Can I change the AWS Marketplace subscription for Cloud Volumes ONTAP working environments?

Yes, you can. When you change the AWS Marketplace subscription that's associated with a set of credentials, all existing and new Cloud Volumes ONTAP working environments will be charged against the new subscription.

[Learn how to associate an AWS subscription.](#)

Can I add multiple AWS credentials, each with different marketplace subscriptions?

All AWS credentials that belong to the same AWS account will be associated with the same AWS Marketplace subscription.

If you have multiple AWS credentials that belong to different AWS accounts, then those credentials can be associated with the same AWS Marketplace subscription or with different subscriptions.

Can I move existing Cloud Volumes ONTAP working environments to a different AWS account?

No, it's not possible to move the AWS resources associated with your Cloud Volumes ONTAP working environment to a different AWS account.

How do credentials work for marketplace deployments and on-premises 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 manually install the Connector software on your own Linux host.

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 using AWS access keys.

To learn how to set up permissions, refer to the following pages:

- Standard mode
 - [Set up permissions for an AWS Marketplace deployment](#)
 - [Set up permissions for on-premises deployments](#)
- [Set up permissions for restricted mode](#)
- [Set up permissions for private mode](#)

Manage AWS credentials and marketplace subscriptions for BlueXP

Add and manage AWS credentials so that you deploy and manage cloud resources in your AWS accounts from BlueXP. If you manage multiple AWS Marketplace 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

Add AWS credentials to a Connector to manage resources in your 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

Add new AWS credentials to BlueXP 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.

Rotate AWS access keys regularly by updating them in BlueXP. This process is manual.

Add additional credentials to a Connector

Add additional 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.

If you're just getting started with BlueXP, [Learn how BlueXP uses AWS credentials and permissions.](#)

Grant permissions

Provide required permissions before adding AWS credentials to a Connector. The permissions allow the Connector to manage resources and processes within that AWS account. You can provide the permissions with the 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 ensures the necessary permissions are in place for managing resources. [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.

If the Connector is installed on-premises, you can't use this authentication method. You must use AWS keys.

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, select **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.

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

Steps

1. From the IAM console, create 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 begin

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 and then add you add the credentials.

Steps

1. Use the top navigation bar to elect the Connector to which you want to add credentials.
2. In the upper right of the console, select the Settings icon, and select **Credentials**.



3. On the **Organization credentials** or **Account credentials** page, select **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 services at an hourly rate (PAYGO) or with an annual contract, you must associate AWS credentials with your AWS Marketplace subscription.
 - d. **Review:** Confirm the details about the new credentials and select **Add**.

Result

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

Edit Credentials & Add Subscription

Associate Subscription to Credentials ?

Credentials

keys | Account ID:

Instance Profile | Account ID:

casaba QA subscription

+ Add Subscription

Apply

Cancel

Add credentials to BlueXP for creating a Connector

Add AWS credentials by providing the ARN of an IAM role that gives 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 software as a service (SaaS) layer to assume the role.

Steps

1. Go to the IAM console in the target account.
2. Under Access Management, select **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
- For Amazon FSx for NetApp ONTAP specifically, edit the **Trust relationships** policy to include "AWS": "arn:aws:iam::952013314444:root".

For example, the policy should look like this:

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Principal": {
        "AWS": "arn:aws:iam::952013314444:root",
        "Service": "ec2.amazonaws.com"
      },
      "Action": "sts:AssumeRole"
    }
  ]
}
```

Refer to [AWS Identity and Access Management \(IAM\) documentation](#) for more information on cross account resource access in IAM.

- 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 begin

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, select the Settings icon, and select **Credentials**.



2. On the **Organization credentials** or **Account credentials** page, select **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 select **Add**.

Add credentials to BlueXP for Amazon FSx for ONTAP

For details, refer to the [BlueXP documentation for Amazon FSx for ONTAP](#)

Configure an AWS subscription

After you add your AWS credentials, you can configure 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 pay for other data services.

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

- You didn't configure a subscription when you initially added the credentials.
- You want to change the AWS Marketplace subscription that is configured to the AWS credentials.

Replacing the current marketplace subscription with a new subscription changes the marketplace subscription for any existing Cloud Volumes ONTAP working environments and all new working environments.

Before you begin

You need to create a Connector before you can configure a subscription. [Learn how to create a Connector](#).

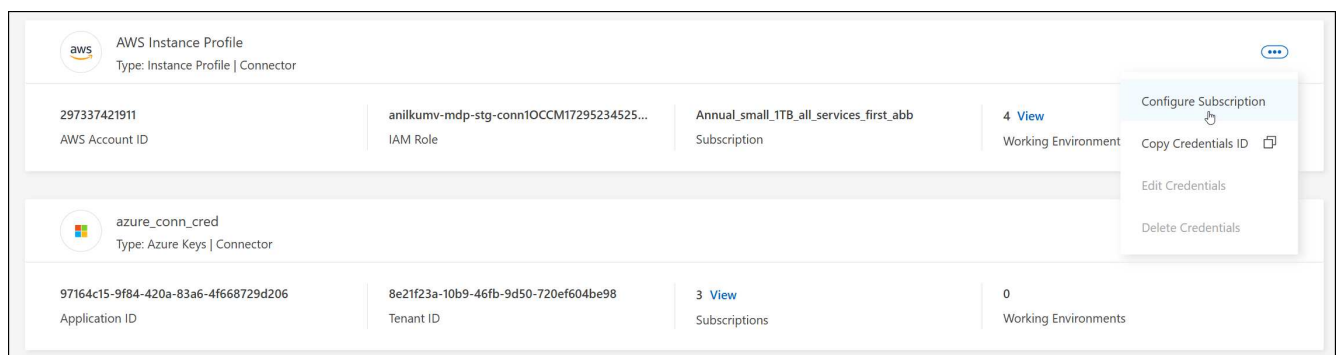
The following video shows the steps to subscribe to NetApp Intelligent Services from the AWS Marketplace:

[Subscribe to NetApp Intelligent Services from the AWS Marketplace](#)

Steps

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

You must select credentials that are associated with a Connector. You can't associate a marketplace subscription with credentials that are associated with BlueXP.



3. To associate the credentials with an existing subscription, select the subscription from the down-down list and select **Configure**.
4. To associate the credentials with a new subscription, select **Add Subscription > Continue** and follow the steps in the AWS Marketplace:
 - a. Select **View purchase options**.
 - b. Select **Subscribe**.

c. Select **Set up your account**.

You'll be redirected to the BlueXP website.

d. From the **Subscription Assignment** page:

- Select the BlueXP organizations or accounts that you'd like to associate this subscription with.
- In the **Replace existing subscription** field, choose whether you'd like to automatically replace the existing subscription for one organization or account with this new subscription.

BlueXP replaces the existing subscription for all credentials in the organization or account with this new subscription. If a set of credentials wasn't ever associated with a subscription, then this new subscription won't be associated with those credentials.

For all other organizations or accounts, you'll need to manually associate the subscription by repeating these steps.

- Select **Save**.

Associate an existing subscription with your organization or account

When you subscribe to from the AWS Marketplace, the last step in the process is to associate the subscription with your organization. If you didn't complete this step, then you can't use the subscription with your organization or account.

- [Learn about BlueXP deployment modes](#)
- [Learn about BlueXP identity and access management](#)

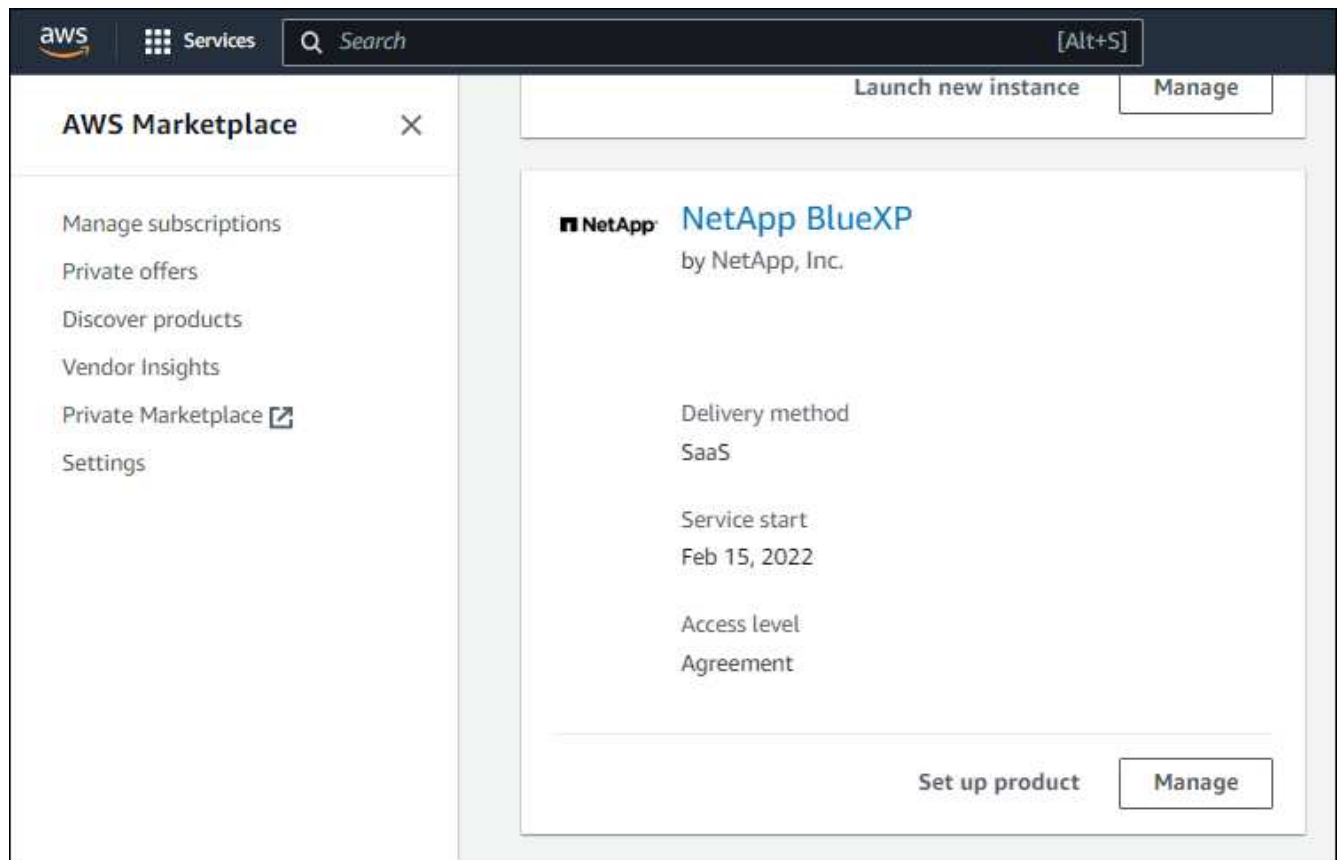
Follow the steps below if you subscribed to NetApp intelligent data services from the AWS Marketplace, but you missed the step to associate the subscription with your account.

Steps

1. Go to the digital wallet to confirm that you didn't associate your subscription with your BlueXP organization or account.
 - a. From the navigation menu, select **Governance > Digital wallet**.
 - b. Select **Subscriptions**.
 - c. Verify that your subscription doesn't appear.

You'll only see the subscriptions that are associated with the organization or account that you're currently viewing. If you don't see your subscription, proceed with the following steps.

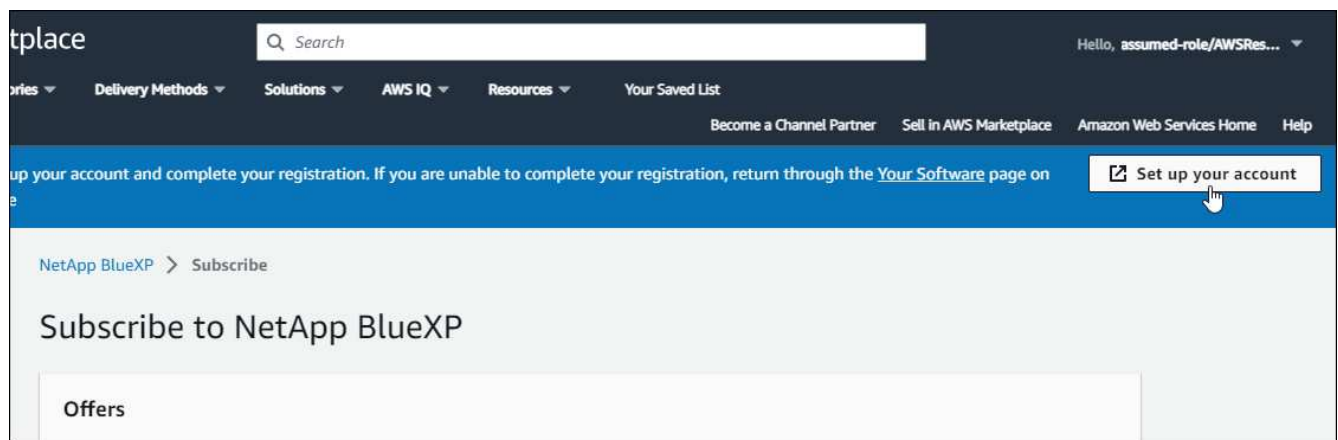
2. Log in to the AWS Console and navigate to **AWS Marketplace Subscriptions**.
3. Find the NetApp Intelligent Data Services subscription.



4. Select **Set up product**.

The subscription offer page should load in a new browser tab or window.

5. Select **Set up your account**.



The **Subscription Assignment** page on netapp.com should load in a new browser tab or window.

Note that you might be prompted to log in to BlueXP first.

6. From the **Subscription Assignment** page:
 - Select the BlueXP organizations or accounts that you'd like to associate this subscription with.
 - In the **Replace existing subscription** field, choose whether you'd like to automatically replace the existing subscription for one organization or account with this new subscription.

BlueXP replaces the existing subscription for all credentials in the organization or account with this new subscription. If a set of credentials wasn't ever associated with a subscription, then this new subscription won't be associated with those credentials.

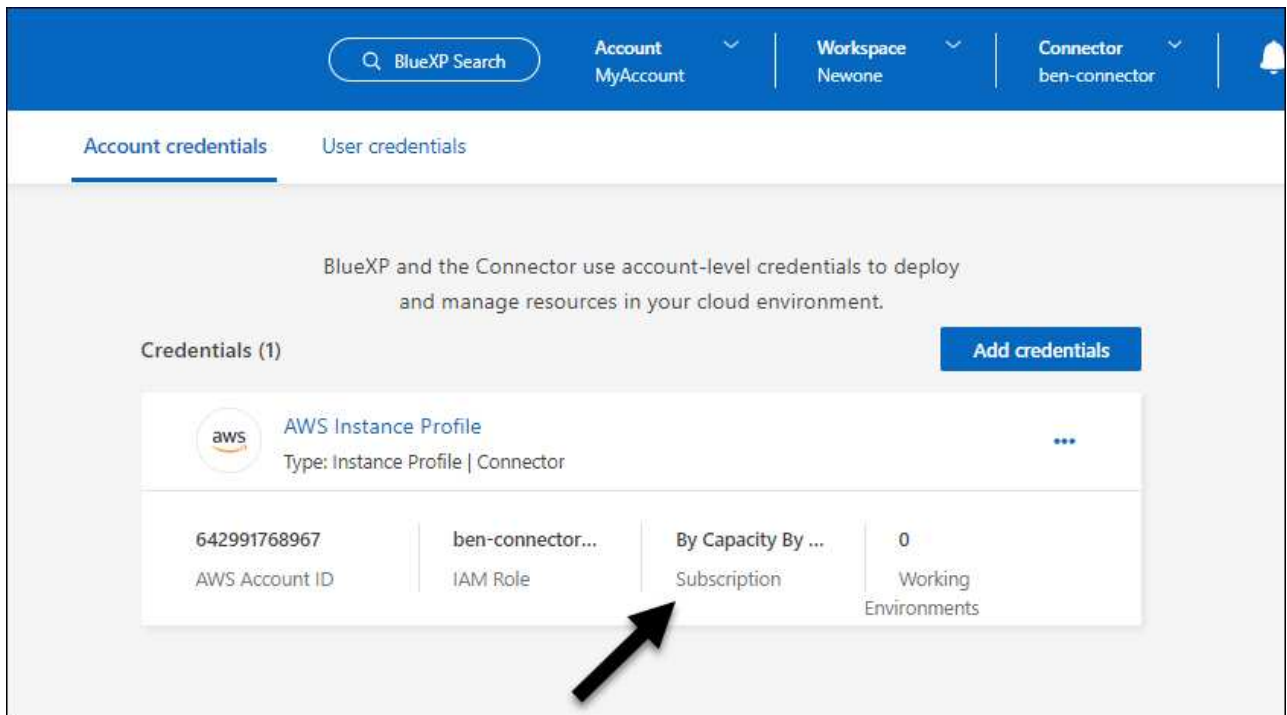
For all other organizations or accounts, you'll need to manually associate the subscription by repeating these steps.

The screenshot shows a 'Subscription Assignment' dialog box. At the top, there is a success message: 'Your subscription to BlueXP / Cloud Volumes ONTAP from the AWS Marketplace was created successfully.' Below this, the 'Subscription name' is set to 'PayAsYouGo'. A section titled 'Select the NetApp accounts that you'd like to associate this subscription with.' contains a table with three rows. The first two rows have their 'Replace existing subscription' toggle switches turned off, while the third row, for 'benAccount', has its toggle switch turned on. A blue 'Save' button is located at the bottom right of the dialog.

NetApp account	Replace existing subscription
<input checked="" type="checkbox"/> cloudTiering_undefined	<input type="checkbox"/>
<input checked="" type="checkbox"/> CS-HhewH	<input type="checkbox"/>
<input checked="" type="checkbox"/> benAccount	<input checked="" type="checkbox"/>

7. Go to the digital wallet to confirm that the subscription is associated with your organization or account.
 - a. From the navigation menu, select **Governance > Digital wallet**.
 - b. Select **Subscriptions**.
 - c. Verify that your subscription appears.
8. Confirm that the subscription is associated with your AWS credentials.
 - a. In the upper right of the console, select the Settings icon, and select **Credentials**.
 - b. On the **Organization credentials** or **Account credentials** page, verify that the subscription is associated with your AWS credentials.

Here's an example.



Edit credentials

Edit your AWS credentials 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 or an Amazon FSx for ONTAP instance. You can only rename the credentials for an FSx for ONTAP instance.

Steps

1. In the upper right of the console, select the Settings icon, and select **Credentials**.
2. On the **Organization credentials** or **Account credentials** page, select the action menu for a set of credentials and then select **Edit Credentials**.
3. Make the required changes and then select **Apply**.

Delete credentials

If you no longer need a set of credentials, you can delete them. 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 console, select the Settings icon, and select **Credentials**.
2. On the **Organization credentials** or **Account credentials** page, select the action menu for a set of credentials and then select **Delete Credentials**.

3. Select **Delete** to confirm.

Azure

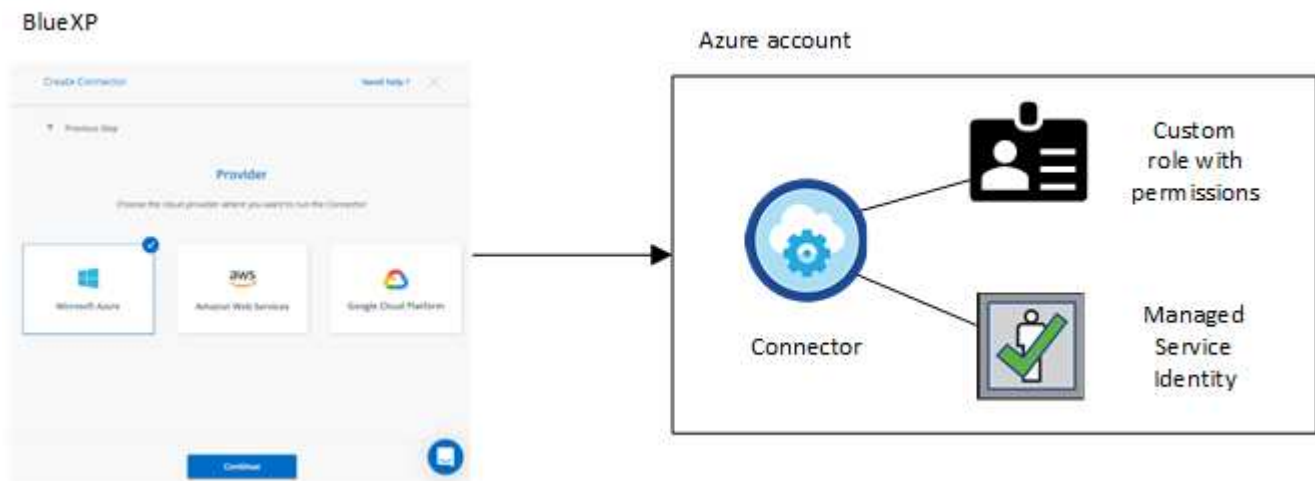
Learn about Azure credentials and permissions in BlueXP

Learn how BlueXP uses Azure credentials to perform actions on your behalf and how those credentials are associated with marketplace subscriptions. Understanding these details can be helpful as you manage the credentials for one or more Azure subscriptions. For example, you might want to learn when to add additional Azure credentials to BlueXP.

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 the 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](#).



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

Details & Credentials			
Managed Service Ide...	OCCM QA1	ⓘ No subscription is associated	Edit Credentials
Credential Name	Azure Subscription	Marketplace Subscription	

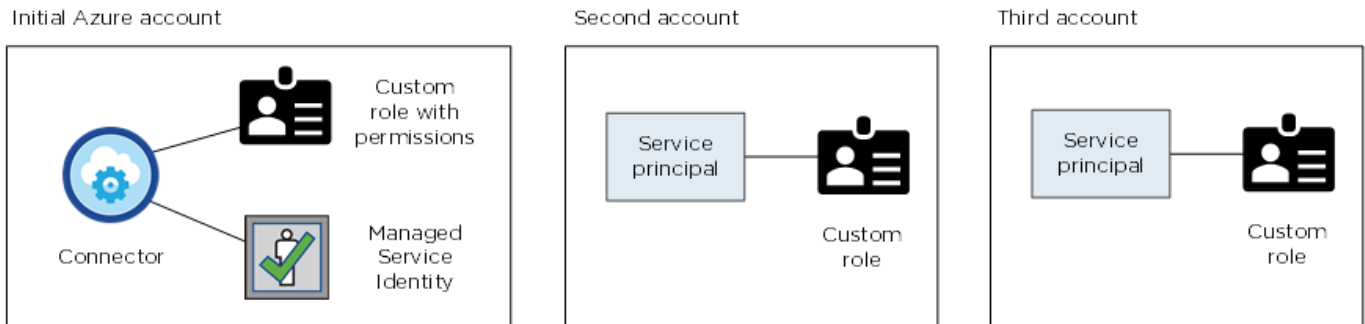
You can deploy all of your Cloud Volumes ONTAP systems using the initial Azure credentials, or you can add additional credentials.

Additional Azure subscriptions for a managed identity

The system-assigned managed identity assigned to the Connector VM 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](#).

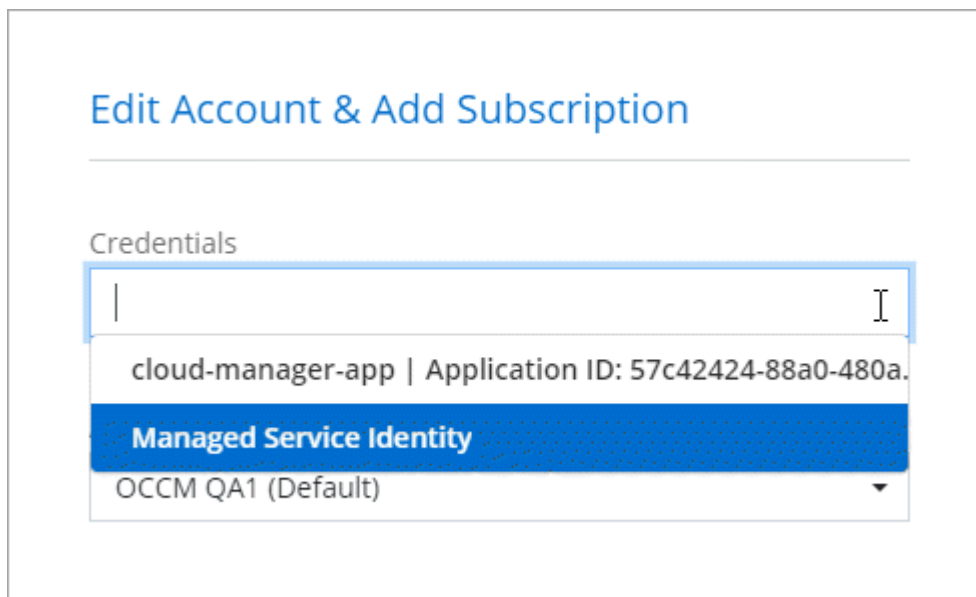
Additional Azure credentials

If you want to use different Azure credentials with BlueXP, then you must grant the required permissions by [creating and setting up a service principal in Microsoft Entra ID](#) 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.

For example, you can switch between credentials when creating a new Cloud Volumes ONTAP working environment:



Credentials and marketplace subscriptions

The credentials that you add to a Connector must be associated with an Azure Marketplace subscription so that you can pay for Cloud Volumes ONTAP at an hourly rate (PAYGO) or through an annual contract, and to use other BlueXP services.

[Learn how to associate an Azure subscription.](#)

Note the following about Azure credentials and marketplace subscriptions:

- You can associate only one Azure Marketplace subscription with a set of Azure credentials
- You can replace an existing marketplace subscription with a new subscription

FAQ

The following question is related to credentials and subscriptions.

Can I change the Azure Marketplace subscription for Cloud Volumes ONTAP working environments?

Yes, you can. When you change the Azure Marketplace subscription that's associated with a set of Azure credentials, all existing and new Cloud Volumes ONTAP working environments will be charged against the new subscription.

[Learn how to associate an Azure subscription.](#)

Can I add multiple Azure credentials, each with different marketplace subscriptions?

All Azure credentials that belong to the same Azure subscription will be associated with the same Azure Marketplace subscription.

If you have multiple Azure credentials that belong to different Azure subscriptions, then those credentials can be associated with the same Azure Marketplace subscription or with different marketplace subscriptions.

Can I move existing Cloud Volumes ONTAP working environments to a different Azure subscription?

No, it's not possible to move the Azure resources associated with your Cloud Volumes ONTAP working environment to a different Azure subscription.

How do credentials work for marketplace deployments and on-premises deployments?

The sections above describe the recommended deployment method for the Connector, which is from BlueXP. You can also deploy a Connector in Azure from the Azure Marketplace, and you can install the Connector software on your own Linux host.

If you use the Marketplace, you can provide permissions by assigning a custom role to the Connector VM and to a system-assigned managed identity, or you can use a Microsoft Entra service principal.

For on-premises deployments, you can't set up a managed identity for the Connector, but you can provide permissions by using a service principal.

To learn how to set up permissions, refer to the following pages:

- Standard mode
 - [Set up permissions for an Azure Marketplace deployment](#)
 - [Set up permissions for on-premises deployments](#)
- [Set up permissions for restricted mode](#)
- [Set up permissions for private mode](#)

Manage Azure credentials and marketplace subscriptions for BlueXP

Add and manage Azure credentials so that BlueXP has the permissions that it needs to deploy and manage cloud resources in your Azure subscriptions. If you manage multiple

Azure Marketplace subscriptions, you can assign each one of them to different Azure credentials from the Credentials page.

Follow the steps on this page if you need to use multiple Azure credentials or multiple Azure Marketplace subscriptions for Cloud Volumes ONTAP.

Overview

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.

Associate 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. Select **Access control (IAM)**.
 - a. Select **Add > Add role assignment** and then add the permissions:
 - Select the **BlueXP Operator** role.

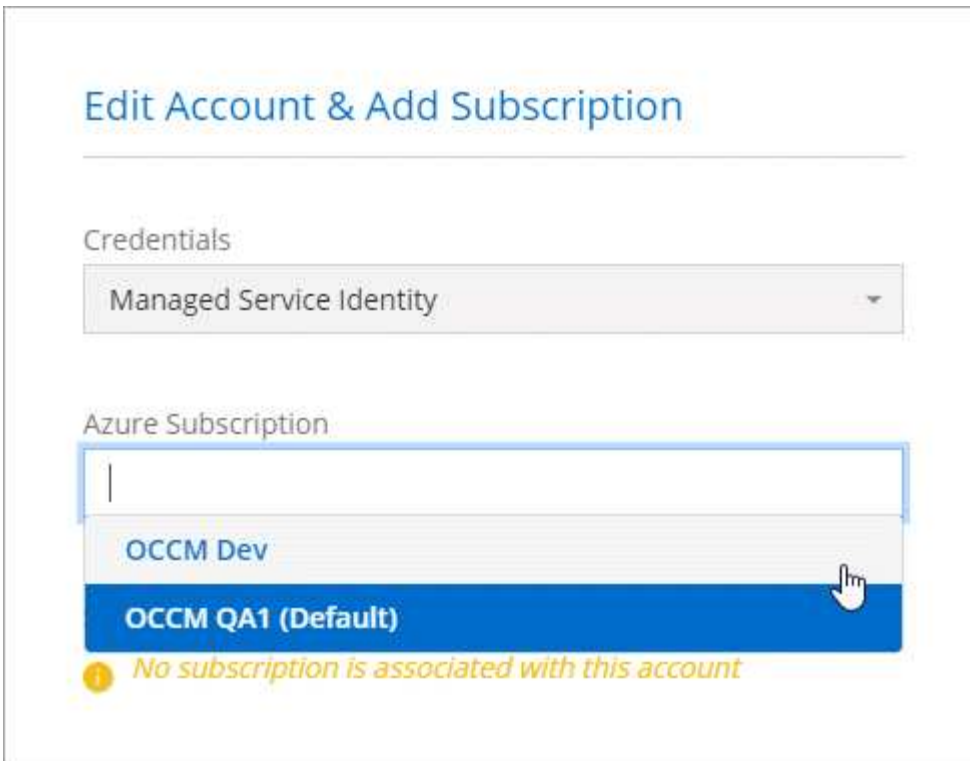


BlueXP Operator is the default name provided in the Connector policy. If you chose a different name for the role, then select that name instead.

- Assign access to a **Virtual Machine**.
 - Select the subscription in which the Connector virtual machine was created.
 - Select the Connector virtual machine.
 - Select **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.



Edit Account & Add Subscription

Credentials

Managed Service Identity

Azure Subscription

OCCM Dev

OCCM QA1 (Default)

No subscription is associated with this account

Add 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.](#)

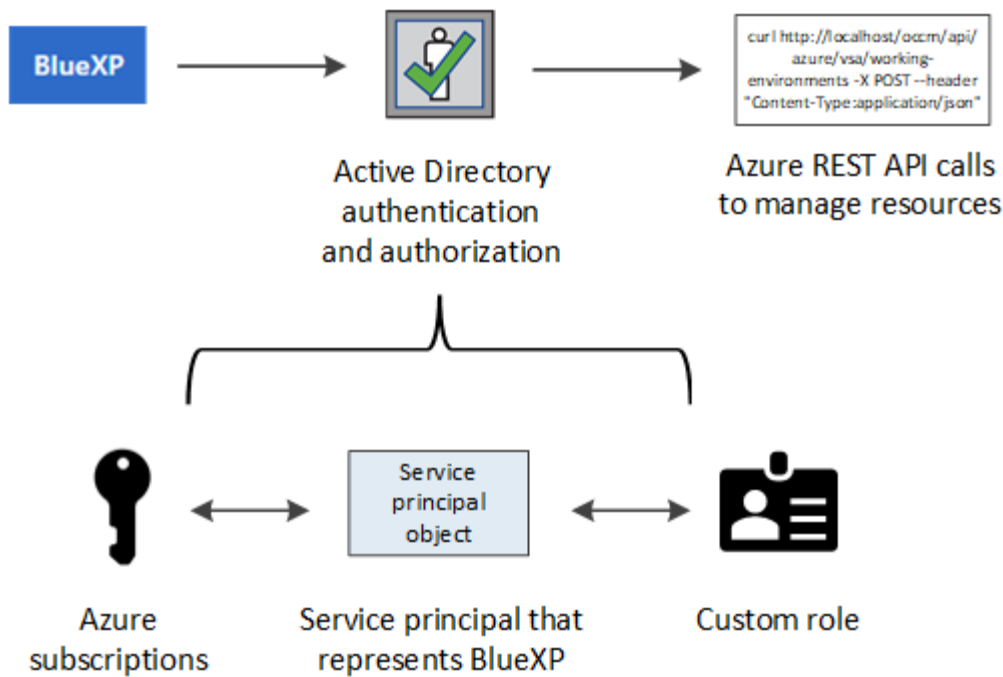
If you want to deploy Cloud Volumes ONTAP using *different* Azure credentials, then you must grant the required permissions by creating and setting up a service principal in Microsoft Entra ID for each Azure account. You can then add the new credentials to BlueXP.

Grant 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 Microsoft Entra ID 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 Microsoft Entra ID and is assigned to a custom role that allows the required permissions.



Steps

1. [Create a Microsoft Entra 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.](#)

Create a Microsoft Entra application

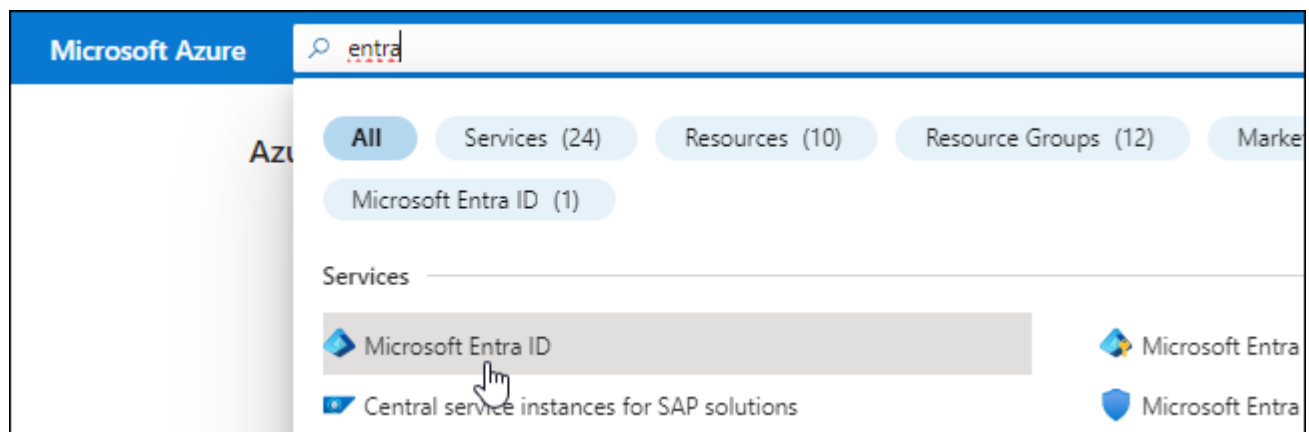
Create a Microsoft Entra application and service principal that BlueXP can use for role-based access control.

Steps

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

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

2. From the Azure portal, open the **Microsoft Entra ID** service.



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

You've created the AD application and service principal.

Result

You've created the AD application and service principal.

Assign 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:

Note that you can create an Azure custom role using the Azure portal, Azure PowerShell, Azure CLI, or REST API. The following steps show how to create the role using the Azure CLI. If you would prefer to use a different method, refer to [Azure documentation](#)

- 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.

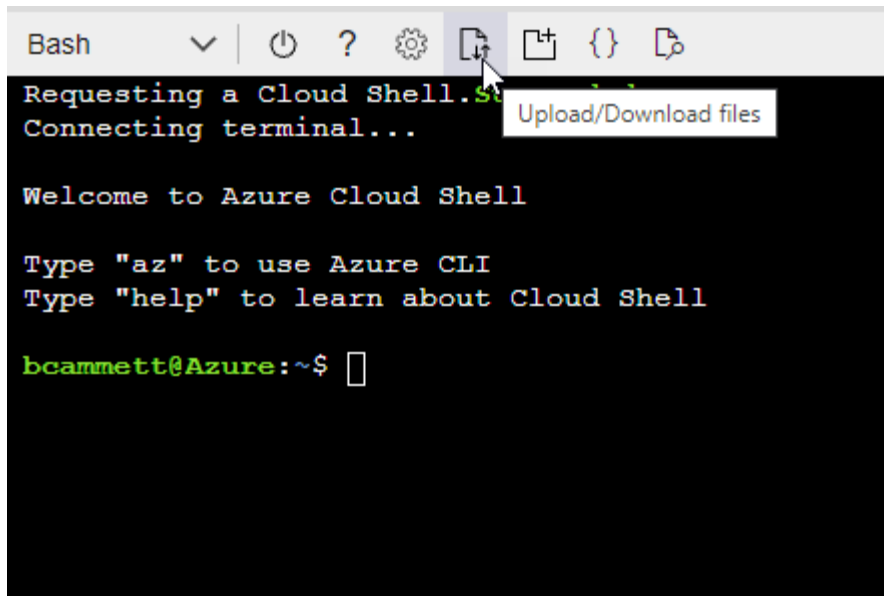
Example

```
"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.



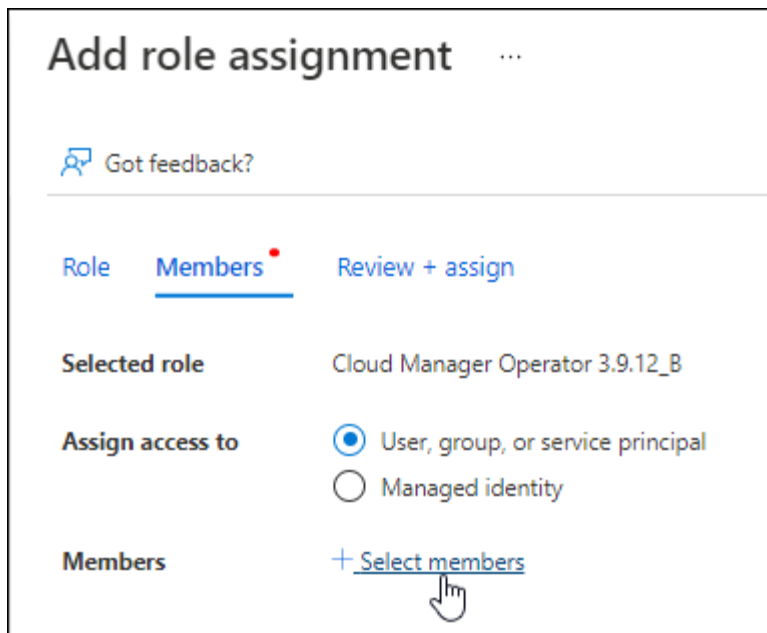
- Use the Azure CLI to create the custom role:

```
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.

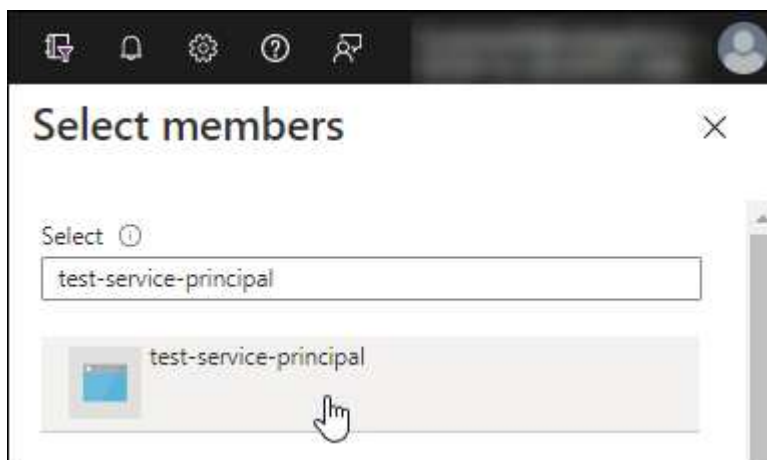
2. Assign the application to the role:

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



- Search for the name of the application.

Here's an example:



- Select the application and select **Select**.
- Select **Next**.

f. Select **Review + assign**.

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

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

Add Windows Azure Service Management API permissions

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

Steps


1. In the **Microsoft Entra ID** service, select **App registrations** and select the application.
2. Select **API permissions > Add a permission**.
3. Under **Microsoft APIs**, select **Azure Service Management**.

Request API permissions













Select an API

Microsoft APIs **APIs my organization uses** My APIs

Commonly used Microsoft APIs



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

 <p>Azure Batch Schedule large-scale parallel and HPC applications in the cloud</p>	 <p>Azure Data Catalog Programmatic access to Data Catalog resources to register, annotate and search data assets</p>	 <p>Azure Data Explorer Perform ad-hoc queries on terabytes of data to build near real-time and complex analytics solutions</p>
 <p>Azure Data Lake Access to storage and compute for big data analytic scenarios</p>	 <p>Azure DevOps Integrate with Azure DevOps and Azure DevOps server</p>	 <p>Azure Import/Export Programmatic control of import/export jobs</p>
 <p>Azure Key Vault Manage your key vaults as well as the keys, secrets, and certificates within your Key Vaults</p>	 <p>Azure Rights Management Services Allow validated users to read and write protected content</p>	 <p>Azure Service Management Programmatic access to much of the functionality available through the Azure portal</p>
 <p>Azure Storage Secure, massively scalable object and data lake storage for unstructured and semi-structured data</p>	 <p>Customer Insights Create profile and interaction models for your products</p>	 <p>Data Export Service for Microsoft Dynamics 365 Export data from Microsoft Dynamics CRM organization to an external destination</p>

4. Select **Access Azure Service Management as organization users** and then select **Add permissions**.

Request API permissions

[← All APIs](#)



Azure Service Management

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

What type of permissions does your application require?

Delegated permissions

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

Application permissions

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

Select permissions

[expand all](#)

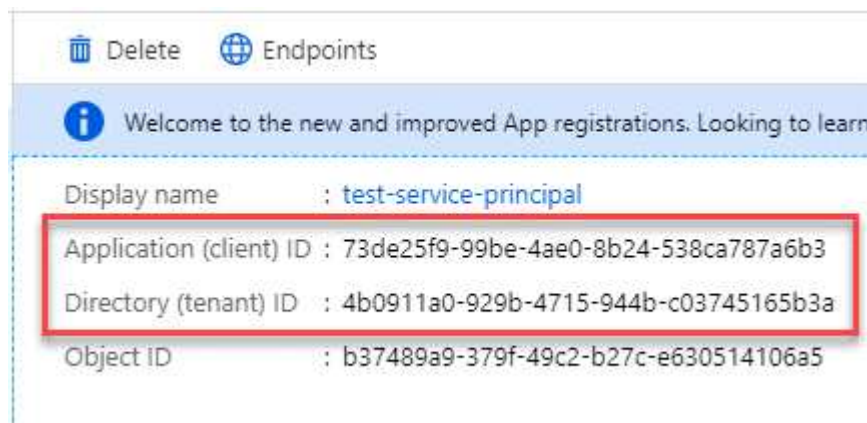
Type to search	
PERMISSION	ADMIN CONSENT REQUIRED
<input checked="" type="checkbox"/> user_impersonation Access Azure Service Management as organization users (preview) ⓘ	-

Get 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 **Microsoft Entra ID** service, select **App registrations** and select the application.
2. Copy the **Application (client) ID** and the **Directory (tenant) ID**.



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

Create a client secret

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 Microsoft Entra ID.

Steps

1. Open the **Microsoft Entra ID** service.

2. Select **App registrations** and select your application.
3. Select **Certificates & secrets > New client secret**.
4. Provide a description of the secret and a duration.
5. Select **Add**.
6. Copy the value of the client secret.

Client secrets

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

+ New client secret		
DESCRIPTION	EXPIRES	VALUE
test secret	8/16/2020	*sZ1jSe2By:D*-ZRoV4NLfdAcY7:+0vA

Copy to clipboard

You now have a client secret that BlueXP can use it to authenticate with Microsoft Entra ID.

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.

Add 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 begin

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.

Before you begin

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, select the Settings icon, and select **Credentials**.

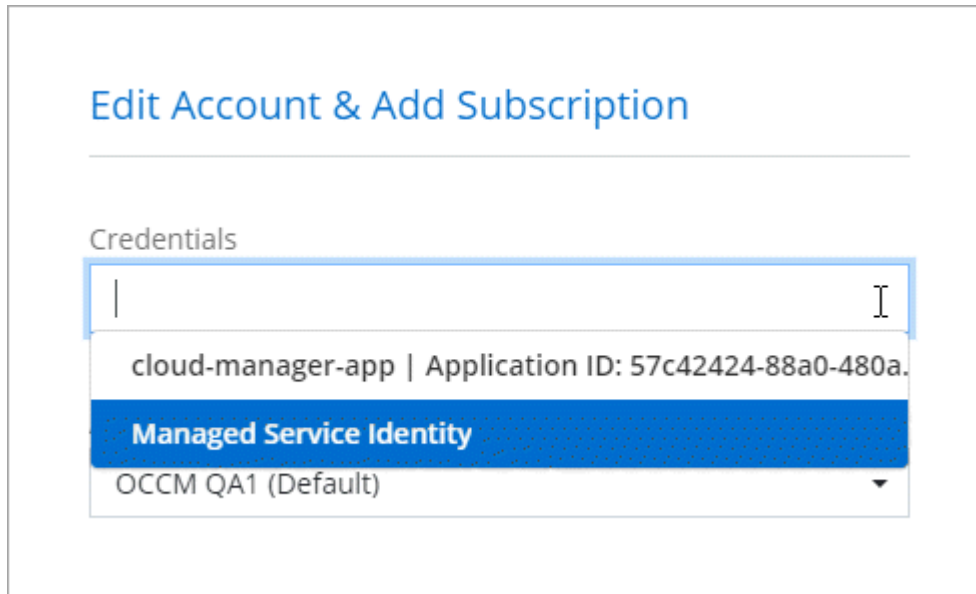


2. Select **Add Credentials** and follow the steps in the wizard.
 - a. **Credentials Location:** Select **Microsoft Azure > Connector**.
 - b. **Define Credentials:** Enter information about the Microsoft Entra service principal that grants the required permissions:
 - Application (client) ID
 - Directory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

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

Associate 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 BlueXP 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 change the Azure Marketplace subscription that is associated with Azure credentials.

Replacing the current marketplace subscription with a new subscription changes the marketplace subscription for any existing Cloud Volumes ONTAP working environments and all new working environments.

Before you begin

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 console, select the Settings icon, and select **Credentials**.
2. Select the action menu for a set of credentials and then select **Configure Subscription**.

You must select credentials that are associated with a Connector. You can't associate a marketplace subscription with credentials that are associated with BlueXP.

3. To associate the credentials with an existing subscription, select the subscription from the down-down list and select **Configure**.
4. To associate the credentials with a new subscription, select **Add Subscription > Continue** and follow the steps in the Azure Marketplace:
 - a. If prompted, log in to your Azure account.
 - b. Select **Subscribe**.
 - c. Fill out the form and select **Subscribe**.
 - d. After the subscription process is complete, select **Configure account now**.

You'll be redirected to BlueXP.

- e. From the **Subscription Assignment** page:
 - Select the BlueXP organizations or accounts that you'd like to associate this subscription with.
 - In the **Replace existing subscription** field, choose whether you'd like to automatically replace the existing subscription for one organization or account with this new subscription.

BlueXP replaces the existing subscription for all credentials in the organization or account with this new subscription. If a set of credentials wasn't ever associated with a subscription, then this new subscription won't be associated with those credentials.

For all other organizations or accounts, you'll need to manually associate the subscription by repeating these steps.

- Select **Save**.

The following video shows the steps to subscribe from the Azure Marketplace:

[Subscribe to NetApp Intelligent Services from the Azure Marketplace](#)

Edit 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, select the Settings icon, and select **Credentials**.
2. On the **Organization credentials** or **Account credentials** page, select the action menu for a set of credentials and then select **Edit Credentials**.
3. Make the required changes and then select **Apply**.

Delete 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, select the Settings icon, and select **Credentials**.
2. On the **Organization credentials** or **Account credentials** page, select the action menu for a set of credentials and then select **Delete Credentials**.
3. Select **Delete** to confirm.

Google Cloud

Learn about Google Cloud projects and permissions

Learn how BlueXP uses Google Cloud credentials to perform actions on your behalf and how those credentials are associated with marketplace subscriptions. Understanding these details can be helpful as you manage the credentials for one or more Google Cloud projects. For example, you might want to learn about the service account that's associated with the Connector VM.

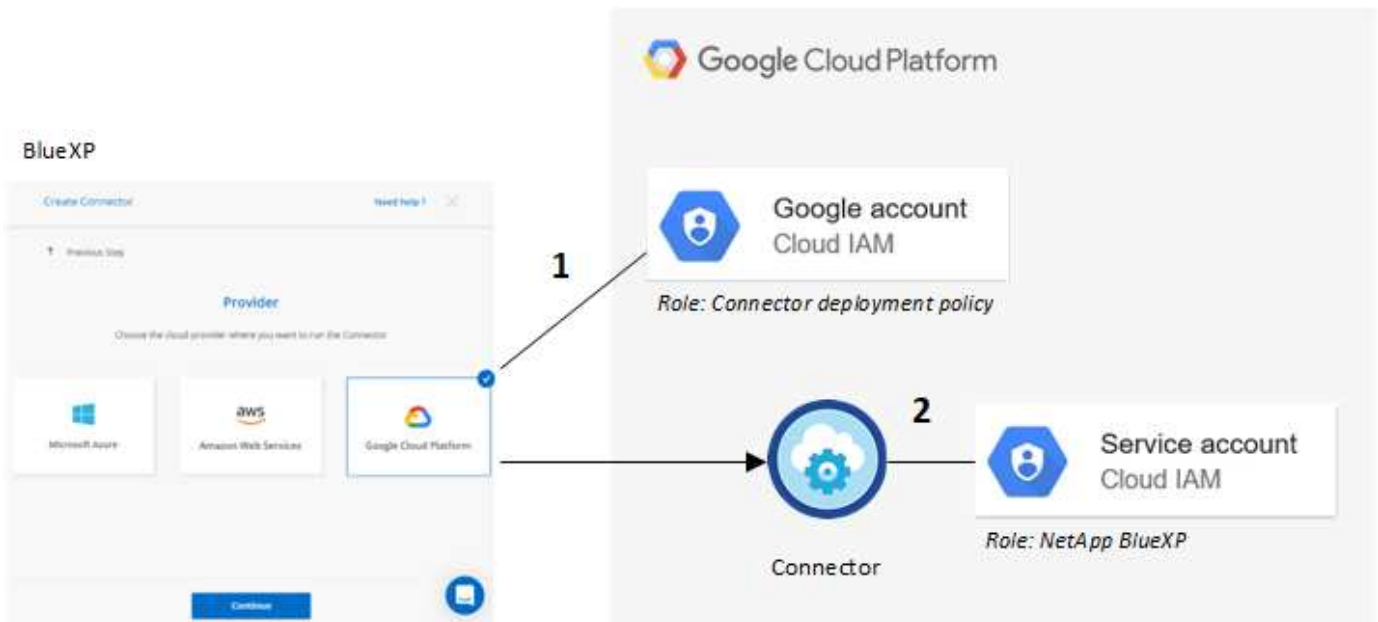
Project and permissions for BlueXP

Before you can use BlueXP to manage resources in your Google Cloud project, you must first deploy a Connector. 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, to manage backups using BlueXP backup and recovery, and more. Permissions are provided by attaching a custom role to the service account.

The following image depicts the permission requirements described in numbers 1 and 2 above:



To learn how to set up permissions, refer to the following pages:

- [Set up Google Cloud permissions for standard mode](#)
- [Set up permissions for restricted mode](#)
- [Set up permissions for private mode](#)

Credentials and marketplace subscriptions

When you deploy a Connector in Google Cloud, BlueXP creates a default set of credentials for the Google Cloud service account in the project in which the Connector resides. These credentials must be associated with a Google Cloud Marketplace subscription so that you can pay for Cloud Volumes ONTAP at an hourly rate (PAYGO) and use other BlueXP services.

[Learn how to associate a Google Cloud Marketplace subscription.](#)

Note the following about Google Cloud credentials and marketplace subscriptions:

- Only one set of Google Cloud credentials can be associated with a Connector
- You can associate only one Google Cloud Marketplace subscription with the credentials
- You can replace an existing marketplace subscription with a new subscription

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 the service account](#)
- [Learn how to deploy Cloud Volumes ONTAP in Google Cloud and select a project](#)

Manage Google Cloud credentials and subscriptions for BlueXP

You can manage the Google Cloud credentials that are associated with the Connector

VM instance by associating a marketplace subscription and by troubleshooting the subscription process. Both of these tasks ensure that you can use your marketplace subscription to pay for data services.

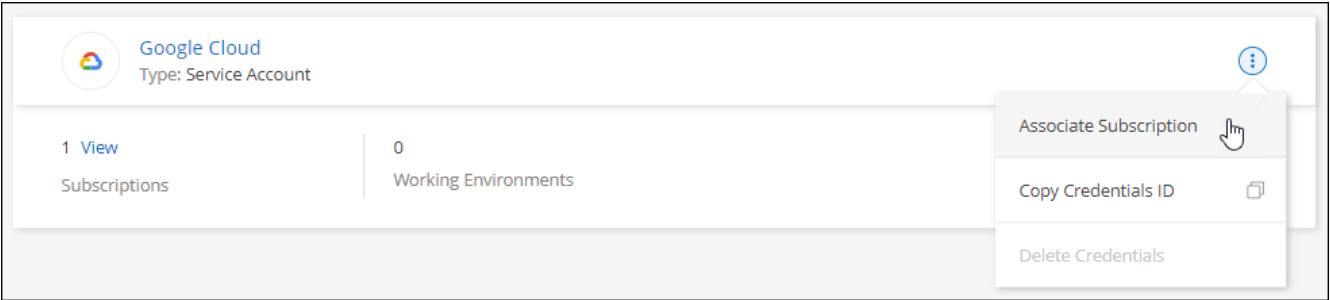
Associate a Marketplace subscription with Google Cloud credentials

When you deploy a Connector in Google Cloud, BlueXP creates a default set of credentials that are associated with the Connector VM instance. At any time, you can change the Google Cloud Marketplace subscription that is associated with these credentials. The subscription enables you to create a pay-as-you-go Cloud Volumes ONTAP system, and to use other data services.

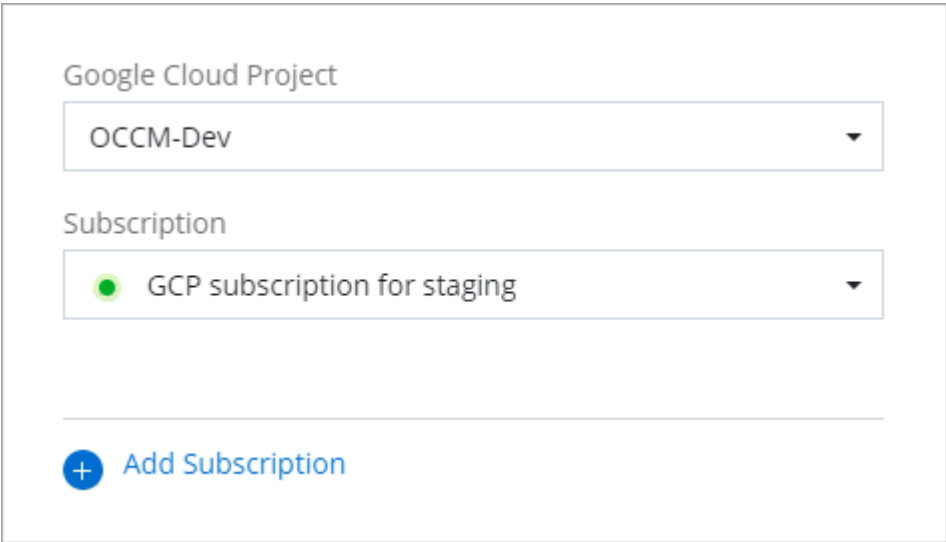
Replacing the current marketplace subscription with a new subscription changes the marketplace subscription for any existing Cloud Volumes ONTAP working environments and all new working environments.

Steps

- 1. In the upper right of the console, select the Settings icon, and select **Credentials**.
- 2. Select the action menu for a set of credentials and then select **Configure Subscription**.
+new screenshot needed (TS)



- 3. To configure an existing subscription with the selected credentials, select a Google Cloud project and subscription from the drop-down list, and then select **Configure**.

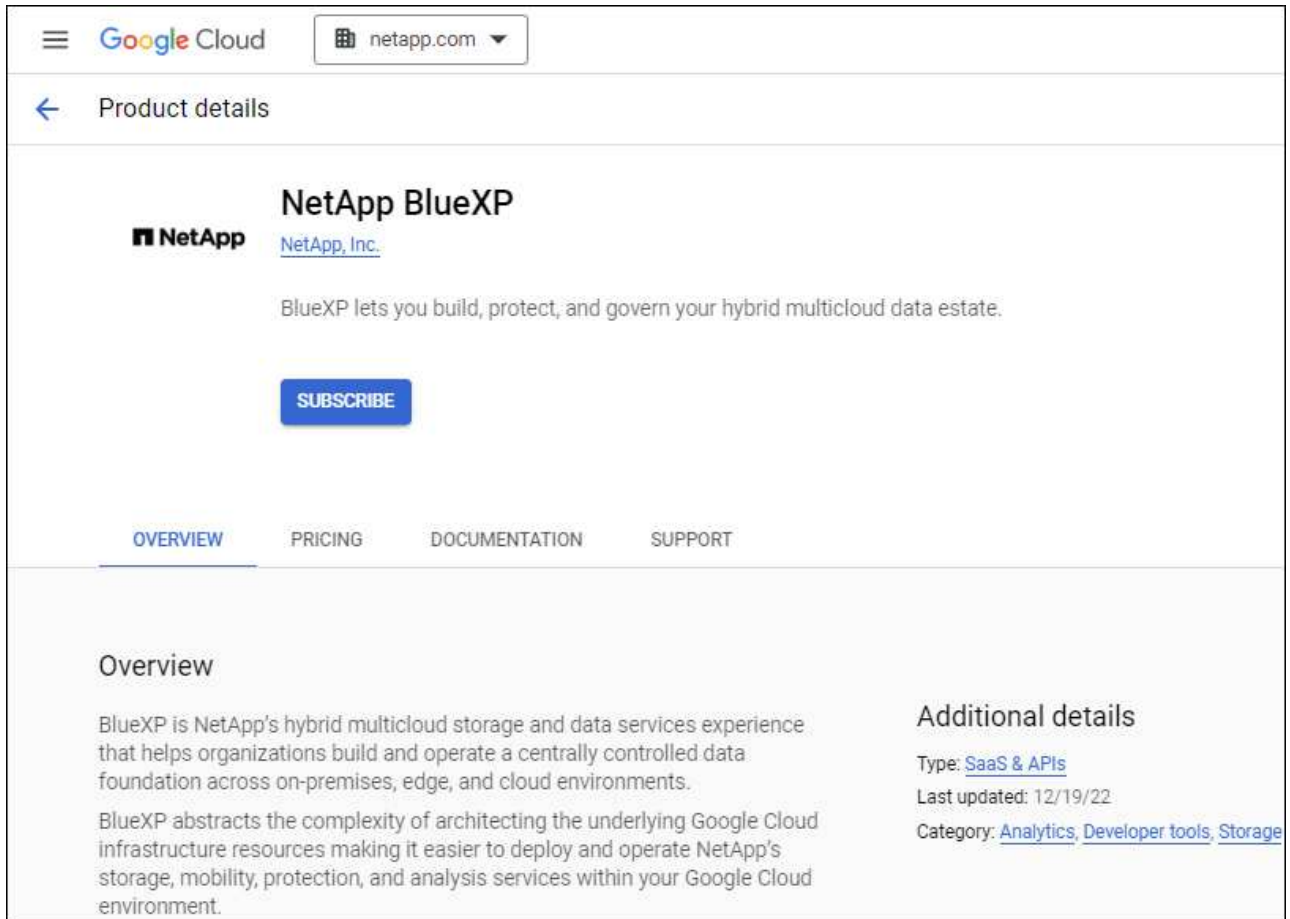


- 4. If you don't already have a subscription, select **Add Subscription > Continue** and follow the steps in the Google Cloud Marketplace.



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.

- a. After you're redirected to the [NetApp Intelligent Services page on the Google Cloud Marketplace](#), ensure that the correct project is selected at the top navigation menu.

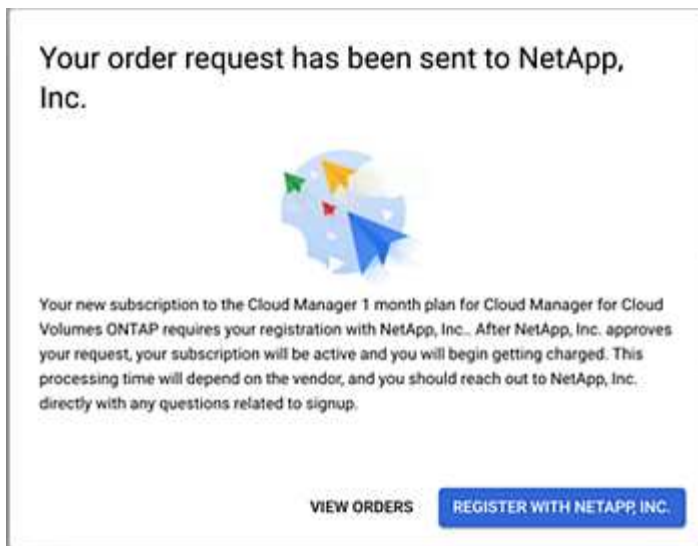


- b. Select **Subscribe**.
- c. Select the appropriate billing account and agree to the terms and conditions.
- d. Select **Subscribe**.

This step sends your transfer request to NetApp.

- e. On the pop-up dialog box, select **Register with NetApp, Inc.**

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



f. Complete the steps on the **Subscription Assignment** page:



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.

- Select the BlueXP organizations or accounts that you'd like to associate this subscription with.
- In the **Replace existing subscription** field, choose whether you'd like to automatically replace the existing subscription for one organization or account with this new subscription.

BlueXP replaces the existing subscription for all credentials in the organization or account with this new subscription. If a set of credentials wasn't ever associated with a subscription, then this new subscription won't be associated with those credentials.

For all other organizations or accounts, you'll need to manually associate the subscription by repeating these steps.

- Select **Save**.

The following video shows the steps to subscribe from the Google Cloud Marketplace:


[Subscribe to BlueXP from the Google Cloud Marketplace](#)


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

Google Cloud Project

OCCM-Dev

Subscription

 GCP subscription for staging

 Add Subscription

Troubleshoot the Marketplace subscription process

Sometimes subscribing to NetApp Intelligent Services 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 select **Manage Orders**.

Pricing






The product was purchased on 12/9/20.

[MANAGE ORDERS](#)

- 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.

Filter Enter property name or value										
Status	Order number	Plan	Discount	Start date ↓	Plan duration	End date	Payment Schedule	Auto-renew	Next plan	
	2eebbc... 	Cloud Manager	-	10/21/21	1 month	-	Postpay	N/A	N/A	

- 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.

Filter Enter property name or value										
Status	Order number	Plan	Discount	Start date ↓	Plan duration	End date	Payment Schedule	Auto-renew	Next plan	
	d56c66... 	Cloud Manager	-	Pending	1 month	Pending	Postpay	N/A	N/A	

Manage NSS credentials associated with BlueXP

Associate a NetApp Support Site account with your BlueXP organization to enable key workflows for Cloud Volumes ONTAP. These NSS credentials are associated with the entire BlueXP organization.

BlueXP also supports associating one NSS account per BlueXP user account. [Learn how to manage user-level credentials.](#)

- [Learn about BlueXP deployment modes](#)
- [Learn about BlueXP identity and access management](#)

Overview

Associating NetApp Support Site credentials with your specific BlueXP account serial number is required to enable the following tasks in BlueXP:

- Deploying 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.

- Registering 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.

- Upgrading Cloud Volumes ONTAP software to the latest release

These credentials are associated with your specific BlueXP account serial number. Users who belong to the BlueXP organization or account can access these credentials from **Support > NSS Management**.

Add an NSS account

You can add and manage your NetApp Support Site accounts for use with BlueXP from the Support Dashboard within BlueXP.

When you have added your NSS account, BlueXP can use this information for things like license downloads, software upgrade verification, and future support registrations.

You can associate multiple NSS accounts with your BlueXP organization; however, you cannot have customer accounts and partner accounts within the same organization.



NetApp uses Microsoft Entra ID as the identity provider for authentication services specific to support and licensing.

Steps

1. In the upper right of the BlueXP console, select the Help icon, and select **Support**.
2. Select **NSS Management > Add NSS Account**.
3. Select **Continue** to be redirected to a Microsoft login page.
4. At the login page, provide your NetApp Support Site registered email address and password.

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. Note that the token for these accounts expire after 90 days. A notification will be posted to alert you of this.

What's next?

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

- [Launching Cloud Volumes ONTAP in AWS](#)
- [Launching Cloud Volumes ONTAP in Azure](#)
- [Launching Cloud Volumes ONTAP in Google Cloud](#)
- [Registering pay-as-you-go systems](#)

Update NSS credentials

For security reasons, you must update your NSS credentials every 90 days. You'll be notified in the BlueXP notification center if your NSS credential has expired. [Learn about the Notification Center](#).

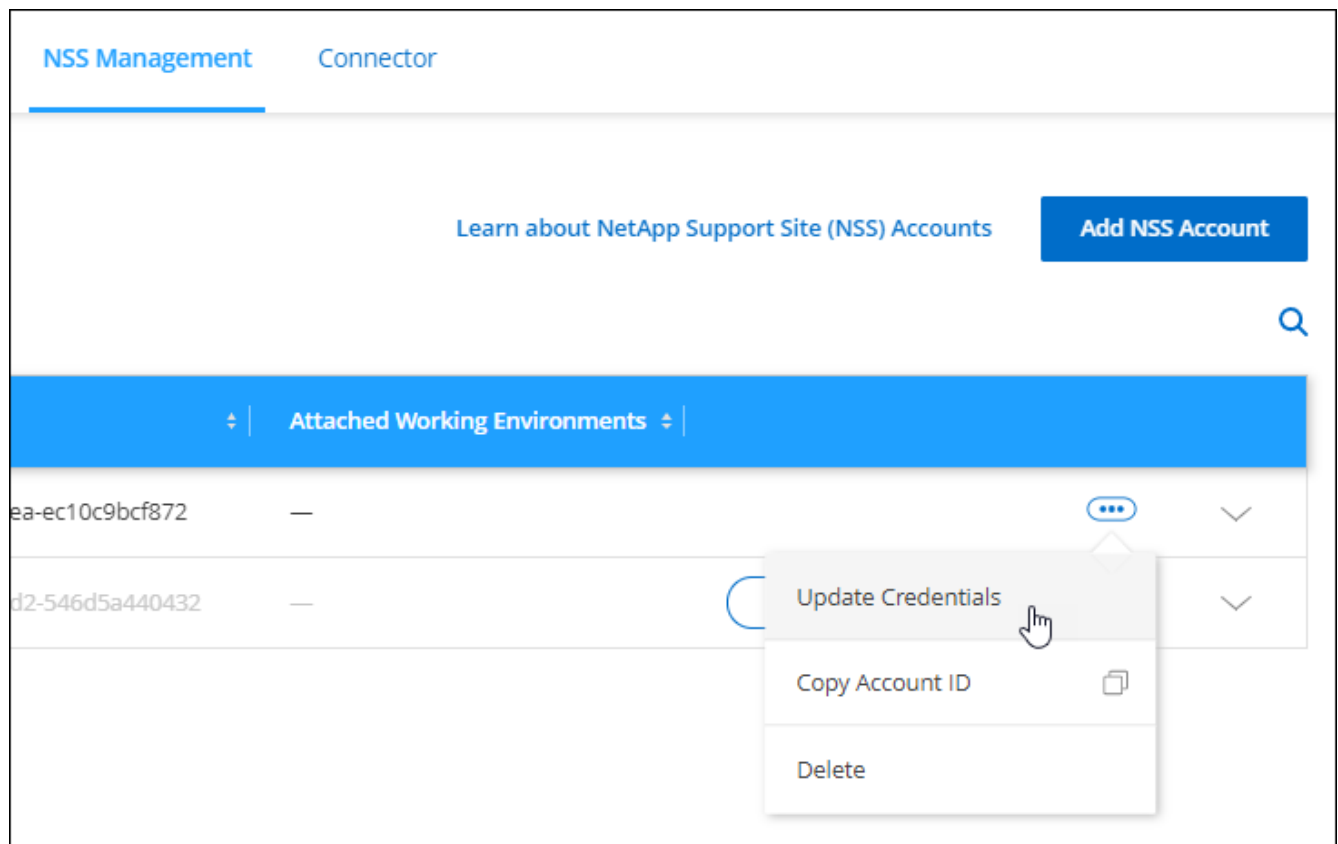
Expired credentials can disrupt the following, but are not limited to:

- License updates in digital wallet, which means you won't be able to take advantage of newly purchased capacity.
- Ability to submit and track support cases.

Additionally, you can update the NSS credentials associated with your organization if you want to change the NSS account associated with your BlueXP organization. For example, if the person associated with your NSS account has left your company.

Steps

1. In the upper right of the BlueXP console, select the Help icon, and select **Support**.
2. Select **NSS Management**.
3. For the NSS account that you want to update, select **...** and then select **Update Credentials**.



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

NetApp uses Microsoft Entra ID as the identity provider for authentication services related to support and licensing.

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

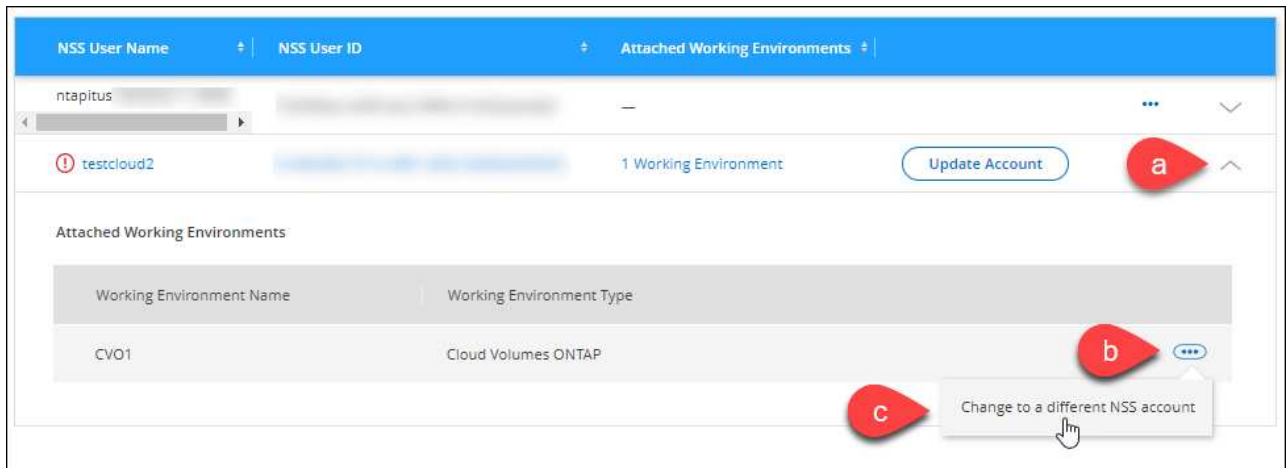
Attach a working environment to a different NSS account

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

You must first have associated the account with BlueXP.

Steps

1. In the upper right of the BlueXP console, select the Help icon, and select **Support**.
2. Select **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, select **...**
 - c. Select **Change to a different NSS account**.



d. Select the account and then select **Save**.

Display the email address for an NSS account

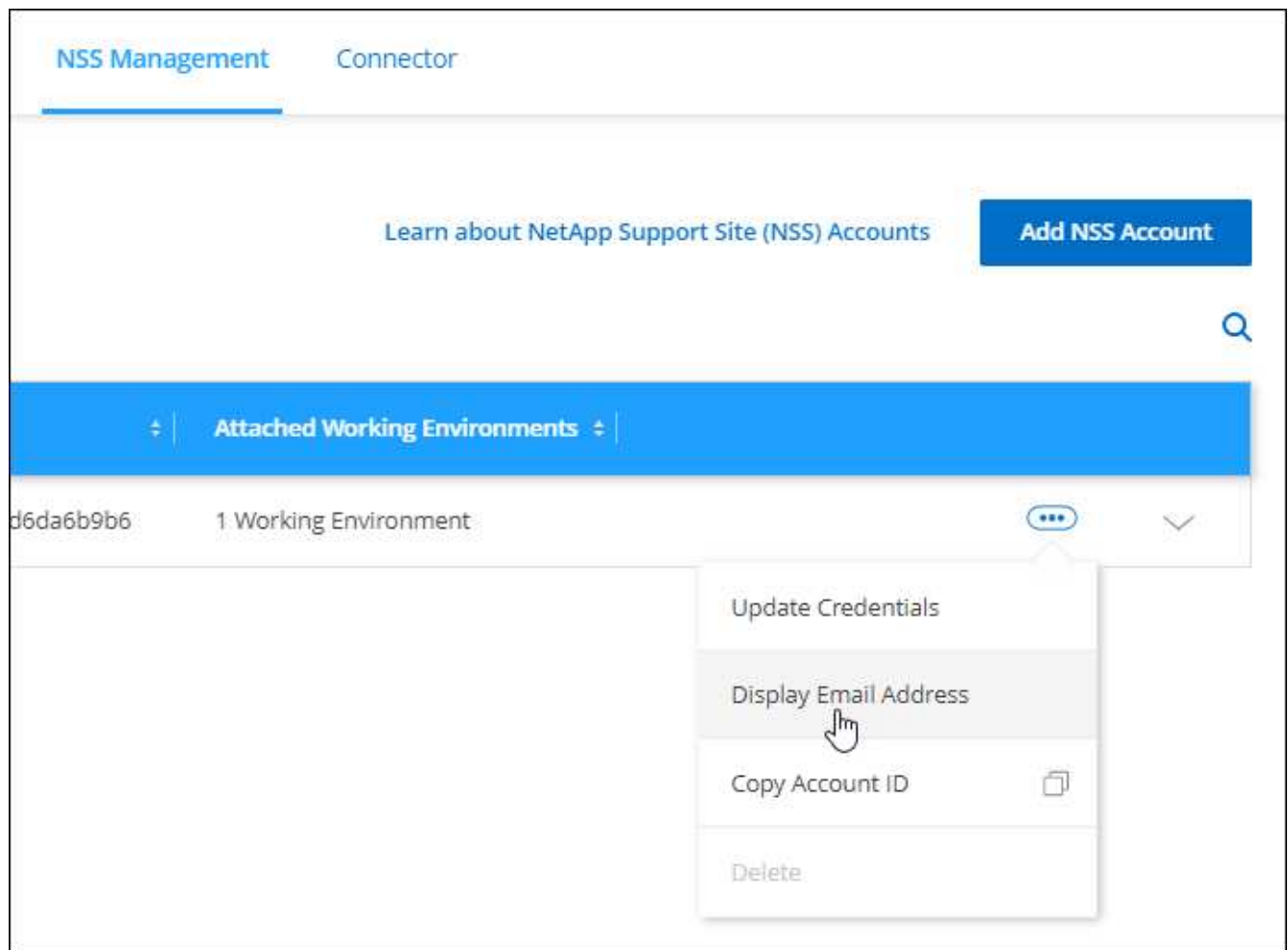
For security, the email address associated with an NSS account is not displayed by default. You can view the email address and associated user name for an NSS account.



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 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, select the Help icon, and select **Support**.
2. Select **NSS Management**.
3. For the NSS account that you want to update, select **...** and then select **Display Email Address**. You can use the copy button to copy the email address.



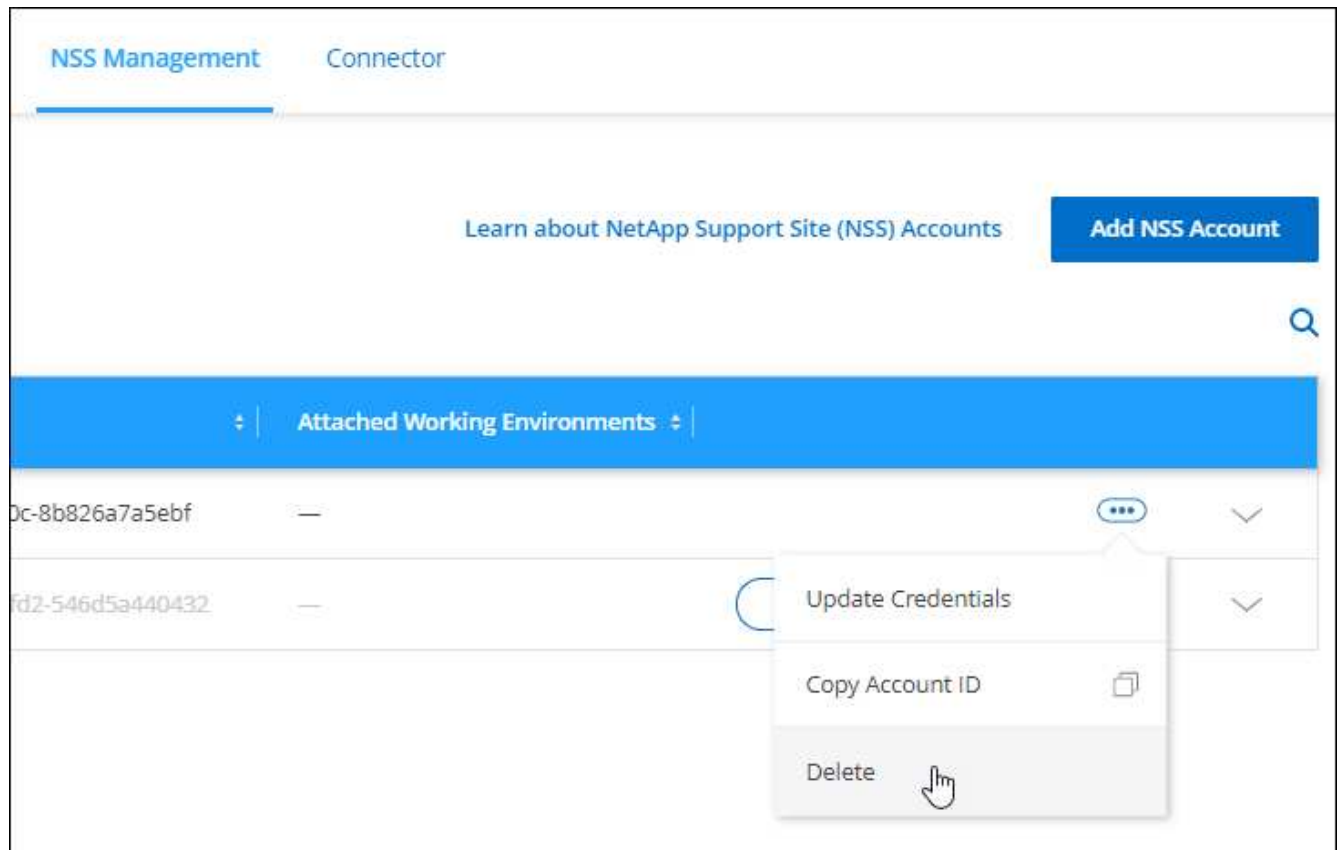
Remove an NSS account

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

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, select the Help icon, and select **Support**.
2. Select **NSS Management**.
3. For the NSS account that you want to delete, select **...** and then select **Delete**.



4. Select **Delete** to confirm.

Manage credentials associated with your BlueXP login

Depending on the actions that you've taken in BlueXP, you might have associated ONTAP credentials and NetApp Support Site (NSS) credentials with your BlueXP user login. You can view and manage those credentials in BlueXP after you've associated them. For example, if you change the password for these credentials, then you'll need to update the password in BlueXP.

ONTAP credentials

Users need ONTAP admin credentials to discover ONTAP clusters in BlueXP. However, ONTAP System Manager access depends on whether or not you are using a Connector.

Without a Connector

Users are prompted to enter their ONTAP credentials to access ONTAP System Manager for the cluster. Users can choose to save these credentials in BlueXP which means they won't be prompted to enter them each time. User credentials are only visible to the respective user and can be managed from the User credentials page.

With a Connector

By default, users are not prompted to enter their ONTAP credentials to access ONTAP System Manager. However, a BlueXP administrator (with the Organization admin role) can configure BlueXP to prompt users to enter their ONTAP credentials. When this setting is enabled, users need enter their ONTAP credentials each time.

[Learn more.](#)

NSS credentials

The NSS credentials associated with your BlueXP login enable support registration, case management, and access to Digital Advisor.

- When you access **Support > Resources** and register for support, you're prompted to associate NSS credentials with your BlueXP login.

This registers your organization or account for support and activates support entitlement. Only one user in your BlueXP organization or account must associate a NetApp Support Site account with their BlueXP login to register for support and activate support entitlement. After this is completed, the **Resources** page shows that your account is registered for support.

[Learn how to register for support](#)

- When you access **Support > Case Management**, you're prompted to enter your NSS credentials, if you haven't already done so. This page enables you to create and manage the support cases associated with your NSS account and with your company.
- When you access Digital Advisor in BlueXP, you're prompted to log in to Digital Advisor by entering your NSS credentials.

Note the following about the NSS account associated with your BlueXP login:

- The account is managed at the user level, which means it isn't viewable by other users who log in.
- There can be only one NSS account associated with Digital Advisor and support case management, per user.
- If you're trying to associate a NetApp Support Site account with a Cloud Volumes ONTAP working environment, you can only choose from the NSS accounts that were added to the BlueXP organization or account that you are a member of.

NSS account-level credentials are different than the NSS account that's associated with your BlueXP login. NSS account-level credentials enable you to deploy Cloud Volumes ONTAP with BYOL, register PAYGO systems, and upgrade its software.

[Learn more about using NSS credentials with your BlueXP organization or account.](#)

Manage your user credentials

Manage your user credentials by updating the user name and password or by deleting the credentials.

Steps

1. In the upper right of the BlueXP console, select the Settings icon, and select **Credentials**.
2. Select **User Credentials**.
3. If you don't have any user credentials yet, you can select **Add NSS credentials** to add your NetApp Support Site account.
4. Manage existing credentials by choosing the following options from the Actions menu:
 - **Update credentials:** Update the user name and password for the account.
 - **Delete credentials:** Remove the account associated with your BlueXP user account.

Result

BlueXP updates your credentials, and you see the changes when accessing the ONTAP cluster, digital advisor,

or the Case Management page.

Monitor BlueXP operations

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 Timeline, the Notification Center, or have notifications sent to your email.

The table compares the Timeline and Notification Center to highlight their features.


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 does not 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
Filter results by importance	Filter by service, action, user, status, and more
Provides the ability to email notifications to users and to others	No email capability

Audit user activity from the BlueXP timeline

The Timeline shows the actions that users completed to manage your organization or account. This includes management actions such as associating users, creating working environments, creating Connectors, and more.

The Timeline helps identify who performed an action or its status.

Steps

1. In the upper right of the BlueXP console, select  > **Timeline**.
2. Use the filters above the table to change which actions display in the table.

For example, you can use the **Service** filter to show actions related to a specific BlueXP service, or you can use the **User** filter to show actions related to a specific user account.

Download audit logs from the Timeline

You can download the audit logs from the Timeline to a CSV file. This enables you to keep a record of the actions that users performed in your organization. The downloaded CSV file contains all available columns from the Timeline, regardless of which ones you are filtering or displaying in the Timeline.

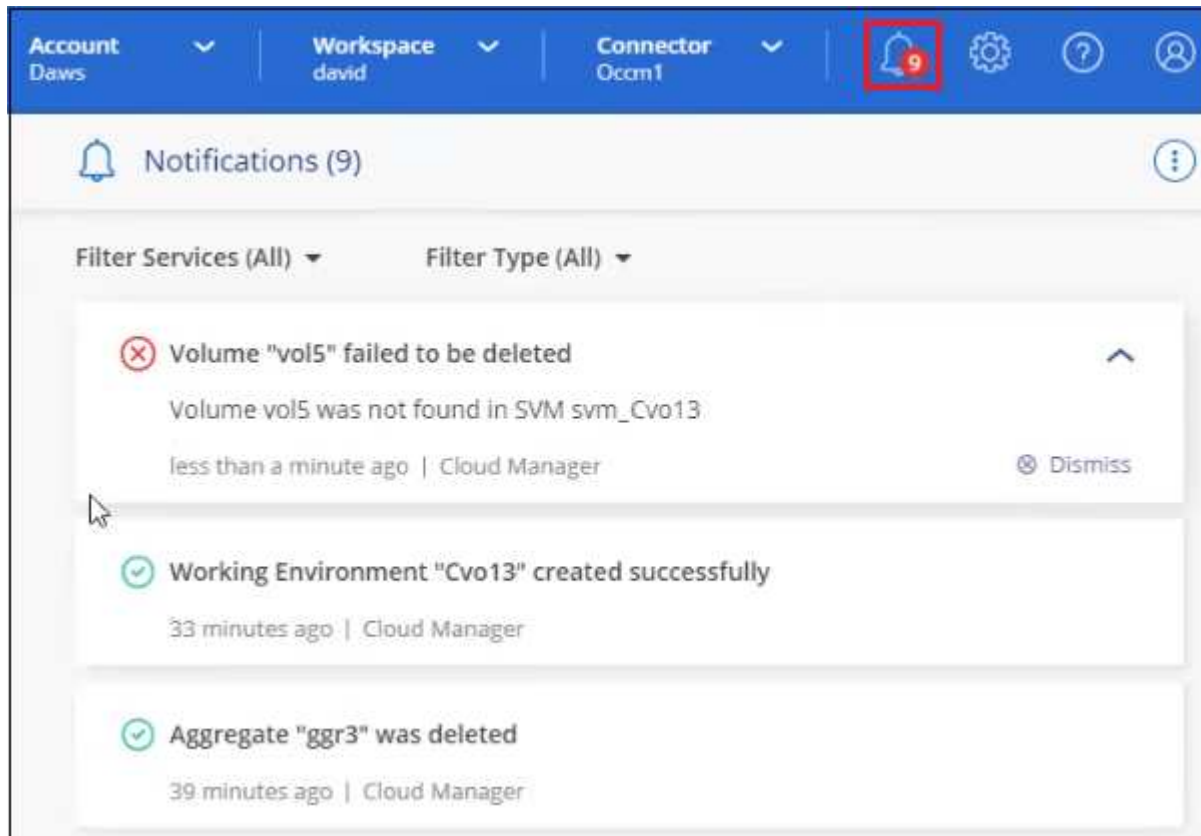
Steps

1. In the Timeline, select the download icon in the upper right corner of the table.

Monitor activities using the Notification Center

Notifications track the progress of your BlueXP operations to verify success. They enable you to view the status for many BlueXP actions that you initiated during your current login session. Not all BlueXP services report information into the Notification Center at this time.

You can display the notifications by selecting 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 certain types of 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 BlueXP organization or account, or to any other recipients who need to be aware of certain types of system activity. See how to [set email notification settings](#).

Comparing the Notification Center with BlueXP alerts

The Notification Center enables you to view the status of operations you've initiated from BlueXP and set up alert notifications for certain types of system activities. Meanwhile, BlueXP alerts enables you to view issues or potential risks in your ONTAP storage environment related to capacity, availability, performance, protection, and security.

[Learn more about BlueXP alerts](#)

Notification types

BlueXP classifies notifications into 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.

Filter notifications

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

Filter Services (All) ▲

☒ Digital Wallet (3)
☒ Active IQ (2)
☐ AppTemplate (1)

Clear
Apply

Filter Type (All) ▲

☐ Information (0)
☐ Success (1)
☒ Warning (2)
☒ Error (1)
☒ Critical (0)
☐ Recommendation (0)

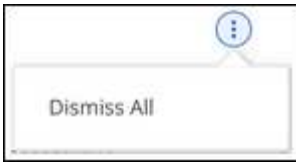
Clear
Apply

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.

Dismiss notifications

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

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



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



Set 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 BlueXP organization or account, or to any other recipients who need to be aware of certain types of system activity.



- BlueXP sends email notifications for the Connector, digital wallet, copy and sync, and backup and recovery.
- Sending email notifications is not supported when the Connector is installed in a site without internet access.

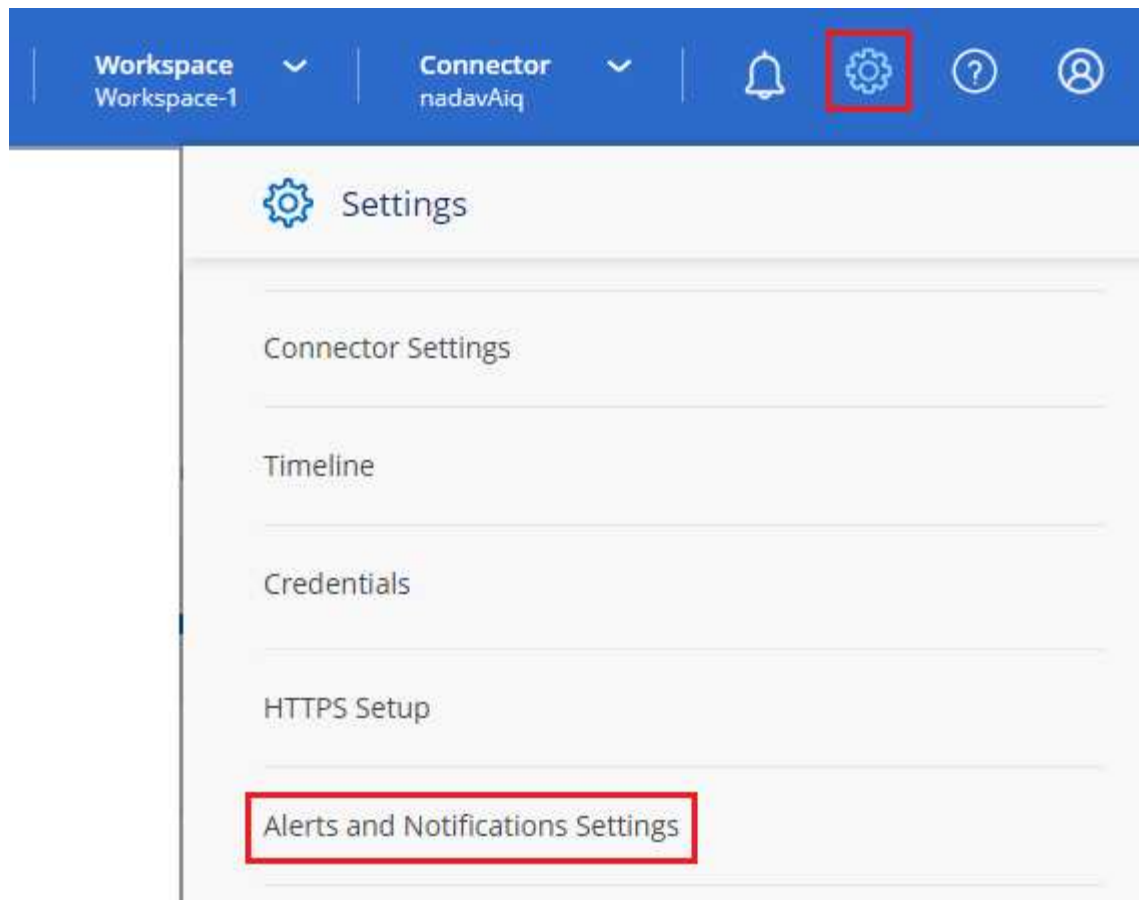
The filters you set in the Notification Center do not determine the types of notifications you'll receive by email. By default, any BlueXP admin will receive emails for all "Critical" and "Recommendation" notifications. These notifications are across all services - you can't choose to receive notifications for only certain services, for example Connectors or BlueXP backup and recovery.

All other users and recipients are configured not to receive any notification emails - so you'll need to configure notification settings for any additional users.

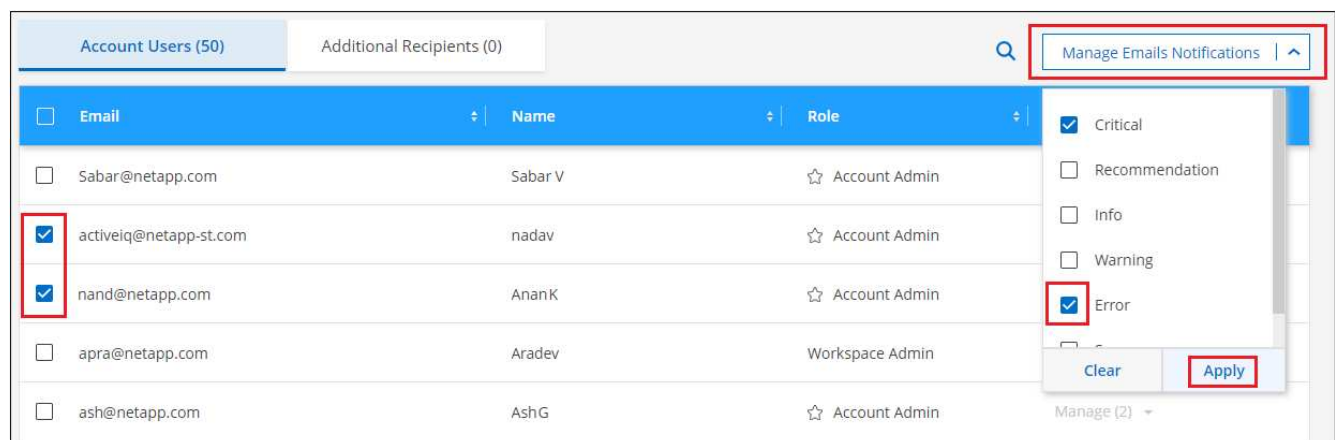
You must have the Organization admin role to customize the notifications settings.

Steps

1. From the BlueXP menu bar, select **Settings > Alerts and Notifications Settings**.



2. Select a user, or multiple users, from either the *Users* tab or the *Additional Recipients* tab, and choose the type of notifications to be sent:
 - To make changes for a single user, select the menu in the Notifications column for that user, check the types of Notifications to be sent, and select **Apply**.
 - To make changes for multiple users, check the box for each user, select **Manage Email Notifications**, check the types of Notifications to be sent, and select **Apply**.

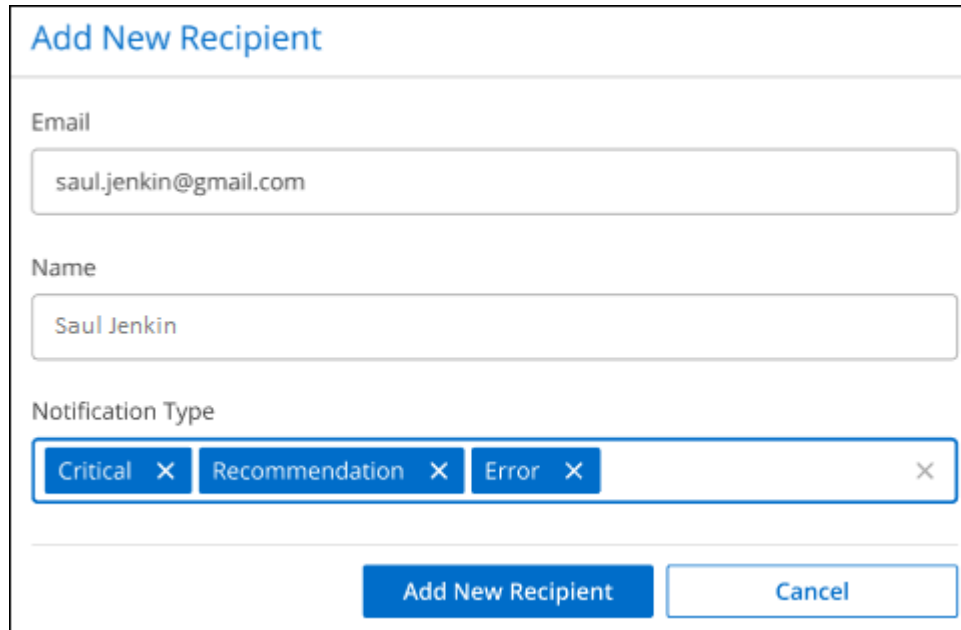


Add additional email recipients

The users who appear in the *Users* tab are populated automatically from the users in your organization or account. 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, select **Add New Recipients**.



The screenshot shows a web form titled "Add New Recipient" in blue text. The form has three input fields: "Email" with the value "saul.jenkin@gmail.com", "Name" with the value "Saul Jenkin", and "Notification Type" which is a multi-select dropdown containing "Critical", "Recommendation", and "Error". Each item in the dropdown has a small "x" icon to its right. At the bottom of the form, there are two buttons: a blue "Add New Recipient" button and a white "Cancel" button with a blue border.

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

Reference

Connector maintenance console

Connector maintenance console

You can use the Maintenance Console to configure the Connector to use a transparent proxy server.

Access the Maintenance Console

You can access the Maintenance Console from the Connector host. Navigate to the following directory:

```
/opt/application/netapp/service-manager-2/connector-maint-console
```

Transparent proxy commands

The Maintenance Console provides commands to configure the Connector to use a transparent proxy server.

View the current transparent proxy configuration

To view the current transparent proxy configuration, use the following command:

```
./connector-maint-console proxy get
```

Add a transparent proxy server

To add a transparent proxy server, use the following command, where `/home/ubuntu/myCA1.pem` is the path to the certificate file for the proxy server. The certificate file must be in PEM format:

```
./connector-maint-console proxy add -c /home/ubuntu/myCA1.pem
```

Ensure that the certificate file is in the same directory as the command or specify the full path to the certificate file.

Update the certificate for a transparent proxy server

To update the certificate for a transparent proxy server, use the following command, where `/home/ubuntu/myCA1.pem` is the path to the new certificate file for the proxy server. The certificate file must be in PEM format:

```
./connector-maint-console proxy update -c /home/ubuntu/myCA1.pem
```

Ensure that the certificate file is in the same directory as the command or specify the full path to the certificate file.

Remove a transparent proxy server

To remove transparent proxy server, use the following command:

```
./connector-maint-console proxy remove
```

View help for any command

To view help for any command, append `--help` to the command. For example, to view help for the `proxy add` command, use the following command:

```
./connector-maint-console proxy add --help
```

Permissions

Permissions summary for BlueXP

To use BlueXP features and services, you'll need to provide permissions so that BlueXP can perform operations in your cloud environment. Use the links on this page to quickly access the permissions that you need based on your goal.

AWS permissions

BlueXP requires AWS permissions for the Connector and for individual services.

Connectors

Goal	Description	Link
Deploy the Connector from BlueXP	The user who creates a Connector from BlueXP needs specific permissions to deploy the instance in AWS.	Set up AWS permissions
Provide permissions for the Connector	<p>When BlueXP launches the Connector, it attaches a policy to the instance that provides the permissions required to manage resources and processes in your AWS account.</p> <p>You need to set up the policy yourself if you launch a Connector from the AWS Marketplace, if you manually install the Connector, or if you add more AWS credentials to a Connector.</p> <p>You also need to ensure that the policy is up to date as new permissions are added in subsequent releases.</p>	AWS permissions for the Connector

Backup and recovery

Goal	Description	Link
Back up on-premises ONTAP clusters to Amazon S3 with BlueXP backup and recovery	When activating backups on your ONTAP volumes, BlueXP backup and recovery prompts you to enter an access key and secret for an IAM user that has specific permissions.	Set up S3 permissions for backups

Cloud Volumes ONTAP

Goal	Description	Link
Provide permissions for Cloud Volumes ONTAP nodes	An IAM role must be attached to each Cloud Volumes ONTAP node in AWS. The same is true for the HA mediator. The default option is to let BlueXP create the IAM roles for you, but you can use your own when creating the working environment.	Learn how to set up the IAM roles yourself

Copy and sync

Goal	Description	Link
Deploy the data broker in AWS	The AWS user account that you use to deploy the data broker must have specific permissions.	Permissions required to deploy the data broker in AWS
Provide permissions for the data broker	When BlueXP copy and sync deploys the data broker, it creates an IAM role for the data broker instance. You can deploy the data broker using your own IAM role, if you prefer.	Requirements to use your own IAM role with the AWS data broker
Enable AWS access for a manually installed data broker	If you use the data broker with a sync relationship that includes an S3 bucket, then you should prepare the Linux host for AWS access. When you install the data broker, you'll need to provide AWS keys for an IAM user that has programmatic access and specific permissions.	Enabling access to AWS

FSx for ONTAP

Goal	Description	Link
Create and manage FSx for ONTAP	To create or manage an Amazon FSx for NetApp ONTAP working environment, you need to add AWS credentials to BlueXP by providing the ARN of an IAM role that gives BlueXP the permissions needed to create the working environment.	Learn how to set up AWS credentials for FSx

Tiering

Goal	Description	Link
Tier on-premises ONTAP clusters to Amazon S3	When you enable BlueXP tiering to AWS, the wizard prompts you to enter an access key and secret key. These credentials are passed to the ONTAP cluster so that ONTAP can tier data to the S3 bucket.	Set up S3 permissions for tiering

Azure permissions

BlueXP requires Azure permissions for the Connector and for individual services.

Connectors

Goal	Description	Link
Deploy the Connector from BlueXP	When you deploy a Connector from BlueXP, you need to use an Azure account or service principal that has permissions to deploy the Connector VM in Azure.	Set up Azure permissions
Provide permissions for the Connector	<p>When BlueXP deploys the Connector VM in Azure, it creates a custom role that provides the permissions required to manage resources and processes within that Azure subscription.</p> <p>You need to set up the custom role yourself if you launch a Connector from the marketplace, if you manually install the Connector, or if you add more Azure credentials to a Connector.</p> <p>You also need to ensure that the policy is up to date as new permissions are added in subsequent releases.</p>	Azure permissions for the Connector

Backup and recovery

Goal	Description	Link
Back up Cloud Volumes ONTAP to Azure blob storage	<p>When using BlueXP backup and recovery to back up Cloud Volumes ONTAP, you need to add permissions to the Connector in the following scenarios:</p> <ul style="list-style-type: none">• You want to use "Search & Restore" functionality• You want to use customer-managed encryption keys (CMEK)	<ul style="list-style-type: none">• Back up Cloud Volumes ONTAP data to Azure Blob storage with Backup and Recovery
Back up on-premises ONTAP clusters to Azure blob storage	When using BlueXP backup and recovery to back up on-premises ONTAP clusters, you need to add permissions to the Connector in order to use the "Search & Restore" functionality.	Back up on-premises ONTAP data to Azure Blob storage with Backup and Recovery

Copy and sync

Goal	Description	Link
Deploy the data broker in Azure	The Azure user account that you use to deploy the data broker must have the required permissions.	Permissions required to deploy the data broker in Azure

Google Cloud permissions

BlueXP requires Google Cloud permissions for the Connector and for individual services.

Connectors

Goal	Description	Link
Deploy the Connector from BlueXP	The Google Cloud user who deploys a Connector from BlueXP needs specific permissions to deploy the Connector in Google Cloud.	Set up permissions to create the Connector
Provide permissions for the Connector	<p>The service account for the Connector VM instance must have specific permissions for day-to-day operations. You need to associate the service account with the Connector during deployment.</p> <p>You also need to ensure that the policy is up to date as new permissions are added in subsequent releases.</p>	Set up permissions for the Connector

Backup and recovery

Goal	Description	Link
Back up Cloud Volumes ONTAP to Google Cloud	<p>When using BlueXP backup and recovery to back up Cloud Volumes ONTAP, you need to add permissions to the Connector in the following scenarios:</p> <ul style="list-style-type: none">• You want to use "Search & Restore" functionality• You want to use customer-managed encryption keys (CMEK)	<ul style="list-style-type: none">• Back up Cloud Volumes ONTAP data to Google Cloud Storage with Backup and Recovery• https://docs.netapp.com/us-en/bluexp-backup-recovery/prev-ontap-backup-cvo-gcp.html[Permissions for CMEKs^]
Back up on-premises ONTAP clusters to Google Cloud	When using BlueXP backup and recovery to back up on-premises ONTAP clusters, you need to add permissions to the Connector in order to use the "Search & Restore" functionality.	Permissions for Search & Restore functionality

Cloud Volumes Service for Google Cloud

Goal	Description	Link
Discover Cloud Volumes Service for Google Cloud	BlueXP needs access to the Cloud Volumes Service API and the right permissions through a Google Cloud service account.	Set up a service account

Copy and sync

Goal	Description	Link
Deploy the data broker in Google Cloud	Ensure that the Google Cloud user who deploys the data broker has the required permissions.	Permissions required to deploy the data broker in Google Cloud
Enable Google Cloud access for a manually installed data broker	If you plan to use the data broker with a sync relationship that includes a Google Cloud Storage bucket, then you should prepare the Linux host for Google Cloud access. When you install the data broker, you'll need to provide a key for a service account that has specific permissions.	Enabling access to Google Cloud

StorageGRID permissions

BlueXP requires StorageGRID permissions for two services.

Backup and recovery

Goal	Description	Link
Back up on-premises ONTAP clusters to StorageGRID	When you prepare StorageGRID as a backup target for ONTAP clusters, BlueXP backup and recovery prompts you to enter an access key and secret for an IAM user that has specific permissions.	Prepare StorageGRID as your backup target

Tiering

Goal	Description	Link
Tier on-premises ONTAP clusters to StorageGRID	When you set up BlueXP tiering to StorageGRID, you need to provide BlueXP tiering with an S3 access key and secret key. BlueXP tiering uses the keys to access your buckets.	Prepare tiering to StorageGRID

AWS permissions for the Connector

When BlueXP launches the Connector instance in AWS, it attaches a policy to the instance that provides the Connector with permissions to manage resources and processes within that AWS account. The Connector uses the permissions to make API calls to several AWS services, including EC2, S3, CloudFormation, IAM, the Key Management Service (KMS), and more.

IAM policies

The IAM policies available below provide the permissions that a Connector needs to manage resources and processes within your public cloud environment based on your AWS region.

Note the following:

- If you create a Connector in a standard AWS region directly from BlueXP, BlueXP automatically applies policies to the Connector.
- You need to set up the policies yourself if you deploy the Connector from the AWS Marketplace, if you manually install the Connector on a Linux host, or if you want to add additional AWS credentials to BlueXP.

- In either case, you need to ensure that the policies are up to date as new permissions are added in subsequent releases. If new permissions are required, they will be listed in the release notes.
- If needed, you can restrict the IAM policies by using the IAM `Condition` element. [AWS documentation: Condition element](#)
- To view step-by-step instructions for using these policies, refer to the following pages:
 - [Set up permissions for an AWS Marketplace deployment](#)
 - [Set up permissions for on-premises deployments](#)
 - [Set up permissions for restricted mode](#)
 - [Set up permissions for private mode](#)

Select your region to view the required policies:

Standard regions

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

Policy #1

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": [
        "ec2:DescribeAvailabilityZones",
        "ec2:DescribeInstances",
        "ec2:DescribeInstanceStatus",
        "ec2:RunInstances",
        "ec2:ModifyInstanceAttribute",
        "ec2:DescribeInstanceAttribute",
        "ec2:DescribeRouteTables",
        "ec2:DescribeImages",
        "ec2:CreateTags",
        "ec2:CreateVolume",
        "ec2:DescribeVolumes",
        "ec2:ModifyVolumeAttribute",
        "ec2:CreateSecurityGroup",
        "ec2:DescribeSecurityGroups",
        "ec2:RevokeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:RevokeSecurityGroupIngress",
        "ec2:CreateNetworkInterface",
        "ec2:DescribeNetworkInterfaces",
        "ec2:ModifyNetworkInterfaceAttribute",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:DescribeDhcpOptions",
        "ec2:CreateSnapshot",
        "ec2:DescribeSnapshots",
        "ec2:GetConsoleOutput",
        "ec2:DescribeKeyPairs",
        "ec2:DescribeRegions",
        "ec2:DescribeTags",
        "ec2:AssociateIamInstanceProfile",
        "ec2:DescribeIamInstanceProfileAssociations",
        "ec2:DisassociateIamInstanceProfile",
        "ec2:CreatePlacementGroup",
        "ec2:DescribeReservedInstancesOfferings",
        "ec2:AssignPrivateIpAddresses",
        "ec2:CreateRoute",
        "ec2:DescribeVpcs",
        "ec2:ReplaceRoute",
```

```
"ec2:UnassignPrivateIpAddresses",
"ec2:DeleteSecurityGroup",
"ec2:DeleteNetworkInterface",
"ec2:DeleteSnapshot",
"ec2:DeleteTags",
"ec2:DeleteRoute",
"ec2:DeletePlacementGroup",
"ec2:DescribePlacementGroups",
"ec2:DescribeVolumesModifications",
"ec2:ModifyVolume",
"cloudformation:CreateStack",
"cloudformation:DescribeStacks",
"cloudformation:DescribeStackEvents",
"cloudformation:ValidateTemplate",
"cloudformation>DeleteStack",
"iam:PassRole",
"iam:CreateRole",
"iam:PutRolePolicy",
"iam:CreateInstanceProfile",
"iam:AddRoleToInstanceProfile",
"iam:RemoveRoleFromInstanceProfile",
"iam:ListInstanceProfiles",
"iam>DeleteRole",
"iam>DeleteRolePolicy",
"iam>DeleteInstanceProfile",
"iam:GetRolePolicy",
"iam:GetRole",
"sts:DecodeAuthorizationMessage",
"sts:AssumeRole",
"s3:GetBucketTagging",
"s3:GetBucketLocation",
"s3:ListBucket",
"s3:CreateBucket",
"s3:GetLifecycleConfiguration",
"s3:ListBucketVersions",
"s3:GetBucketPolicyStatus",
"s3:GetBucketPublicAccessBlock",
"s3:GetBucketPolicy",
"s3:GetBucketAcl",
"s3:PutObjectTagging",
"s3:GetObjectTagging",
"s3>DeleteObject",
"s3>DeleteObjectVersion",
"s3:PutObject",
"s3:ListAllMyBuckets",
"s3:GetObject",
```

```

        "s3:GetEncryptionConfiguration",
        "kms:List*",
        "kms:ReEncrypt*",
        "kms:Describe*",
        "kms:CreateGrant",
        "fsx:Describe*",
        "fsx:List*",
        "kms:GenerateDataKeyWithoutPlaintext"
    ],
    "Resource": "*",
    "Effect": "Allow",
    "Sid": "cvoServicePolicy"
},
{
    "Action": [
        "ec2:StartInstances",
        "ec2:StopInstances",
        "ec2:DescribeInstances",
        "ec2:DescribeInstanceStatus",
        "ec2:RunInstances",
        "ec2:TerminateInstances",
        "ec2:DescribeInstanceAttribute",
        "ec2:DescribeImages",
        "ec2:CreateTags",
        "ec2:CreateVolume",
        "ec2:CreateSecurityGroup",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:DescribeRegions",
        "cloudformation:CreateStack",
        "cloudformation>DeleteStack",
        "cloudformation:DescribeStacks",
        "kms:List*",
        "kms:Describe*",
        "ec2:DescribeVpcEndpoints",
        "kms:ListAliases",
        "athena:StartQueryExecution",
        "athena:GetQueryResults",
        "athena:GetQueryExecution",
        "glue:GetDatabase",
        "glue:GetTable",
        "glue:CreateTable",
        "glue:CreateDatabase",
        "glue:GetPartitions",
        "glue:BatchCreatePartition",
        "glue:BatchDeletePartition"
    ]
}

```

```

    ],
    "Resource": "*",
    "Effect": "Allow",
    "Sid": "backupPolicy"
  },
  {
    "Action": [
      "s3:GetBucketLocation",
      "s3:ListAllMyBuckets",
      "s3:ListBucket",
      "s3:CreateBucket",
      "s3:GetLifecycleConfiguration",
      "s3:PutLifecycleConfiguration",
      "s3:PutBucketTagging",
      "s3:ListBucketVersions",
      "s3:GetBucketAcl",
      "s3:PutBucketPublicAccessBlock",
      "s3:GetObject",
      "s3:PutEncryptionConfiguration",
      "s3:DeleteObject",
      "s3:DeleteObjectVersion",
      "s3:ListBucketMultipartUploads",
      "s3:PutObject",
      "s3:PutBucketAcl",
      "s3:AbortMultipartUpload",
      "s3:ListMultipartUploadParts",
      "s3:DeleteBucket",
      "s3:GetObjectVersionTagging",
      "s3:GetObjectVersionAcl",
      "s3:GetObjectRetention",
      "s3:GetObjectTagging",
      "s3:GetObjectVersion",
      "s3:PutObjectVersionTagging",
      "s3:PutObjectRetention",
      "s3:DeleteObjectTagging",
      "s3:DeleteObjectVersionTagging",
      "s3:GetBucketObjectLockConfiguration",
      "s3:GetBucketVersioning",
      "s3:PutBucketObjectLockConfiguration",
      "s3:PutBucketVersioning",
      "s3:BypassGovernanceRetention",
      "s3:PutBucketPolicy",
      "s3:PutBucketOwnershipControls"
    ],
    "Resource": [
      "arn:aws:s3:::netapp-backup-*"
    ]
  }
]

```

```

    ],
    "Effect": "Allow",
    "Sid": "backupS3Policy"
  },
  {
    "Action": [
      "s3:CreateBucket",
      "s3:GetLifecycleConfiguration",
      "s3:PutLifecycleConfiguration",
      "s3:PutBucketTagging",
      "s3:ListBucketVersions",
      "s3:GetBucketPolicyStatus",
      "s3:GetBucketPublicAccessBlock",
      "s3:GetBucketAcl",
      "s3:GetBucketPolicy",
      "s3:PutBucketPublicAccessBlock",
      "s3:DeleteBucket"
    ],
    "Resource": [
      "arn:aws:s3:::fabric-pool*"
    ],
    "Effect": "Allow",
    "Sid": "fabricPoolS3Policy"
  },
  {
    "Action": [
      "ec2:DescribeRegions"
    ],
    "Resource": "*",
    "Effect": "Allow",
    "Sid": "fabricPoolPolicy"
  },
  {
    "Condition": {
      "StringLike": {
        "ec2:ResourceTag/netapp-adc-manager": "*"
      }
    },
    "Action": [
      "ec2:StartInstances",
      "ec2:StopInstances",
      "ec2:TerminateInstances"
    ],
    "Resource": [
      "arn:aws:ec2:*:*:instance/*"
    ],

```



```

        "Effect": "Allow"
    },
    {
        "Condition": {
            "StringLike": {
                "ec2:ResourceTag/WorkingEnvironment": "*"
            }
        },
        "Action": [
            "ec2:StartInstances",
            "ec2:TerminateInstances",
            "ec2:AttachVolume",
            "ec2:DetachVolume",
            "ec2:StopInstances",
            "ec2>DeleteVolume"
        ],
        "Resource": [
            "arn:aws:ec2:*:*:instance/*"
        ],
        "Effect": "Allow"
    },
    {
        "Action": [
            "ec2:AttachVolume",
            "ec2:DetachVolume"
        ],
        "Resource": [
            "arn:aws:ec2:*:*:volume/*"
        ],
        "Effect": "Allow"
    },
    {
        "Condition": {
            "StringLike": {
                "ec2:ResourceTag/WorkingEnvironment": "*"
            }
        },
        "Action": [
            "ec2>DeleteVolume"
        ],
        "Resource": [
            "arn:aws:ec2:*:*:volume/*"
        ],
        "Effect": "Allow"
    }
]

```

```
}
```

Policy #2

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Action": [
        "ec2:CreateTags",
        "ec2>DeleteTags",
        "ec2:DescribeTags",
        "tag:getResources",
        "tag:getTagKeys",
        "tag:getTagValues",
        "tag:TagResources",
        "tag:UntagResources"
      ],
      "Resource": "*",
      "Effect": "Allow",
      "Sid": "tagServicePolicy"
    }
  ]
}
```

```

{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "iam:ListInstanceProfiles",
        "iam:CreateRole",
        "iam:DeleteRole",
        "iam:PutRolePolicy",
        "iam:CreateInstanceProfile",
        "iam:DeleteRolePolicy",
        "iam:AddRoleToInstanceProfile",
        "iam:RemoveRoleFromInstanceProfile",
        "iam:DeleteInstanceProfile",
        "ec2:ModifyVolumeAttribute",
        "sts:DecodeAuthorizationMessage",
        "ec2:DescribeImages",
        "ec2:DescribeRouteTables",
        "ec2:DescribeInstances",
        "iam:PassRole",
        "ec2:DescribeInstanceStatus",
        "ec2:RunInstances",
        "ec2:ModifyInstanceAttribute",
        "ec2:CreateTags",
        "ec2:CreateVolume",
        "ec2:DescribeVolumes",
        "ec2:DeleteVolume",
        "ec2:CreateSecurityGroup",
        "ec2:DeleteSecurityGroup",
        "ec2:DescribeSecurityGroups",
        "ec2:RevokeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupEgress",
        "ec2:AuthorizeSecurityGroupIngress",
        "ec2:RevokeSecurityGroupIngress",
        "ec2:CreateNetworkInterface",
        "ec2:DescribeNetworkInterfaces",
        "ec2:DeleteNetworkInterface",
        "ec2:ModifyNetworkInterfaceAttribute",
        "ec2:DescribeSubnets",
        "ec2:DescribeVpcs",
        "ec2:DescribeDhcpOptions",
        "ec2:CreateSnapshot",
        "ec2:DeleteSnapshot",

```

```

        "ec2:DescribeSnapshots",
        "ec2:StopInstances",
        "ec2:GetConsoleOutput",
        "ec2:DescribeKeyPairs",
        "ec2:DescribeRegions",
        "ec2>DeleteTags",
        "ec2:DescribeTags",
        "cloudformation:CreateStack",
        "cloudformation>DeleteStack",
        "cloudformation:DescribeStacks",
        "cloudformation:DescribeStackEvents",
        "cloudformation:ValidateTemplate",
        "s3:GetObject",
        "s3:ListBucket",
        "s3:ListAllMyBuckets",
        "s3:GetBucketTagging",
        "s3:GetBucketLocation",
        "s3:CreateBucket",
        "s3:GetBucketPolicyStatus",
        "s3:GetBucketPublicAccessBlock",
        "s3:GetBucketAcl",
        "s3:GetBucketPolicy",
        "kms:List*",
        "kms:ReEncrypt*",
        "kms:Describe*",
        "kms:CreateGrant",
        "ec2:AssociateIamInstanceProfile",
        "ec2:DescribeIamInstanceProfileAssociations",
        "ec2:DisassociateIamInstanceProfile",
        "ec2:DescribeInstanceAttribute",
        "ec2:CreatePlacementGroup",
        "ec2>DeletePlacementGroup"
    ],
    "Resource": "*"
},
{
    "Sid": "fabricPoolPolicy",
    "Effect": "Allow",
    "Action": [
        "s3:DeleteBucket",
        "s3:GetLifecycleConfiguration",
        "s3:PutLifecycleConfiguration",
        "s3:PutBucketTagging",
        "s3:ListBucketVersions",
        "s3:GetBucketPolicyStatus",
        "s3:GetBucketPublicAccessBlock",

```

```

        "s3:GetBucketAcl",
        "s3:GetBucketPolicy",
        "s3:PutBucketPublicAccessBlock"
    ],
    "Resource": [
        "arn:aws-us-gov:s3:::fabric-pool*"
    ]
},
{
    "Sid": "backupPolicy",
    "Effect": "Allow",
    "Action": [
        "s3:DeleteBucket",
        "s3:GetLifecycleConfiguration",
        "s3:PutLifecycleConfiguration",
        "s3:PutBucketTagging",
        "s3:ListBucketVersions",
        "s3:GetObject",
        "s3:ListBucket",
        "s3:ListAllMyBuckets",
        "s3:GetBucketTagging",
        "s3:GetBucketLocation",
        "s3:GetBucketPolicyStatus",
        "s3:GetBucketPublicAccessBlock",
        "s3:GetBucketAcl",
        "s3:GetBucketPolicy",
        "s3:PutBucketPublicAccessBlock"
    ],
    "Resource": [
        "arn:aws-us-gov:s3:::netapp-backup-*"
    ]
},
{
    "Effect": "Allow",
    "Action": [
        "ec2:StartInstances",
        "ec2:TerminateInstances",
        "ec2:AttachVolume",
        "ec2:DetachVolume"
    ],
    "Condition": {
        "StringLike": {
            "ec2:ResourceTag/WorkingEnvironment": "*"
        }
    },
    "Resource": [

```

```
        "arn:aws-us-gov:ec2:*:*:instance/*"
    ],
    {
        "Effect": "Allow",
        "Action": [
            "ec2:AttachVolume",
            "ec2:DetachVolume"
        ],
        "Resource": [
            "arn:aws-us-gov:ec2:*:*:volume/*"
        ]
    }
]
```

```

{
  "Version": "2012-10-17",
  "Statement": [{
    "Effect": "Allow",
    "Action": [
      "ec2:DescribeInstances",
      "ec2:DescribeInstanceStatus",
      "ec2:RunInstances",
      "ec2:ModifyInstanceAttribute",
      "ec2:DescribeRouteTables",
      "ec2:DescribeImages",
      "ec2:CreateTags",
      "ec2:CreateVolume",
      "ec2:DescribeVolumes",
      "ec2:ModifyVolumeAttribute",
      "ec2>DeleteVolume",
      "ec2:CreateSecurityGroup",
      "ec2>DeleteSecurityGroup",
      "ec2:DescribeSecurityGroups",
      "ec2:RevokeSecurityGroupEgress",
      "ec2:RevokeSecurityGroupIngress",
      "ec2:AuthorizeSecurityGroupEgress",
      "ec2:AuthorizeSecurityGroupIngress",
      "ec2:CreateNetworkInterface",
      "ec2:DescribeNetworkInterfaces",
      "ec2>DeleteNetworkInterface",
      "ec2:ModifyNetworkInterfaceAttribute",
      "ec2:DescribeSubnets",
      "ec2:DescribeVpcs",
      "ec2:DescribeDhcpOptions",
      "ec2:CreateSnapshot",
      "ec2>DeleteSnapshot",
      "ec2:DescribeSnapshots",
      "ec2:GetConsoleOutput",
      "ec2:DescribeKeyPairs",
      "ec2:DescribeRegions",
      "ec2>DeleteTags",
      "ec2:DescribeTags",
      "cloudformation:CreateStack",
      "cloudformation>DeleteStack",
      "cloudformation:DescribeStacks",
      "cloudformation:DescribeStackEvents",
      "cloudformation:ValidateTemplate",
      "iam:PassRole",

```

```

        "iam:CreateRole",
        "iam:DeleteRole",
        "iam:PutRolePolicy",
        "iam:CreateInstanceProfile",
        "iam:DeleteRolePolicy",
        "iam:AddRoleToInstanceProfile",
        "iam:RemoveRoleFromInstanceProfile",
        "iam:DeleteInstanceProfile",
        "s3:GetObject",
        "s3:ListBucket",
        "s3:GetBucketTagging",
        "s3:GetBucketLocation",
        "s3:ListAllMyBuckets",
        "kms:List*",
        "kms:Describe*",
        "ec2:AssociateIamInstanceProfile",
        "ec2:DescribeIamInstanceProfileAssociations",
        "ec2:DisassociateIamInstanceProfile",
        "ec2:DescribeInstanceAttribute",
        "ec2:CreatePlacementGroup",
        "ec2:DeletePlacementGroup",
        "iam:ListInstanceProfiles"
    ],
    "Resource": "*"
},
{
    "Sid": "fabricPoolPolicy",
    "Effect": "Allow",
    "Action": [
        "s3:DeleteBucket",
        "s3:GetLifecycleConfiguration",
        "s3:PutLifecycleConfiguration",
        "s3:PutBucketTagging",
        "s3:ListBucketVersions"
    ],
    "Resource": [
        "arn:aws-iso-b:s3:::fabric-pool*"
    ]
},
{
    "Effect": "Allow",
    "Action": [
        "ec2:StartInstances",
        "ec2:StopInstances",
        "ec2:TerminateInstances",
        "ec2:AttachVolume",

```



```

        "ec2:DetachVolume"
    ],
    "Condition": {
        "StringLike": {
            "ec2:ResourceTag/WorkingEnvironment": "*"
        }
    },
    "Resource": [
        "arn:aws-iso-b:ec2:*:*:instance/*"
    ]
},
{
    "Effect": "Allow",
    "Action": [
        "ec2:AttachVolume",
        "ec2:DetachVolume"
    ],
    "Resource": [
        "arn:aws-iso-b:ec2:*:*:volume/*"
    ]
}
]
}

```

```

{
  "Version": "2012-10-17",
  "Statement": [{
    "Effect": "Allow",
    "Action": [
      "ec2:DescribeInstances",
      "ec2:DescribeInstanceStatus",
      "ec2:RunInstances",
      "ec2:ModifyInstanceAttribute",
      "ec2:DescribeRouteTables",
      "ec2:DescribeImages",
      "ec2:CreateTags",
      "ec2:CreateVolume",
      "ec2:DescribeVolumes",
      "ec2:ModifyVolumeAttribute",
      "ec2>DeleteVolume",
      "ec2:CreateSecurityGroup",
      "ec2>DeleteSecurityGroup",
      "ec2:DescribeSecurityGroups",
      "ec2:RevokeSecurityGroupEgress",
      "ec2:RevokeSecurityGroupIngress",
      "ec2:AuthorizeSecurityGroupEgress",
      "ec2:AuthorizeSecurityGroupIngress",
      "ec2:CreateNetworkInterface",
      "ec2:DescribeNetworkInterfaces",
      "ec2>DeleteNetworkInterface",
      "ec2:ModifyNetworkInterfaceAttribute",
      "ec2:DescribeSubnets",
      "ec2:DescribeVpcs",
      "ec2:DescribeDhcpOptions",
      "ec2:CreateSnapshot",
      "ec2>DeleteSnapshot",
      "ec2:DescribeSnapshots",
      "ec2:GetConsoleOutput",
      "ec2:DescribeKeyPairs",
      "ec2:DescribeRegions",
      "ec2>DeleteTags",
      "ec2:DescribeTags",
      "cloudformation:CreateStack",
      "cloudformation>DeleteStack",
      "cloudformation:DescribeStacks",
      "cloudformation:DescribeStackEvents",
      "cloudformation:ValidateTemplate",
      "iam:PassRole",

```

```

        "iam:CreateRole",
        "iam:DeleteRole",
        "iam:PutRolePolicy",
        "iam:CreateInstanceProfile",
        "iam:DeleteRolePolicy",
        "iam:AddRoleToInstanceProfile",
        "iam:RemoveRoleFromInstanceProfile",
        "iam:DeleteInstanceProfile",
        "s3:GetObject",
        "s3:ListBucket",
        "s3:GetBucketTagging",
        "s3:GetBucketLocation",
        "s3:ListAllMyBuckets",
        "kms:List*",
        "kms:Describe*",
        "ec2:AssociateIamInstanceProfile",
        "ec2:DescribeIamInstanceProfileAssociations",
        "ec2:DisassociateIamInstanceProfile",
        "ec2:DescribeInstanceAttribute",
        "ec2:CreatePlacementGroup",
        "ec2:DeletePlacementGroup",
        "iam:ListInstanceProfiles"
    ],
    "Resource": "*"
},
{
    "Sid": "fabricPoolPolicy",
    "Effect": "Allow",
    "Action": [
        "s3:DeleteBucket",
        "s3:GetLifecycleConfiguration",
        "s3:PutLifecycleConfiguration",
        "s3:PutBucketTagging",
        "s3:ListBucketVersions"
    ],
    "Resource": [
        "arn:aws-iso:s3:::fabric-pool*"
    ]
},
{
    "Effect": "Allow",
    "Action": [
        "ec2:StartInstances",
        "ec2:StopInstances",
        "ec2:TerminateInstances",
        "ec2:AttachVolume",

```

```

        "ec2:DetachVolume"
    ],
    "Condition": {
        "StringLike": {
            "ec2:ResourceTag/WorkingEnvironment": "*"
        }
    },
    "Resource": [
        "arn:aws-iso:ec2:*:*:instance/*"
    ]
},
{
    "Effect": "Allow",
    "Action": [
        "ec2:AttachVolume",
        "ec2:DetachVolume"
    ],
    "Resource": [
        "arn:aws-iso:ec2:*:*:volume/*"
    ]
}
]
}

```

How the AWS permissions are used

The following sections describe how the permissions are used for each BlueXP service. This information can be helpful if your corporate policies dictate that permissions are only provided as needed.

Amazon FSx for ONTAP

The Connector makes the following API requests to manage an Amazon FSx for ONTAP file system:

- ec2:DescribeInstances
- ec2:DescribeInstanceStatus
- ec2:DescribeInstanceAttribute
- ec2:DescribeRouteTables
- ec2:DescribeImages
- ec2:CreateTags
- ec2:DescribeVolumes
- ec2:DescribeSecurityGroups
- ec2:DescribeNetworkInterfaces
- ec2:DescribeSubnets
- ec2:DescribeVpcs

- ec2:DescribeDhcpOptions
- ec2:DescribeSnapshots
- ec2:DescribeKeyPairs
- ec2:DescribeRegions
- ec2:DescribeTags
- ec2:DescribeIamInstanceProfileAssociations
- ec2:DescribeReservedInstancesOfferings
- ec2:DescribeVpcEndpoints
- ec2:DescribeVpcs
- ec2:DescribeVolumesModifications
- ec2:DescribePlacementGroups
- kms:List*
- kms:Describe*
- kms:CreateGrant
- kms:ListAliases
- fsx:Describe*
- fsx:List*

Amazon S3 bucket discovery

The Connector makes the following API request to discover Amazon S3 buckets:

s3:GetEncryptionConfiguration

Backup and recovery

The Connector makes the following API requests to manage backups in Amazon S3:

- s3:GetBucketLocation
- s3:ListAllMyBuckets
- s3:ListBucket
- s3>CreateBucket
- s3:GetLifecycleConfiguration
- s3:PutLifecycleConfiguration
- s3:PutBucketTagging
- s3:ListBucketVersions
- s3:GetBucketAcl
- s3:PutBucketPublicAccessBlock
- kms:List*
- kms:Describe*
- s3:GetObject

- ec2:DescribeVpcEndpoints
- kms:ListAliases
- s3:PutEncryptionConfiguration

The Connector makes the following API requests when you use the Search & Restore method to restore volumes and files:

- s3:CreateBucket
- s3:DeleteObject
- s3:DeleteObjectVersion
- s3:GetBucketAcl
- s3:ListBucket
- s3:ListBucketVersions
- s3:ListBucketMultipartUploads
- s3:PutObject
- s3:PutBucketAcl
- s3:PutLifecycleConfiguration
- s3:PutBucketPublicAccessBlock
- s3:AbortMultipartUpload
- s3:ListMultipartUploadParts
- athena:StartQueryExecution
- athena:GetQueryResults
- athena:GetQueryExecution
- athena:StopQueryExecution
- glue:CreateDatabase
- glue:CreateTable
- glue:BatchDeletePartition

The Connector makes the following API requests when you use DataLock and Ransomware protection for your volume backups:

- s3:GetObjectVersionTagging
- s3:GetBucketObjectLockConfiguration
- s3:GetObjectVersionAcl
- s3:PutObjectTagging
- s3:DeleteObject
- s3:DeleteObjectTagging
- s3:GetObjectRetention
- s3:DeleteObjectVersionTagging
- s3:PutObject

- s3:GetObject
- s3:PutBucketObjectLockConfiguration
- s3:GetLifecycleConfiguration
- s3:ListBucketByTags
- s3:GetBucketTagging
- s3:DeleteObjectVersion
- s3:ListBucketVersions
- s3:ListBucket
- s3:PutBucketTagging
- s3:GetObjectTagging
- s3:PutBucketVersioning
- s3:PutObjectVersionTagging
- s3:GetBucketVersioning
- s3:GetBucketAcl
- s3:BypassGovernanceRetention
- s3:PutObjectRetention
- s3:GetBucketLocation
- s3:GetObjectVersion

The Connector makes the following API requests if you use a different AWS account for your Cloud Volumes ONTAP backups than you're using for the source volumes:

- s3:PutBucketPolicy
- s3:PutBucketOwnershipControls

Classification

The Connector makes the following API requests to deploy the BlueXP classification instance:

- ec2:DescribeInstances
- ec2:DescribeInstanceStatus
- ec2:RunInstances
- ec2:TerminateInstances
- ec2:CreateTags
- ec2:CreateVolume
- ec2:AttachVolume
- ec2:CreateSecurityGroup
- ec2>DeleteSecurityGroup
- ec2:DescribeSecurityGroups
- ec2:CreateNetworkInterface
- ec2:DescribeNetworkInterfaces

- ec2:DeleteNetworkInterface
- ec2:DescribeSubnets
- ec2:DescribeVpcs
- ec2:CreateSnapshot
- ec2:DescribeRegions
- cloudformation:CreateStack
- cloudformation>DeleteStack
- cloudformation:DescribeStacks
- cloudformation:DescribeStackEvents
- iam:AddRoleToInstanceProfile
- ec2:AssociateIamInstanceProfile
- ec2:DescribeIamInstanceProfileAssociations

The Connector makes the following API requests to scan S3 buckets when you use BlueXP classification:

- iam:AddRoleToInstanceProfile
- ec2:AssociateIamInstanceProfile
- ec2:DescribeIamInstanceProfileAssociations
- s3:GetBucketTagging
- s3:GetBucketLocation
- s3:ListAllMyBuckets
- s3:ListBucket
- s3:GetBucketPolicyStatus
- s3:GetBucketPolicy
- s3:GetBucketAcl
- s3:GetObject
- iam:GetRole
- s3>DeleteObject
- s3>DeleteObjectVersion
- s3:PutObject
- sts:AssumeRole

Cloud Volumes ONTAP

The Connector makes the following API requests to deploy and manage Cloud Volumes ONTAP in AWS.

Purpose	Action	Used for deployment?	Used for daily operations?	Used for deletion?
Create and manage IAM roles and instance profiles for Cloud Volumes ONTAP instances	iam:ListInstanceProfiles	Yes	Yes	No
	iam:CreateRole	Yes	No	No
	iam:DeleteRole	No	Yes	Yes
	iam:PutRolePolicy	Yes	No	No
	iam:CreateInstanceProfile	Yes	No	No
	iam:DeleteRolePolicy	No	Yes	Yes
	iam:AddRoleToInstanceProfile	Yes	No	No
	iam:RemoveRoleFromInstanceProfile	No	Yes	Yes
	iam:DeleteInstanceProfile	No	Yes	Yes
	iam:PassRole	Yes	No	No
	ec2:AssociateIamInstanceProfile	Yes	Yes	No
	ec2:DescribeIamInstanceProfileAssociations	Yes	Yes	No
	ec2:DisassociateIamInstanceProfile	No	Yes	No
Decode authorization status messages	sts:DecodeAuthorizationMessage	Yes	Yes	No
Describe the specified images (AMIs) available to the account	ec2:DescribeImages	Yes	Yes	No
Describe the route tables in a VPC (required for HA pairs only)	ec2:DescribeRouteTables	Yes	No	No

Purpose	Action	Used for deployment?	Used for daily operations?	Used for deletion?
Stop, start, and monitor instances	ec2:StartInstances	Yes	Yes	No
	ec2:StopInstances	Yes	Yes	No
	ec2:DescribeInstances	Yes	Yes	No
	ec2:DescribeInstanceStatus	Yes	Yes	No
	ec2:RunInstances	Yes	No	No
	ec2:TerminateInstances	No	No	Yes
	ec2:ModifyInstanceAttribute	No	Yes	No
Verify that enhanced networking is enabled for supported instance types	ec2:DescribeInstanceAttribute	No	Yes	No
Tag resources with the "WorkingEnvironment" and "WorkingEnvironmentId" tags which are used for maintenance and cost allocation	ec2:CreateTags	Yes	Yes	No
Manage EBS volumes that Cloud Volumes ONTAP uses as back-end storage	ec2:CreateVolume	Yes	Yes	No
	ec2:DescribeVolumes	Yes	Yes	Yes
	ec2:ModifyVolumeAttribute	No	Yes	Yes
	ec2:AttachVolume	Yes	Yes	No
	ec2>DeleteVolume	No	Yes	Yes
	ec2:DetachVolume	No	Yes	Yes

Purpose	Action	Used for deployment?	Used for daily operations?	Used for deletion?
Create and manage security groups for Cloud Volumes ONTAP	ec2:CreateSecurityGroup	Yes	No	No
	ec2:DeleteSecurityGroup	No	Yes	Yes
	ec2:DescribeSecurityGroups	Yes	Yes	Yes
	ec2:RevokeSecurityGroupEgress	Yes	No	No
	ec2:AuthorizeSecurityGroupEgress	Yes	No	No
	ec2:AuthorizeSecurityGroupIngress	Yes	No	No
	ec2:RevokeSecurityGroupIngress	Yes	Yes	No
Create and manage network interfaces for Cloud Volumes ONTAP in the target subnet	ec2:CreateNetworkInterface	Yes	No	No
	ec2:DescribeNetworkInterfaces	Yes	Yes	No
	ec2:DeleteNetworkInterface	No	Yes	Yes
	ec2:ModifyNetworkInterfaceAttribute	No	Yes	No
Get the list of destination subnets and security groups	ec2:DescribeSubnets	Yes	Yes	No
	ec2:DescribeVpcs	Yes	Yes	No
Get DNS servers and the default domain name for Cloud Volumes ONTAP instances	ec2:DescribeDhcpOptions	Yes	No	No
Take snapshots of EBS volumes for Cloud Volumes ONTAP	ec2:CreateSnapshot	Yes	Yes	No
	ec2:DeleteSnapshot	No	Yes	Yes
	ec2:DescribeSnapshots	No	Yes	No
Capture the Cloud Volumes ONTAP console, which is attached to AutoSupport messages	ec2:GetConsoleOutput	Yes	Yes	No

Purpose	Action	Used for deployment?	Used for daily operations?	Used for deletion?
Get the list of available key pairs	ec2:DescribeKeyPairs	Yes	No	No
Get the list of available AWS regions	ec2:DescribeRegions	Yes	Yes	No
Manage tags for resources associated with Cloud Volumes ONTAP instances	ec2:DeleteTags	No	Yes	Yes
	ec2:DescribeTags	No	Yes	No
Create and manage stacks for AWS CloudFormation templates	cloudformation:CreateStack	Yes	No	No
	cloudformation:DeleteStack	Yes	No	No
	cloudformation:DescribeStacks	Yes	Yes	No
	cloudformation:DescribeStackEvents	Yes	No	No
	cloudformation:ValidateTemplate	Yes	No	No

Purpose	Action	Used for deployment?	Used for daily operations?	Used for deletion?
Create and manage an S3 bucket that a Cloud Volumes ONTAP system uses as a capacity tier for data tiering	s3:CreateBucket	Yes	Yes	No
	s3:DeleteBucket	No	Yes	Yes
	s3:GetLifecycleConfiguration	No	Yes	No
	s3:PutLifecycleConfiguration	No	Yes	No
	s3:PutBucketTagging	No	Yes	No
	s3:ListBucketVersions	No	Yes	No
	s3:GetBucketPolicyStatus	No	Yes	No
	s3:GetBucketPublicAccessBlock	No	Yes	No
	s3:GetBucketAcl	No	Yes	No
	s3:GetBucketPolicy	No	Yes	No
	s3:PutBucketPublicAccessBlock	No	Yes	No
	s3:GetBucketTagging	No	Yes	No
	s3:GetBucketLocation	No	Yes	No
	s3:ListAllMyBuckets	No	No	No
	s3:ListBucket	No	Yes	No
Enable data encryption of Cloud Volumes ONTAP using the AWS Key Management Service (KMS)	kms:List*	Yes	Yes	No
	kms:ReEncrypt*	Yes	No	No
	kms:Describe*	Yes	Yes	No
	kms:CreateGrant	Yes	Yes	No
	kms:GenerateDataKeyWithoutPlaintext	Yes	Yes	No
Create and manage an AWS spread placement group for two HA nodes and the mediator in a single AWS Availability Zone	ec2:CreatePlacementGroup	Yes	No	No
	ec2:DeletePlacementGroup	No	Yes	Yes

Purpose	Action	Used for deployment?	Used for daily operations?	Used for deletion?
Create reports	fsx:Describe*	No	Yes	No
	fsx:List*	No	Yes	No
Create and manage aggregates that support the Amazon EBS Elastic Volumes feature	ec2:DescribeVolume sModifications	No	Yes	No
	ec2:ModifyVolume	No	Yes	No
Check whether the Availability Zone is an AWS Local Zone and validates that all deployment parameters are compatible	ec2:DescribeAvailabi lityZones	Yes	No	Yes

Change log

As permissions are added and removed, we'll note them in the sections below.

9 September 2024

Permissions were removed from policy #2 for standard regions because BlueXP no longer supports BlueXP edge caching and discovery and management of Kubernetes clusters.

View the permissions that were removed from the policy

```
{
  "Action": [
    "ec2:DescribeRegions",
    "eks:ListClusters",
    "eks:DescribeCluster",
    "iam:GetInstanceProfile"
  ],
  "Resource": "*",
  "Effect": "Allow",
  "Sid": "K8sServicePolicy"
},
{
  "Action": [
    "cloudformation:DescribeStacks",
    "cloudwatch:GetMetricStatistics",
    "cloudformation:ListStacks"
  ],
  "Resource": "*",
  "Effect": "Allow",
  "Sid": "GFCservicePolicy"
},
{
  "Condition": {
    "StringLike": {
      "ec2:ResourceTag/GFCInstance": "*"
    }
  },
  "Action": [
    "ec2:StartInstances",
    "ec2:TerminateInstances",
    "ec2:AttachVolume",
    "ec2:DetachVolume"
  ],
  "Resource": [
    "arn:aws:ec2:*:*:instance/*"
  ],
  "Effect": "Allow"
},
```

9 May 2024

The following permissions is now required for Cloud Volumes ONTAP:

ec2:DescribeAvailabilityZones

6 June 2023

The following permission is now required for Cloud Volumes ONTAP:

kms:GenerateDataKeyWithoutPlaintext

14 February 2023

The following permission is now required for BlueXP tiering:

ec2:DescribeVpcEndpoints

Azure permissions for the Connector

When BlueXP launches the Connector VM in Azure, it attaches a custom role to the VM that provides the Connector with permissions to manage resources and processes within that Azure subscription. The Connector uses the permissions to make API calls to several Azure services.

Whether or not you need to create this custom role for the Connector depends on how you deployed it.

Deploying from BlueXP

When you use BlueXP to deploy the Connector virtual machine in Azure, it enables a [system-assigned managed identity](#) on the 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. The role's permissions are kept up-to-date when the Connector is upgraded. You don't need to create this role for the Connector or manage updates.

Deploying manually or from Azure marketplace

When you deploy the Connector from the Azure Marketplace or if you manually install the Connector on a Linux host, then you need to set up the custom role yourself and maintain its permissions with any changes.

You'll need to ensure that the role is up to date as new permissions are added in subsequent releases. If new permissions are required, they will be listed in the release notes.

- To view step-by-step instructions for using these policies, refer to the following pages:
 - [Set up permissions for an Azure Marketplace deployment](#)
 - [Set up permissions for on-premises deployments](#)
 - [Set up permissions for restricted mode](#)
 - [Set up permissions for private mode](#)

```
{
  "Name": "BlueXP Operator",
  "Actions": [
    "Microsoft.Compute/disks/delete",
    "Microsoft.Compute/disks/read",
    "Microsoft.Compute/disks/write",
    "Microsoft.Compute/locations/operations/read",
```



```

"Microsoft.Compute/locations/vmSizes/read",
"Microsoft.Resources/subscriptions/locations/read",
"Microsoft.Compute/operations/read",
"Microsoft.Compute/virtualMachines/instanceView/read",
"Microsoft.Compute/virtualMachines/powerOff/action",
"Microsoft.Compute/virtualMachines/read",
"Microsoft.Compute/virtualMachines/restart/action",
"Microsoft.Compute/virtualMachines/deallocate/action",
"Microsoft.Compute/virtualMachines/start/action",
"Microsoft.Compute/virtualMachines/vmSizes/read",
"Microsoft.Compute/virtualMachines/write",
"Microsoft.Compute/images/read",
"Microsoft.Network/locations/operationResults/read",
"Microsoft.Network/locations/operations/read",
"Microsoft.Network/networkInterfaces/read",
"Microsoft.Network/networkInterfaces/write",
"Microsoft.Network/networkInterfaces/join/action",
"Microsoft.Network/networkSecurityGroups/read",
"Microsoft.Network/networkSecurityGroups/write",
"Microsoft.Network/networkSecurityGroups/join/action",
"Microsoft.Network/virtualNetworks/read",

"Microsoft.Network/virtualNetworks/checkIpAddressAvailability/read",
"Microsoft.Network/virtualNetworks/subnets/read",
"Microsoft.Network/virtualNetworks/subnets/write",

"Microsoft.Network/virtualNetworks/subnets/virtualMachines/read",

"Microsoft.Network/virtualNetworks/virtualMachines/read",

"Microsoft.Network/virtualNetworks/subnets/join/action",
"Microsoft.Resources/deployments/operations/read",
"Microsoft.Resources/deployments/read",
"Microsoft.Resources/deployments/write",
"Microsoft.Resources/resources/read",

"Microsoft.Resources/subscriptions/operationresults/read",

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

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

"Microsoft.Resources/subscriptions/resourcegroups/resources/read",

"Microsoft.Resources/subscriptions/resourceGroups/write",
"Microsoft.Storage/checknameavailability/read",

```

```

        "Microsoft.Storage/operations/read",
        "Microsoft.Storage/storageAccounts/listkeys/action",
        "Microsoft.Storage/storageAccounts/read",
        "Microsoft.Storage/storageAccounts/delete",
        "Microsoft.Storage/storageAccounts/write",

"Microsoft.Storage/storageAccounts/blobServices/containers/read",

"Microsoft.Storage/storageAccounts/listAccountSas/action",
        "Microsoft.Storage/usages/read",
        "Microsoft.Compute/snapshots/write",
        "Microsoft.Compute/snapshots/read",
        "Microsoft.Compute/availabilitySets/write",
        "Microsoft.Compute/availabilitySets/read",
        "Microsoft.Compute/disks/beginGetAccess/action",

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

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

        "Microsoft.Network/loadBalancers/read",
        "Microsoft.Network/loadBalancers/write",
        "Microsoft.Network/loadBalancers/delete",

"Microsoft.Network/loadBalancers/backendAddressPools/read",

"Microsoft.Network/loadBalancers/backendAddressPools/join/action",

"Microsoft.Network/loadBalancers/loadBalancingRules/read",
        "Microsoft.Network/loadBalancers/probes/read",
        "Microsoft.Network/loadBalancers/probes/join/action",
        "Microsoft.Authorization/locks/*",
        "Microsoft.Network/routeTables/join/action",
        "Microsoft.NetApp/netAppAccounts/read",
        "Microsoft.NetApp/netAppAccounts/capacityPools/read",

"Microsoft.NetApp/netAppAccounts/capacityPools/volumes/write",

"Microsoft.NetApp/netAppAccounts/capacityPools/volumes/read",

"Microsoft.NetApp/netAppAccounts/capacityPools/volumes/delete",
        "Microsoft.Network/privateEndpoints/write",

"Microsoft.Storage/storageAccounts/PrivateEndpointConnectionsApproval/action",

```

```

"Microsoft.Storage/storageAccounts/privateEndpointConnections/read",

"Microsoft.Storage/storageAccounts/managementPolicies/read",

"Microsoft.Storage/storageAccounts/managementPolicies/write",
    "Microsoft.Network/privateEndpoints/read",
    "Microsoft.Network/privateDnsZones/write",

"Microsoft.Network/privateDnsZones/virtualNetworkLinks/write",
    "Microsoft.Network/virtualNetworks/join/action",
    "Microsoft.Network/privateDnsZones/A/write",
    "Microsoft.Network/privateDnsZones/read",

"Microsoft.Network/privateDnsZones/virtualNetworkLinks/read",

"Microsoft.Resources/deployments/operationStatuses/read",
    "Microsoft.Insights/Metrics/Read",
    "Microsoft.Compute/virtualMachines/extensions/write",
    "Microsoft.Compute/virtualMachines/extensions/delete",
    "Microsoft.Compute/virtualMachines/extensions/read",
    "Microsoft.Compute/virtualMachines/delete",
    "Microsoft.Network/networkInterfaces/delete",
    "Microsoft.Network/networkSecurityGroups/delete",
    "Microsoft.Resources/deployments/delete",
    "Microsoft.Compute/diskEncryptionSets/read",
    "Microsoft.Compute/snapshots/delete",
    "Microsoft.Network/privateEndpoints/delete",
    "Microsoft.Compute/availabilitySets/delete",
    "Microsoft.KeyVault/vaults/read",
    "Microsoft.KeyVault/vaults/accessPolicies/write",
    "Microsoft.Compute/diskEncryptionSets/write",
    "Microsoft.KeyVault/vaults/deploy/action",
    "Microsoft.Compute/diskEncryptionSets/delete",
    "Microsoft.Resources/tags/read",
    "Microsoft.Resources/tags/write",
    "Microsoft.Resources/tags/delete",
    "Microsoft.Network/applicationSecurityGroups/write",
    "Microsoft.Network/applicationSecurityGroups/read",

"Microsoft.Network/applicationSecurityGroups/joinIpConfiguration/action",

"Microsoft.Network/networkSecurityGroups/securityRules/write",
    "Microsoft.Network/applicationSecurityGroups/delete",

"Microsoft.Network/networkSecurityGroups/securityRules/delete",

```

```

        "Microsoft.Synapse/workspaces/write",
        "Microsoft.Synapse/workspaces/read",
        "Microsoft.Synapse/workspaces/delete",
        "Microsoft.Synapse/register/action",
        "Microsoft.Synapse/checkNameAvailability/action",
        "Microsoft.Synapse/workspaces/operationStatuses/read",
        "Microsoft.Synapse/workspaces/firewallRules/read",

        "Microsoft.Synapse/workspaces/replaceAllIpFirewallRules/action",
        "Microsoft.Synapse/workspaces/operationResults/read",

        "Microsoft.Synapse/workspaces/privateEndpointConnectionsApproval/action",

        "Microsoft.ManagedIdentity/userAssignedIdentities/assign/action",
        "Microsoft.Compute/images/write",

        "Microsoft.Network/loadBalancers/frontendIPConfigurations/read",
        "Microsoft.Compute/virtualMachineScaleSets/write",
        "Microsoft.Compute/virtualMachineScaleSets/read",
        "Microsoft.Compute/virtualMachineScaleSets/delete"
    ],
    "NotActions": [],
    "AssignableScopes": [],
    "Description": "BlueXP Permissions",
    "IsCustom": "true"
}

```

How Azure permissions are used

The following sections describe how the permissions are used for each BlueXP service. This information can be helpful if your corporate policies dictate that permissions are only provided as needed.

Azure NetApp Files

The Connector makes the following API requests when you use BlueXP classification to scan Azure NetApp Files data:

- Microsoft.NetApp/netAppAccounts/read
- Microsoft.NetApp/netAppAccounts/capacityPools/read
- Microsoft.NetApp/netAppAccounts/capacityPools/volumes/write
- Microsoft.NetApp/netAppAccounts/capacityPools/volumes/read
- Microsoft.NetApp/netAppAccounts/capacityPools/volumes/delete

Backup and recovery

The Connector makes the following API requests for BlueXP backup and recovery:

- Microsoft.Storage/storageAccounts/listkeys/action
- Microsoft.Storage/storageAccounts/read
- Microsoft.Storage/storageAccounts/write
- Microsoft.Storage/storageAccounts/blobServices/containers/read
- Microsoft.Storage/storageAccounts/listAccountSas/action
- Microsoft.KeyVault/vaults/read
- Microsoft.KeyVault/vaults/accessPolicies/write
- Microsoft.Network/networkInterfaces/read
- Microsoft.Resources/subscriptions/locations/read
- Microsoft.Network/virtualNetworks/read
- Microsoft.Network/virtualNetworks/subnets/read
- Microsoft.Resources/subscriptions/resourceGroups/read
- Microsoft.Resources/subscriptions/resourcegroups/resources/read
- Microsoft.Resources/subscriptions/resourceGroups/write
- Microsoft.Authorization/locks/*
- Microsoft.Network/privateEndpoints/write
- Microsoft.Network/privateEndpoints/read
- Microsoft.Network/privateDnsZones/virtualNetworkLinks/write
- Microsoft.Network/virtualNetworks/join/action
- Microsoft.Network/privateDnsZones/A/write
- Microsoft.Network/privateDnsZones/read
- Microsoft.Network/privateDnsZones/virtualNetworkLinks/read
- Microsoft.Network/networkInterfaces/delete
- Microsoft.Network/networkSecurityGroups/delete
- Microsoft.Resources/deployments/delete
- Microsoft.ManagedIdentity/userAssignedIdentities/assign/action

The Connector makes the following API requests when you use the Search & Restore functionality:

- Microsoft.Synapse/workspaces/write
- Microsoft.Synapse/workspaces/read
- Microsoft.Synapse/workspaces/delete
- Microsoft.Synapse/register/action
- Microsoft.Synapse/checkNameAvailability/action
- Microsoft.Synapse/workspaces/operationStatuses/read
- Microsoft.Synapse/workspaces/firewallRules/read
- Microsoft.Synapse/workspaces/replaceAllIpFirewallRules/action
- Microsoft.Synapse/workspaces/operationResults/read

- Microsoft.Synapse/workspaces/privateEndpointConnectionsApproval/action

Classification

The Connector makes the following API requests when you use BlueXP classification.

Action	Used for set up?	Used for daily operations?
Microsoft.Compute/locations/operations/read	Yes	Yes
Microsoft.Compute/locations/vmSizes/read	Yes	Yes
Microsoft.Compute/operations/read	Yes	Yes
Microsoft.Compute/virtualMachines/instanceView/read	Yes	Yes
Microsoft.Compute/virtualMachines/powerOff/action	Yes	No
Microsoft.Compute/virtualMachines/read	Yes	Yes
Microsoft.Compute/virtualMachines/restart/action	Yes	No
Microsoft.Compute/virtualMachines/start/action	Yes	No
Microsoft.Compute/virtualMachines/vmSizes/read	No	Yes
Microsoft.Compute/virtualMachines/write	Yes	No
Microsoft.Compute/images/read	Yes	Yes
Microsoft.Compute/disks/delete	Yes	No
Microsoft.Compute/disks/read	Yes	Yes
Microsoft.Compute/disks/write	Yes	No
Microsoft.Storage/checknameavailability/read	Yes	Yes
Microsoft.Storage/operations/read	Yes	Yes
Microsoft.Storage/storageAccounts/listkeys/action	Yes	No
Microsoft.Storage/storageAccounts/read	Yes	Yes
Microsoft.Storage/storageAccounts/write	Yes	No
Microsoft.Storage/storageAccounts/blobServices/containers/read	Yes	Yes

Action	Used for set up?	Used for daily operations?
Microsoft.Network/networkInterfaces/read	Yes	Yes
Microsoft.Network/networkInterfaces/write	Yes	No
Microsoft.Network/networkInterfaces/join/action	Yes	No
Microsoft.Network/networkSecurityGroups/read	Yes	Yes
Microsoft.Network/networkSecurityGroups/write	Yes	No
Microsoft.Resources/subscriptions/locations/read	Yes	Yes
Microsoft.Network/locations/operationResults/read	Yes	Yes
Microsoft.Network/locations/operations/read	Yes	Yes
Microsoft.Network/virtualNetworks/read	Yes	Yes
Microsoft.Network/virtualNetworks/checkIpAddressAvailability/read	Yes	Yes
Microsoft.Network/virtualNetworks/subnets/read	Yes	Yes
Microsoft.Network/virtualNetworks/subnets/virtualMachines/read	Yes	Yes
Microsoft.Network/virtualNetworks/virtualMachines/read	Yes	Yes
Microsoft.Network/virtualNetworks/subnets/join/action	Yes	No
Microsoft.Network/virtualNetworks/subnets/write	Yes	No
Microsoft.Network/routeTables/join/action	Yes	No
Microsoft.Resources/deployments/operations/read	Yes	Yes
Microsoft.Resources/deployments/read	Yes	Yes
Microsoft.Resources/deployments/write	Yes	No
Microsoft.Resources/resources/read	Yes	Yes

Action	Used for set up?	Used for daily operations?
Microsoft.Resources/subscriptions/operationresults/read	Yes	Yes
Microsoft.Resources/subscriptions/resourceGroups/delete	Yes	No
Microsoft.Resources/subscriptions/resourceGroups/read	Yes	Yes
Microsoft.Resources/subscriptions/resourcegroups/resources/read	Yes	Yes
Microsoft.Resources/subscriptions/resourceGroups/write	Yes	No

Cloud Volumes ONTAP

The Connector makes the following API requests to deploy and manage Cloud Volumes ONTAP in Azure.

Purpose	Action	Used for deployment?	Used for daily operations?	Used for deletion?
Create and manage VMs	Microsoft.Compute/locations/operations/read	Yes	Yes	No
	Microsoft.Compute/locations/vmSizes/read	Yes	Yes	No
	Microsoft.Resources/subscriptions/locations/read	Yes	No	No
	Microsoft.Compute/operations/read	Yes	Yes	No
	Microsoft.Compute/virtualMachines/instanceView/read	Yes	Yes	No
	Microsoft.Compute/virtualMachines/powerOff/action	Yes	Yes	No
	Microsoft.Compute/virtualMachines/read	Yes	Yes	No
	Microsoft.Compute/virtualMachines/restart/action	Yes	Yes	No
	Microsoft.Compute/virtualMachines/start/action	Yes	Yes	No
	Microsoft.Compute/virtualMachines/deallocate/action	No	Yes	Yes
	Microsoft.Compute/virtualMachines/vmSizes/read	No	Yes	No
	Microsoft.Compute/virtualMachines/write	Yes	Yes	No
	Microsoft.Compute/virtualMachines/delete	Yes	Yes	Yes
	Microsoft.Resources/deployments/delete	Yes	No	No
Enable deployment from a VHD	Microsoft.Compute/images/read	Yes	No	No
	Microsoft.Compute/images/write	Yes	No	No

Purpose	Action	Used for deployment?	Used for daily operations?	Used for deletion?
Create and manage network interfaces in the target subnet	Microsoft.Network/networkInterfaces/read	Yes	Yes	No
	Microsoft.Network/networkInterfaces/write	Yes	Yes	No
	Microsoft.Network/networkInterfaces/join/action	Yes	Yes	No
	Microsoft.Network/networkInterfaces/delete	Yes	Yes	No
Create and manage network security groups	Microsoft.Network/networkSecurityGroups/read	Yes	Yes	No
	Microsoft.Network/networkSecurityGroups/write	Yes	Yes	No
	Microsoft.Network/networkSecurityGroups/join/action	Yes	No	No
	Microsoft.Network/networkSecurityGroups/delete	No	Yes	Yes

Purpose	Action	Used for deployment?	Used for daily operations?	Used for deletion?
Get network information about regions, the target VNet and subnet, and add the VMs to VNets	Microsoft.Network/locations/operationResults/read	Yes	Yes	No
	Microsoft.Network/locations/operations/read	Yes	Yes	No
	Microsoft.Network/virtualNetworks/read	Yes	No	No
	Microsoft.Network/virtualNetworks/checkIpAddressAvailability/read	Yes	No	No
	Microsoft.Network/virtualNetworks/subnets/read	Yes	Yes	No
	Microsoft.Network/virtualNetworks/subnets/virtualMachines/read	Yes	Yes	No
	Microsoft.Network/virtualNetworks/virtualMachines/read	Yes	Yes	No
	Microsoft.Network/virtualNetworks/subnets/join/action	Yes	Yes	No

Purpose	Action	Used for deployment?	Used for daily operations?	Used for deletion?
Create and manage resource groups	Microsoft.Resources/deployments/operations/read	Yes	Yes	No
	Microsoft.Resources/deployments/read	Yes	Yes	No
	Microsoft.Resources/deployments/write	Yes	Yes	No
	Microsoft.Resources/resources/read	Yes	Yes	No
	Microsoft.Resources/subscriptions/operationresults/read	Yes	Yes	No
	Microsoft.Resources/subscriptions/resourceGroups/delete	Yes	Yes	Yes
	Microsoft.Resources/subscriptions/resourceGroups/read	No	Yes	No
	Microsoft.Resources/subscriptions/resourcegroups/resources/read	Yes	Yes	No
	Microsoft.Resources/subscriptions/resourceGroups/write	Yes	Yes	No

Purpose	Action	Used for deployment?	Used for daily operations?	Used for deletion?
Manage Azure storage accounts and disks	Microsoft.Compute/disks/read	Yes	Yes	Yes
	Microsoft.Compute/disks/write	Yes	Yes	No
	Microsoft.Compute/disks/delete	Yes	Yes	Yes
	Microsoft.Storage/checknameavailability/read	Yes	Yes	No
	Microsoft.Storage/operations/read	Yes	Yes	No
	Microsoft.Storage/storageAccounts/listkeys/action	Yes	Yes	No
	Microsoft.Storage/storageAccounts/read	Yes	Yes	No
	Microsoft.Storage/storageAccounts/delete	No	Yes	Yes
	Microsoft.Storage/storageAccounts/write	Yes	Yes	No
	Microsoft.Storage/usage/read	No	Yes	No
Enable backups to Blob storage and encryption of storage accounts	Microsoft.Storage/storageAccounts/blobServices/containers/read	Yes	Yes	No
	Microsoft.KeyVault/vaults/read	Yes	Yes	No
	Microsoft.KeyVault/vaults/accessPolicies/write	Yes	Yes	No
Enable VNet service endpoints for data tiering	Microsoft.Network/virtualNetworks/subnets/write	Yes	Yes	No
	Microsoft.Network/routeTables/join/action	Yes	Yes	No

Purpose	Action	Used for deployment?	Used for daily operations?	Used for deletion?
Create and manage Azure managed snapshots	Microsoft.Compute/snapshots/write	Yes	Yes	No
	Microsoft.Compute/snapshots/read	Yes	Yes	No
	Microsoft.Compute/snapshots/delete	No	Yes	Yes
	Microsoft.Compute/disks/beginGetAccess/action	No	Yes	No
Create and manage availability sets	Microsoft.Compute/availabilitySets/write	Yes	No	No
	Microsoft.Compute/availabilitySets/read	Yes	No	No
Enable programmatic deployments from the marketplace	Microsoft.MarketplaceOrdering/offertypes/publishers/offers/plans/agreements/read	Yes	No	No
	Microsoft.MarketplaceOrdering/offertypes/publishers/offers/plans/agreements/write	Yes	Yes	No

Purpose	Action	Used for deployment?	Used for daily operations?	Used for deletion?
Manage a load balancer for HA pairs	Microsoft.Network/loadBalancers/read	Yes	Yes	No
	Microsoft.Network/loadBalancers/write	Yes	No	No
	Microsoft.Network/loadBalancers/delete	No	Yes	Yes
	Microsoft.Network/loadBalancers/backendAddressPools/read	Yes	No	No
	Microsoft.Network/loadBalancers/backendAddressPools/join/action	Yes	No	No
	Microsoft.Network/loadBalancers/frontendIPConfigurations/read	Yes	Yes	No
	Microsoft.Network/loadBalancers/loadBalancingRules/read	Yes	No	No
	Microsoft.Network/loadBalancers/probes/read	Yes	No	No
	Microsoft.Network/loadBalancers/probes/join/action	Yes	No	No
	Microsoft.Authorization/locks/*	Yes	Yes	No
Enable management of locks on Azure disks				

Purpose	Action	Used for deployment?	Used for daily operations?	Used for deletion?
Enable private endpoints for HA pairs when there's no connectivity outside the subnet	Microsoft.Network/privateEndpoints/write	Yes	Yes	No
	Microsoft.Storage/storageAccounts/PrivateEndpointConnectionsApproval/action	Yes	No	No
	Microsoft.Storage/storageAccounts/privateEndpointConnections/read	Yes	Yes	Yes
	Microsoft.Network/privateEndpoints/read	Yes	Yes	Yes
	Microsoft.Network/privateDnsZones/write	Yes	Yes	No
	Microsoft.Network/privateDnsZones/virtualNetworkLinks/write	Yes	Yes	No
	Microsoft.Network/virtualNetworks/join/action	Yes	Yes	No
	Microsoft.Network/privateDnsZones/A/write	Yes	Yes	No
	Microsoft.Network/privateDnsZones/read	Yes	Yes	No
	Microsoft.Network/privateDnsZones/virtualNetworkLinks/read	Yes	Yes	No
Required for some VM deployments, depending on the underlying physical hardware	Microsoft.Resources/deployments/operationStatuses/read	Yes	Yes	No
Remove resources from a resource group in case of deployment failure or deletion	Microsoft.Network/privateEndpoints/delete	Yes	Yes	No
	Microsoft.Compute/availabilitySets/delete	Yes	Yes	No

Purpose	Action	Used for deployment?	Used for daily operations?	Used for deletion?
Enable the use of customer-managed encryption keys when using the API	Microsoft.Compute/diskEncryptionSets/read	Yes	Yes	Yes
	Microsoft.Compute/diskEncryptionSets/write	Yes	Yes	No
	Microsoft.KeyVault/vaults/deploy/action	Yes	No	No
	Microsoft.Compute/diskEncryptionSets/delete	Yes	Yes	Yes
Configure an application security group for an HA pair to isolate the HA interconnect and cluster network NICs	Microsoft.Network/applicationSecurityGroups/write	No	Yes	No
	Microsoft.Network/applicationSecurityGroups/read	No	Yes	No
	Microsoft.Network/applicationSecurityGroups/joinIpConfiguration/action	No	Yes	No
	Microsoft.Network/networkSecurityGroups/securityRules/write	Yes	Yes	No
	Microsoft.Network/applicationSecurityGroups/delete	No	Yes	Yes
	Microsoft.Network/networkSecurityGroups/securityRules/delete	No	Yes	Yes
Read, write, and delete tags associated with Cloud Volumes ONTAP resources	Microsoft.Resources/tags/read	No	Yes	No
	Microsoft.Resources/tags/write	Yes	Yes	No
	Microsoft.Resources/tags/delete	Yes	No	No
Encrypt storage accounts during creation	Microsoft.ManagedIdentity/userAssignedIdentities/assign/action	Yes	Yes	No

Purpose	Action	Used for deployment?	Used for daily operations?	Used for deletion?
Use Virtual Machine Scale Sets in Flexible orchestration mode in order to specify specific zones for Cloud Volumes ONTAP	Microsoft.Compute/virtualMachineScaleSets/write	Yes	No	No
	Microsoft.Compute/virtualMachineScaleSets/read	Yes	No	No
	Microsoft.Compute/virtualMachineScaleSets/delete	No	No	Yes

Tiering

The Connector makes the following API requests when you set up BlueXP tiering.

- Microsoft.Storage/storageAccounts/listkeys/action
- Microsoft.Resources/subscriptions/resourceGroups/read
- Microsoft.Resources/subscriptions/locations/read

The Connector makes the following API requests for daily operations.

- Microsoft.Storage/storageAccounts/blobServices/containers/read
- Microsoft.Storage/storageAccounts/managementPolicies/read
- Microsoft.Storage/storageAccounts/managementPolicies/write
- Microsoft.Storage/storageAccounts/read

Change log

As permissions are added and removed, we'll note them in the sections below.

9 September 2024

The following permissions were removed from the JSON policy because BlueXP no longer supports discovery and management of Kubernetes clusters:

- Microsoft.ContainerService/managedClusters/listClusterUserCredential/action
- Microsoft.ContainerService/managedClusters/read

22 August 2024

The following permissions were added to the JSON policy because they are required for Cloud Volumes ONTAP support of Virtual Machine Scale Sets:

- Microsoft.Compute/virtualMachineScaleSets/write
- Microsoft.Compute/virtualMachineScaleSets/read
- Microsoft.Compute/virtualMachineScaleSets/delete

5 December 2023

The following permissions are no longer needed for BlueXP backup and recovery when backing up volume data to Azure Blob storage:

- Microsoft.Compute/virtualMachines/read
- Microsoft.Compute/virtualMachines/start/action
- Microsoft.Compute/virtualMachines/deallocate/action
- Microsoft.Compute/virtualMachines/extensions/delete
- Microsoft.Compute/virtualMachines/delete

These permissions are required for other BlueXP storage services, so they'll still remain in the custom role for the Connector if you're using those other storage services.

12 May 2023

The following permissions were added to the JSON policy because they are required for Cloud Volumes ONTAP management:

- Microsoft.Compute/images/write
- Microsoft.Network/loadBalancers/frontendIPConfigurations/read

The following permissions were removed from the JSON policy because they are no longer required:

- Microsoft.Storage/storageAccounts/blobServices/containers/write
- Microsoft.Network/publicIPAddresses/delete

23 March 2023

The "Microsoft.Storage/storageAccounts/delete" permission is no longer needed for BlueXP classification.

This permission is still required for Cloud Volumes ONTAP.

5 January 2023

The following permissions were added to the JSON policy:

- Microsoft.Storage/storageAccounts/listAccountSas/action
- Microsoft.Synapse/workspaces/privateEndpointConnectionsApproval/action

These permissions are required for BlueXP backup and recovery.

- Microsoft.Network/loadBalancers/backendAddressPools/join/action

This permission is required for Cloud Volumes ONTAP deployment.

Google Cloud permissions for the Connector

BlueXP requires permissions to perform actions in Google Cloud. These permissions are included in a custom role provided by NetApp. You might want to understand what BlueXP does with these permissions.

Service account permissions

The custom role shown below provides the permissions that a Connector needs to manage resources and processes within your Google Cloud network.

You'll need to apply this custom role to a service account that gets attached to the Connector VM.

- [Set up Google Cloud permissions for standard mode](#)
- [Set up permissions for restricted mode](#)
- [Set up permissions for private mode](#)

You also need to ensure that the role is up to date as new permissions are added in subsequent releases. If new permissions are required, they will be listed in the release notes.

```
title: NetApp BlueXP
description: Permissions for the service account associated with the
Connector instance.
stage: GA
includedPermissions:
- iam.serviceAccounts.actAs
- compute.regionBackendServices.create
- compute.regionBackendServices.get
- compute.regionBackendServices.list
- compute.networks.updatePolicy
- compute.backendServices.create
- compute.addresses.list
- compute.disks.create
- compute.disks.createSnapshot
- compute.disks.delete
- compute.disks.get
- compute.disks.list
- compute.disks.setLabels
- compute.disks.use
- compute.firewalls.create
- compute.firewalls.delete
- compute.firewalls.get
- compute.firewalls.list
- compute.globalOperations.get
- compute.images.get
- compute.images.getFromFamily
- compute.images.list
- compute.images.useReadOnly
- compute.instances.addAccessConfig
- compute.instances.attachDisk
- compute.instances.create
- compute.instances.delete
- compute.instances.detachDisk
```

- `compute.instances.get`
- `compute.instances.getSerialPortOutput`
- `compute.instances.list`
- `compute.instances.setDeletionProtection`
- `compute.instances.setLabels`
- `compute.instances.setMachineType`
- `compute.instances.setMetadata`
- `compute.instances.setTags`
- `compute.instances.start`
- `compute.instances.stop`
- `compute.instances.updateDisplayDevice`
- `compute.instanceGroups.get`
- `compute.addresses.get`
- `compute.instances.updateNetworkInterface`
- `compute.machineTypes.get`
- `compute.networks.get`
- `compute.networks.list`
- `compute.projects.get`
- `compute.regions.get`
- `compute.regions.list`
- `compute.snapshots.create`
- `compute.snapshots.delete`
- `compute.snapshots.get`
- `compute.snapshots.list`
- `compute.snapshots.setLabels`
- `compute.subnetworks.get`
- `compute.subnetworks.list`
- `compute.subnetworks.use`
- `compute.subnetworks.useExternalIp`
- `compute.zoneOperations.get`
- `compute.zones.get`
- `compute.zones.list`
- `compute.instances.setServiceAccount`
- `deploymentmanager.compositeTypes.get`
- `deploymentmanager.compositeTypes.list`
- `deploymentmanager.deployments.create`
- `deploymentmanager.deployments.delete`
- `deploymentmanager.deployments.get`
- `deploymentmanager.deployments.list`
- `deploymentmanager.manifests.get`
- `deploymentmanager.manifests.list`
- `deploymentmanager.operations.get`
- `deploymentmanager.operations.list`
- `deploymentmanager.resources.get`
- `deploymentmanager.resources.list`
- `deploymentmanager.typeProviders.get`

- deploymentmanager.typeProviders.list
- deploymentmanager.types.get
- deploymentmanager.types.list
- logging.logEntries.list
- logging.privateLogEntries.list
- resourcemanager.projects.get
- storage.buckets.create
- storage.buckets.delete
- storage.buckets.get
- storage.buckets.list
- cloudkms.cryptoKeyVersions.useToEncrypt
- cloudkms.cryptoKeys.get
- cloudkms.cryptoKeys.list
- cloudkms.keyRings.list
- storage.buckets.update
- iam.serviceAccounts.getIamPolicy
- iam.serviceAccounts.list
- storage.objects.get
- storage.objects.list
- monitoring.timeSeries.list
- storage.buckets.getIamPolicy
- cloudkms.cryptoKeys.getIamPolicy
- cloudkms.cryptoKeys.setIamPolicy
- cloudkms.keyRings.get
- cloudkms.keyRings.getIamPolicy
- cloudkms.keyRings.setIamPolicy

How Google Cloud permissions are used

Actions	Purpose
<ul style="list-style-type: none"> - compute.disks.create - compute.disks.createSnapshot - compute.disks.delete - compute.disks.get - compute.disks.list - compute.disks.setLabels - compute.disks.use 	To create and manage disks for Cloud Volumes ONTAP.
<ul style="list-style-type: none"> - compute.firewalls.create - compute.firewalls.delete - compute.firewalls.get - compute.firewalls.list 	To create firewall rules for Cloud Volumes ONTAP.
<ul style="list-style-type: none"> - compute.globalOperations.get 	To get the status of operations.
<ul style="list-style-type: none"> - compute.images.get - compute.images.getFromFamily - compute.images.list - compute.images.useReadOnly 	To get images for VM instances.

Actions	Purpose
<ul style="list-style-type: none"> - compute.instances.attachDisk - compute.instances.detachDisk 	To attach and detach disks to Cloud Volumes ONTAP.
<ul style="list-style-type: none"> - compute.instances.create - compute.instances.delete 	To create and delete Cloud Volumes ONTAP VM instances.
<ul style="list-style-type: none"> - compute.instances.get 	To list VM instances.
<ul style="list-style-type: none"> - compute.instances.getSerialPortOutput 	To get console logs.
<ul style="list-style-type: none"> - compute.instances.list 	To retrieve the list of instances in a zone.
<ul style="list-style-type: none"> - compute.instances.setDeletionProtection 	To set deletion protection on the instance.
<ul style="list-style-type: none"> - compute.instances.setLabels 	To add labels.
<ul style="list-style-type: none"> - compute.instances.setMachineType - compute.instances.setMinCpuPlatform 	To change the machine type for Cloud Volumes ONTAP.
<ul style="list-style-type: none"> - compute.instances.setMetadata 	To add metadata.
<ul style="list-style-type: none"> - compute.instances.setTags 	To add tags for firewall rules.
<ul style="list-style-type: none"> - compute.instances.start - compute.instances.stop - compute.instances.updateDisplayDevice 	To start and stop Cloud Volumes ONTAP.
<ul style="list-style-type: none"> - compute.machineTypes.get 	To get the numbers of cores to check quotas.
<ul style="list-style-type: none"> - compute.projects.get 	To support multi-projects.
<ul style="list-style-type: none"> - compute.snapshots.create - compute.snapshots.delete - compute.snapshots.get - compute.snapshots.list - compute.snapshots.setLabels 	To create and manage persistent disk snapshots.
<ul style="list-style-type: none"> - compute.networks.get - compute.networks.list - compute.regions.get - compute.regions.list - compute.subnetworks.get - compute.subnetworks.list - compute.zoneOperations.get - compute.zones.get - compute.zones.list 	To get the networking information needed to create a new Cloud Volumes ONTAP virtual machine instance.

Actions	Purpose
<ul style="list-style-type: none"> - deploymentmanager.compositeTypes.get - deploymentmanager.compositeTypes.list - deploymentmanager.deployments.create - deploymentmanager.deployments.delete - deploymentmanager.deployments.get - deploymentmanager.deployments.list - deploymentmanager.manifests.get - deploymentmanager.manifests.list - deploymentmanager.operations.get - deploymentmanager.operations.list - deploymentmanager.resources.get - deploymentmanager.resources.list - deploymentmanager.typeProviders.get - deploymentmanager.typeProviders.list - deploymentmanager.types.get - deploymentmanager.types.list 	To deploy the Cloud Volumes ONTAP virtual machine instance using Google Cloud Deployment Manager.
<ul style="list-style-type: none"> - logging.logEntries.list - logging.privateLogEntries.list 	To get stack log drives.
<ul style="list-style-type: none"> - resourcemanager.projects.get 	To support multi-projects.
<ul style="list-style-type: none"> - storage.buckets.create - storage.buckets.delete - storage.buckets.get - storage.buckets.list - storage.buckets.update 	To create and manage a Google Cloud Storage bucket for data tiering.
<ul style="list-style-type: none"> - cloudkms.cryptoKeyVersions.useToEncrypt - cloudkms.cryptoKeys.get - cloudkms.cryptoKeys.list - cloudkms.keyRings.list 	To use customer-managed encryption keys from the Cloud Key Management Service with Cloud Volumes ONTAP.
<ul style="list-style-type: none"> - compute.instances.setServiceAccount - iam.serviceAccounts.actAs - iam.serviceAccounts.getIamPolicy - iam.serviceAccounts.list - storage.objects.get - storage.objects.list 	To set a service account on the Cloud Volumes ONTAP instance. This service account provides permissions for data tiering to a Google Cloud Storage bucket.
<ul style="list-style-type: none"> - compute.addresses.list 	To retrieve the addresses in a region when deploying an HA pair.
<ul style="list-style-type: none"> - compute.backendServices.create - compute.regionBackendServices.create - compute.regionBackendServices.get - compute.regionBackendServices.list 	To configure a backend service for distributing traffic in an HA pair.
<ul style="list-style-type: none"> - compute.networks.updatePolicy 	To apply firewall rules on the VPCs and subnets for an HA pair.
<ul style="list-style-type: none"> - compute.subnetworks.use - compute.subnetworks.useExternallp - compute.instances.addAccessConfig 	To enable BlueXP classification.

Actions	Purpose
<ul style="list-style-type: none"> - compute.instanceGroups.get - compute.addresses.get - compute.instances.updateNetworkInterface 	To create and manage storage VMs on Cloud Volumes ONTAP HA pairs.
<ul style="list-style-type: none"> - monitoring.timeSeries.list - storage.buckets.getIamPolicy 	To discover information about Google Cloud Storage buckets.
<ul style="list-style-type: none"> - cloudkms.cryptoKeys.get - cloudkms.cryptoKeys.getIamPolicy - cloudkms.cryptoKeys.list - cloudkms.cryptoKeys.setIamPolicy - cloudkms.keyRings.get - cloudkms.keyRings.getIamPolicy - cloudkms.keyRings.list - cloudkms.keyRings.setIamPolicy 	To select your own customer-managed keys in the BlueXP backup and recovery activation wizard instead of using the default Google-managed encryption keys.

Change log

As permissions are added and removed, we'll note them in the sections below.

6 February, 2023

The following permission was added to this policy:

- compute.instances.updateNetworkInterface

This permission is required for Cloud Volumes ONTAP.

27 January, 2023

The following permissions were added to the policy:

- cloudkms.cryptoKeys.getIamPolicy
- cloudkms.cryptoKeys.setIamPolicy
- cloudkms.keyRings.get
- cloudkms.keyRings.getIamPolicy
- cloudkms.keyRings.setIamPolicy

These permissions are required for BlueXP backup and recovery.

Ports

Connector security group rules in AWS

The AWS security group for the Connector requires both inbound and outbound rules. BlueXP automatically creates this security group when you create a Connector from BlueXP. You need to set up this security group for all other installation options.

Inbound rules

Protocol	Port	Purpose
SSH	22	Provides SSH access to the Connector host
HTTP	80	<ul style="list-style-type: none">• Provides HTTP access from client web browsers to the local user interface• Used during the Cloud Volumes ONTAP upgrade process
HTTPS	443	Provides HTTPS access from client web browsers to the local user interface, and connections from the BlueXP classification instance
TCP	3128	Provides Cloud Volumes ONTAP with internet access. You must manually open this port after deployment.

Outbound rules

The predefined security group for the Connector opens all outbound traffic. If that is acceptable, follow the basic outbound rules. If you need more rigid rules, use the advanced outbound rules.

Basic outbound rules

The predefined security group for the Connector includes the following outbound rules.

Protocol	Port	Purpose
All TCP	All	All outbound traffic
All UDP	All	All outbound traffic

Advanced outbound rules

If you need rigid rules for outbound traffic, you can use the following information to open only those ports that are required for outbound communication by the Connector.



The source IP address is the Connector host.

Service	Protocol	Port	Destination	Purpose
API calls and AutoSupport	HTTPS	443	Outbound internet and ONTAP cluster management LIF	API calls to AWS, to ONTAP, to BlueXP classification, and sending AutoSupport messages to NetApp
API calls	TCP	3000	ONTAP HA mediator	Communication with the ONTAP HA mediator
	TCP	8080	BlueXP classification	Probe to BlueXP classification instance during deployment
DNS	UDP	53	DNS	Used for DNS resolve by BlueXP

Connector security group rules in Azure

The Azure security group for the Connector requires both inbound and outbound rules.

BlueXP automatically creates this security group when you create a Connector from BlueXP. You need to set up this security group for all other installation options.

Inbound rules

Protocol	Port	Purpose
SSH	22	Provides SSH access to the Connector host
HTTP	80	<ul style="list-style-type: none">Provides HTTP access from client web browsers to the local user interfaceUsed during the Cloud Volumes ONTAP upgrade process
HTTPS	443	Provides HTTPS access from client web browsers to the local user interface, and connections from the BlueXP classification instance
TCP	3128	Provides Cloud Volumes ONTAP with internet access to send AutoSupport messages to NetApp Support. You must manually open this port after deployment. Learn how the Connector is used as a proxy for AutoSupport messages

Outbound rules

The predefined security group for the Connector opens all outbound traffic. If that is acceptable, follow the basic outbound rules. If you need more rigid rules, use the advanced outbound rules.

Basic outbound rules

The predefined security group for the Connector includes the following outbound rules.

Protocol	Port	Purpose
All TCP	All	All outbound traffic
All UDP	All	All outbound traffic

Advanced outbound rules

If you need rigid rules for outbound traffic, you can use the following information to open only those ports that are required for outbound communication by the Connector.



The source IP address is the Connector host.

Service	Protocol	Port	Destination	Purpose
API calls and AutoSupport	HTTPS	443	Outbound internet and ONTAP cluster management LIF	API calls to Azure, to ONTAP, to BlueXP classification, and sending AutoSupport messages to NetApp
API calls	TCP	8080	BlueXP classification	Probe to BlueXP classification instance during deployment
DNS	UDP	53	DNS	Used for DNS resolve by BlueXP

Connector firewall rules in Google Cloud

The Google Cloud firewall rules for the Connector requires both inbound and outbound rules. BlueXP automatically creates this security group when you create a Connector from BlueXP. You need to set up this security group for all other installation options.

Inbound rules

Protocol	Port	Purpose
SSH	22	Provides SSH access to the Connector host
HTTP	80	<ul style="list-style-type: none">• Provides HTTP access from client web browsers to the local user interface• Used during the Cloud Volumes ONTAP upgrade process
HTTPS	443	Provides HTTPS access from client web browsers to the local user interface
TCP	3128	Provides Cloud Volumes ONTAP with internet access. You must manually open this port after deployment.

Outbound rules

The predefined firewall rules for the Connector opens all outbound traffic. If that is acceptable, follow the basic outbound rules. If you need more rigid rules, use the advanced outbound rules.

Basic outbound rules

The predefined firewall rules for the Connector includes the following outbound rules.

Protocol	Port	Purpose
All TCP	All	All outbound traffic
All UDP	All	All outbound traffic

Advanced outbound rules

If you need rigid rules for outbound traffic, you can use the following information to open only those ports that are required for outbound communication by the Connector.



The source IP address is the Connector host.

Service	Protocol	Port	Destination	Purpose
API calls and AutoSupport	HTTPS	443	Outbound internet and ONTAP cluster management LIF	API calls to Google Cloud, to ONTAP, to BlueXP classification, and sending AutoSupport messages to NetApp
API calls	TCP	8080	BlueXP classification	Probe to BlueXP classification instance during deployment
DNS	UDP	53	DNS	Used for DNS resolve by BlueXP

Ports for the on-premisesConnector

The Connector uses *inbound* ports when installed manually on an on-premises Linux host. You might need to refer to these ports for planning purposes.

These inbound rules apply to all BlueXP deployment models.

Protocol	Port	Purpose
HTTP	80	<ul style="list-style-type: none">• Provides HTTP access from client web browsers to the local user interface• Used during the Cloud Volumes ONTAP upgrade process
HTTPS	443	Provides HTTPS access from client web browsers to the local user interface

Knowledge and support

Register for support

Support registration is required to receive technical support specific to BlueXP and its storage solutions and services. Support registration is also required to enable key workflows for Cloud Volumes ONTAP systems.

Registering for support does not enable NetApp support for a cloud provider file service. For technical support related to a cloud provider file service, its infrastructure, or any solution using the service, refer to "Getting help" in the BlueXP documentation for that product.

- [Amazon FSx for ONTAP](#)
- [Azure NetApp Files](#)
- [Google Cloud NetApp Volumes](#)

Support registration overview

There are two forms of registration to activate support entitlement:

- Registering your BlueXP account serial number (your 20 digit 960xxxxxxx serial number located on the Support Resources page in BlueXP).

This serves as your single support subscription ID for any service within BlueXP. Each BlueXP account-level support subscription must be registered.

- Registering the Cloud Volumes ONTAP serial numbers associated with a subscription in your cloud provider's marketplace (these are 20 digit 909201xxxxxxx serial numbers).

These serial numbers are commonly referred to as *PAYGO serial numbers* and get generated by BlueXP at the time of Cloud Volumes ONTAP deployment.

Registering both types of serial numbers enables capabilities like opening support tickets and automatic case generation. Registration is completed by adding NetApp Support Site (NSS) accounts to BlueXP as described below.

Register BlueXP for NetApp support

To register for support and activate support entitlement, one user in your BlueXP organization (or account) must associate a NetApp Support Site account with their BlueXP login. How you register for NetApp support depends on whether you already have a NetApp Support Site (NSS) account.

Existing customer with an NSS account

If you're a NetApp customer with an NSS account, you simply need to register for support through BlueXP.

Steps

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

3. Select **Add NSS credentials** and follow the NetApp Support Site (NSS) Authentication prompt.
4. To confirm that the registration process was successful, select the Help icon, and select **Support**.

The **Resources** page should show that your BlueXP organization is registered for support.

Note that other BlueXP users will not see this same support registration status if they have not associated a NetApp Support Site account with their BlueXP login. However, that doesn't mean that your BlueXP organization is not registered for support. As long as one user in the organization has followed these steps, then your organization has been registered.

Existing customer but no NSS account

If you're an existing NetApp customer with existing licenses and serial numbers but *no* NSS account, you need to create an NSS account and associate it with your BlueXP login.

Steps

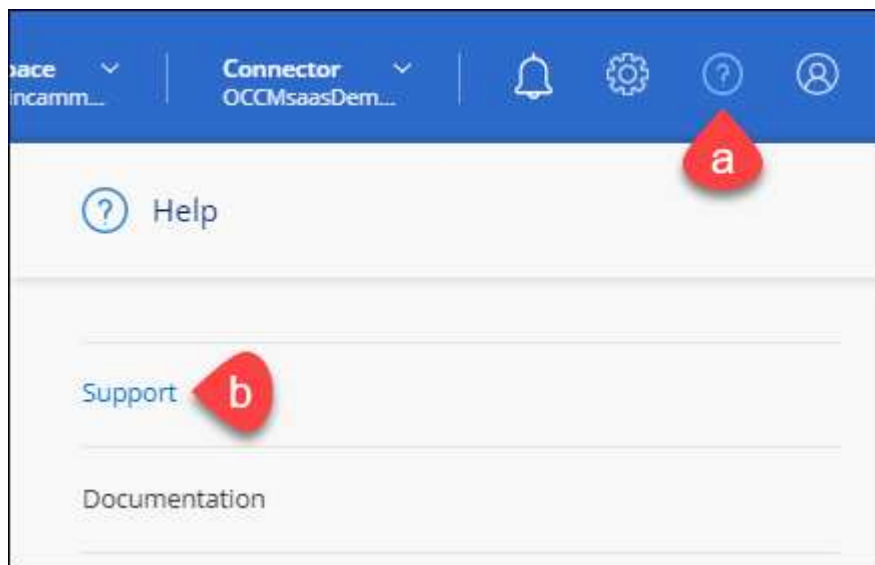
1. Create a NetApp Support Site account by completing the [NetApp Support Site User Registration form](#)
 - a. Be sure to select the appropriate User Level, which is typically **NetApp Customer/End User**.
 - b. Be sure to copy the BlueXP account serial number (960xxxx) used above for the serial number field. This will speed up the account processing.
2. Associate your new NSS account with your BlueXP login by completing the steps under [Existing customer with an NSS account](#).

Brand new to NetApp

If you are brand new to NetApp and you don't have an NSS account, follow each step below.

Steps

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



2. Locate your account ID serial number from the Support Registration page.



96015585434285107893
Account serial number

⚠ Not Registered

Add your NetApp Support Site (NSS) [credentials](#) to BlueXP
Follow these [instructions](#) to register for support in case you don't have an NSS account yet.

3. Navigate to [NetApp's support registration site](#) and select **I am not a registered NetApp Customer**.
4. Fill out the mandatory fields (those with red asterisks).
5. In the **Product Line** field, select **Cloud Manager** and then select your applicable billing provider.
6. Copy your account serial number from step 2 above, complete the security check, and then confirm that you read NetApp's Global Data Privacy Policy.

An email is immediately sent to the mailbox provided to finalize this secure transaction. Be sure to check your spam folders if the validation email doesn't arrive in few minutes.

7. Confirm the action from within the email.

Confirming submits your request to NetApp and recommends that you create a NetApp Support Site account.

8. Create a NetApp Support Site account by completing the [NetApp Support Site User Registration form](#)
 - a. Be sure to select the appropriate User Level, which is typically **NetApp Customer/End User**.
 - b. Be sure to copy the account serial number (960xxxx) used above for the serial number field. This will speed up processing.

After you finish

NetApp should reach out to you during this process. This is a one-time onboarding exercise for new users.

Once you have your NetApp Support Site account, associate the account with your BlueXP login by completing the steps under [Existing customer with an NSS account](#).

Associate NSS credentials for Cloud Volumes ONTAP support

Associating NetApp Support Site credentials with your BlueXP organization is required to enable the following key workflows for Cloud Volumes ONTAP:

- Registering pay-as-you-go Cloud Volumes ONTAP systems for support

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

- Deploying 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.

- Upgrading Cloud Volumes ONTAP software to the latest release

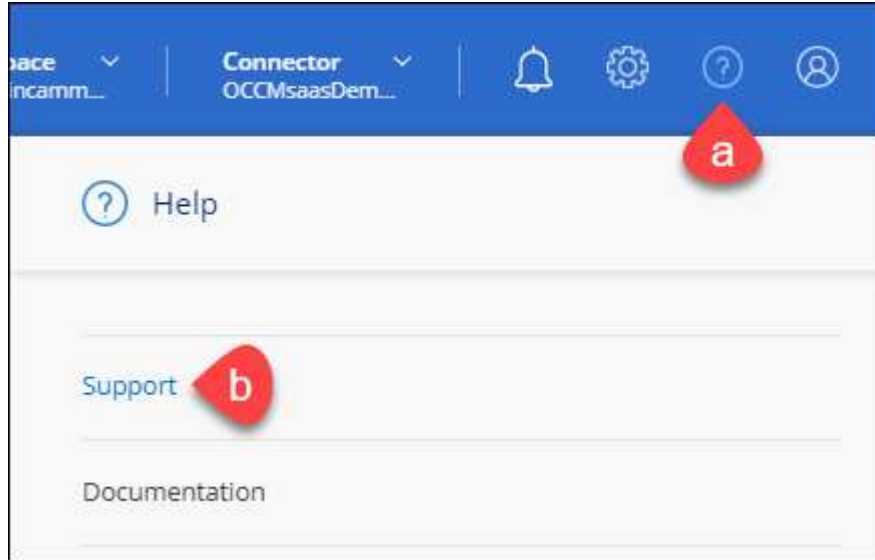
Associating NSS credentials with your BlueXP organization is different than the NSS account that is associated with a BlueXP user login.

These NSS credentials are associated with your specific BlueXP organization ID. Users who belong to the BlueXP organization can access these credentials from **Support > NSS Management**.

- 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, select the Help icon, and select **Support**.



2. Select **NSS Management > Add NSS Account**.
3. When you're prompted, select **Continue** to be redirected to a Microsoft login page.

NetApp uses Microsoft Entra ID 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 NSS account must be a customer-level account (not a guest or temp account). You can have multiple customer-level NSS accounts.
- There can be only one NSS account if that account is a partner-level account. If you try to add customer-level NSS accounts and a partner-level account exists, you'll get the following error message:

"The NSS customer type is not allowed for this account as there are already NSS Users of different type."

The same is true if you have pre-existing customer-level NSS accounts and try to add a partner-level 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. Note that the token for these accounts expire after 90 days. A notification will be posted to alert you of this.

Get help

NetApp provides support for BlueXP and its cloud services in a variety of ways. Extensive free self-support options are available 24/7, such as knowledgebase (KB) articles and a community forum. Your support registration includes remote technical support via web ticketing.

Get support for a cloud provider file service

For technical support related to a cloud provider file service, its infrastructure, or any solution using the service, refer to "Getting help" in the BlueXP documentation for that product.

- [Amazon FSx for ONTAP](#)
- [Azure NetApp Files](#)
- [Google Cloud NetApp Volumes](#)

To receive technical support specific to BlueXP and its storage solutions and services, use the support options described below.

Use self-support options

These options are available for free, 24 hours a day, 7 days a week:

- **Documentation**

The BlueXP documentation that you're currently viewing.

- [Knowledge base](#)

Search through the BlueXP knowledge base to find helpful articles to troubleshoot issues.

- [Communities](#)

Join the BlueXP community to follow ongoing discussions or create new ones.

Create a case with NetApp support

In addition to the self-support options above, you can work with a NetApp Support specialist to resolve any issues after you activate support.

Before you get started

- To use the **Create a Case** capability, you must first associate your NetApp Support Site credentials with your BlueXP login. [Learn how to manage credentials associated with your BlueXP login.](#)
- If you're opening a case for an ONTAP system that has a serial number, then your NSS account must be

associated with the serial number for that system.

Steps

1. In BlueXP, select **Help > Support**.
2. On the **Resources** page, choose one of the available options under Technical Support:
 - a. Select **Call Us** if you'd like to speak with someone on the phone. You'll be directed to a page on netapp.com that lists the phone numbers that you can call.
 - b. Select **Create a Case** to open a ticket with a NetApp Support specialist:
 - **Service:** Select the service that the issue is associated with. For example, BlueXP when specific to a technical support issue with workflows or functionality within the service.
 - **Working Environment:** If applicable to storage, select **Cloud Volumes ONTAP** or **On-Prem** and then the associated working environment.

The list of working environments are within scope of the BlueXP organization (or account), project (or workspace), and Connector you have selected in the top banner of the service.

- **Case Priority:** Choose the priority for the case, which can be Low, Medium, High, or Critical.

To learn more details about these priorities, hover your mouse over the information icon next to the field name.

- **Issue Description:** Provide a detailed description of your problem, including any applicable error messages or troubleshooting steps that you performed.
- **Additional Email Addresses:** Enter additional email addresses if you'd like to make someone else aware of this issue.
- **Attachment (Optional):** Upload up to five attachments, one at a time.

Attachments are limited to 25 MB per file. The following file extensions are supported: txt, log, pdf, jpg/jpeg, rtf, doc/docx, xls/xlsx, and csv.

ntapitdemo
NetApp Support Site Account

Service

Select

Working Enviroment

Select

Case Priority

Low - General guidance

Issue Description

Provide detailed description of problem, applicable error messages and troubleshooting steps taken.

Additional Email Addresses (Optional)

Type here

Attachment (Optional)

No files selected

Upload

After you finish

A pop-up will appear with your support case number. A NetApp Support specialist will review your case and get back to you soon.

For a history of your support cases, you can select **Settings > Timeline** and look for actions named "create support case." A button to the far right lets you expand the action to see details.

It's possible that you might encounter the following error message when trying to create a case:

"You are not authorized to Create a Case against the selected service"

This error could mean that the NSS account and the company of record it's associated with is not the same company of record for the BlueXP account serial number (ie. 960xxxx) or the working environment serial number. You can seek assistance using one of the following options:

- Use the in-product chat
- Submit a non-technical case at <https://mysupport.netapp.com/site/help>

Manage your support cases (Preview)

You can view and manage active and resolved support cases directly from BlueXP. You can manage the cases associated with your NSS account and with your company.

Case management is available as a Preview. We plan to refine this experience and add enhancements in upcoming releases. Please send us feedback by using the in-product chat.

Note the following:

- The case management dashboard at the top of the page offers two views:
 - The view on the left shows the total cases opened in the past 3 months by the user NSS account you provided.
 - The view on the right shows the total cases opened in the past 3 months at your company level based on your user NSS account.

The results in the table reflect the cases related to the view that you selected.

- You can add or remove columns of interest and you can filter the contents of columns like Priority and Status. Other columns provide just sorting capabilities.

View the steps below for more details.

- At a per-case level, we offer the ability to update case notes or close a case that is not already in Closed or Pending Closed status.

Steps

1. In BlueXP, select **Help > Support**.
2. Select **Case Management** and if you're prompted, add your NSS account to BlueXP.

The **Case management** page shows open cases related to the NSS account that is associated with your BlueXP user account. This is the same NSS account that appears at the top of the **NSS management** page.

3. Optionally modify the information that displays in the table:
 - Under **Organization's cases**, select **View** to view all cases associated with your company.
 - Modify the date range by choosing an exact date range or by choosing a different time frame.

Search icon Cases opened on the last 3 months Create a case

Date created	Last updated		Status (5)	
December 22, 2022	December 29, 2022	Last 7 days	Assigned	...
December 21, 2022	December 28, 2022	Last 30 days	Active	...
December 15, 2022	December 27, 2022	Last 3 months	Pending customer	...
December 14, 2022	December 26, 2022	Medium (P3)	Solution proposed	...
		Low (P4)		

Apply Reset

- Filter the contents of the columns.

Search icon Cases opened on the last 3 months Create a case

Last updated	Priority	Status (5)	
December 29, 2022	Critical (P1)	Active	...
December 28, 2022	High (P2)	Pending customer	...
December 27, 2022	Medium (P3)	Solution proposed	...
December 26, 2022	Low (P4)	Pending closed	...
		Closed	...

Apply Reset

- Change the columns that appear in the table by selecting  and then choosing the columns that you'd like to display.

Search icon Cases opened on the last 3 months Create a case

Last updated	Priority	Status (5)	
December 29, 2022	Critical (P1)	Last updated	...
December 28, 2022	High (P2)	Priority	...
December 27, 2022	Medium (P3)	Cluster name	...
December 26, 2022	Low (P4)	Case owner	...
		Opened by	...

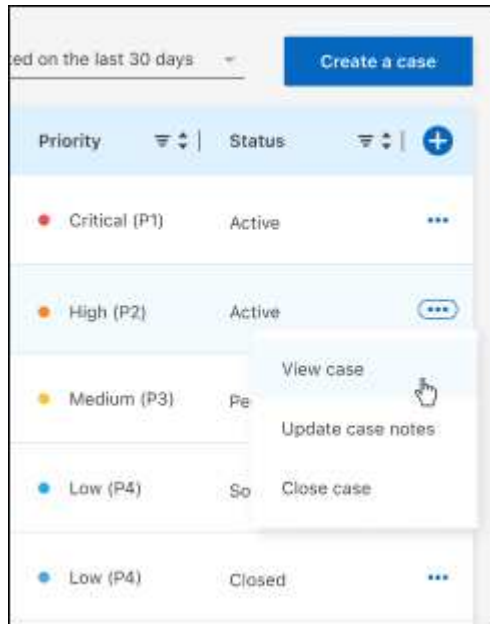
Apply Reset

4. Manage an existing case by selecting ... and selecting one of the available options:

- **View case:** View full details about a specific case.
- **Update case notes:** Provide additional details about your problem or select **Upload files** to attach up to a maximum of five files.

Attachments are limited to 25 MB per file. The following file extensions are supported: txt, log, pdf, jpg/jpeg, rtf, doc/docx, xls/xlsx, and csv.

- **Close case:** Provide details about why you're closing the case and select **Close case**.



Legal notices

Legal notices provide access to copyright statements, trademarks, patents, and more.

Copyright

<https://www.netapp.com/company/legal/copyright/>

Trademarks

NETAPP, the NETAPP logo, and the marks listed on the NetApp Trademarks page are trademarks of NetApp, Inc. Other company and product names may be trademarks of their respective owners.

<https://www.netapp.com/company/legal/trademarks/>

Patents

A current list of NetApp owned patents can be found at:

<https://www.netapp.com/pdf.html?item=/media/11887-patentspage.pdf>

Privacy policy

<https://www.netapp.com/company/legal/privacy-policy/>

Open source

Notice files provide information about third-party copyright and licenses used in NetApp software.

[Notice for BlueXP](#)

Copyright information

Copyright © 2025 NetApp, Inc. All Rights Reserved. Printed in the U.S. No part of this document covered by copyright may be reproduced in any form or by any means—graphic, electronic, or mechanical, including photocopying, recording, taping, or storage in an electronic retrieval system—without prior written permission of the copyright owner.

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

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

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

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

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

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

Trademark information

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