



# **NetApp Console setup and administration documentation**

NetApp Console setup and administration

NetApp  
October 06, 2025

# Table of Contents

- NetApp Console setup and administration documentation . . . . . 1
- Release notes . . . . . 2
  - What's new . . . . . 2
    - 6 October 2025 . . . . . 2
    - BlueXP is now NetApp Console . . . . . 2
    - Console agent 4.0.0 . . . . . 8
    - NetApp Console . . . . . 9
    - 11 August 2025 . . . . . 10
    - 31 July 2025 . . . . . 10
    - 21 July 2025 . . . . . 11
    - 14 July 2025 . . . . . 11
    - 9 June 2025 . . . . . 13
    - 29 May 2025 . . . . . 13
    - 12 May 2025 . . . . . 14
    - 14 April 2025 . . . . . 15
    - 28 March 2025 . . . . . 16
    - 10 March 2025 . . . . . 16
    - 6 March 2025 . . . . . 16
    - 18 February 2025 . . . . . 17
    - 10 February 2025 . . . . . 17
    - 13 January 2025 . . . . . 19
    - 16 December 2024 . . . . . 20
    - 9 December 2024 . . . . . 20
    - 26 November 2024 . . . . . 21
    - 11 November 2024 . . . . . 21
    - 10 October 2024 . . . . . 22
    - 7 October 2024 . . . . . 22
    - 30 September 2024 . . . . . 23
    - 9 September 2024 . . . . . 24
    - 22 August 2024 . . . . . 25
    - 8 August 2024 . . . . . 26
    - 31 July 2024 . . . . . 26
    - 15 July 2024 . . . . . 27
    - 8 July 2024 . . . . . 28
    - 12 June 2024 . . . . . 28
    - 4 June 2024 . . . . . 28
    - 17 May 2024 . . . . . 29
  - Known limitations of NetApp Console . . . . . 30
    - Console agent limitations . . . . . 30
  - Changes to supported Linux operating systems . . . . . 30
    - Supported operating systems . . . . . 31
    - Support for RHEL 8 and 9 . . . . . 31
    - End of support for RHEL 7 and CentOS 7 . . . . . 32

Related information .....	32
Get started .....	34
Learn the basics .....	34
Learn about NetApp Console .....	34
Learn about NetApp Console agents .....	37
Learn about NetApp Console deployment modes .....	41
Get started with the NetApp assistant .....	48
Get started using the NetApp Console Assistant .....	48
Get started with standard mode .....	49
Getting started workflow (standard mode) .....	49
Prepare network access for NetApp Console .....	50
Sign up or log in to NetApp Console .....	52
Create a Console agent .....	53
Subscribe to NetApp Intelligent Services (standard mode) .....	191
What you can do next (standard mode) .....	198
Get started with restricted mode .....	198
Getting started workflow (restricted mode) .....	198
Prepare for deployment in restricted mode .....	199
Deploy the Console agent in restricted mode .....	219
Subscribe to NetApp Intelligent Services (restricted mode) .....	229
What you can do next (restricted mode) .....	236
Get started with BlueXP legacy interface (private mode) .....	236
Getting started workflow (BlueXP private mode) .....	237
Use NetApp Console .....	239
Log in to the NetApp Console .....	239
View metrics on the NetApp Console Home page .....	241
Required NetApp Console roles .....	241
Enable metrics to appear on the Home page .....	243
View the overall storage capacity .....	243
View ONTAP alerts .....	243
View storage performance capacity .....	244
View the licenses and subscriptions that you have .....	245
View Ransomware Resilience status .....	245
View Backup and Recovery status .....	245
Manage your NetApp Console user settings .....	246
Change your display name .....	246
Configure multi-factor authentication .....	246
Regenerate your MFA recovery code .....	247
Delete your MFA configuration .....	247
Contact your Organization administrator .....	247
Configure dark mode (dark theme) .....	248
Administer NetApp Console .....	249
Identity and access management .....	249
Learn about NetApp Console identity and access management .....	249
Get started with identity and access in NetApp Console .....	256

Organize your NetApp Console resources with folders and projects. . . . .	257
Add members and service accounts to NetApp Console. . . . .	261

# **NetApp Console setup and administration documentation**

# Release notes

## What's new

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

**6 October 2025**

### BlueXP is now NetApp Console

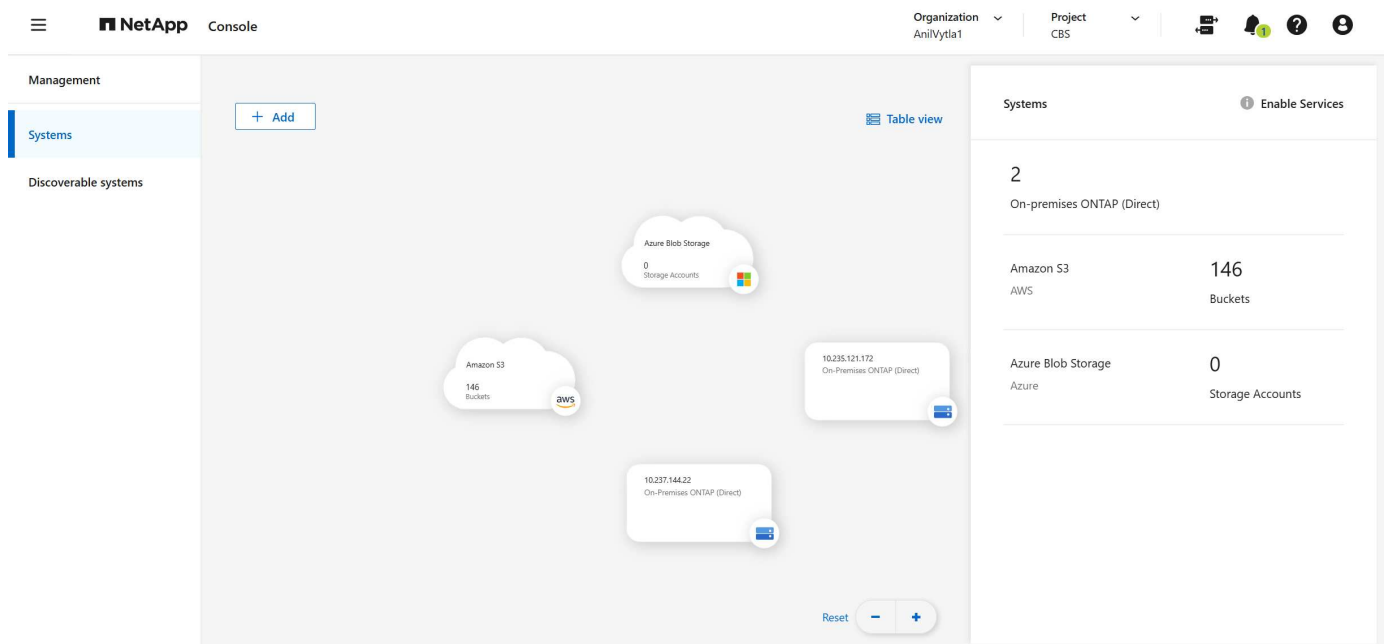
The NetApp Console, built on the enhanced and restructured BlueXP foundation, provides centralized management of NetApp storage and NetApp Data Services across on-premises and cloud environments at enterprise grade—delivering real-time insights, faster workflows, and simplified administration, that is highly secure and compliant.

#### Navigation menus and pages

NetApp moved most menu options to the left-navigation pane and reorganized menus for easier navigation in the NetApp Console.

#### Canvas is replaced by the Systems page

NetApp renamed the Canvas to the **Systems** page. Navigate to the **System** page from the **Storage > Management** menu.

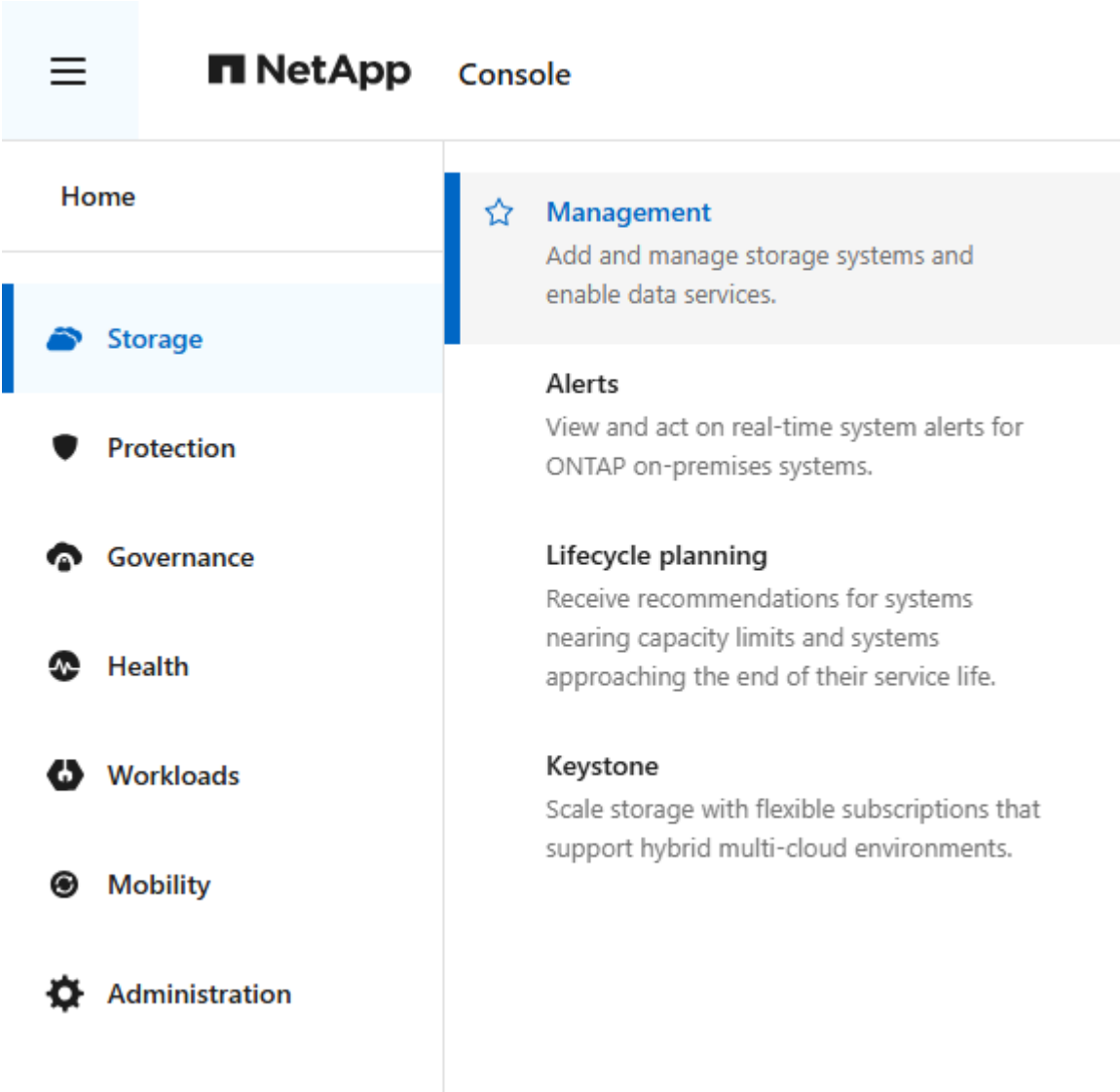


#### Expanded Storage menu

The **Storage** menu also includes **Alerts** to view ONTAP system alerts and **Lifecycle planning** (formerly **Economic efficiency**) to identify unused or underutilized resources.

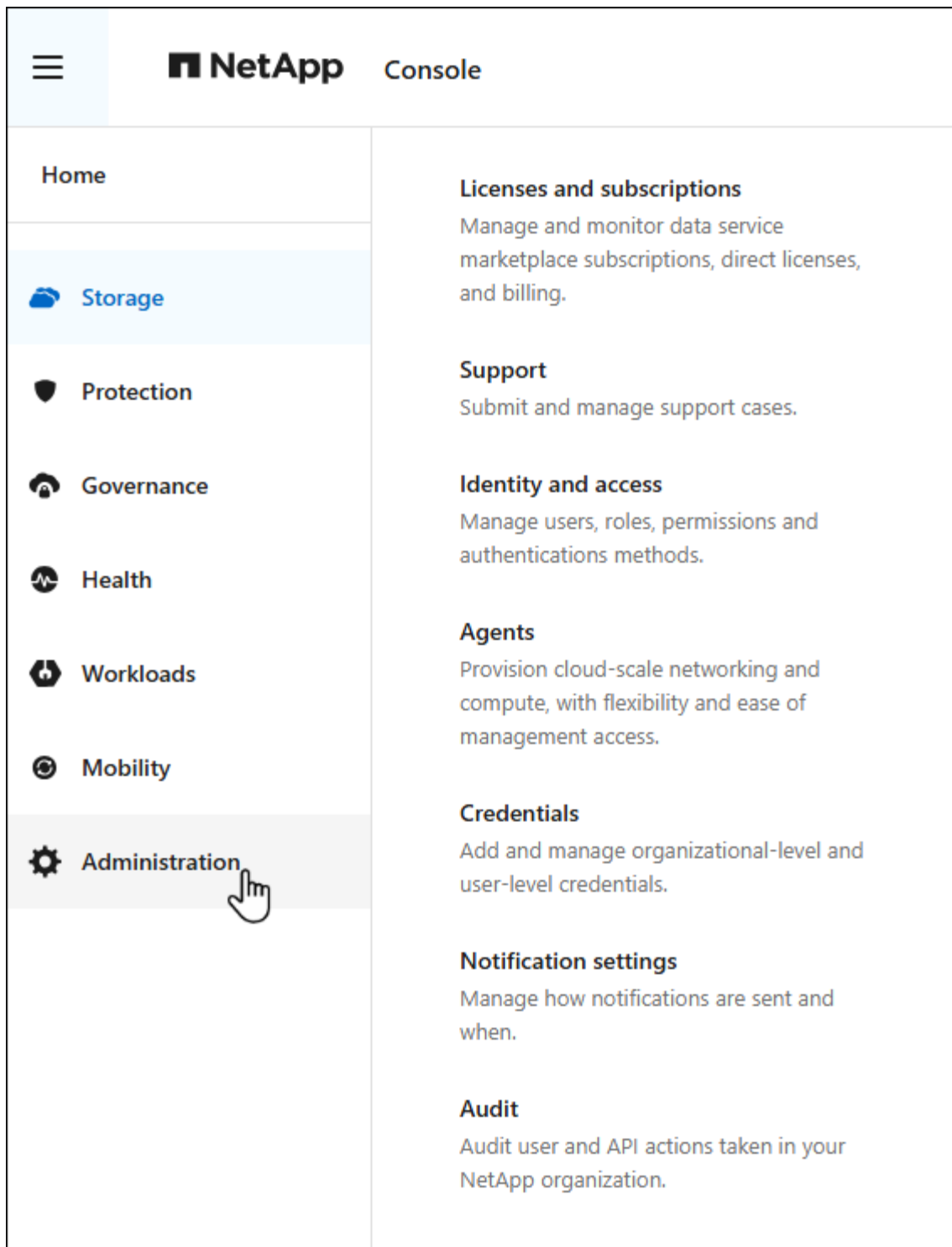
NetApp has also moved Keystone to the **Storage** menu, where you can manage your NetApp Keystone

subscriptions and view your usage.



**Administration menu**

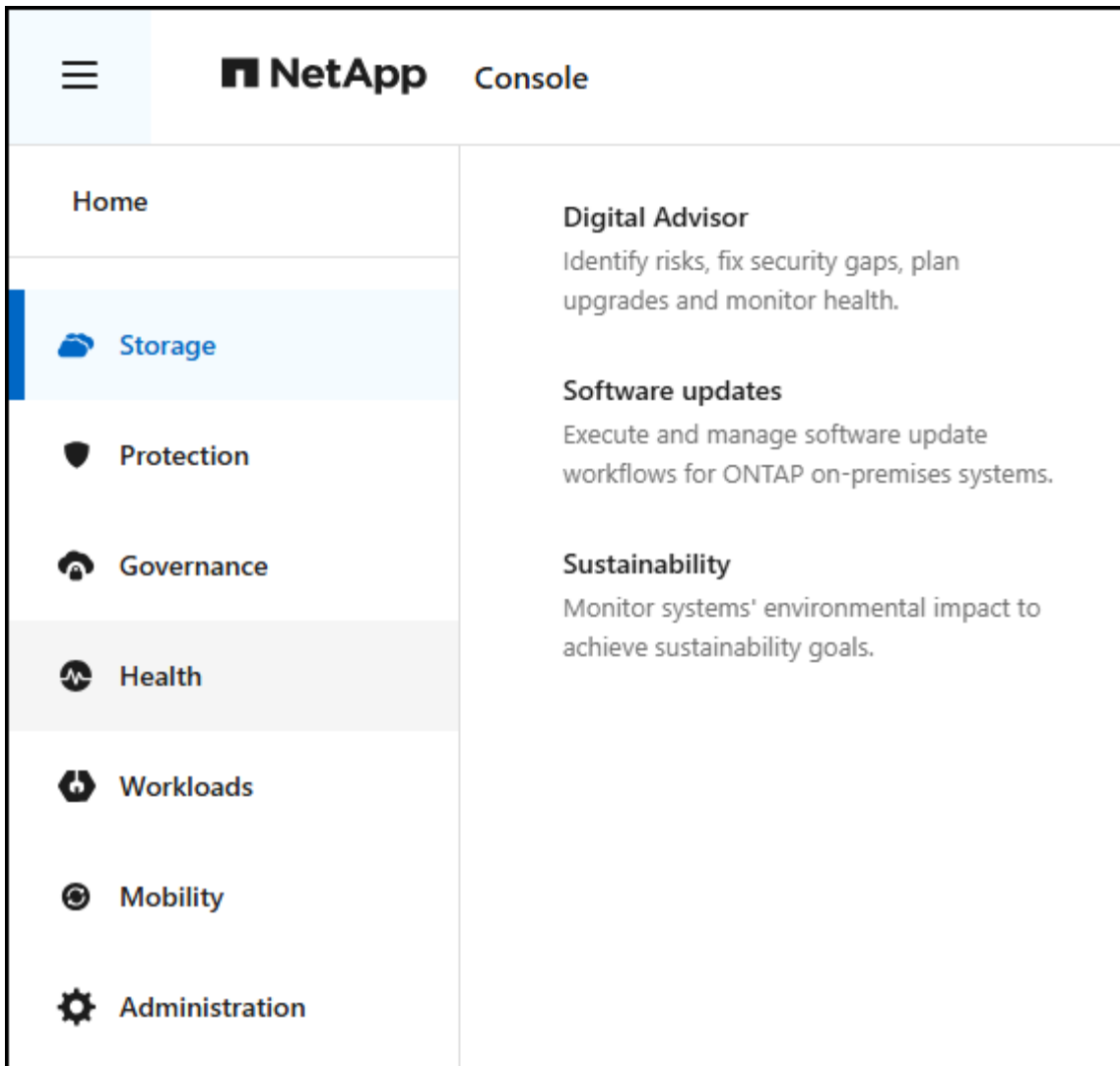
Use the centralized **Administration** menu to manage the NetApp Console, support cases, licenses, and subscriptions (previously called digital wallet).



#### Health menu

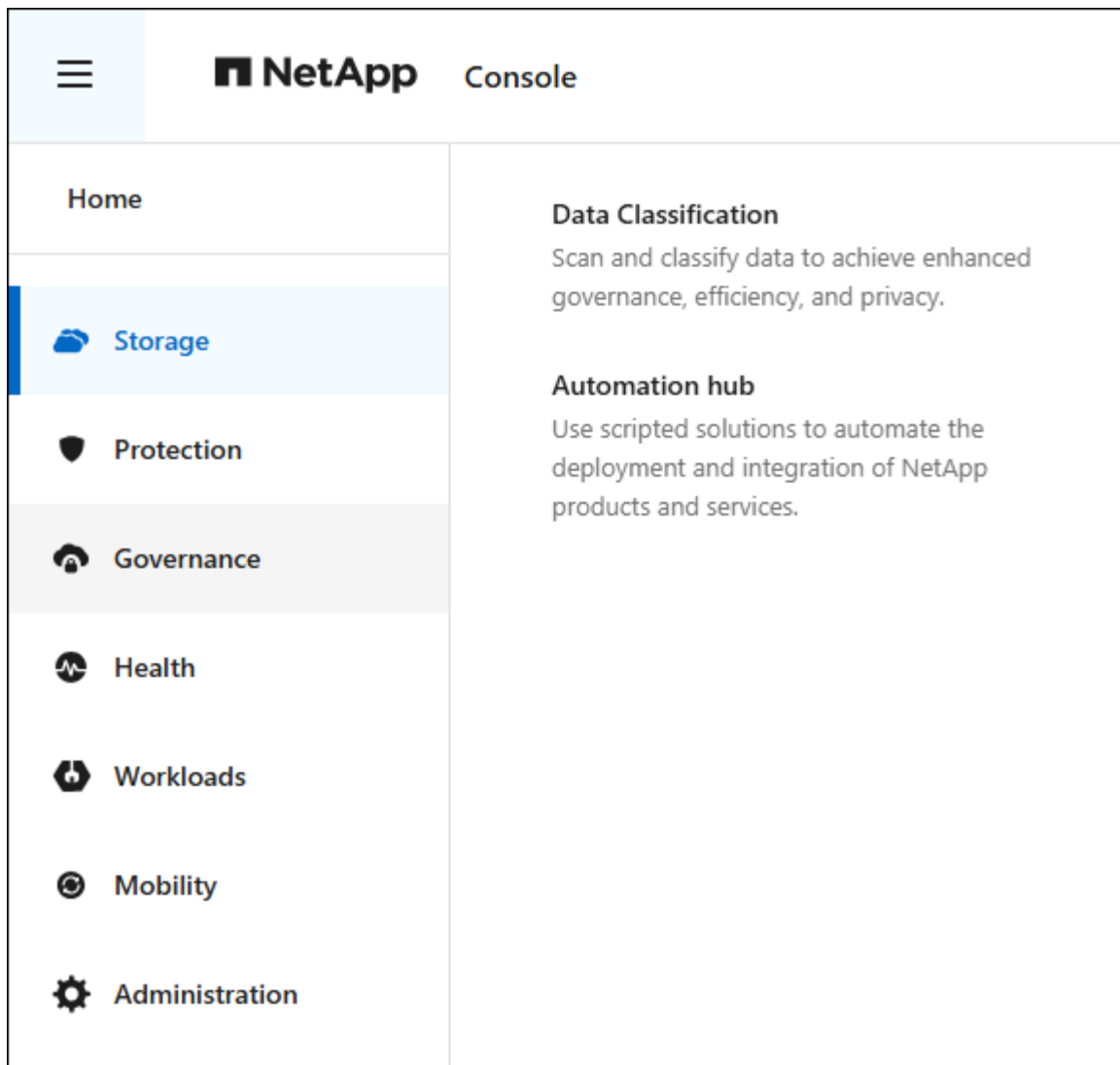
An efficient **Health** menu includes **Software updates** where you can manage ONTAP software updates, **Sustainability** where you can monitor your environmental impact, and **Digital Advisor** where you can get proactive recommendations to optimize your storage environment.





#### Governance menu

The **Governance** menu includes **Data Classification** where you can manage data classification and compliance and the **Automation hub** where you can create and manage automation workflows.




### More intuitive naming of elements, data services, and features

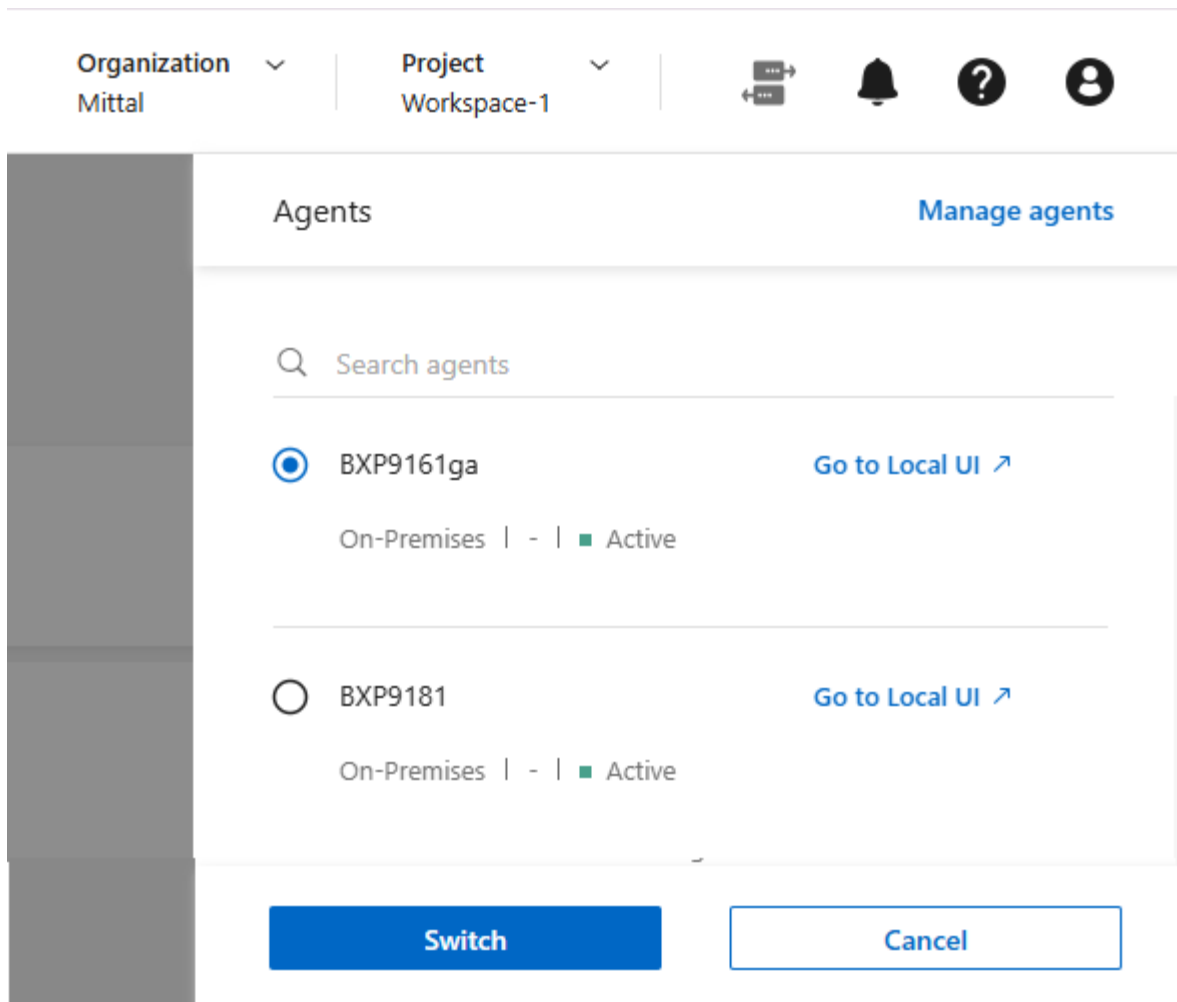
NetApp renamed several elements, data services, and features to clarify their purpose. Key changes include:

Previous name	NetApp Console name
Connectors	<p>Console agents.</p> <p>View, add, and manage your agents from the <b>Administration &gt; Agents</b> menu.</p>
Timeline page	<p>Audit page</p> <p>View audit Console activity from the <b>Administration &gt; Audit</b> menu.</p>
Working environments	<p>Systems</p> <p>View, add, and manage your systems from the <b>Storage &gt; Management</b> menu.</p>

Previous name	NetApp Console name
BlueXP Ransomware protection	<p>NetApp Ransomware Resilience.</p> <p>Ransomware Resilience helps you protect your data and recover quickly from a ransomware attack.</p>
BlueXP Economic Efficiency	<p>Lifecycle planning.</p> <p>Lifecycle planning helps you optimize your storage costs by identifying unused and underutilized resources.</p> <p>Access Lifecycle planning from the <b>Storage &gt; Lifecycle planning</b> menu.</p>
BlueXP digital wallet	<p>Licenses and subscriptions</p> <p>Access your licenses and subscriptions from the <b>Administration &gt; Licenses and subscriptions</b> menu.</p>

## Console agents

Access and manage your Console agents from the **Administration > Agents** menu. NetApp has changed how to select a Console agent for the **Systems** page (formerly the Canvas). NetApp has replaced the Connector menu name with an icon , allowing you to select the Console agent that you want to view systems for.



You can also manage your agents from the **Administration > Agents** menu.

## Console agent 4.0.0

This release of the Console agent includes security improvements, bug fixes and the following new features.

The 4.0.0 release is available for standard mode and restricted mode.

### Consolidation and reduction of required network endpoints

NetApp has reduced the required network endpoints for the Console and Console agents, enhancing security and simplifying deployment. Importantly, all deployments prior to version 4.0.0 continue to be fully supported. While previous endpoints remain available for existing agents, NetApp strongly recommends updating firewall rules to the current endpoints after confirming successful agent upgrades.

- [Learn how to update your endpoint list.](#)
- [Learn more about required endpoints.](#)

### Support for VCenter deployment of Console agents

You can deploy Console agents in VMware environments using an OVA file. The OVA file includes a pre-configured VM image with Console agent software and settings to connect to the NetApp Console. A file download or URL deployment is available directly from the NetApp Console. [Learn how to deploy a Console agent in VMware environments.](#)

The Console agent OVA for VMware offers a pre-configured VM image for quick deployment.

### Validation reports for failed agent deployments

When you deploy a Console agent from the NetApp Console, you now have the option to validate the agent configuration. If the Console fails to deploy the agent, it provides a downloadable report to help you troubleshoot.

### Improved troubleshooting for Console agents

The Console agent has improved error messages that help you better understand issues. [Learn how to troubleshoot Console agents.](#)

## NetApp Console

NetApp Console administration includes the following new features:

### Home page dashboard

The NetApp Console's Home page dashboard provides real-time visibility into storage infrastructure with metrics for health, capacity, license status, and data services. [Learn more about the Home page.](#)

### NetApp assistant

New users with the Organization admin role can use the NetApp assistant to configure the Console, including adding an agent, linking a NetApp Support account, and adding a storage system. [Learn about the NetApp assistant.](#)

### Service account authentication

The NetApp Console supports service account authentication using either a system-generated client ID and secret or customer-managed JWTs, allowing organizations to select the approach that best fits their security requirements and integration workflows. Private Key JWT Client Authentication uses asymmetric cryptography, providing stronger security than traditional client ID and secret methods. Private Key JWT Client Authentication uses asymmetric cryptography, keeping the private key secure in the customer's environment, reducing credential theft risks, and improving the security of your automation stack and client applications. [Learn how to add a service account.](#)

### Session timeouts

The system logs out users after 24 hours or when they close their web browser.

### Support for partnerships between organizations

You can create partnerships in the NetApp Console that let partners securely manage NetApp resources across organizational boundaries, making collaboration easier and security stronger. [Learn how to manage partnerships.](#)

### Super admin and Super viewer roles

Added the **Super admin** and **Super viewer** roles. **Super admin** grants full management access to Console features, storage, and data services. **Super viewer** provides read-only visibility for auditors and stakeholders. These roles are useful for smaller teams of senior members where broad access is common. For improved security and auditability, organizations are encouraged to use **Super admin** access sparingly and assign fine-

grained roles where possible. [Learn more about access roles.](#)

### **Additional role for Ransomware Resilience**

Added the **Ransomware Resilience user behavior admin** role and the **Ransomware Resilience user behavior viewer** role. These roles allow users to configure and view user behavior and analytics data, respectively. [Learn more about access roles.](#)

### **Removed support chat**

NetApp has removed the support chat feature from the NetApp Console. Use the **Administration > Support** page to create and manage support cases.

## **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 <a href="#">what's new in BlueXP</a> page and refer to the changes included for versions 3.9.54 and 3.9.53.
Backup and recovery	28 July 2025	Go to the <a href="#">what's new in BlueXP backup and recovery</a> page and refer to the changes included in the July 2025 release.
Classification	14 July 2025 (version 1.45)	Go to the <a href="#">what's new in BlueXP classification</a> 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 <a href="#">what's new in BlueXP connector page</a> and refer to the changes included for versions 3.9.52 and 3.9.50.

Component or service	Version included in this release	Changes since the previous private mode release
Backup and recovery	12 May 2025	Go to the <a href="#">what's new in BlueXP backup and recovery page</a> and refer to the changes included in the May 2025 release.
Classification	12 May 2025 (version 1.43)	Go to the <a href="#">what's new in BlueXP classification page</a> 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 <a href="#">what's new in BlueXP connector page</a> and refer to the changes included for versions 3.9.50 and 3.9.49.
Backup and recovery	17 March 2025	Go to the <a href="#">what's new in BlueXP backup and recovery page</a> and refer to the changes included in the March 2024 release.
Classification	10 March 2025 (version 1.41)	Go to the <a href="#">what's new in BlueXP classification page</a> 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 <a href="#">what's new in BlueXP connector page</a> and refer to the changes included for versions 3.9.48.
Backup and recovery	21 February 2025	Go to the <a href="#">what's new in BlueXP backup and recovery page</a> and refer to the changes included in the February 2025 release.
Classification	22 January 2025 (version 1.39)	Go to the <a href="#">what's new in BlueXP classification page</a> 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 <a href="#">what's new in BlueXP connector page</a> and refer to the changes included for versions 3.9.48.
Backup and recovery	21 February 2025	Go to the <a href="#">what's new in BlueXP backup and recovery page</a> and refer to the changes included in the February 2025 release.
Classification	22 January 2025 (version 1.39)	Go to the <a href="#">what's new in BlueXP classification page</a> 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://*.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://bluexpinfraeastus2.data.azurecr.io>
- <https://bluexpinfra.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 <a href="#">what's new in BlueXP backup and recovery page</a> and refer to the changes included in the November 2024 release
Classification	4 November 2024 (version 1.37)	Go to the <a href="#">what's new in BlueXP classification page</a> and refer to the changes included in the 1.32 to 1.37 releases
Cloud Volumes ONTAP management	11 November 2024	Go to the <a href="#">what's new with Cloud Volumes ONTAP management page</a> 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 <a href="#">what's new with on-premises ONTAP cluster management page</a> 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 is 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
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



Service	Version included
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 of NetApp Console

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 the set up for the NetApp Console and administration: the agent, the software as a service (SaaS) platform, and more.

## Console agent limitations

### Possible conflict with IP addresses in the 172 range

The NetApp Console deploys an agent 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 the Console. For example, discovering on-premises ONTAP clusters in the Console might fail.

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

### SSL decryption isn't supported

The Console doesn't support firewall configurations that have SSL decryption enabled. If SSL decryption is enabled, error messages appear in the Console and the agent 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 an agent, 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 agent isn't supported on a VM that is shared with other applications. The VM must be dedicated to the agent software.

### 3rd-party agents and extensions

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

## Changes to supported Linux operating systems

NetApp sometimes adds and removes support for the Console agent on specific Linux operating systems, learn how this support affects your existing Console agents.

## Supported operating systems

NetApp supports the agent 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 NetApp Console

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

NetApp Data Classification is supported if you install the agent 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 Console agent 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 the Console in standard mode and restricted mode.

## Supported Console agent versions

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

- 3.9.40 when using the Console in standard mode or restricted mode

## New manual installations only

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

## RHEL upgrades

If you have an existing agent running on a RHEL 7 host, NetApp does not support upgrading the RHEL 7 operating system to RHEL 8 or 9. [Learn more about existing Console agents 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 discontinued support for agents on these Linux distributions on June 30, 2024.

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

## Existing Console agents on RHEL 7 or CentOS 7

If you have an existing agent running on RHEL 7 or CentOS 7, NetApp does not support upgrading or converting the operating system to RHEL 8 or 9. You need to create a new agent on a supported operating system.

1. Set up a RHEL 8 or 9 host.
2. Install Podman.
3. Install a *new* agent.
4. Configure the agent to discover the systems that the previous agent 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 Cagent:

**Standard mode**

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

**Restricted mode**

[Prepare for deployment in restricted mode](#)

**How to rediscover your systems**

Refer to the following pages to rediscover your systems after you deploy a new Console agent.

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

# Get started

## Learn the basics

### Learn about NetApp Console

The NetApp Console provides centralized management of NetApp storage and NetApp Data Services across on-premises and cloud environments at enterprise grade—delivering real-time insights, faster workflows, and simplified administration, that is highly secure and compliant.

It is available as a service (SaaS) platform that provides storage management, data mobility, data protection, and data analysis and control. Management capabilities are provided through a web-based console and APIs.

### Features

The Console unifies storage management and protection across hybrid multi-cloud with integrated data services to protect and optimize data.

#### Centralized storage management

Discover, deploy, and manage cloud and on-premises storage with the Console.

#### Supported cloud and on-premises storage

You can manage the following types of storage from the Console:

##### Cloud storage solutions

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

##### On-premises flash and object storage

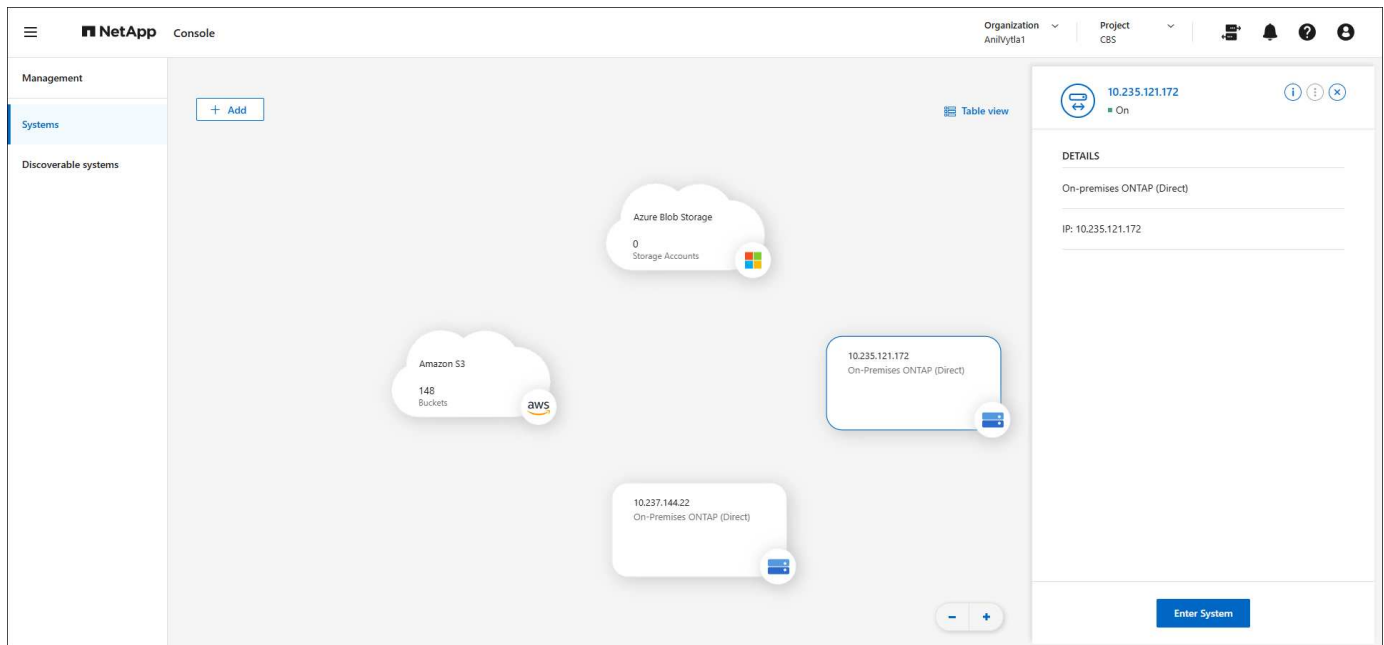
- E-Series systems
- ONTAP clusters
- StorageGRID systems

##### Cloud object storage

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

### Storage management

Within the Console, *systems* represent discovered or deployed storage. You can select a *system* to integrate it with NetApp data services or manage storage, such as adding volumes.



## Integrated data services and storage management to protect, secure, and optimize data

The Console provides data services to secure and maintain storage availability.

### Storage alerts

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

### Automation hub

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

### NetApp Backup and Recovery

Back up and restore cloud and on-premises data.

### NetApp Data Classification

Get your application data and cloud environments privacy ready.

### NetApp Copy and Sync

Sync data between on-premises and cloud data stores.

### NetApp digital advisor (Active IQ)

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

### Licenses and subscriptions

Manage and monitor your licenses and subscriptions.

### NetApp Disaster Recovery

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

### Lifecycle planning

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

## NetApp Ransomware Resilience

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

## NetApp Replication

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

## Software updates

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

## Sustainability dashboard

Analyze the sustainability of your storage systems.

## NetApp Cloud Tiering

Extend your on-premises ONTAP storage to the cloud.

## NetApp Volume Caching

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

## NetApp Workloads

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

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

## Supported cloud providers

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

## Cost

There is no charge for the NetApp Console. You incur costs if you deploy Console agents in the cloud or use Restricted mode deployed in the cloud. There are costs associated with some NetApp data services.

[Learn about NetApp data services pricing](#)

## How NetApp Console works

The NetApp Console is web-based console that's provided through the SaaS layer, a resource and access management system, Console agents that manage storage systems and enable NetApp data services, and different deployment modes to meet your business requirements.

## Software-as-a-service

You access the Console through a [web-based interface](#) and APIs. This SaaS experience enables you to automatically access the latest features as they're released.

## Identity and access management (IAM)

The Console provides identity and access management (IAM) for resource and access management. This IAM model 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
- [Learn more about IAM in NetApp Console](#)

### Console agents

A Console agent is needed for some additional features and data services. It enables you to manage resources and processes across your on-premises and cloud environments. You need it to manage some systems (for example, Cloud Volumes ONTAP) and to use some NetApp data services.

[Learn more about Console agents.](#)

### Deployment modes

NetApp offers two deployment modes for the NetApp Console: *Standard mode* uses a software as a service (SaaS) layer for full functionality, while *restricted mode* limits outbound connectivity.

NetApp continues to offer BlueXP for sites that need no outbound connectivity. BlueXP is available in private mode only. [Learn about BlueXP \(private mode\) for sites with no internet connectivity.](#)

[Learn more about deployment modes.](#)

### SOC 2 Type 2 certification

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

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

## Learn about NetApp Console agents

A *Console agent* runs in your cloud network or on-premises network. You use a Console agent to connect NetApp Console services to your storage environments.

### What you can do without a Console agent

Some Console features and services are available if you don't deploy a Console agent:

- Amazon FSx for NetApp ONTAP

Some actions require a Console agent or a NetApp Workloads link. [Learn which actions require a Console agent or link](#)

- Automation hub
- Azure NetApp Files

You don't need a Console agent to manage Azure NetApp Files, but one is required to use NetApp Data Classification to scan Azure NetApp Files.

- Google Cloud NetApp Volumes
- NetApp Copy and Sync

- Digital advisor
- Monitor license usage, subscription monitoring requires a Console agent

You can usually add a license to the NetApp Console without a Console agent.

An agent is required to add Cloud Volumes ONTAP *node-based* licenses because the data comes from the licenses installed on Cloud Volumes ONTAP systems.

- Direct discovery of on-premises ONTAP clusters

You don't need a Console agent to add an on-premises ONTAP cluster to the Console, but one is required for additional Console features and data services.

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

- Software updates
- Sustainability
- NetApp Workloads

### **When a Console agent is required**

In standard mode, the Console requires a Console agent for:

- Alerts
- Amazon FSx for ONTAP management features
- Amazon S3 storage
- Azure Blob storage
- NetApp Backup and Recovery
- Data Classification
- Cloud Volumes ONTAP
- NetApp Disaster Recovery
- E-Series systems
- Economic efficiency <sup>1</sup>
- Google Cloud Storage buckets
- On-premises ONTAP cluster integration with NetApp data services
- NetApp Ransomware resilience
- StorageGRID systems
- NetApp Cloud Tiering
- NetApp Volume Caching

<sup>1</sup> You can access these services without a Console agent, but a Console agent is required to initiate actions.

You always need a Console agent to use the Console in restricted mode.

## Console agents must be operational at all times

Console agents are a fundamental part of the NetApp Console. It's your responsibility (the customer) to ensure that relevant agents are up, operational, and accessible at all times. The Console can handle short agent outages, but you must fix infrastructure failures quickly.

This documentation is governed by the EULA. Operating the product outside the documentation may impact its functionality and your EULA rights.

## Supported locations

You can install agents in the following locations:

- Amazon Web Services
- Microsoft Azure

Deploy a Console agent in Azure in the same region as the Cloud Volumes ONTAP systems it manages. Alternatively, deploy it in the [Azure region pair](#). This 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

To use the Console and data services with Google Cloud, deploy your agent in Google Cloud.

- On your premises

## Communication with cloud providers

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

## Restricted mode

To use the Console in restricted mode, you install a Console agent and access the Console interface that's running locally on the Console agent.

[Learn about NetApp Console deployment modes.](#)

## How to install a Console agent

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

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

## Cloud Permissions

You need specific permissions to create the Console agent directly from the NetApp Console and another set of permissions for the Console agent instance itself. If you create the Console agent in AWS or Azure directly from the Console, then the Console creates the Console agent with the permissions that it needs.

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

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

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

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

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

It's your responsibility to update the Console agent policies as new permissions are added in subsequent releases. The release notes list new permissions.

## Agent upgrades

NetApp updates agent software monthly to add features and improve stability. Some Console features, like Cloud Volumes ONTAP and on-premises ONTAP cluster management, rely on the Console agent version and settings.

In standard or restricted mode, the Console agent updates automatically if it has internet access.

## Operating system and VM maintenance

Maintaining the operating system on the Console agent host is your (customer's) responsibility. For example, you (customer) should apply security updates to the operating system on the Console agent 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 Console agent host when applying minor security updates.

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

[The Console agent must be operational at all times.](#)

## Multiple systems and agents

An agent can manage multiple systems and support data services in the Console. You can use a single agent to manage multiple systems based on deployment size and the data services you use.

For large-scale deployments, work with your NetApp representative to size your environment. Contact NetApp Support if you experience issues.

Here are a few examples of agent deployments:

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

## Learn about NetApp Console deployment modes

The NetApp Console offers multiple *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. Users access the Console through a web-based hosted interface
- *Restricted mode* is available for organizations that have connectivity restrictions who want to install the NetApp Console in their own public cloud. Users access the Console through a web-based interface that's hosted on a Console agent in their cloud environment.

NetApp Console restricts traffic, communication, and data in restricted mode, and you must ensure your environment (on-premises and in the cloud) complies with required regulations.

### 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 Console organization admin creates one or more Console agents to manage data within your hybrid cloud environment.

This mode uses encrypted data transmission over the public internet.

#### Restricted mode

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

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

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

#### BlueXP private mode (legacy BlueXP interface only)

BlueXP private mode (legacy BlueXP interface) 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. NetApp continues to support these environments with the legacy BlueXP interface.

[PDF documentation for BlueXP private mode](#)

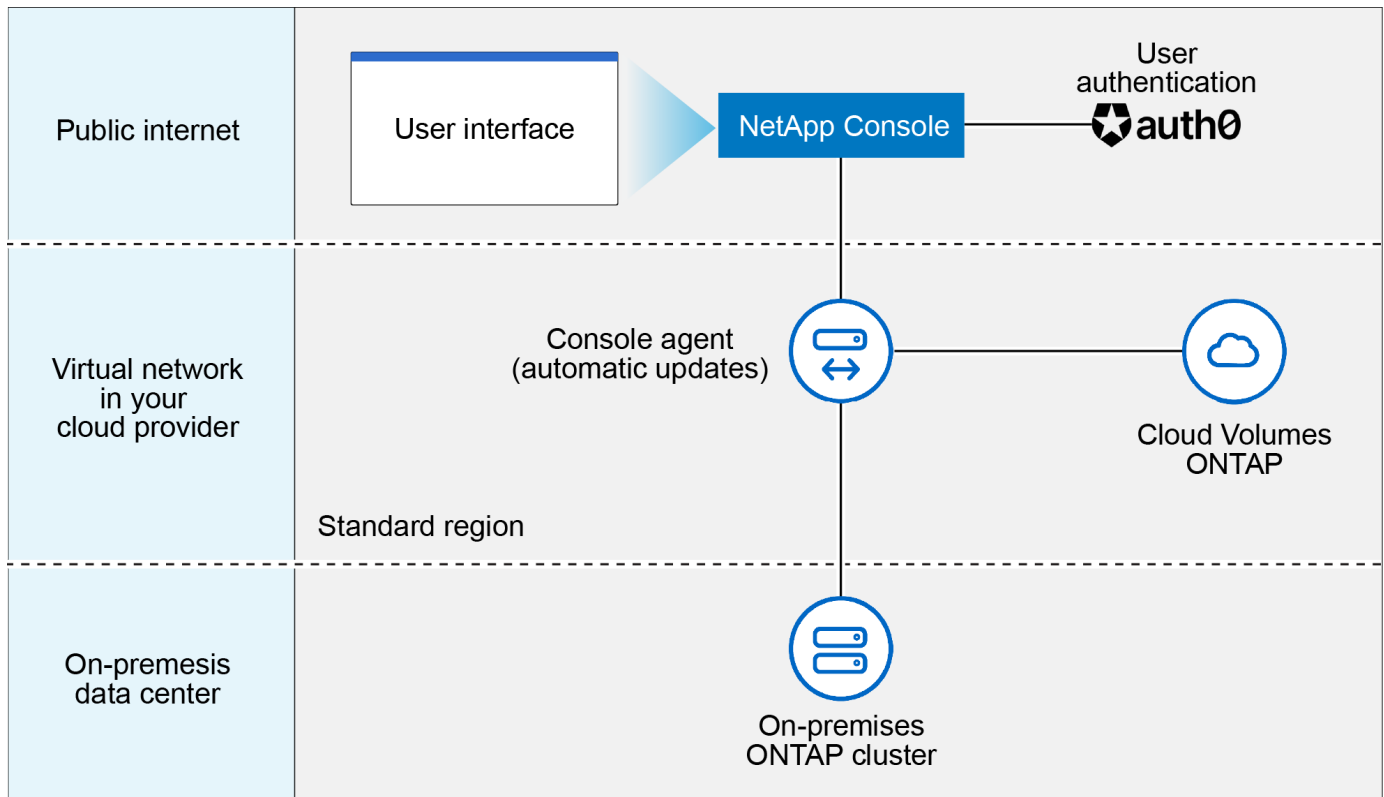
The following table provides a comparison of the NetApp console.

	<b>Standard mode</b>	<b>Restricted mode</b>
<b>Connection required to NetApp Console SaaS layer?</b>	Yes	Outbound only
<b>Connection required to your cloud provider?</b>	Yes	Yes, within the region
<b>Console agent installation</b>	From the Console, cloud marketplace, or manual install	Cloud marketplace or manual install
<b>Console agent upgrades</b>	Automatic upgrades	Automatic upgrades
<b>UI access</b>	From the Console SaaS layer	Locally from an agent VM
<b>API endpoint</b>	The Console SaaS layer	A Console agent
<b>Authentication</b>	Through SaaS using auth0, NSS login, or identity federation	Through SaaS using auth0 or identity federation
<b>Multi-factor authentication</b>	Available for local users	Not available
<b>Storage and data services</b>	All are supported	Many are supported
<b>Data service licensing options</b>	Marketplace subscriptions and BYOL	Marketplace subscriptions and BYOL

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

### **Standard mode**

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



The Console works as follows in standard mode:

### Outbound communication

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

- [Endpoints that an agent contacts in AWS](#)
- [Endpoints that an agent contacts in Azure](#)
- [Endpoints that an agent contacts in Google Cloud](#)

### Supported location for an agent

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

### Console agent installation

You can install an agent using one of the following methods:

- From the Console
- From the AWS or Azure Marketplace
- From the Google Cloud SDK
- Manually using an installer on a Linux host in your data center or cloud
- Use the provided OVA in your VCenter environment.

### Console agent upgrades

NetApp automatically upgrades your agent monthly.

## 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://api.bluedp.netapp.com>

## Authentication

Authentication with auth0 or NetApp Support Site (NSS) logins. Identity federation is available.

## Supported data services

All NetApp data services are supported. [Learn more about NetApp data services.](#)

## Supported licensing options

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

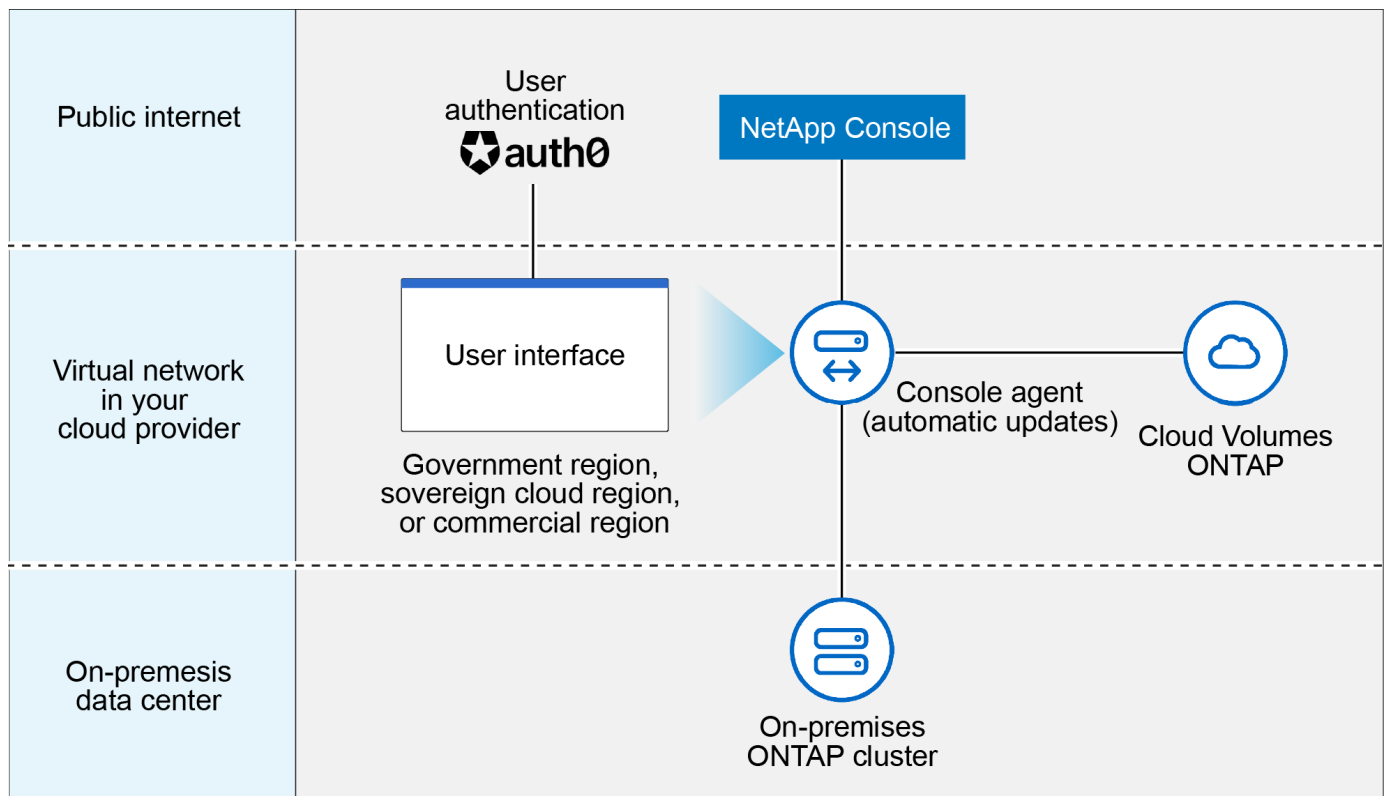
## How to get started with standard mode

Go to the [NetApp 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.



The Console works as follows in restricted mode:



## Outbound communication

An agent requires outbound connectivity to the Console SaaS layer for data services, software upgrades, authentication, and metadata transmission.

The Console SaaS layer does not initiate communication to an agent. Agents initiate all communication with the Console SaaS layer, pulling or pushing data as needed.

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

## Supported location for an agent

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

## Console agent installation

You can install from the AWS or Azure Marketplace or a manual installation on your own Linux host or use a downloadable OVA in your vCenter environment.

## Console agent upgrades

NetApp automatically upgrades your agent software with monthly updates.

## User interface access

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

## API endpoint

API calls are made to the agent virtual machine.

## Authentication

Authentication is provided through auth0. Identity federation is also available.

## Supported storage management and data services

The following storage and data services with restricted mode:

Supported services	Notes
Azure NetApp Files	Full support
Backup and recovery	Supported in Government regions and commercial regions with restricted mode. Not supported in sovereign regions with restricted mode.  In restricted mode, NetApp Backup and Recovery supports back up and restore of ONTAP volume data only. <a href="#">View the list of supported backup destinations for ONTAP data</a>  Back up and restore of application data and virtual machine data is not supported.
NetApp Data 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
Licenses and subscriptions	You can access license and subscription information with the supported licensing options listed below for restricted mode.

Supported services	Notes
On-premises ONTAP clusters	Discovery with a Console agent and discovery without a Console agent (direct discovery) are both supported.  When you discover an on-premises cluster without a Console agent, the Advanced view (System Manager) is not supported.
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 NetApp Console organization.

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



You cannot change the restricted mode setting after creating the organization.

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

## Service and feature comparison

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

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

Product area	NetApp data service or feature	Restricted mode
<b>Storage</b>  This portion of the table lists support for storage systems management from the Console. It does not indicate the supported backup destinations for NetApp Backup and Recovery.	Amazon FSx for ONTAP	No
	Amazon S3	No
	Azure Blob	No
	Azure NetApp Files	Yes
	Cloud Volumes ONTAP	Yes
	Google Cloud NetApp Volumes	No
	Google Cloud Storage	No
	On-premises ONTAP clusters	Yes
	E-Series	No
	StorageGRID	No
<b>Data Services</b>	NetApp Backup and recovery	Yes  <a href="#">View the list of supported backup destinations for ONTAP volume data</a>
	NetApp Data Classification	Yes
	NetApp Copy and Sync	No
	NetApp Disaster Recovery	No
	NetApp Ransomware Resilience	No
	NetApp Replication	Yes
	NetApp Cloud Tiering	No
	NetApp Volume caching	No
	NetApp Workload factory	No

Product area	NetApp data service or feature	Restricted mode
Features	Alerts	No
	Digital Advisor	No
	License and subscription management	Yes
	Identity and access management	Yes
	Credentials	Yes
	Federation	Yes
	Lifecycle planning	No
	Multi-factor authentication	Yes
	NSS accounts	Yes
	Notifications	Yes
	Search	Yes
	Software updates	No
	Sustainability	No
	Audit	Yes

## Get started with the NetApp assistant

### Get started using the NetApp Console Assistant

If you are a first-time user of the NetApp Console with the Organization admin role, you can use the Console Assistant to guide you through the initial setup process. The Assistant helps you add a NetApp Support Site (NSS) account, add a Console agent, add a cluster, and add a license or subscription, making it easier to get started with managing your data.

#### Required roles to access the Console Assistant

The Console Assistant is only available to users with the Organization admin role.

#### When does the Console Assistant appear?

The Console Assistant is available on the NetApp Console Home page until mandatory setup tasks are completed.

Use the Assistant to complete these tasks, some of which are mandatory:

- Add a NetApp Support Site (NSS) account.
- Connect to your storage estate by deploying a Console agent (mandatory step).
- Manage your system by adding or discovering a cluster (mandatory step).
- Add a marketplace subscription or PAYGO license.

- Open data services links.

## Enable the Console Assistant

By default, the NetApp Console displays the Console Assistant on the Home page for first-time users who have the Organization admin role.



You can dismiss the Assistant for yourself only after you or someone else completes the mandatory items. After you complete the mandatory items, the Assistant is dismissed for all users in your organization and does not appear again.

## Use the Console Assistant to get started

The Console Assistant guides you through setting up your NetApp Console environment with these tasks:

- Add a NetApp Support Site (NSS) account.
- Connect to your storage estate by deploying a Console agent, either on-premises or in the cloud. You can deploy it manually or by downloading an OVA. This step is mandatory.
- Manage your system by adding or discovering a cluster. This step is mandatory.
- Add a marketplace subscription or PAYGO license.
- Learn more about NetApp data services.

# Get started with standard mode

## Getting started workflow (standard mode)

Get started with the NetApp Console in standard mode by preparing networking for the Console, signing up and creating an account, and optionally creating a Console agent.

In standard mode, you access a web-based console that is hosted as a Software-as-a-service (SaaS) product from NetApp. Before starting, ensure you understand [deployment modes](#) and [Console agents](#).

1

### Prepare networking for using the NetApp console

Computers that access the NetApp console should have connections to specific endpoints. If your network restricts outbound access, you should ensure that these endpoints are allowed.

2

### Sign up and create an organization

Go to the [NetApp console](#) and sign up. You'll be given the option to create an organization, but you should skip that step if your company already has an existing organization.

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

3

### Create a Console agent

Advanced storage management features and some NetApp data services require that you install a Console

agent. The Console agent enables the Console to manage resources and processes within your hybrid cloud environment.

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

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

To use NetApp Intelligent Data Services for managing storage and data in Google Cloud, ensure the Console agent runs in Google Cloud.



#### **Subscribe to NetApp Intelligent Services (optional)**

Sign up for NetApp Intelligent Services through your cloud provider to pay hourly (PAYGO) or through an annual contract. NetApp Intelligent Services include NetApp Backup and Recovery, Cloud Volumes ONTAP, NetApp Cloud Tiering, NetApp Ransomware Resilience and NetApp Disaster Recovery. NetApp Data Classification is included with your subscription at no additional cost.

## **Prepare network access for NetApp Console**

NetApp Console, the NetApp Console agent, and NetApp data services require outbound internet access and the ability to contact the necessary endpoints.

You'll need to set up network access for the following:

- Computers that access the NetApp Console as software as a service (SaaS)
- Network locations where you deploy Console agents you install on-premises or in the cloud.
- Additional endpoints for certain NetApp data services, including Cloud Volumes ONTAP.



NetApp has reduced the required network endpoints for the Console and Console agents, enhancing security and simplifying deployment. Importantly, all deployments prior to version 4.0.0 continue to be fully supported. While previous endpoints remain available for existing agents, NetApp strongly recommends updating firewall rules to the current endpoints after confirming successful agent upgrades. [Learn how to update your endpoint list.](#)

## **Endpoints contacted by the NetApp Console**

Each computer that accesses the NetApp Console must have connections to the endpoints listed below.

The system contacts these endpoints in two scenarios:

- From a computer accessing the [NetApp Console](#) as software as a service (SaaS).
- From a computer directly accessing an Console agent host, either to log in and set it up or access the Console from the agent host.

Endpoints	Purpose
<a href="https://mysupport.netapp.com">https://mysupport.netapp.com</a>	To obtain licensing information and to send AutoSupport messages to NetApp support.
<a href="https://signin.b2c.netapp.com">https://signin.b2c.netapp.com</a>	To update NetApp Support Site (NSS) credentials or to add new NSS credentials to the NetApp Console.
<a href="https://api.blueexp.netapp.com">https://api.blueexp.netapp.com</a> <a href="https://netapp-cloud-account.auth0.com">https://netapp-cloud-account.auth0.com</a> <a href="https://netapp-cloud-account.us.auth0.com">https://netapp-cloud-account.us.auth0.com</a> <a href="https://console.netapp.com">https://console.netapp.com</a> <a href="https://components.console.blueexp.netapp.com">https://components.console.blueexp.netapp.com</a> <a href="https://cdn.auth0.com">https://cdn.auth0.com</a>	To provide features and services within the NetApp Console.
<a href="https://blueexpinfraprod.eastus2.data.azurecr.io">https://blueexpinfraprod.eastus2.data.azurecr.io</a> <a href="https://blueexpinfraprod.azurecr.io">https://blueexpinfraprod.azurecr.io</a>	<p>To obtain images for Console agent upgrades.</p> <ul style="list-style-type: none"> <li>When you deploy a new agent, the validation check tests connectivity to current endpoints. If you use <a href="#">xref:./previous endpoints</a>, the validation check fails. To avoid this failure, skip the validation check.</li> </ul> <p>Although the previous endpoints are still supported, NetApp recommends updating your firewall rules to the current endpoints as soon as possible. <a href="#">Learn how to update your endpoint list.</a></p> <ul style="list-style-type: none"> <li>When you update to the current endpoints in your firewall, your existing agents will continue to work.</li> </ul>

## Prepare networking for the Console agent

You install the Console agent on-premises or in the cloud, and it contacts endpoints to complete Console-initiated actions.

Console agents must have access to the same endpoints as the NetApp Console, plus additional endpoints depending on where you install the agent.

Set up network endpoint access before installing the Console agent.

- [Set up AWS network access for a Console agent](#)
- [Set up Azure network access for a Console agent](#)
- [Set up Google Cloud network access for a Console agent](#)
- [Set up on-premises network access for a Console agent](#)

## Prepare networking for Cloud Volumes ONTAP

Some NetApp data services as well as Cloud Volumes ONTAP require the agent to have additional outbound internet access.

## Endpoints for Cloud Volumes ONTAP

- [Endpoints for Cloud Volumes ONTAP in AWS](#)
- [Endpoints for Cloud Volumes ONTAP in Azure](#)
- [Endpoints for Cloud Volumes ONTAP in Google Cloud](#)

[Refer to the respective NetApp data services documentation.](#)

## Sign up or log in to NetApp Console

The NetApp Console is accessible from a web-based console. To get started with the Console your first step is to sign up or to log in using your NetApp Support Site credentials or creating a NetApp Console login.

### About this task

When you access the Console for the first time, you can sign up or log in using one of the following options:

#### NetApp Console login

You can sign up by creating a 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 an 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 for the Console. You log in using your NSS credentials and then the Console prompts you to create an organization, if you don't already belong to one.

You are sent one-time passcode (OTP) to the registered email address. A new OTP is generated with each sign-in attempt.

#### Federated connection

If your company already has a NetApp Console instance, your Console administrator may have set up single sign-on to log in using credentials from your corporate directory (federated identity).

[Learn how to use identity federation with the NetApp Console.](#)

### Steps

1. Open a web browser and go to the [NetApp 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, you are signed up for the Console as part of this initial login.

3. If you want to sign up by creating a Console 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 the Console.



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 Console organization, you'll be prompted to create one.

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

The Console defines an organization as the top-level element in the Console identity and access management (IAM). [Learn about IAM](#).

If your business already has an organization and you want to join it, close out of the Console and ask the organization administrator to associate you with the organization. After you are added, you can log in and you'll have access to the Console organization. [Learn how to add members to an existing organization](#).

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

## Create a Console agent

### AWS

#### Console agent installation options in AWS

There are a few different ways to create a Console agent in AWS. Directly from the NetApp Console is the most common way.

The following installation options are available:

- [Create the Console agent directly from the Console](#) (this is the standard option)

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

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

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

- [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 the Console with the required permissions that it needs to authenticate and manage resources in AWS.

#### Create a Console agent in AWS from NetApp Console

You can create a Console agent in AWS directly from the NetApp Console. Before creating a Console agent in AWS from the Console, you need to set up your networking and prepare AWS permissions.

#### Before you begin

- You should have an [understanding of Console agents](#).
- You should review [Console agent limitations](#).

## Step 1: Set up networking for deploying a Console agent in AWS

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

### VPC and subnet

When you create the Console agent, you need to specify the VPC and subnet where it should reside.

### Connections to target networks

The Console agent requires a network connection to the location where you're planning to create and manage systems. 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 Console agent must have an outbound internet connection to contact specific endpoints.

### Endpoints contacted from the Console agent

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

The endpoints listed below are all CNAME entries.

Endpoints	Purpose
AWS services (amazonaws.com): <ul style="list-style-type: none"><li>• CloudFormation</li><li>• Elastic Compute Cloud (EC2)</li><li>• Identity and Access Management (IAM)</li><li>• Key Management Service (KMS)</li><li>• Security Token Service (STS)</li><li>• Simple Storage Service (S3)</li></ul>	To manage AWS resources. The endpoint depends on your AWS region. <a href="#">Refer to AWS documentation for details</a>
<a href="https://mysupport.netapp.com">https://mysupport.netapp.com</a>	To obtain licensing information and to send AutoSupport messages to NetApp support.
<a href="https://signin.b2c.netapp.com">https://signin.b2c.netapp.com</a>	To update NetApp Support Site (NSS) credentials or to add new NSS credentials to the NetApp Console.
<a href="https://api.bluexp.netapp.com">https://api.bluexp.netapp.com</a> <a href="https://netapp-cloud-account.auth0.com">https://netapp-cloud-account.auth0.com</a> <a href="https://netapp-cloud-account.us.auth0.com">https://netapp-cloud-account.us.auth0.com</a> <a href="https://console.netapp.com">https://console.netapp.com</a> <a href="https://components.console.bluexp.netapp.com">https://components.console.bluexp.netapp.com</a> <a href="https://cdn.auth0.com">https://cdn.auth0.com</a>	To provide features and services within the NetApp Console.

Endpoints	Purpose
<a href="https://bluexpinfraprod.eastus2.data.azurecr.io">https://bluexpinfraprod.eastus2.data.azurecr.io</a> <a href="https://bluexpinfraprod.azurecr.io">https://bluexpinfraprod.azurecr.io</a>	<p>To obtain images for Console agent upgrades.</p> <ul style="list-style-type: none"> <li>When you deploy a new agent, the validation check tests connectivity to current endpoints. If you use <a href="#">xref:./previous endpoints</a>, the validation check fails. To avoid this failure, skip the validation check.</li> </ul> <p>Although the previous endpoints are still supported, NetApp recommends updating your firewall rules to the current endpoints as soon as possible. <a href="#">Learn how to update your endpoint list.</a></p> <ul style="list-style-type: none"> <li>When you update to the current endpoints in your firewall, your existing agents will continue to work.</li> </ul>

### Endpoints contacted from the NetApp console

As you use the web-based NetApp 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 Console agent from the the Console.

[View the list of endpoints contacted from the NetApp 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 Console agent, unless you initiate it or if it 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, the Console automatically configures those systems to use a proxy server that's included with the Console agent. The only requirement is to ensure that the Console agent's security group allows inbound connections over port 3128. You'll need to open this port after you deploy the Console agent.

## Enable NTP

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

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

## Step 2: Set up AWS permissions for the Console agent

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

- Let the Console 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 Console agent instance in AWS from the Console.

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 Console agent instance in AWS from the Console. When the Console creates the Console agent, it applies a new set of permissions to the Console agent instance that enables the Console agent to manage AWS resources. [View permissions required for the Console agent 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 the Console can assume or to an IAM user so that you can provide the Console with access keys:
  - (Option 1) Set up an IAM role that the Console 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 Console 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 the Console when you create the Console agent.
  - (Option 2) Set up permissions for an IAM user so that you can provide the Console 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 Console agent from the Console, you can provide information about the role or access keys.

## Step 3: Create the Console agent

Create the Console agent directly from the the Console web-based console.

### About this task

- Creating the Console agent from the Console deploys an EC2 instance in AWS using a default configuration. Do not switch to a smaller EC2 instance with fewer CPUs or less RAM after creating the Console agent. [Learn about the default configuration for the Console agent](#).

- When the Console creates the Console agent, it creates an IAM role and an instance profile for the instance. This role includes permissions that enables the Console agent to manage AWS resources. Ensure the role is updated as new permissions are added in future releases.  
[Learn more about the IAM policy for the Console agent.](#)

## 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 Console agent.
- Set up [networking requirements](#).
- Set up [AWS permissions](#).

## Steps

1. Select **Administration > Agents**.
2. On the **Overview** page, select **Deploy agent > AWS**
3. Follow the steps in the wizard to create the Console agent:
4. On the **Introduction** page provides an overview of the process
5. On the **AWS Credentials** page, specify your AWS region and then choose an authentication method, which is either an IAM role that the Console 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 Console agent 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.](#)

6. On the **Details** page, provide details about the Console agent.
  - Enter a name for the instance.
  - Add custom tags (metadata) to the instance.
  - Choose whether you want the Console 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 Console agent's EBS disks. You have the option to use the default encryption key or to use a custom key.
7. On the **Network** page, Specify a VPC, subnet, and key pair for the instance, choose whether to enable a public IP address, and optionally specify a proxy configuration.

Ensure you have the correct key pair to access the Console agent virtual machine. Without a key pair, you cannot access it.

8. On the **Security Group** page, 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.](#)

9. Review your selections to verify that your set up is correct.

- a. The **Validate agent configuration** check box is marked by default to have the Console validate the network connectivity requirements when you deploy. If the Console fails to deploy the agent, it provides a report to help you troubleshoot. If the deployment succeeds, no report is provided.

If you are still using the [previous endpoints](#) used for agent upgrades, the validation fails with an error. To avoid this, unmark the check box to skip the validation check.

10. Select **Add**.

The Console prepares the instance in about 10 minutes. Stay on the page until the process completes.

## Result

After the process is complete, the Console agent is available for use from the Console.



If the deployment fails, you can download a report and logs from the Console to help you fix the issues. [Learn how to troubleshoot installation issues.](#)

If you have Amazon S3 buckets in the same AWS account where you created the Console agent, you'll see an Amazon S3 working environment appear on the **Systems** page automatically. [Learn how to manage S3 buckets from NetApp Console](#)

## Create a Console agent from the AWS Marketplace

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

### Before you begin

- You should have an [understanding of Console agents](#).
- You should review [Console agent limitations](#).

## Step 1: Set up networking

Ensure the network location for the Console agent meets the following requirements to manage hybrid cloud resources.

### VPC and subnet

When you create the Console agent, you need to specify the VPC and subnet where it should reside.

### Connections to target networks

The Console agent requires a network connection to the location where you're planning to create and manage systems. 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 Console agent must have an outbound internet connection to contact specific endpoints.



## Endpoints contacted from the Console agent

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

The endpoints listed below are all CNAME entries.

Endpoints	Purpose
AWS services (amazonaws.com): <ul style="list-style-type: none"><li>• CloudFormation</li><li>• Elastic Compute Cloud (EC2)</li><li>• Identity and Access Management (IAM)</li><li>• Key Management Service (KMS)</li><li>• Security Token Service (STS)</li><li>• Simple Storage Service (S3)</li></ul>	To manage AWS resources. The endpoint depends on your AWS region. <a href="#">Refer to AWS documentation for details</a>
https://mysupport.netapp.com	To obtain licensing information and to send AutoSupport messages to NetApp support.
https://signin.b2c.netapp.com	To update NetApp Support Site (NSS) credentials or to add new NSS credentials to the NetApp Console.
https://api.bluexp.netapp.com https://netapp-cloud-account.auth0.com https://netapp-cloud-account.us.auth0.com https://console.netapp.com https://components.console.bluexp.netapp.com https://cdn.auth0.com	To provide features and services within the NetApp Console.
https://bluexpinfraprod.eastus2.data.azurecr.io https://bluexpinfraprod.azurecr.io	<p>To obtain images for Console agent upgrades.</p> <ul style="list-style-type: none"><li>• When you deploy a new agent, the validation check tests connectivity to current endpoints. If you use xref:./previous endpoints, the validation check fails. To avoid this failure, skip the validation check.</li></ul> <p>Although the previous endpoints are still supported, NetApp recommends updating your firewall rules to the current endpoints as soon as possible. <a href="#">Learn how to update your endpoint list.</a></p> <ul style="list-style-type: none"><li>• When you update to the current endpoints in your firewall, your existing agents will continue to work.</li></ul>

## 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 Console agent, unless you initiate it or if it 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, the Console automatically configures those systems to use a proxy server that's included with the Console agent. The only requirement is to ensure that the Console agent's security group allows inbound connections over port 3128. You'll need to open this port after you deploy the Console agent.

## Enable NTP

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

Implement this network access after you create the Console agent.

## 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 Console agent from the AWS Marketplace, you are 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 Console agent](#).
  - c. Finish the remaining steps to create the policy.

You may need to create a second policy based on the NetApp data services you plan to use. 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 Console agent](#).

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 Console agent, 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 Console agent

Create the Console agent directly from the AWS Marketplace.

### About this task

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

### 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 Console agent.
- 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 [NetApp Console agent 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.

Use the EC2 Console to launch the instance and attach an IAM role. This is not possible with 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 Console agent 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 Console agent 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 Console agent.
- **Summary:** Review the summary and select **Launch instance**.

AWS launches the Console agent with the specified settings, and the Console agent runs in about ten minutes.



If the installation fails, you can view logs and a report to help you troubleshoot. [Learn how to troubleshoot installation issues.](#)

8. Open a web browser from a host that has a connection to the Console agent virtual machine and URL of the Console agent.

9. After you log in, set up the Console agent:

- a. Specify the Console organization to associate with the Console agent.
- 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 the Console in standard mode. You should enable restricted mode only if you have a secure environment and want to disconnect this account from the Console backend services. If that's the case, [follow steps to get started with NetApp Console in restricted mode.](#)

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

## Result

The Console agent is now installed and set up with your Console organization.

Open a web browser and go to the [NetApp Console](#) to start using the Console agent with the Console.

If you have Amazon S3 buckets in the same AWS account where you created the Console agent, you'll see an Amazon S3 working environment appear on the **Systems** page automatically. [Learn how to manage S3 buckets from NetApp Console](#)

### Manually install the Console agent in AWS

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

#### Before you begin

- You should have an [understanding of Console agents](#).
- You should review [Console agent limitations](#).

#### Step 1: Review host requirements

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



The Console agent 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 agent installation will fail. NetApp recommends using a host that is free of third-party software to avoid conflicts.

#### Dedicated host

The Console agent is not supported on a host that is shared with other applications. The host must be a dedicated host. The host can be of any architecture that meets the following size requirements:

- CPU: 8 cores or 8 vCPUs
- RAM: 32 GB
- Disk space: 165 GB is recommended for the host, with the following partition requirements:
  - `/opt`: 120 GiB of space must be available

The agent uses `/opt` to install the `/opt/application/netapp` directory and its contents.

- `/var`: 40 GiB of space must be available

The Console agent 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.

#### Hypervisor

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

## Operating system and container requirements

The Console agent is supported with the following operating systems when using the Console in standard mode or restricted mode. A container orchestration tool is required before you install the agent.

Operating system	Supported OS versions	Supported agent versions	Required container tool	SELinux
Red Hat Enterprise Linux	9.1 to 9.4 8.6 to 8.10 <ul style="list-style-type: none"><li>English language versions only.</li><li>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 agent installation.</li></ul>	3.9.50 or later with the Console in standard mode or restricted mode	Podman version 4.6.1 or 4.9.4 <a href="#">View Podman configuration requirements.</a>	Supported in enforcing mode or permissive mode <ul style="list-style-type: none"><li>Management of Cloud Volumes ONTAP systems is NOT supported by agents that have SELinux enabled on the operating system.</li></ul>
Ubuntu	24.04 LTS	3.9.45 or later with the NetApp Console in standard mode or restricted mode	Docker Engine 23.06 to 28.0.0.	Not supported
	22.04 LTS	3.9.50 or later	Docker Engine 23.0.6 to 28.0.0.	Not supported

## 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 Console agent, 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 agent.

- [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

The agent uses `/opt` to install the `/opt/application/netapp` directory and its contents.

### **Disk space in /var**

20 GiB of space must be available

The Console agent 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 installing the agent.

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

[View the supported Podman versions.](#)

- Docker Engine is required for Ubuntu.

[View the supported Docker Engine versions.](#)

## Example 1. Steps

### Podman

Follow these steps to install and configure Podman:

- 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
- If using Red Hat Enterprise Linux 8, verify that your Podman version is using Aardvark DNS instead of CNI



Adjust the aardvark-dns port (default: 53) after installing the agent to avoid DNS port conflicts. 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.

You can obtain Podman 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 supported Podman versions](#).

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 supported Podman versions](#).

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.

6. If using Red Hat Enterprise:

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
```

7. 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.

8. If using Red Hat Enterprise Linux 8, verify that your Podman version is using NetAvark with Aardvark DNS instead of CNI.

a. Check to see if your networkBackend is set to CNI by running the following command:

```
podman info | grep networkBackend
```

b. If the networkBackend is set to CNI, you'll need to change it to netavark.

c. Install netavark and aardvark-dns using the following command:

```
dnf install aardvark-dns netavark
```

d. Open the `/etc/containers/containers.conf` file and modify the `network_backend` option to use "netavark" instead of "cni".

If `/etc/containers/containers.conf` doesn't exist, make the configuration changes to

```
/usr/share/containers/containers.conf.
```

9. Restart podman.

```
systemctl restart podman
```

10. Confirm networkBackend is now changed to "netavark" using the following command:

```
podman info | grep networkBackend
```

## Docker Engine

Follow the documentation from Docker to install Docker Engine.

### Steps

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

Follow the steps to install a supported Docker Engine version. Do not install the latest version, as it is unsupported by the Console.

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 Console agent supports the following requirements. Meeting these requirements enables the Console agent to manage resources and processes within your hybrid cloud environment.

### Connections to target networks

The Console agent requires a network connection to the location where you're planning to create and manage systems. 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 Console agent must have an outbound internet connection to contact specific endpoints.

### Endpoints contacted from computers when using the web-based NetApp Console

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

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

### Endpoints contacted from the Console agent

The Console agent requires outbound internet access to contact the following endpoints to manage

resources and processes within your public cloud environment for day-to-day operations.

The endpoints listed below are all CNAME entries.

Endpoints	Purpose
AWS services (amazonaws.com): <ul style="list-style-type: none"><li>• CloudFormation</li><li>• Elastic Compute Cloud (EC2)</li><li>• Identity and Access Management (IAM)</li><li>• Key Management Service (KMS)</li><li>• Security Token Service (STS)</li><li>• Simple Storage Service (S3)</li></ul>	To manage AWS resources. The endpoint depends on your AWS region. <a href="#">Refer to AWS documentation for details</a>
https://mysupport.netapp.com	To obtain licensing information and to send AutoSupport messages to NetApp support.
https://signin.b2c.netapp.com	To update NetApp Support Site (NSS) credentials or to add new NSS credentials to the NetApp Console.
https://api.bluexp.netapp.com https://netapp-cloud-account.auth0.com https://netapp-cloud-account.us.auth0.com https://console.netapp.com https://components.console.bluexp.netapp.com https://cdn.auth0.com	To provide features and services within the NetApp Console.
https://bluexpinfrasprod.eastus2.data.azurecr.io https://bluexpinfrasprod.azurecr.io	<p>To obtain images for Console agent upgrades.</p> <ul style="list-style-type: none"><li>• When you deploy a new agent, the validation check tests connectivity to current endpoints. If you use xref:./previous endpoints, the validation check fails. To avoid this failure, skip the validation check.</li></ul> <p>Although the previous endpoints are still supported, NetApp recommends updating your firewall rules to the current endpoints as soon as possible. <a href="#">Learn how to update your endpoint list.</a></p> <ul style="list-style-type: none"><li>• When you update to the current endpoints in your firewall, your existing agents will continue to work.</li></ul>

## 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 Console agent, unless you initiate it or if it 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, the Console automatically configures those systems to use a proxy server that's included with the Console agent. The only requirement is to ensure that the Console agent's security group allows inbound connections over port 3128. You'll need to open this port after you deploy the Console agent.

## Enable NTP

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

## Step 4: Set up AWS permissions for the Console

You need to provide AWS permissions to the NetApp Console 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 the Console with the AWS access key for an IAM user who has the required permissions.

Follow the steps to prepare permissions for the Console.

## 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 Console agent](#).
  - c. Finish the remaining steps to create the policy.

Depending on the NetApp data services you plan 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 Console agent](#).

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 Console agent.

## 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 Console agent](#).
  - c. Finish the remaining steps to create the policy.

Depending on the NetApp data 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 Console agent](#).

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 the NetApp Console after you install the Console agent.

### Result

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

## Step 5: Install the Console agent

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

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

- 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 Console agent. If you need to set a certificate for a transparent proxy server, you must use the Maintenance Console after installation. Learn more about the [Agent Maintenance Console](#).

### About this task

The installer that is available on the NetApp Support Site might be an earlier version. After installation, the Console agent 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 fails.

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

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

3. Assign permissions to run the script.

```
chmod +x NetApp_Console_Agent_Cloud_<version>
```

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

4. If installing in a Government Cloud environment, disable the configuration checks. [Learn how to disable configuration checks for manual installations](#).
5. Run the installation script.

```
./NetApp_Console_Agent_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:

```
./NetApp_Console_Agent_Cloud_v4.0.0--proxy  
https://user:password@10.0.0.30:8080/ --cacert  
/tmp/cacert/certificate.cer
```

`--proxy` configures the Console agent 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.
- The Console agent 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 Console agent 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 Console agent host:

+

```
./NetApp_Console_Agent_Cloud_v4.0.0 --cacert /tmp/cacert/certificate.cer
```

1. If you used Podman, you'll need to adjust the aardvark-dns port.
  - a. SSH to the Console agent 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 Console agent virtual machine.
2. Wait for the installation to complete.

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



If the installation fails, you can view the installation report and logs to help you fix the issues.  
[Learn how to troubleshoot installation issues.](#)

1. Open a web browser from a host that has a connection to the Console agent virtual machine and enter the following URL:

`https://ipaddress`

2. After you log in, set up the Console agent:
  - a. Specify the organization to associate with the Console agent.
  - 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 the Console in standard mode. You should enable restricted mode only if you have a secure environment and want to disconnect this account from backend services. If that's the case, [follow steps to get started with the NetApp Console in restricted mode.](#)

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



If you have Amazon S3 buckets in the same AWS account where you created the Console agent, you'll see an Amazon S3 storage system appear on the **Systems** page automatically. [Learn how to manage S3 buckets from NetApp ConsoleP](#)

## Step 6: Provide permissions to NetApp Console

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

### IAM role

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

#### Steps

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

Go to the [NetApp Console](#) to start using the Console agent.

### AWS access key

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

#### Steps

1. Ensure that the correct Console agent is currently selected in the Console.
2. Select **Administration > Credentials**.
3. Select **Organization credentials**.
4. Select **Add Credentials** and follow the steps in the wizard.
  - a. **Credentials Location**: Select **\*Amazon Web Services > Agent**.
  - 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**.

Go to the [NetApp Console](#) to start using the Console agent.

## Azure

### Console agent installation options in Azure

There are a few different ways to create a Console agent in Azure. Directly from the NetApp Console is the most common way.

The following installation options are available:

- [Create a Console agent directly from the NetApp Console](#) (this is the standard option)

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

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

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

- [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 the Console agent with the required permissions that it needs to authenticate and manage resources in Azure.

### Create a Console agent in Azure from NetApp Console

To create a Console agent in Azure from the NetApp Console, you need to set up your networking, prepare Azure permissions, and then create the Console agent.

#### Before you begin

- You should have an [understanding of Console agents](#).
- You should review [Console agent limitations](#).

### Step 1: Set up networking

Ensure that the network location where you plan to install the Console agent supports the following requirements. These requirements allow the Console agent to manage hybrid cloud resources.

#### Azure region

If you use Cloud Volumes ONTAP, the Console agent 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 Console agent, you need to specify the VNet and subnet where it should reside.

#### Connections to target networks

The Console agent requires a network connection to the location where you're planning to create and manage systems. 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 Console agent must have an outbound internet connection to contact specific endpoints.

#### Endpoints contacted from the Console agent

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

The endpoints listed below are all CNAME entries.

Endpoints	Purpose
<a href="https://management.azure.com">https://management.azure.com</a> <a href="https://login.microsoftonline.com">https://login.microsoftonline.com</a> <a href="https://blob.core.windows.net">https://blob.core.windows.net</a> <a href="https://core.windows.net">https://core.windows.net</a>	To manage resources in Azure public regions.
<a href="https://management.chinacloudapi.cn">https://management.chinacloudapi.cn</a> <a href="https://login.chinacloudapi.cn">https://login.chinacloudapi.cn</a> <a href="https://blob.core.chinacloudapi.cn">https://blob.core.chinacloudapi.cn</a> <a href="https://core.chinacloudapi.cn">https://core.chinacloudapi.cn</a>	To manage resources in Azure China regions.
<a href="https://mysupport.netapp.com">https://mysupport.netapp.com</a>	To obtain licensing information and to send AutoSupport messages to NetApp support.
<a href="https://signin.b2c.netapp.com">https://signin.b2c.netapp.com</a>	To update NetApp Support Site (NSS) credentials or to add new NSS credentials to the NetApp Console.
<a href="https://api.blueexp.netapp.com">https://api.blueexp.netapp.com</a> <a href="https://netapp-cloud-account.auth0.com">https://netapp-cloud-account.auth0.com</a> <a href="https://netapp-cloud-account.us.auth0.com">https://netapp-cloud-account.us.auth0.com</a> <a href="https://console.netapp.com">https://console.netapp.com</a> <a href="https://components.console.blueexp.netapp.com">https://components.console.blueexp.netapp.com</a> <a href="https://cdn.auth0.com">https://cdn.auth0.com</a>	To provide features and services within the NetApp Console.
<a href="https://blueexpinfraprod.eastus2.data.azurecr.io">https://blueexpinfraprod.eastus2.data.azurecr.io</a> <a href="https://blueexpinfraprod.azurecr.io">https://blueexpinfraprod.azurecr.io</a>	<p>To obtain images for Console agent upgrades.</p> <ul style="list-style-type: none"> <li>When you deploy a new agent, the validation check tests connectivity to current endpoints. If you use <a href="#">xref:./previous endpoints</a>, the validation check fails. To avoid this failure, skip the validation check.</li> </ul> <p>Although the previous endpoints are still supported, NetApp recommends updating your firewall rules to the current endpoints as soon as possible. <a href="#">Learn how to update your endpoint list.</a></p> <ul style="list-style-type: none"> <li>When you update to the current endpoints in your firewall, your existing agents will continue to work.</li> </ul>

### Endpoints contacted from the NetApp console

As you use the web-based NetApp 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 Console agent from the the Console.

[View the list of endpoints contacted from the NetApp 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 Console agent, unless you initiate it or if it 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, the Console automatically configures those systems to use a proxy server that's included with the Console agent. The only requirement is to ensure that the Console agent's security group allows inbound connections over port 3128. You'll need to open this port after you deploy the Console agent.

## Enable NTP

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

You need to implement this networking requirement after you create the Console agent.

## Step 2: Create a Console agent deployment policy (custom role)

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

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

The Console deploys the Console agent VM in Azure, enables a [system-assigned managed identity](#), creates the required role, and assigns it to the VM. [Review how the Console 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 Console agent VM in Azure from the Console. Don't use this policy for other situations. When the Console creates the Console agent, it applies a new set of permissions to the Console agent VM that enables the Console agent 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/rea
```

```

d",
    "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

```

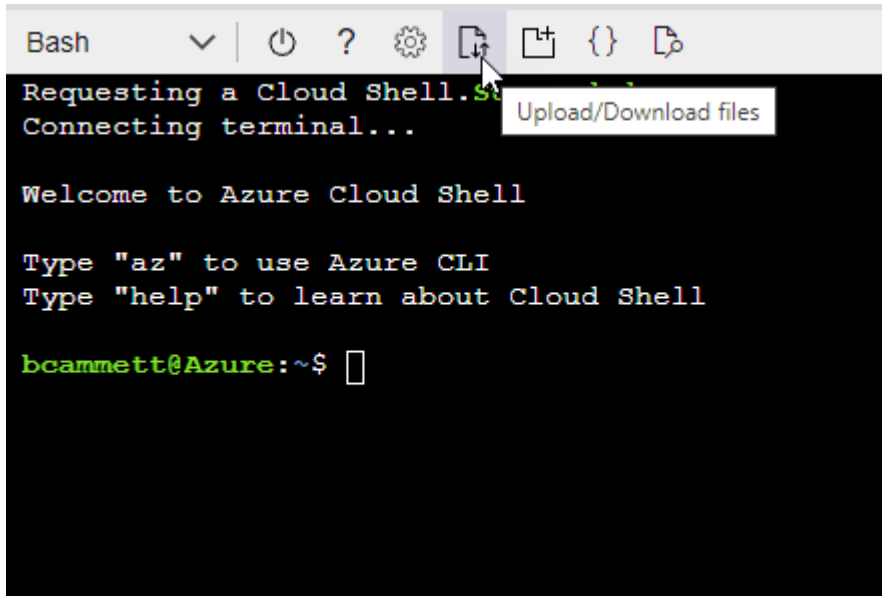
"AssignableScopes": [
    "/subscriptions/d333af45-0d07-4154-943d-c25fbzzzzzz"
],

```

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

### Step 3: Set up authentication

When creating the Console agent from the Console, you need to provide a login that enables the Console 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 the Console.

## Azure account

Assign the custom role to the user who will deploy the Console agent from the Console.

### 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 Console agent 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**.

## Service principal

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

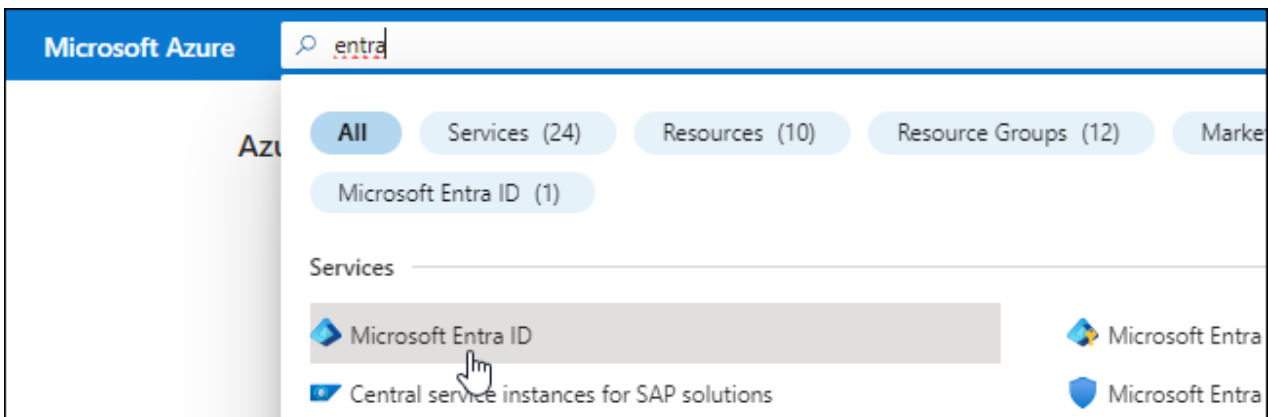
Create and set up a service principal in Microsoft Entra ID and obtain the Azure credentials that the Console needs.

### 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:

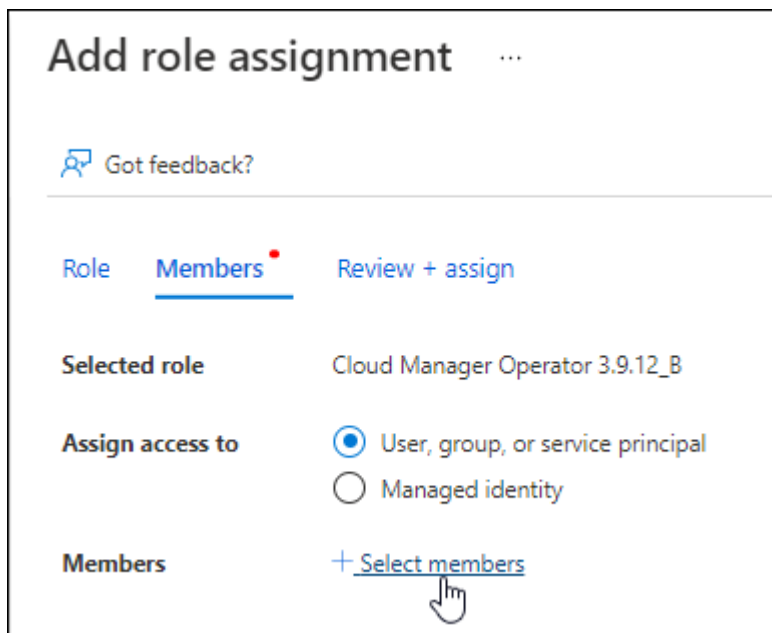
- **Name:** Enter a name for the application.
- **Account type:** Select an account type (any will work with the NetApp Console).
- **Redirect URI:** You can leave this field blank.

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



**Add role assignment** ...

 Got feedback?

---

**Role**   **Members** <sup>•</sup>   [Review + assign](#)

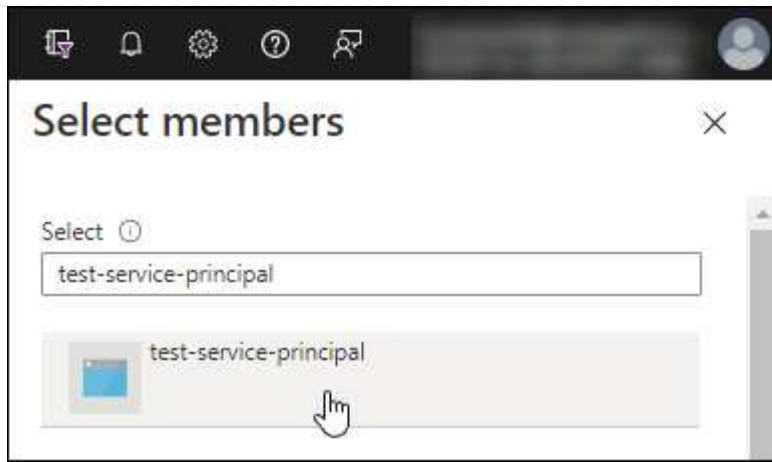
**Selected role**   Cloud Manager Operator 3.9.12\_B

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

**Members**   [+ Select members](#)

- c. Search for the name of the application.

Here's an example:



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

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

If you want to manage resources in multiple Azure subscriptions, then you must bind the service principal to each of those subscriptions. For example, the Console 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

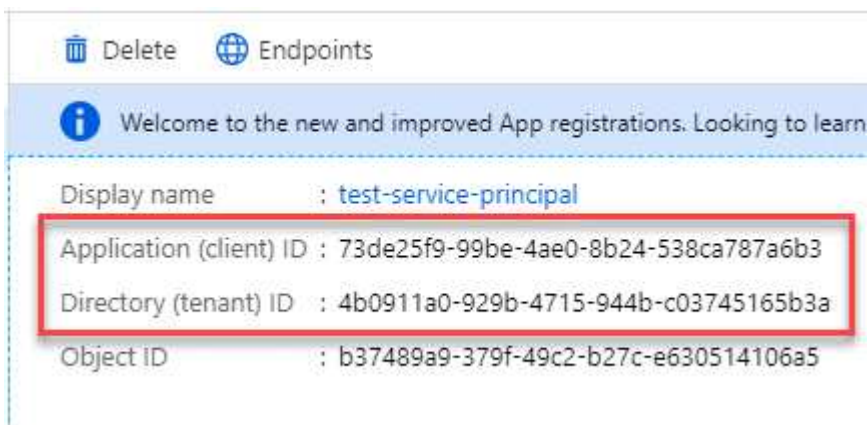


user\_impersonation

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 the Console, you need to provide the application (client) ID and the directory (tenant) ID for the application. The Console 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	

### 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 the Console when you create the Console agent.

## Step 4: Create the Console agent

Create the Console agent directly from the NetApp Console.

### About this task

- Creating the Console agent from the Console deploys a virtual machine in Azure using a default configuration. Do not switch to a smaller VM instance with fewer CPUs or less RAM after creating the Console agent. [Learn about the default configuration for the Console agent.](#)
- When the Console deploys the Console agent, it creates a custom role and assigns it to the Console agent VM. This role includes permissions that enables the Console agent 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 Console agent.](#)

### 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 Console agent 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 the Console to automatically create an Azure role for the Console agent, then you'll need to create your own [using the policy on this page.](#)

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

## Steps

1. Select **Administration > Agents**.
2. On the **Overview** page, select **Deploy agent > Azure**
3. On the **Review** page, review the requirements for deploying an agent. Those requirements are also detailed above on this page.
4. On the **Virtual Machine Authentication** page, select the authentication option that matches how you set up Azure permissions:

- Select **Log in** 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 the Console automatically uses 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.](#)

5. On the **Virtual Machine Authentication** page, choose an Azure subscription, a location, a new resource group or an existing resource group, and then choose an authentication method for the Console agent 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](#)

6. On the **Details** page, enter a name for the instance, specify tags, and choose whether you want the Console 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 Console agent permissions to manage resources in that subscription (for example, Cloud Volumes ONTAP).

7. On the **Network** page, choose a VNet and subnet, whether to enable a public IP address, and optionally specify a proxy configuration.
  - On the **Security Group** page, 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.](#)

8. Review your selections to verify that your set up is correct.
  - a. The **Validate agent configuration** check box is marked by default to have the Console validate the network connectivity requirements when you deploy. If the Console fails to deploy the agent, it provides a report to help you troubleshoot. If the deployment succeeds, no report is provided.

If you are still using the [previous endpoints](#) used for agent upgrades, the validation fails with an error. To avoid this, unmark the check box to skip the validation check.

#### 9. Select **Add**.

The Console prepares the instance in about 10 minutes. Stay on the page until the process completes.

### Result

After the process is complete, the Console agent is available for use from the Console.



If the deployment fails, you can download a report and logs from the Console to help you fix the issues. [Learn how to troubleshoot installation issues.](#)

If you have Azure Blob storage in the same Azure subscription where you created the Console agent, you'll see an Azure Blob storage system appear on the **Systems** page automatically. [Learn how to manage Azure Blob storage from NetApp Console](#)

### Create a Console agent from the Azure Marketplace

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

#### Before you begin

- You should have an [understanding of Console agents](#).
- Review [Console agent limitations](#).

### Step 1: Set up networking

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

#### Azure region

If you use Cloud Volumes ONTAP, the Console agent 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 Console agent, you need to specify the VNet and subnet where it should reside.

#### Connections to target networks

The Console agent requires a network connection to the location where you're planning to create and manage systems. 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 Console agent must have an outbound internet connection to contact specific endpoints.

## Endpoints contacted from the Console agent

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

The endpoints listed below are all CNAME entries.

Endpoints	Purpose
<a href="https://management.azure.com">https://management.azure.com</a> <a href="https://login.microsoftonline.com">https://login.microsoftonline.com</a> <a href="https://blob.core.windows.net">https://blob.core.windows.net</a> <a href="https://core.windows.net">https://core.windows.net</a>	To manage resources in Azure public regions.
<a href="https://management.chinacloudapi.cn">https://management.chinacloudapi.cn</a> <a href="https://login.chinacloudapi.cn">https://login.chinacloudapi.cn</a> <a href="https://blob.core.chinacloudapi.cn">https://blob.core.chinacloudapi.cn</a> <a href="https://core.chinacloudapi.cn">https://core.chinacloudapi.cn</a>	To manage resources in Azure China regions.
<a href="https://mysupport.netapp.com">https://mysupport.netapp.com</a>	To obtain licensing information and to send AutoSupport messages to NetApp support.
<a href="https://signin.b2c.netapp.com">https://signin.b2c.netapp.com</a>	To update NetApp Support Site (NSS) credentials or to add new NSS credentials to the NetApp Console.
<a href="https://api.blueexp.netapp.com">https://api.blueexp.netapp.com</a> <a href="https://netapp-cloud-account.auth0.com">https://netapp-cloud-account.auth0.com</a> <a href="https://netapp-cloud-account.us.auth0.com">https://netapp-cloud-account.us.auth0.com</a> <a href="https://console.netapp.com">https://console.netapp.com</a> <a href="https://components.console.blueexp.netapp.com">https://components.console.blueexp.netapp.com</a> <a href="https://cdn.auth0.com">https://cdn.auth0.com</a>	To provide features and services within the NetApp Console.
<a href="https://blueexpinfraprod.eastus2.data.azurecr.io">https://blueexpinfraprod.eastus2.data.azurecr.io</a> <a href="https://blueexpinfraprod.azurecr.io">https://blueexpinfraprod.azurecr.io</a>	<p>To obtain images for Console agent upgrades.</p> <ul style="list-style-type: none"><li>When you deploy a new agent, the validation check tests connectivity to current endpoints. If you use <a href="#">xref:./previous endpoints</a>, the validation check fails. To avoid this failure, skip the validation check.</li></ul> <p>Although the previous endpoints are still supported, NetApp recommends updating your firewall rules to the current endpoints as soon as possible. <a href="#">Learn how to update your endpoint list.</a></p> <ul style="list-style-type: none"><li>When you update to the current endpoints in your firewall, your existing agents will continue to work.</li></ul>



## 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 Console agent, unless you initiate it or if it 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, the Console automatically configures those systems to use a proxy server that's included with the Console agent. The only requirement is to ensure that the Console agent's security group allows inbound connections over port 3128. You'll need to open this port after you deploy the Console agent.

## Enable NTP

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

Implement the networking requirements after creating the Console agent.

## Step 2: Review VM requirements

When you create the Console agent, 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 the Console with the credentials for an Azure service principal that has the required permissions.

Follow these steps to set up permissions for the Console.

## 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 the NetApp Console.

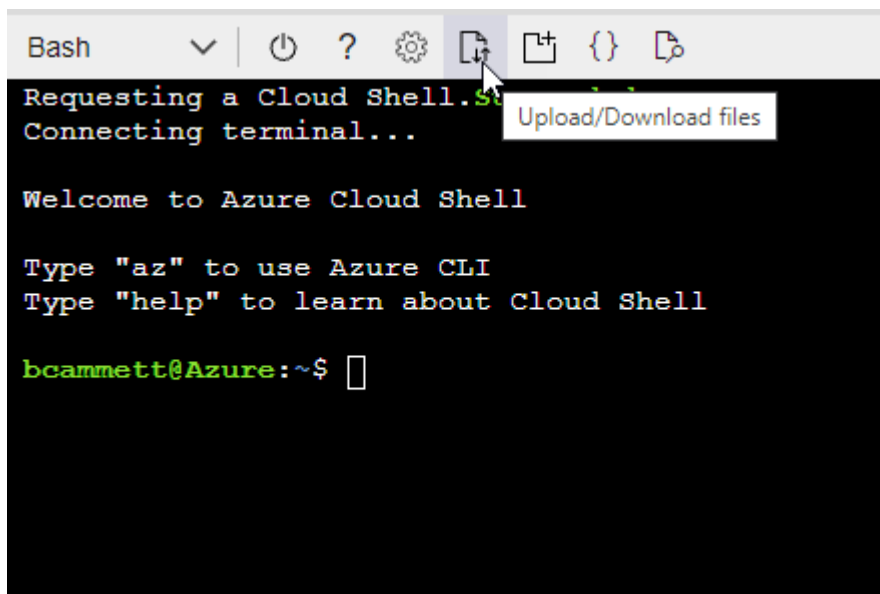
## Example

```
"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
```

### Service principal

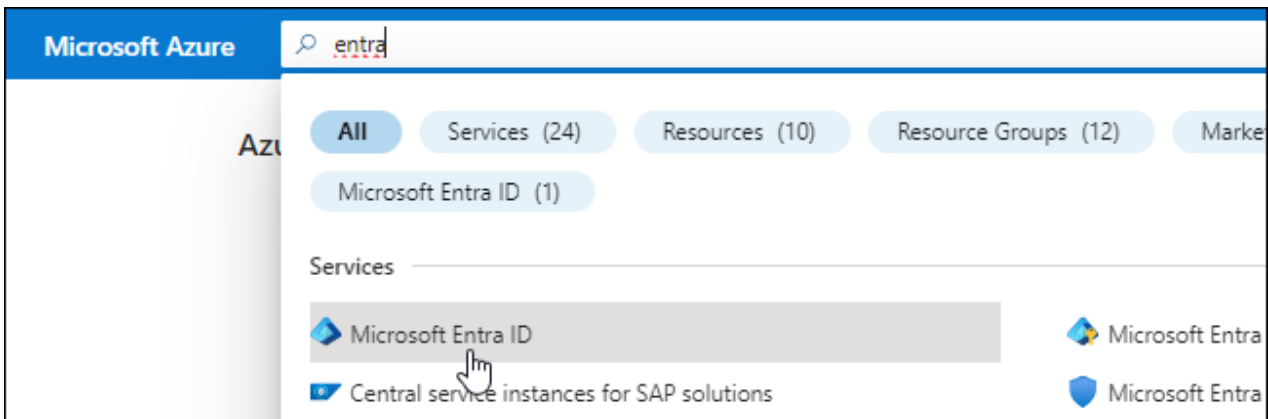
Create and set up a service principal in Microsoft Entra ID and obtain the Azure credentials that the Console needs.

#### 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 the NetApp Console).
  - **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 Console agent](#) 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.

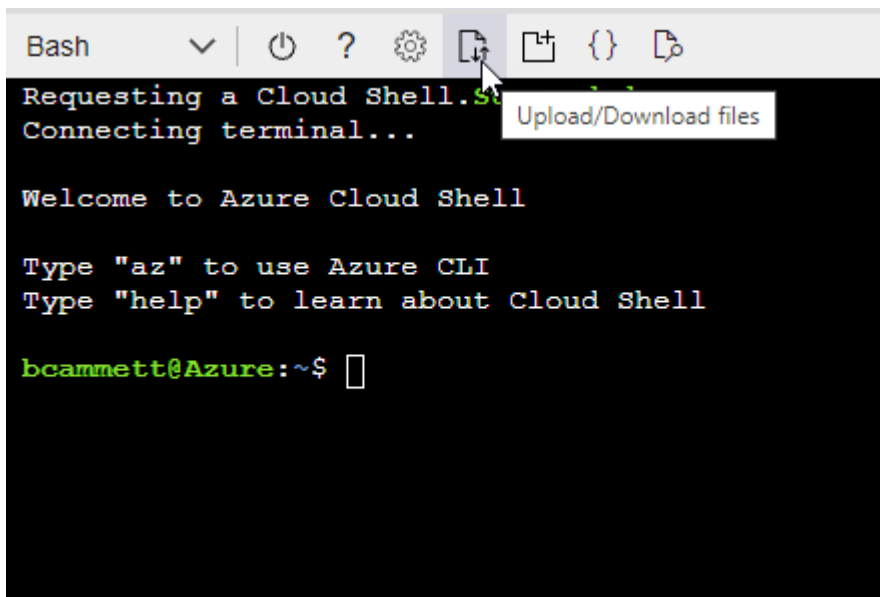
### Example

```
"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.



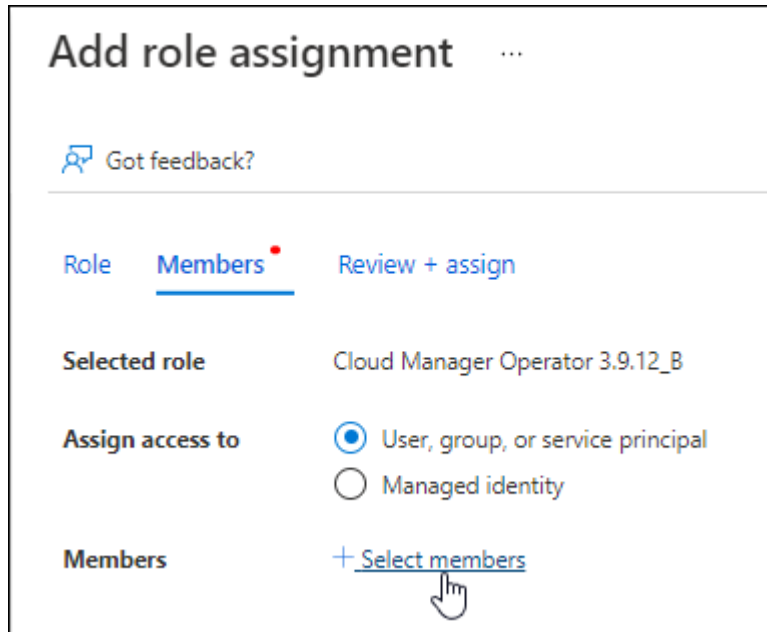
- Use the Azure CLI to create the custom role:

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

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

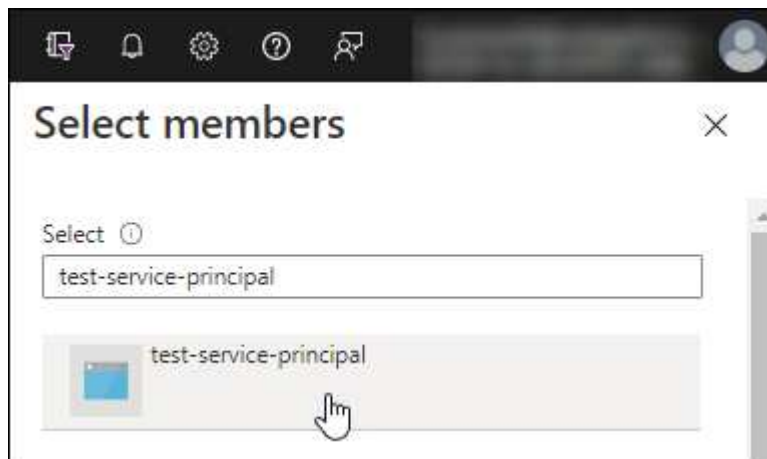
2. Assign the application to the role:
  - a. From the Azure portal, open the **Subscriptions** service.
  - b. Select the subscription.

- c. Select **Access control (IAM) > Add > Add role assignment**.
- d. In the **Role** tab, select the **Console 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 Console agent.

If you want to deploy Cloud Volumes ONTAP from multiple Azure subscriptions, then you must bind the service principal to each of those subscriptions. In the NetApp Console, you can 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.

 <b>Azure Batch</b> Schedule large-scale parallel and HPC applications in the cloud	 <b>Azure Data Catalog</b> Programmatic access to Data Catalog resources to register, annotate and search data assets	 <b>Azure Data Explorer</b> Perform ad-hoc queries on terabytes of data to build near real-time and complex analytics solutions
 <b>Azure Data Lake</b> Access to storage and compute for big data analytic scenarios	 <b>Azure DevOps</b> Integrate with Azure DevOps and Azure DevOps server	 <b>Azure Import/Export</b> Programmatic control of import/export jobs
 <b>Azure Key Vault</b> Manage your key vaults as well as the keys, secrets, and certificates within your Key Vaults	 <b>Azure Rights Management Services</b> Allow validated users to read and write protected content	 <b>Azure Service Management</b> Programmatic access to much of the functionality available through the Azure portal
 <b>Azure Storage</b> Secure, massively scalable object and data lake storage for unstructured and semi-structured data	 <b>Customer Insights</b> Create profile and interaction models for your products	 <b>Data Export Service for Microsoft Dynamics 365</b> 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

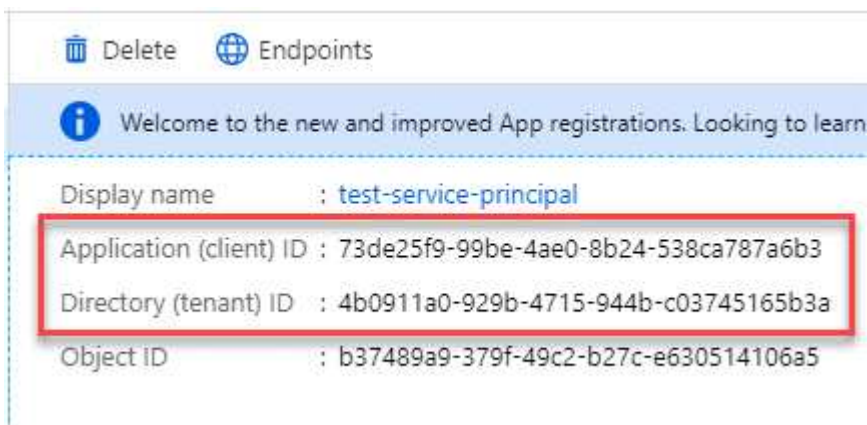


user\_impersonation

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 the Console, you need to provide the application (client) ID and the directory (tenant) ID for the application. The Console 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

## Step 4: Create the Console agent

Launch the Console agent directly from the Azure Marketplace.

### About this task

Creating the Console agent from the Azure Marketplace sets up a virtual machine with a default configuration. [Learn about the default configuration for the Console agent.](#)

### 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 Console agent 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 the Console to automatically create an Azure role for the Console agent, then you'll need to create your own [using the policy on this page](#).

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

### Steps

1. Go to the NetApp Console agent 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 Console agent can perform optimally with either HDD or SSD disks.
- **Network security group:** The Console agent 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 Console agent 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 Console agent software running in about ten minutes.



If the installation fails, you can view logs and a report to help you troubleshoot. [Learn how to troubleshoot installation issues.](#)

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

`https://ipaddress`

6. After you log in, set up the Console agent:
  - a. Specify the the Console organization to associate with the Console agent.
  - 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 the Console in standard mode. You should enable restricted mode only if you have a secure environment and want to disconnect this account from the Console backend services. If that's the case, [follow steps to get started with the Console in restricted mode.](#)

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

## Result

You have now installed the Console agent and set it up with your the Console organization.

If you have Azure Blob storage in the same Azure subscription where you created the Console agent, you'll see an Azure Blob storage system appear on the **Systems** page automatically. [Learn how to manage Azure Blob storage from the Console](#)

## Step 5: Provide permissions to the Console agent

Now that you've created the Console agent, you need to provide it with the permissions that you previously set up. Providing the permissions enables the Console agent to manage your data and storage infrastructure in Azure.

## Custom role

Go to the Azure portal and assign the Azure custom role to the Console agent 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 the NetApp Console 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 **Console Operator** role and select **Next**.



Console Operator is the default name provided in the 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 Console agent virtual machine was created, under **Managed identity**, choose **Virtual machine**, and then select the Console agent 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.

### What's next?

Go to the [NetApp Console](#) to start using the Console agent.

## Service principal

### Steps

1. Select **Administration > Credentials**.
2. Select **Add Credentials** and follow the steps in the wizard.
  - a. **Credentials Location**: Select **Microsoft Azure > Agent**.
  - 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

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

## Manually install the Console agent in Azure

To manually install the Console agent on your own Linux host, you need to review host requirements, set up your networking, prepare Azure permissions, install the Console agent, and then provide the permissions that you prepared.

### Before you begin

- You should have an [understanding of Console agents](#).
- You should review [Console agent limitations](#).

### Step 1: Review host requirements

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



The Console agent 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 agent installation will fail. NetApp recommends using a host that is free of third-party software to avoid conflicts.

### Dedicated host

The Console agent is not supported on a host that is shared with other applications. The host must be a dedicated host. The host can be of any architecture that meets the following size requirements:

- CPU: 8 cores or 8 vCPUs
- RAM: 32 GB
- Disk space: 165 GB is recommended for the host, with the following partition requirements:
  - `/opt`: 120 GiB of space must be available

The agent uses `/opt` to install the `/opt/application/netapp` directory and its contents.

- `/var`: 40 GiB of space must be available

The Console agent 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.

### Hypervisor

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

### Operating system and container requirements

The Console agent is supported with the following operating systems when using the Console in standard mode or restricted mode. A container orchestration tool is required before you install the agent.

Operating system	Supported OS versions	Supported agent versions	Required container tool	SELinux
Red Hat Enterprise Linux	9.1 to 9.4 8.6 to 8.10 <ul style="list-style-type: none"> <li>English language versions only.</li> <li>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 agent installation.</li> </ul>	3.9.50 or later with the Console in standard mode or restricted mode	Podman version 4.6.1 or 4.9.4  <a href="#">View Podman configuration requirements.</a>	Supported in enforcing mode or permissive mode  <ul style="list-style-type: none"> <li>Management of Cloud Volumes ONTAP systems is NOT supported by agents that have SELinux enabled on the operating system.</li> </ul>
Ubuntu	24.04 LTS	3.9.45 or later with the NetApp Console in standard mode or restricted mode	Docker Engine 23.06 to 28.0.0.	Not supported
	22.04 LTS	3.9.50 or later	Docker Engine 23.0.6 to 28.0.0.	Not supported

### 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

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

### Disk space in /var

20 GiB of space must be available

The Console agent 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 installing the agent.

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

[View the supported Podman versions.](#)

- Docker Engine is required for Ubuntu.

[View the supported Docker Engine versions.](#)

## Example 2. Steps

### Podman

Follow these steps to install and configure Podman:

- 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
- If using Red Hat Enterprise Linux 8, verify that your Podman version is using Aardvark DNS instead of CNI



Adjust the aardvark-dns port (default: 53) after installing the agent to avoid DNS port conflicts. 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.

You can obtain Podman 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 supported Podman versions](#).

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 supported Podman versions](#).

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.

6. If using Red Hat Enterprise:

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
```

7. 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.

8. If using Red Hat Enterprise Linux 8, verify that your Podman version is using NetAvark with Aardvark DNS instead of CNI.

a. Check to see if your networkBackend is set to CNI by running the following command:

```
podman info | grep networkBackend
```

b. If the networkBackend is set to CNI, you'll need to change it to netavark.

c. Install netavark and aardvark-dns using the following command:

```
dnf install aardvark-dns netavark
```

d. Open the `/etc/containers/containers.conf` file and modify the `network_backend` option to use "netavark" instead of "cni".

If `/etc/containers/containers.conf` doesn't exist, make the configuration changes to



```
/usr/share/containers/containers.conf.
```

9. Restart podman.

```
systemctl restart podman
```

10. Confirm networkBackend is now changed to "netavark" using the following command:

```
podman info | grep networkBackend
```

## Docker Engine

Follow the documentation from Docker to install Docker Engine.

### Steps

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

Follow the steps to install a supported Docker Engine version. Do not install the latest version, as it is unsupported by the Console.

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 Console agent supports the following requirements. Meeting these requirements enables the Console agent to manage resources and processes within your hybrid cloud environment.

### Azure region

If you use Cloud Volumes ONTAP, the Console agent 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

The Console agent requires a network connection to the location where you're planning to create and manage systems. 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 Console agent must have an outbound internet connection to contact specific endpoints.

## Endpoints contacted from computers when using the web-based NetApp Console

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

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

## Endpoints contacted from the Console agent

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

The endpoints listed below are all CNAME entries.

Endpoints	Purpose
<a href="https://management.azure.com">https://management.azure.com</a> <a href="https://login.microsoftonline.com">https://login.microsoftonline.com</a> <a href="https://blob.core.windows.net">https://blob.core.windows.net</a> <a href="https://core.windows.net">https://core.windows.net</a>	To manage resources in Azure public regions.
<a href="https://management.chinacloudapi.cn">https://management.chinacloudapi.cn</a> <a href="https://login.chinacloudapi.cn">https://login.chinacloudapi.cn</a> <a href="https://blob.core.chinacloudapi.cn">https://blob.core.chinacloudapi.cn</a> <a href="https://core.chinacloudapi.cn">https://core.chinacloudapi.cn</a>	To manage resources in Azure China regions.
<a href="https://mysupport.netapp.com">https://mysupport.netapp.com</a>	To obtain licensing information and to send AutoSupport messages to NetApp support.
<a href="https://signin.b2c.netapp.com">https://signin.b2c.netapp.com</a>	To update NetApp Support Site (NSS) credentials or to add new NSS credentials to the NetApp Console.
<a href="https://api.blueexp.netapp.com">https://api.blueexp.netapp.com</a> <a href="https://netapp-cloud-account.auth0.com">https://netapp-cloud-account.auth0.com</a> <a href="https://netapp-cloud-account.us.auth0.com">https://netapp-cloud-account.us.auth0.com</a> <a href="https://console.netapp.com">https://console.netapp.com</a> <a href="https://components.console.blueexp.netapp.com">https://components.console.blueexp.netapp.com</a> <a href="https://cdn.auth0.com">https://cdn.auth0.com</a>	To provide features and services within the NetApp Console.

Endpoints	Purpose
<a href="https://bluexpinfraprod.eastus2.data.azurecr.io">https://bluexpinfraprod.eastus2.data.azurecr.io</a> <a href="https://bluexpinfraprod.azurecr.io">https://bluexpinfraprod.azurecr.io</a>	<p>To obtain images for Console agent upgrades.</p> <ul style="list-style-type: none"> <li>When you deploy a new agent, the validation check tests connectivity to current endpoints. If you use <a href="#">xref:./previous endpoints</a>, the validation check fails. To avoid this failure, skip the validation check.</li> </ul> <p>Although the previous endpoints are still supported, NetApp recommends updating your firewall rules to the current endpoints as soon as possible. <a href="#">Learn how to update your endpoint list.</a></p> <ul style="list-style-type: none"> <li>When you update to the current endpoints in your firewall, your existing agents will continue to work.</li> </ul>

### 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 Console agent, unless you initiate it or if it 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, the Console automatically configures those systems to use a proxy server that's included with the Console agent. The only requirement is to ensure that the Console agent's security group allows inbound connections over port 3128. You'll need to open this port after you deploy the Console agent.

### Enable NTP

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

## Step 4: Set up Console agent deployment permissions

You need to provide Azure permissions to the Console agent 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 the Console agent with the credentials for an Azure service principal that has the required permissions.

Follow the steps to prepare permissions for the Console agent.

## Create a custom role for Console agent 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 the NetApp Console.

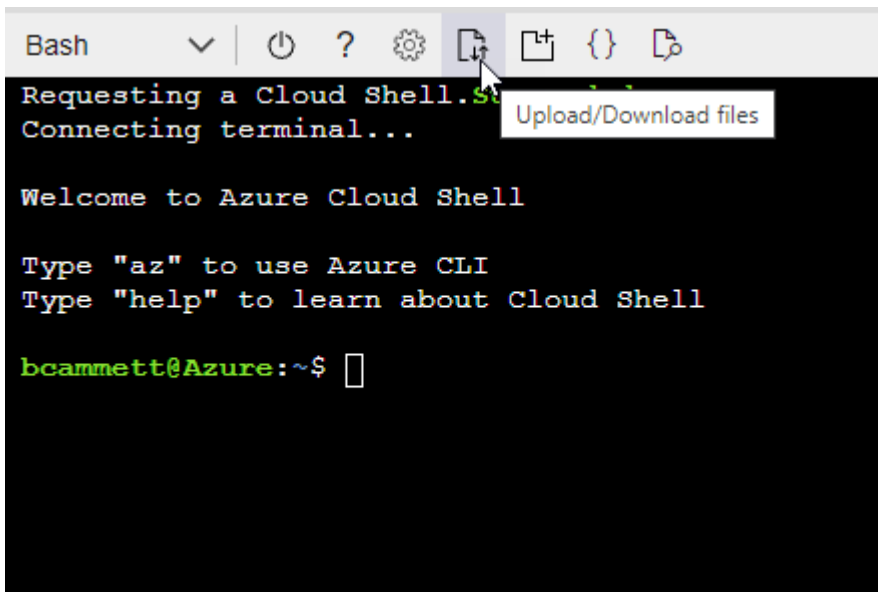
### Example

```
"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
```

### Service principal

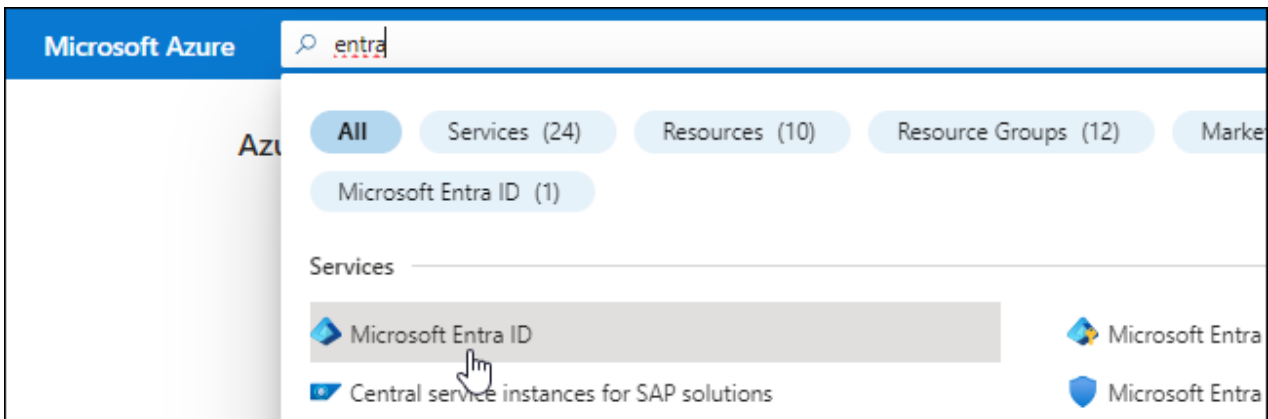
Create and set up a service principal in Microsoft Entra ID and obtain the Azure credentials that the Console agent needs.

#### 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 the NetApp Console).
  - **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 Console agent](#) 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.

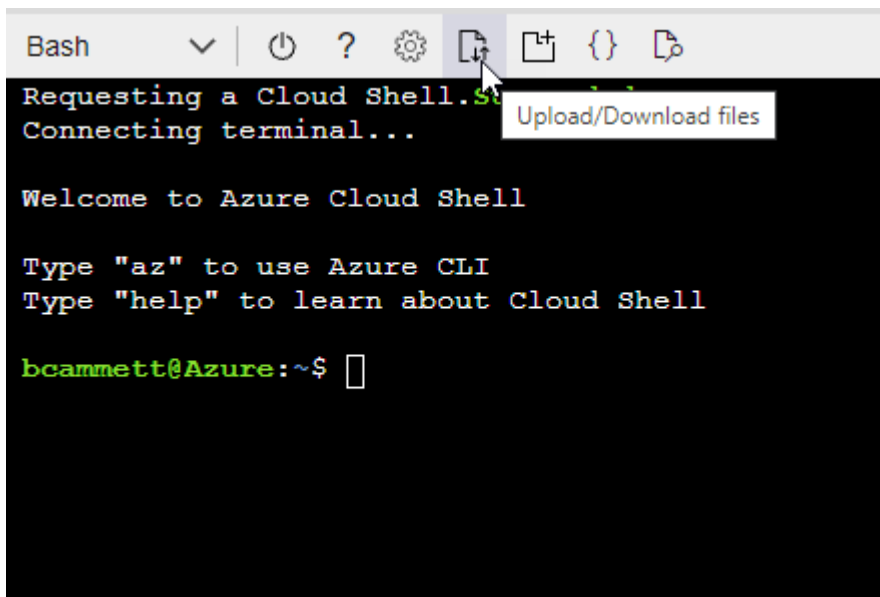
### Example

```
"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.



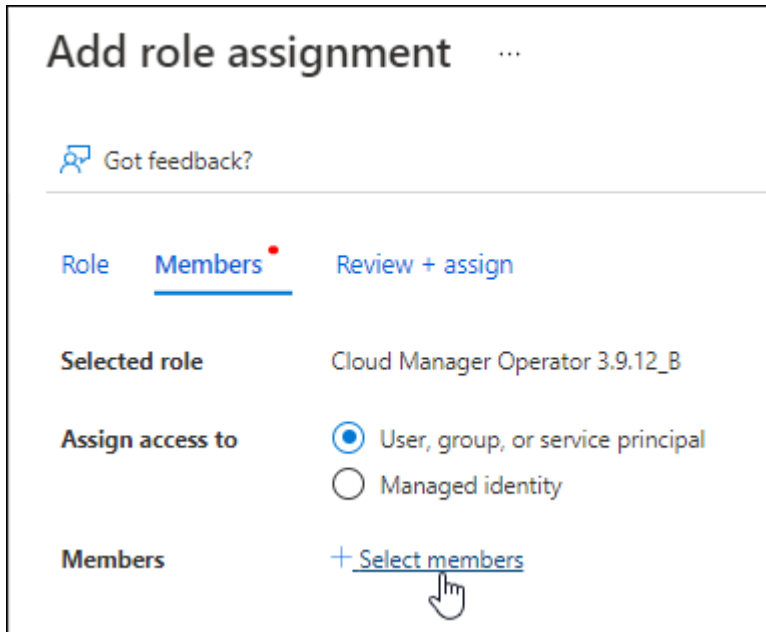
- Use the Azure CLI to create the custom role:

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

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

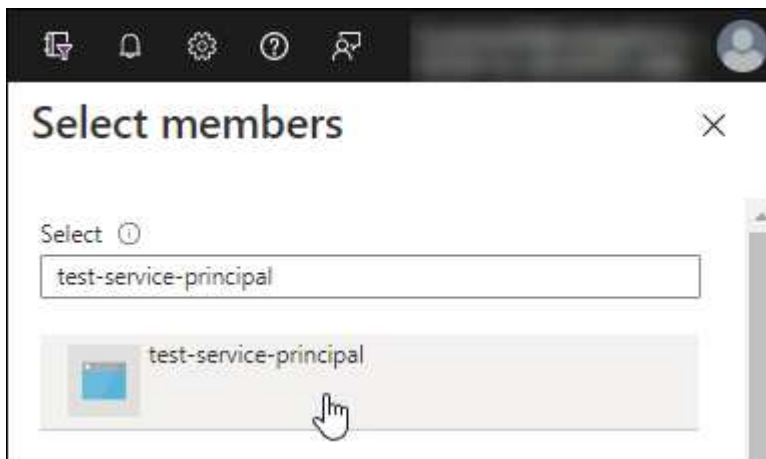
2. Assign the application to the role:
  - a. From the Azure portal, open the **Subscriptions** service.
  - b. Select the subscription.

- c. Select **Access control (IAM) > Add > Add role assignment**.
- d. In the **Role** tab, select the **Console 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 Console agent.

If you want to deploy Cloud Volumes ONTAP from multiple Azure subscriptions, then you must bind the service principal to each of those subscriptions. In the NetApp Console, you can 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.

 <b>Azure Batch</b> Schedule large-scale parallel and HPC applications in the cloud	 <b>Azure Data Catalog</b> Programmatic access to Data Catalog resources to register, annotate and search data assets	 <b>Azure Data Explorer</b> Perform ad-hoc queries on terabytes of data to build near real-time and complex analytics solutions
 <b>Azure Data Lake</b> Access to storage and compute for big data analytic scenarios	 <b>Azure DevOps</b> Integrate with Azure DevOps and Azure DevOps server	 <b>Azure Import/Export</b> Programmatic control of import/export jobs
 <b>Azure Key Vault</b> Manage your key vaults as well as the keys, secrets, and certificates within your Key Vaults	 <b>Azure Rights Management Services</b> Allow validated users to read and write protected content	 <b>Azure Service Management</b> Programmatic access to much of the functionality available through the Azure portal
 <b>Azure Storage</b> Secure, massively scalable object and data lake storage for unstructured and semi-structured data	 <b>Customer Insights</b> Create profile and interaction models for your products	 <b>Data Export Service for Microsoft Dynamics 365</b> 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

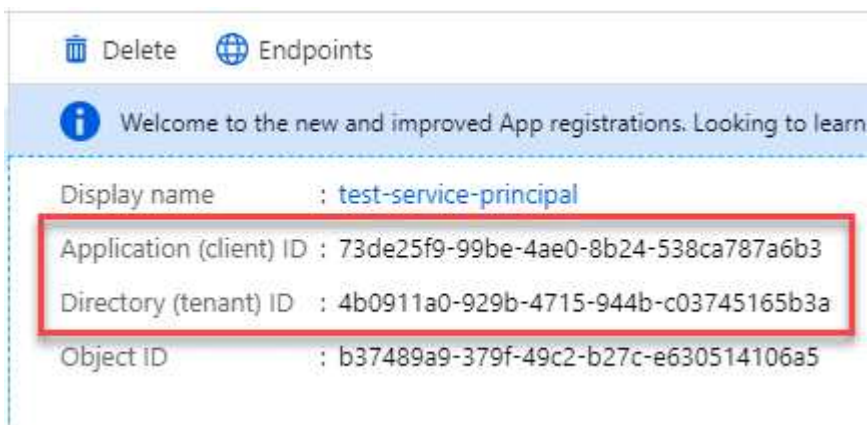


user\_impersonation

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 the Console, you need to provide the application (client) ID and the directory (tenant) ID for the application. The Console 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	

### 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 the Console when you add an Azure account.

## Step 5: Install the Console agent

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

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

- 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 Console agent. If you need to set a certificate for a transparent proxy server, you must use the Maintenance Console after installation. Learn more about the [Agent 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 Console agent 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 fails.

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

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

3. Assign permissions to run the script.

```
chmod +x NetApp_Console_Agent_Cloud_<version>
```

Where <version> is the version of the Console agent that you downloaded.

4. If installing in a Government Cloud environment, disable the configuration checks. [Learn how to disable configuration checks for manual installations.](#)
5. Run the installation script.

```
./NetApp_Console_Agent_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:

```
./NetApp_Console_Agent_Cloud_v4.0.0--proxy  
https://user:password@10.0.0.30:8080/ --cacert  
/tmp/cacert/certificate.cer
```

--proxy configures the Console agent 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.
- The Console agent 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 Console agent 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 Console agent host:

+

```
./NetApp_Console_Agent_Cloud_v4.0.0 --cacert /tmp/cacert/certificate.cer
```

1. If you used Podman, you'll need to adjust the aardvark-dns port.
  - a. SSH to the Console agent 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 Console agent virtual machine.
2. Wait for the installation to complete.

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



If the installation fails, you can view the installation report and logs to help you fix the issues.  
[Learn how to troubleshoot installation issues.](#)

1. Open a web browser from a host that has a connection to the Console agent virtual machine and enter the following URL:

`https://ipaddress`

2. After you log in, set up the Console agent:

- a. Specify the organization to associate with the Console agent.
- 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 the Console in standard mode. You should enable restricted mode only if you have a secure environment and want to disconnect this account from backend services. If that's the case, [follow steps to get started with the NetApp Console in restricted mode](#).

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

If you have Azure Blob storage in the same Azure subscription where you created the Console agent, you'll see an Azure Blob storage system appear on the **Systems** page automatically. [Learn how to manage Azure Blob storage from NetApp Console](#)

## Step 6: Provide permissions to NetApp Console

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

## Custom role

Go to the Azure portal and assign the Azure custom role to the Console agent 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 the NetApp Console 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 **Console Operator** role and select **Next**.



Console Operator is the default name provided in the 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 Console agent virtual machine was created, under **Managed identity**, choose **Virtual machine**, and then select the Console agent 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.

### What's next?

Go to the [NetApp Console](#) to start using the Console agent.

## Service principal

### Steps

1. Select **Administration > Credentials**.
2. Select **Add Credentials** and follow the steps in the wizard.
  - a. **Credentials Location**: Select **Microsoft Azure > Agent**.
  - 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

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

## Google Cloud

### Console agent installation options in Google Cloud

There are a few different ways to create a Console agent in Google Cloud. Directly from the NetApp Console is the most common way.

---

The following installation options are available:

- [Create the Console agent directly from the Console](#) (this is the standard option)

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

- [Create the Console agent using Google Platform](#)

This action also launches a VM instance running Linux and the Console agent software, but the deployment is initiated directly from Google Cloud, rather than from the Console.

- [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 the Console with the required permissions that it needs to authenticate and manage resources in Google Cloud.

### Create a Console agent in Google Cloud from NetApp Console

You can create a Console agent in Google Cloud from the Console. You need to set up your networking, prepare Google Cloud permissions, enable Google Cloud APIs, and then create the Console agent.

### Before you begin

- You should have an [understanding of Console agents](#).
- You should review [Console agent limitations](#).

### Step 1: Set up networking

Set up networking to ensure the Console agent can manage resources, with connections to target networks and outbound internet access.

### VPC and subnet

When you create the Console agent, you need to specify the VPC and subnet where it should reside.

### Connections to target networks

The Console agent requires a network connection to the location where you're planning to create and manage systems. 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 Console agent must have an outbound internet connection to contact specific endpoints.

### Endpoints contacted from the Console agent

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

The endpoints listed below are all CNAME entries.

Endpoints	Purpose
<a href="https://www.googleapis.com/compute/v1/">https://www.googleapis.com/compute/v1/</a> <a href="https://compute.googleapis.com/compute/v1">https://compute.googleapis.com/compute/v1</a> <a href="https://cloudresourcemanager.googleapis.com/v1/projects">https://cloudresourcemanager.googleapis.com/v1/projects</a> <a href="https://www.googleapis.com/compute/beta">https://www.googleapis.com/compute/beta</a> <a href="https://storage.googleapis.com/storage/v1">https://storage.googleapis.com/storage/v1</a> <a href="https://www.googleapis.com/storage/v1">https://www.googleapis.com/storage/v1</a> <a href="https://iam.googleapis.com/v1">https://iam.googleapis.com/v1</a> <a href="https://cloudkms.googleapis.com/v1">https://cloudkms.googleapis.com/v1</a> <a href="https://www.googleapis.com/deploymentmanager/v2/projects">https://www.googleapis.com/deploymentmanager/v2/projects</a>	To manage resources in Google Cloud.
<a href="https://mysupport.netapp.com">https://mysupport.netapp.com</a>	To obtain licensing information and to send AutoSupport messages to NetApp support.
<a href="https://signin.b2c.netapp.com">https://signin.b2c.netapp.com</a>	To update NetApp Support Site (NSS) credentials or to add new NSS credentials to the NetApp Console.
<a href="https://api.blueexp.netapp.com">https://api.blueexp.netapp.com</a> <a href="https://netapp-cloud-account.auth0.com">https://netapp-cloud-account.auth0.com</a> <a href="https://netapp-cloud-account.us.auth0.com">https://netapp-cloud-account.us.auth0.com</a> <a href="https://console.netapp.com">https://console.netapp.com</a> <a href="https://components.console.blueexp.netapp.com">https://components.console.blueexp.netapp.com</a> <a href="https://cdn.auth0.com">https://cdn.auth0.com</a>	To provide features and services within the NetApp Console.

Endpoints	Purpose
<a href="https://bluexpinfraprod.eastus2.data.azurecr.io">https://bluexpinfraprod.eastus2.data.azurecr.io</a> <a href="https://bluexpinfraprod.azurecr.io">https://bluexpinfraprod.azurecr.io</a>	<p>To obtain images for Console agent upgrades.</p> <ul style="list-style-type: none"> <li>When you deploy a new agent, the validation check tests connectivity to current endpoints. If you use <a href="#">xref:./previous endpoints</a>, the validation check fails. To avoid this failure, skip the validation check.</li> </ul> <p>Although the previous endpoints are still supported, NetApp recommends updating your firewall rules to the current endpoints as soon as possible. <a href="#">Learn how to update your endpoint list.</a></p> <ul style="list-style-type: none"> <li>When you update to the current endpoints in your firewall, your existing agents will continue to work.</li> </ul>

### Endpoints contacted from the NetApp console

As you use the web-based NetApp 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 Console agent from the the Console.

[View the list of endpoints contacted from the NetApp 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 Console agent, unless you initiate it or if it 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, the Console automatically configures those systems to use a proxy server that's included with the Console agent. The only requirement is to ensure that the Console agent's security group allows inbound connections over port 3128. You'll need to open this port after you deploy the Console agent.

## Enable NTP

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

Implement this networking requirement after creating the Console agent.

## Step 2: Set up permissions to create the Console agent

Before you can deploy a Console agent from the Console, you need to set up permissions for the Google Platform user who deploys the Console agent VM.

### Steps

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

```
title: Console agent deployment policy
description: Permissions for the user who deploys the Console agent
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 Console agent from the Console or by using `gcloud`.

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

### Step 3: Set up permissions for the Console agent operations

A Google Cloud service account is required to provide the Console agent with the permissions that the

Console needs to manage resources in Google Cloud. When you create the Console agent, you'll need to associate this service account with the Console agent 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 Console agent](#).
  - 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 Console agent resides, then you'll need to provide the Console agent's service account with access to those projects.

For example, let's say the Console agent 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 Console agent's service account.
  - Select the Console agent's custom role.
  - Select **Save**.

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

## 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 agent	Custom	Service Project	<a href="#">Agent deployment policy</a>	compute.network User	Deploying the agent in the service project
agent service account	Custom	Service project	<a href="#">Agent service account policy</a>	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: NetApp Console service account as serviceAccount.user	N/A	(Optional) For NetApp Cloud Tiering and NetApp 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 the Console 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 the Console 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 the Console create them for you. The NetApp Console creates 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 the Console create them for you. These permissions reside in the Console 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 Cloud 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 Console agent 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 NetApp Backup and Recovery with customer-managed encryption keys (CMEK))

[Google Cloud documentation: Enabling APIs](#)

## Step 6: Create the Console agent

Create a Console agent directly from the Console.

### About this task

Creating the Console agent deploys a virtual machine instance in Google Cloud using a default configuration. Do not switch to a smaller VM instance with fewer CPUs or less RAM after creating the Console agent. [Learn about the default configuration for the Console agent.](#)

### Before you begin

You should have the following:

- The required Google Cloud permissions to create the Console agent and a service account for the Console agent VM.
- A VPC and subnet that meets networking requirements.
- Details about a proxy server, if a proxy is required for internet access from the Console agent.

### Steps

1. Select **Administration > Agents**.
2. On the **Overview** page, select **Deploy agent > Google Cloud**
3. On the **Deploying an agent** 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 Console agent:
  - 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 Console agent 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 "console-agent-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

5. Review your selections to verify that your set up is correct.

- The **Validate agent configuration** check box is marked by default to have the Console validate the network connectivity requirements when you deploy. If the Console fails to deploy the agent, it provides a report to help you troubleshoot. If the deployment succeeds, no report is provided.

If you are still using the [previous endpoints](#) used for agent upgrades, the validation fails with an error. To avoid this, unmark the check box to skip the validation check.

6. Select **Add**.

The instance is ready in approximately 10 minutes; stay on the page until the process completes.

### Result

After the process completes, the Console agent is available for use.



If the deployment fails, you can download a report and logs from the Console to help you fix the issues. [Learn how to troubleshoot installation issues.](#)

If you have Google Cloud Storage buckets in the same Google Cloud account where you created the Console agent, you'll see a Google Cloud Storage system appear on the **Systems** page automatically. [Learn how to manage Google Cloud Storage from the Console](#)

### Create a Console agent from Google Cloud

To create a Console agent in Google Cloud by using Google Cloud, you need to set up your networking, prepare Google Cloud permissions, enable Google Cloud APIs, and then create the Console agent.

#### Before you begin

- You should have a [understanding of Console agents](#).
- You should review [Console agent limitations](#).

### Step 1: Set up networking

Set up networking to enable the Console agent to manage resources and connect to target networks and the internet.



## VPC and subnet

When you create the Console agent, you need to specify the VPC and subnet where it should reside.

## Connections to target networks

The Console agent requires a network connection to the location where you're planning to create and manage systems. 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 Console agent must have an outbound internet connection to contact specific endpoints.

## Endpoints contacted from the Console agent

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

The endpoints listed below are all CNAME entries.

Endpoints	Purpose
<a href="https://www.googleapis.com/compute/v1/">https://www.googleapis.com/compute/v1/</a> <a href="https://compute.googleapis.com/compute/v1">https://compute.googleapis.com/compute/v1</a> <a href="https://cloudresourcemanager.googleapis.com/v1/projects">https://cloudresourcemanager.googleapis.com/v1/projects</a> <a href="https://www.googleapis.com/compute/beta">https://www.googleapis.com/compute/beta</a> <a href="https://storage.googleapis.com/storage/v1">https://storage.googleapis.com/storage/v1</a> <a href="https://www.googleapis.com/storage/v1">https://www.googleapis.com/storage/v1</a> <a href="https://iam.googleapis.com/v1">https://iam.googleapis.com/v1</a> <a href="https://cloudkms.googleapis.com/v1">https://cloudkms.googleapis.com/v1</a> <a href="https://www.googleapis.com/deploymentmanager/v2/projects">https://www.googleapis.com/deploymentmanager/v2/projects</a>	To manage resources in Google Cloud.
<a href="https://mysupport.netapp.com">https://mysupport.netapp.com</a>	To obtain licensing information and to send AutoSupport messages to NetApp support.
<a href="https://signin.b2c.netapp.com">https://signin.b2c.netapp.com</a>	To update NetApp Support Site (NSS) credentials or to add new NSS credentials to the NetApp Console.
<a href="https://api.blueexp.netapp.com">https://api.blueexp.netapp.com</a> <a href="https://netapp-cloud-account.auth0.com">https://netapp-cloud-account.auth0.com</a> <a href="https://netapp-cloud-account.us.auth0.com">https://netapp-cloud-account.us.auth0.com</a> <a href="https://console.netapp.com">https://console.netapp.com</a> <a href="https://components.console.blueexp.netapp.com">https://components.console.blueexp.netapp.com</a> <a href="https://cdn.auth0.com">https://cdn.auth0.com</a>	To provide features and services within the NetApp Console.

Endpoints	Purpose
<a href="https://bluexpinfraprod.eastus2.data.azurecr.io">https://bluexpinfraprod.eastus2.data.azurecr.io</a> <a href="https://bluexpinfraprod.azurecr.io">https://bluexpinfraprod.azurecr.io</a>	<p>To obtain images for Console agent upgrades.</p> <ul style="list-style-type: none"> <li>When you deploy a new agent, the validation check tests connectivity to current endpoints. If you use <a href="#">xref:./previous endpoints</a>, the validation check fails. To avoid this failure, skip the validation check.</li> </ul> <p>Although the previous endpoints are still supported, NetApp recommends updating your firewall rules to the current endpoints as soon as possible. <a href="#">Learn how to update your endpoint list.</a></p> <ul style="list-style-type: none"> <li>When you update to the current endpoints in your firewall, your existing agents will continue to work.</li> </ul>

### Endpoints contacted from the NetApp console

As you use the web-based NetApp 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 Console agent from the the Console.

[View the list of endpoints contacted from the NetApp 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 Console agent, unless you initiate it or if it 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, the Console automatically configures those systems to use a proxy server that's included with the Console agent. The only requirement is to ensure that the Console agent's security group allows inbound connections over port 3128. You'll need to open this port after you deploy the Console agent.

## Enable NTP

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

Implement this networking requirement after creating the Console agent.

## Step 2: Set up permissions to create the Console agent

Set up permissions for the Google Cloud user to deploy the Console agent VM from Google Cloud.

### Steps

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

```
title: Console agent deployment policy
description: Permissions for the user who deploys the NetApp Console agent
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 deploys the Console agent from Google Cloud.

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

### Step 3: Set up permissions for the Console agent operations

A Google Cloud service account is required to provide the Console agent with the permissions that the

Console needs to manage resources in Google Cloud. When you create the Console agent, you'll need to associate this service account with the Console agent 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 Console agent](#).
  - 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 Console agent resides, then you'll need to provide the Console agent's service account with access to those projects.

For example, let's say the Console agent 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 Console agent's service account.
  - Select the Console agent's custom role.
  - Select **Save**.

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

### 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 agent	Custom	Service Project	<a href="#">Agent deployment policy</a>	compute.network User	Deploying the agent in the service project
agent service account	Custom	Service project	<a href="#">Agent service account policy</a>	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: NetApp Console service account as serviceAccount.user	N/A	(Optional) For NetApp Cloud Tiering and NetApp 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 the Console 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 the Console 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 the Console create them for you. The NetApp Console creates 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 the Console create them for you. These permissions reside in the Console 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 Cloud 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

Enable several Google Cloud APIs before deploying the Console agent 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 NetApp Backup and Recovery with customer-managed encryption keys (CMEK))

[Google Cloud documentation: Enabling APIs](#)

## Step 6: Create the Console agent

Create a Console agent by using Google Cloud.

Creating the Console agent deploys a VM instance in Google Cloud with the default configuration. Do not switch to a smaller VM instance with fewer CPUs or less RAM after you create the Console agent. [Learn about the default configuration for the Console agent.](#)

### Before you begin

You should have the following:

- The required Google Cloud permissions to create the Console agent and a service account for the Console agent 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 Console agent is supported in Google Cloud on a VM instance with an OS that supports Shielded VM features.

### Steps

1. Log in to the Google Cloud SDK using your preferred method.

This example uses a local shell with the gcloud SDK installed, but you can also use the Google Cloud Shell.

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 Console agent instance

**network-path**

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

**subnet-path**

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

**kms-key-path**

(Optional) Add a KMS key to encrypt the Console agent'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 Console agent. The Console agent instance and software should be running in approximately five minutes.

4. Open a web browser and enter the Console agent host URL:

The Console host URL can be a localhost, a private IP address, or a public IP address, depending on the configuration of the host. For example, if the Console agent 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 Console agent host.

5. After you log in, set up the Console agent:

- a. Specify the Console organization to associate with the Console agent.

[Learn about identity and access management](#).

- b. Enter a name for the system.

**Result**

The Console agent is now installed and set up with your Console organization.

Open a web browser and go to the [NetApp Console](#) to start using the Console agent.

**Manually install the Console agent in Google Cloud**

To manually install the Console agent on your own Linux host, you need to review host requirements, set up your networking, prepare Google Cloud permissions, enable Google Cloud APIs, install the Console, and then provide the permissions that you prepared.

**Before you begin**

- You should have an [understanding of Console agents](#).
- You should review [Console agent limitations](#).

## Step 1: Review host requirements

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



The Console agent 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 agent installation will fail. NetApp recommends using a host that is free of third-party software to avoid conflicts.

### Dedicated host

The Console agent is not supported on a host that is shared with other applications. The host must be a dedicated host. The host can be of any architecture that meets the following size requirements:

- CPU: 8 cores or 8 vCPUs
- RAM: 32 GB
- Disk space: 165 GB is recommended for the host, with the following partition requirements:
  - `/opt`: 120 GiB of space must be available

The agent uses `/opt` to install the `/opt/application/netapp` directory and its contents.

- `/var`: 40 GiB of space must be available

The Console agent 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.

### Hypervisor

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

### Operating system and container requirements

The Console agent is supported with the following operating systems when using the Console in standard mode or restricted mode. A container orchestration tool is required before you install the agent.

Operating system	Supported OS versions	Supported agent versions	Required container tool	SELinux
Red Hat Enterprise Linux	9.1 to 9.4 8.6 to 8.10 <ul style="list-style-type: none"> <li>English language versions only.</li> <li>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 agent installation.</li> </ul>	3.9.50 or later with the Console in standard mode or restricted mode	Podman version 4.6.1 or 4.9.4  <a href="#">View Podman configuration requirements.</a>	Supported in enforcing mode or permissive mode <ul style="list-style-type: none"> <li>Management of Cloud Volumes ONTAP systems is NOT supported by agents that have SELinux enabled on the operating system.</li> </ul>
Ubuntu	24.04 LTS	3.9.45 or later with the NetApp Console in standard mode or restricted mode	Docker Engine 23.06 to 28.0.0.	Not supported
	22.04 LTS	3.9.50 or later	Docker Engine 23.0.6 to 28.0.0.	Not supported

### Google Cloud machine type

An instance type that meets the CPU and RAM requirements above. We recommend n2-standard-8.

The Console agent 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

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

### Disk space in /var

20 GiB of space must be available

The Console agent 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 installing the agent.

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

[View the supported Podman versions.](#)

- Docker Engine is required for Ubuntu.

[View the supported Docker Engine versions.](#)

### Example 3. Steps

#### Podman

Follow these steps to install and configure Podman:

- 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
- If using Red Hat Enterprise Linux 8, verify that your Podman version is using Aardvark DNS instead of CNI



Adjust the aardvark-dns port (default: 53) after installing the agent to avoid DNS port conflicts. 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.

You can obtain Podman 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 supported Podman versions](#).

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 supported Podman versions](#).

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.

6. If using Red Hat Enterprise:

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
```

7. 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.

8. If using Red Hat Enterprise Linux 8, verify that your Podman version is using NetAvark with Aardvark DNS instead of CNI.

a. Check to see if your networkBackend is set to CNI by running the following command:

```
podman info | grep networkBackend
```

b. If the networkBackend is set to CNI, you'll need to change it to netavark.

c. Install netavark and aardvark-dns using the following command:

```
dnf install aardvark-dns netavark
```

d. Open the `/etc/containers/containers.conf` file and modify the `network_backend` option to use "netavark" instead of "cni".

If `/etc/containers/containers.conf` doesn't exist, make the configuration changes to

```
/usr/share/containers/containers.conf.
```

9. Restart podman.

```
systemctl restart podman
```

10. Confirm networkBackend is now changed to "netavark" using the following command:

```
podman info | grep networkBackend
```

## Docker Engine

Follow the documentation from Docker to install Docker Engine.

### Steps

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

Follow the steps to install a supported Docker Engine version. Do not install the latest version, as it is unsupported by the Console.

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 Console agent 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

The Console agent requires a network connection to the location where you're planning to create and manage systems. 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 Console agent must have an outbound internet connection to contact specific endpoints.

### Endpoints contacted from computers when using the web-based NetApp Console

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

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

### Endpoints contacted from the Console agent

The Console agent requires outbound internet access to contact the following endpoints to manage

resources and processes within your public cloud environment for day-to-day operations.

The endpoints listed below are all CNAME entries.

Endpoints	Purpose
<a href="https://www.googleapis.com/compute/v1/">https://www.googleapis.com/compute/v1/</a> <a href="https://compute.googleapis.com/compute/v1">https://compute.googleapis.com/compute/v1</a> <a href="https://cloudresourcemanager.googleapis.com/v1/projects">https://cloudresourcemanager.googleapis.com/v1/projects</a> <a href="https://www.googleapis.com/compute/beta">https://www.googleapis.com/compute/beta</a> <a href="https://storage.googleapis.com/storage/v1">https://storage.googleapis.com/storage/v1</a> <a href="https://www.googleapis.com/storage/v1">https://www.googleapis.com/storage/v1</a> <a href="https://iam.googleapis.com/v1">https://iam.googleapis.com/v1</a> <a href="https://cloudkms.googleapis.com/v1">https://cloudkms.googleapis.com/v1</a> <a href="https://www.googleapis.com/deploymentmanager/v2/projects">https://www.googleapis.com/deploymentmanager/v2/projects</a>	To manage resources in Google Cloud.
<a href="https://mysupport.netapp.com">https://mysupport.netapp.com</a>	To obtain licensing information and to send AutoSupport messages to NetApp support.
<a href="https://signin.b2c.netapp.com">https://signin.b2c.netapp.com</a>	To update NetApp Support Site (NSS) credentials or to add new NSS credentials to the NetApp Console.
<a href="https://api.blueexp.netapp.com">https://api.blueexp.netapp.com</a> <a href="https://netapp-cloud-account.auth0.com">https://netapp-cloud-account.auth0.com</a> <a href="https://netapp-cloud-account.us.auth0.com">https://netapp-cloud-account.us.auth0.com</a> <a href="https://console.netapp.com">https://console.netapp.com</a> <a href="https://components.console.blueexp.netapp.com">https://components.console.blueexp.netapp.com</a> <a href="https://cdn.auth0.com">https://cdn.auth0.com</a>	To provide features and services within the NetApp Console.
<a href="https://blueexpinfraprod.eastus2.data.azurecr.io">https://blueexpinfraprod.eastus2.data.azurecr.io</a> <a href="https://blueexpinfraprod.azurecr.io">https://blueexpinfraprod.azurecr.io</a>	<p>To obtain images for Console agent upgrades.</p> <ul style="list-style-type: none"><li>When you deploy a new agent, the validation check tests connectivity to current endpoints. If you use <a href="#">xref:./previous endpoints</a>, the validation check fails. To avoid this failure, skip the validation check.</li></ul> <p>Although the previous endpoints are still supported, NetApp recommends updating your firewall rules to the current endpoints as soon as possible. <a href="#">Learn how to update your endpoint list.</a></p> <ul style="list-style-type: none"><li>When you update to the current endpoints in your firewall, your existing agents will continue to work.</li></ul>

## 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 Console agent, unless you initiate it or if it 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, the Console automatically configures those systems to use a proxy server that's included with the Console agent. The only requirement is to ensure that the Console agent's security group allows inbound connections over port 3128. You'll need to open this port after you deploy the Console agent.

## Enable NTP

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

## Step 4: Set up permissions for the Console agent

A Google Cloud service account is required to provide the Console agent with the permissions that the Console needs to manage resources in Google Cloud. When you create the Console agent, you'll need to associate this service account with the Console agent 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 Console agent](#).
  - 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 Console agent resides, then you'll need to provide the Console agent's service account with access to those projects.

For example, let's say the Console agent 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 Console agent's service account.
  - Select the Console agent's custom role.
  - Select **Save**.

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

## 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 agent	Custom	Service Project	<a href="#">Agent deployment policy</a>	compute.network User	Deploying the agent in the service project
agent service account	Custom	Service project	<a href="#">Agent service account policy</a>	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: NetApp Console service account as serviceAccount.user	N/A	(Optional) For NetApp Cloud Tiering and NetApp 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 the Console 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 the Console 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 the Console create them for you. The NetApp Console creates 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 the Console create them for you. These permissions reside in the Console 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 Cloud 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 NetApp Backup and Recovery with customer-managed encryption keys (CMEK))

[Google Cloud documentation: Enabling APIs](#)

## Step 7: Install the Console agent

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

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

- 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 Console agent. If you need to set a certificate for a transparent proxy server, you must use the Maintenance Console after installation. Learn more about the [Agent Maintenance Console](#).

### About this task

The installer that is available on the NetApp Support Site might be an earlier version. After installation, the Console agent 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 fails.

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

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

3. Assign permissions to run the script.

```
chmod +x NetApp_Console_Agent_Cloud_<version>
```

Where <version> is the version of the Console agent that you downloaded.

4. If installing in a Government Cloud environment, disable the configuration checks. [Learn how to disable configuration checks for manual installations.](#)

5. Run the installation script.

```
./NetApp_Console_Agent_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:

```
./NetApp_Console_Agent_Cloud_v4.0.0--proxy  
https://user:password@10.0.0.30:8080/ --cacert  
/tmp/cacert/certificate.cer
```

--proxy configures the Console agent 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.
- The Console agent 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 Console agent 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 Console agent host:

+

```
./NetApp_Console_Agent_Cloud_v4.0.0 --cacert /tmp/cacert/certificate.cer
```

1. If you used Podman, you'll need to adjust the aardvark-dns port.
  - a. SSH to the Console agent 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 Console agent virtual machine.
2. Wait for the installation to complete.

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



If the installation fails, you can view the installation report and logs to help you fix the issues.  
[Learn how to troubleshoot installation issues.](#)

1. Open a web browser from a host that has a connection to the Console agent virtual machine and enter the following URL:

`https://ipaddress`

2. After you log in, set up the Console agent:
  - a. Specify the organization to associate with the Console agent.

- 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 the Console in standard mode. You should enable restricted mode only if you have a secure environment and want to disconnect this account from backend services. If that's the case, [follow steps to get started with the NetApp Console in restricted mode](#).

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



If the installation fails, you can view logs and a report to help you troubleshoot. [Learn how to troubleshoot installation issues](#).

If you have Google Cloud Storage buckets in the same Google Cloud account where you created the Console agent, you'll see a Google Cloud Storage system appear on the **Systems** page automatically. [Learn how to manage Google Cloud Storage from the NetApp Console](#)

## Step 8: Provide permissions to Console agent

You need to provide the Console agent with the Google Cloud permissions that you previously set up. Providing the permissions enables the Console agent 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 Console agent 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 Console agent role to that project. You'll need to repeat this step for each project.

## Install an agent on-premises

### Manually install a Console agent on-premises

Install a Console agent on-premises and then log in and set it up to work with your Console organization.



If you are a VMWare user, you can use an OVA to install a Console agent in your VCenter. [Learn more about installing an agent in a VCenter](#).

Before you install, you'll need to ensure your host (VM or Linux host) meets requirements and ensure that the Console agent will have outbound access to the internet as well as targeted networks. If you plan to NetApp data services, or cloud storage options such as Cloud Volumes ONTAP, you'll need to create credentials in your cloud provider to add to the Console so that the Console agent can perform actions in the cloud on your behalf.

## Prepare to install the Console agent

Before you install a Console agent, you should ensure you have a host machine that meets installation requirements. You'll also need to work with your network administrator to ensure that the Console agent has outbound access to required endpoints and connections to targeted networks.

## Review Console agent host requirements

Run the Console agent on a x86 host that meets operating system, RAM, and port requirements. Ensure that your host meets these requirements before you install the Console agent.



The Console agent 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 agent installation will fail. NetApp recommends using a host that is free of third-party software to avoid conflicts.

### Dedicated host

The Console agent is not supported on a host that is shared with other applications. The host must be a dedicated host. The host can be of any architecture that meets the following size requirements:

- CPU: 8 cores or 8 vCPUs
- RAM: 32 GB
- Disk space: 165 GB is recommended for the host, with the following partition requirements:
  - `/opt`: 120 GiB of space must be available

The agent uses `/opt` to install the `/opt/application/netapp` directory and its contents.

- `/var`: 40 GiB of space must be available

The Console agent 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.

### Hypervisor

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

### Operating system and container requirements

The Console agent is supported with the following operating systems when using the Console in standard mode or restricted mode. A container orchestration tool is required before you install the agent.



Operating system	Supported OS versions	Supported agent versions	Required container tool	SELinux
Red Hat Enterprise Linux	9.1 to 9.4 8.6 to 8.10 <ul style="list-style-type: none"> <li>English language versions only.</li> <li>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 agent installation.</li> </ul>	3.9.50 or later with the Console in standard mode or restricted mode	Podman version 4.6.1 or 4.9.4  <a href="#">View Podman configuration requirements.</a>	Supported in enforcing mode or permissive mode <ul style="list-style-type: none"> <li>Management of Cloud Volumes ONTAP systems is NOT supported by agents that have SELinux enabled on the operating system.</li> </ul>
Ubuntu	24.04 LTS	3.9.45 or later with the NetApp Console in standard mode or restricted mode	Docker Engine 23.06 to 28.0.0.	Not supported
	22.04 LTS	3.9.50 or later	Docker Engine 23.0.6 to 28.0.0.	Not supported

## Set up network access for the Console agent

Set up network access to ensure the Console agent can manage resources. It needs connections to target networks and outbound internet access to specific endpoints.

### Connections to target networks

The Console agent requires a network connection to the location where you're planning to create and manage systems. 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 Console agent must have an outbound internet connection to contact specific endpoints.

### Endpoints contacted from computers when using the web-based NetApp Console

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

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

### Endpoints contacted from the Console agent

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

The endpoints listed below are all CNAME entries.



A Console agent installed on your premises cannot manage resources in Google Cloud. If you want to manage Google Cloud resources, you need to install an agent in Google Cloud.

## AWS

When the Console agent is installed on-premises, it needs network access to the following AWS endpoints in order to manage NetApp systems (such as Cloud Volumes ONTAP) deployed in AWS.

### Endpoints contacted from the Console agent

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

The endpoints listed below are all CNAME entries.

Endpoints	Purpose
AWS services (amazonaws.com): <ul style="list-style-type: none"><li>• CloudFormation</li><li>• Elastic Compute Cloud (EC2)</li><li>• Identity and Access Management (IAM)</li><li>• Key Management Service (KMS)</li><li>• Security Token Service (STS)</li><li>• Simple Storage Service (S3)</li></ul>	To manage AWS resources. The endpoint depends on your AWS region. <a href="#">Refer to AWS documentation for details</a>
https://mysupport.netapp.com	To obtain licensing information and to send AutoSupport messages to NetApp support.
https://signin.b2c.netapp.com	To update NetApp Support Site (NSS) credentials or to add new NSS credentials to the NetApp Console.
https://api.bluelxp.netapp.com https://netapp-cloud-account.auth0.com https://netapp-cloud-account.us.auth0.com https://console.netapp.com https://components.console.bluelxp.netapp.com https://cdn.auth0.com	To provide features and services within the NetApp Console.

Endpoints	Purpose
<a href="https://bluexpinfraprod.eastus2.data.azurecr.io">https://bluexpinfraprod.eastus2.data.azurecr.io</a> <a href="https://bluexpinfraprod.azurecr.io">https://bluexpinfraprod.azurecr.io</a>	<p>To obtain images for Console agent upgrades.</p> <ul style="list-style-type: none"> <li>When you deploy a new agent, the validation check tests connectivity to current endpoints. If you use xref:./previous endpoints, the validation check fails. To avoid this failure, skip the validation check.</li> </ul> <p>Although the previous endpoints are still supported, NetApp recommends updating your firewall rules to the current endpoints as soon as possible. <a href="#">Learn how to update your endpoint list.</a></p> <ul style="list-style-type: none"> <li>When you update to the current endpoints in your firewall, your existing agents will continue to work.</li> </ul>

## Azure

When the Console agent is installed on-premises, it needs network access to the following Azure endpoints in order to manage NetApp systems (such as Cloud Volumes ONTAP) deployed in Azure.

Endpoints	Purpose
<a href="https://management.azure.com">https://management.azure.com</a> <a href="https://login.microsoftonline.com">https://login.microsoftonline.com</a> <a href="https://blob.core.windows.net">https://blob.core.windows.net</a> <a href="https://core.windows.net">https://core.windows.net</a>	To manage resources in Azure public regions.
<a href="https://management.chinacloudapi.cn">https://management.chinacloudapi.cn</a> <a href="https://login.chinacloudapi.cn">https://login.chinacloudapi.cn</a> <a href="https://blob.core.chinacloudapi.cn">https://blob.core.chinacloudapi.cn</a> <a href="https://core.chinacloudapi.cn">https://core.chinacloudapi.cn</a>	To manage resources in Azure China regions.
<a href="https://mysupport.netapp.com">https://mysupport.netapp.com</a>	To obtain licensing information and to send AutoSupport messages to NetApp support.
<a href="https://signin.b2c.netapp.com">https://signin.b2c.netapp.com</a>	To update NetApp Support Site (NSS) credentials or to add new NSS credentials to the NetApp Console.
<a href="https://api.bluexp.netapp.com">https://api.bluexp.netapp.com</a> <a href="https://netapp-cloud-account.auth0.com">https://netapp-cloud-account.auth0.com</a> <a href="https://netapp-cloud-account.us.auth0.com">https://netapp-cloud-account.us.auth0.com</a> <a href="https://console.netapp.com">https://console.netapp.com</a> <a href="https://components.console.bluexp.netapp.com">https://components.console.bluexp.netapp.com</a> <a href="https://cdn.auth0.com">https://cdn.auth0.com</a>	To provide features and services within the NetApp Console.

Endpoints	Purpose
<a href="https://bluexpinfraprod.eastus2.data.azurecr.io">https://bluexpinfraprod.eastus2.data.azurecr.io</a> <a href="https://bluexpinfraprod.azurecr.io">https://bluexpinfraprod.azurecr.io</a>	<p>To obtain images for Console agent upgrades.</p> <ul style="list-style-type: none"> <li>When you deploy a new agent, the validation check tests connectivity to current endpoints. If you use xref:./previous endpoints, the validation check fails. To avoid this failure, skip the validation check.</li> </ul> <p>Although the previous endpoints are still supported, NetApp recommends updating your firewall rules to the current endpoints as soon as possible. <a href="#">Learn how to update your endpoint list.</a></p> <ul style="list-style-type: none"> <li>When you update to the current endpoints in your firewall, your existing agents will continue to work.</li> </ul>

## 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 Console agent, unless you initiate it or if it 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, the Console automatically configures those systems to use a proxy server that's included with the Console agent. The only requirement is to ensure that the Console agent's security group allows inbound connections over port 3128. You'll need to open this port after you deploy the Console agent.

## Enable NTP

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

## Create Console agent cloud permissions for AWS or Azure

If you want to use NetApp data services in AWS or Azure with an on-premises Console agent, then you need to set up permissions in your cloud provider and then you add the credentials to the Console agent after you install it.



You must install the Console agent in Google Cloud to manage any resources that reside there.

## AWS

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

You must use this authentication method if the Console agent 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 Console agent](#).
  - c. Finish the remaining steps to create the policy.

Depending on the NetApp data 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 Console agent](#).

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 the NetApp Console after you install the Console agent.

### Result

You should now have access keys for an IAM user who has the required permissions. After you install the Console agent, associate these credentials with the Console agent from the Console.

## Azure

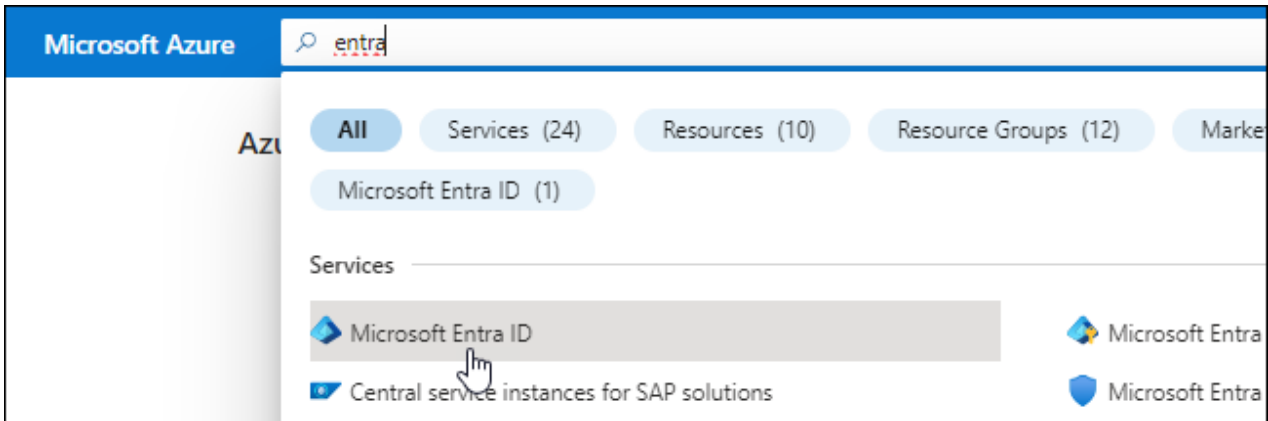
When the Console agent is installed on-premises, you need to provide the Console agent with Azure permissions by setting up a service principal in Microsoft Entra ID and obtaining the Azure credentials that the Console agent needs.

### 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 the NetApp Console).
  - **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 Console agent](#) 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

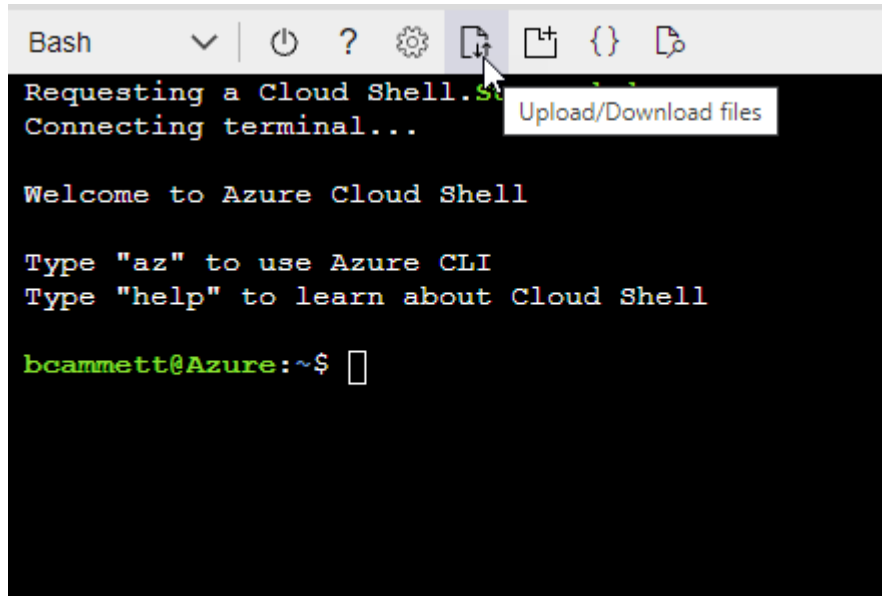
```
"AssignableScopes": [
  "/subscriptions/d333af45-0d07-4154-943d-c25fbzzzzzzz",
  "/subscriptions/54b91999-b3e6-4599-908e-416e0zzzzzzz",
  "/subscriptions/398e471c-3b42-4ae7-9b59-ce5bbzzzzzzz"
```

- 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 Console Operator that you can assign to the Console agent 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 **Console 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 Console agent.

If you want to deploy Cloud Volumes ONTAP from multiple Azure subscriptions, then you must bind the service principal to each of those subscriptions. In the NetApp Console, you can 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

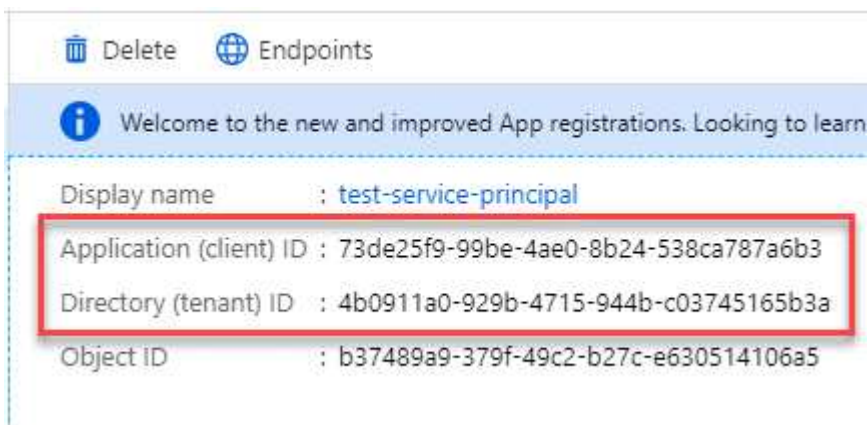


user\_impersonation

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 the Console, you need to provide the application (client) ID and the directory (tenant) ID for the application. The Console 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	

## Manually install a Console agent

When you manually install a Console agent, you need to prepare your machine environment so that it meets requirements. You'll need an Linux machine and you'll need to install Podman or Docker, depending on your Linux operating system.

### Install Podman or Docker Engine

Depending on your operating system, either Podman or Docker Engine is required before installing the agent.

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

[View the supported Podman versions.](#)

- Docker Engine is required for Ubuntu.

[View the supported Docker Engine versions.](#)

## Example 4. Steps

### Podman

Follow these steps to install and configure Podman:

- 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
- If using Red Hat Enterprise Linux 8, verify that your Podman version is using Aardvark DNS instead of CNI



Adjust the aardvark-dns port (default: 53) after installing the agent to avoid DNS port conflicts. 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.

You can obtain Podman 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 supported Podman versions](#).

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 supported Podman versions](#).

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.

6. If using Red Hat Enterprise:

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
```

7. 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.

8. If using Red Hat Enterprise Linux 8, verify that your Podman version is using NetAvark with Aardvark DNS instead of CNI.

a. Check to see if your networkBackend is set to CNI by running the following command:

```
podman info | grep networkBackend
```

b. If the networkBackend is set to CNI, you'll need to change it to netavark.

c. Install netavark and aardvark-dns using the following command:

```
dnf install aardvark-dns netavark
```

d. Open the `/etc/containers/containers.conf` file and modify the `network_backend` option to use "netavark" instead of "cni".

If `/etc/containers/containers.conf` doesn't exist, make the configuration changes to

```
/usr/share/containers/containers.conf.
```

#### 9. Restart podman.

```
systemctl restart podman
```

#### 10. Confirm networkBackend is now changed to "netavark" using the following command:

```
podman info | grep networkBackend
```

### Docker Engine

Follow the documentation from Docker to install Docker Engine.

#### Steps

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

Follow the steps to install a supported Docker Engine version. Do not install the latest version, as it is unsupported by the Console.

##### 2. Verify that Docker is enabled and running.

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

### Install the Console agent manually

Download and install the Console agent software on an existing Linux host on-premises.

#### Before you begin

You should have the following:

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

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

- 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 Console agent. If you need to set a certificate for a transparent proxy server, you must use the Maintenance Console after installation. Learn more about the [Agent Maintenance Console](#).

#### About this task

The installer that is available on the NetApp Support Site might be an earlier version. After installation, the Console agent 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 fails.

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

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

3. Assign permissions to run the script.

```
chmod +x NetApp_Console_Agent_Cloud_<version>
```

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

4. If installing in a Government Cloud environment, disable the configuration checks. [Learn how to disable configuration checks for manual installations.](#)
5. Run the installation script.

```
./NetApp_Console_Agent_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:

```
./NetApp_Console_Agent_Cloud_v4.0.0--proxy
https://user:password@10.0.0.30:8080/ --cacert
/tmp/cacert/certificate.cer
```

`--proxy` configures the Console agent 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.
- The Console agent 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 Console agent 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 Console agent host:

+

```
./NetApp_Console_Agent_Cloud_v4.0.0 --cacert /tmp/cacert/certificate.cer
```

1. If you used Podman, you'll need to adjust the aardvark-dns port.
  - a. SSH to the Console agent 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 Console agent virtual machine.

### What's next?

You'll need to register the Console agent within the NetApp Console.

## Register the Console agent with NetApp Console

Log into the Console and associate the Console agent with your organization. How you log in depends on the mode in which you are using Console. If you are using the Console in standard mode, you log in through the SaaS website. If you are using the Console in restricted mode, you log in locally from the Console agent host.

### Steps

1. Open a web browser and enter the Console agent host URL:

The Console host URL can be a localhost, a private IP address, or a public IP address, depending on the configuration of the host. For example, if the Console agent 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 Console agent host.

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

Restricted mode isn't supported when the Console agent is installed on-premises.

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

## Provide cloud provider credentials to NetApp Console

After you install and set up the Console agent, add your cloud credentials so that the Console agent 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 the Console.

### Steps

1. Select **Administration > Credentials**.
2. Select **Organization credentials**.
3. Select **Add Credentials** and follow the steps in the wizard.
  - a. **Credentials Location**: Select \*Amazon Web Services > Agent.
  - 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**.

You can now go to the [NetApp Console](#) to start using the Console agent.

## 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 the Console agent.

### Steps

1. Select **Administration > Credentials**.
2. Select **Add Credentials** and follow the steps in the wizard.
  - a. **Credentials Location**: Select **Microsoft Azure > Agent**.
  - 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

The Console agent now has the permissions that it needs to perform actions in Azure on your behalf. You can now go to the [NetApp Console](#) to start using the Console agent.

## Install a Console agent on-premises using VCenter

If you are a VMWare user, you can use an OVA to install a Console agent in your VCenter. The OVA download or URL is available through the NetApp Console.



When you install a Console agent with your vCenter tools, you can use the VM web console to perform maintenance tasks. [Learn more about the VM console for the agent.](#)

## Prepare to install the Console agent

Before installation, make sure your VM host meets the requirements and the Console agent can access the internet and targeted networks. To use NetApp data services or Cloud Volumes ONTAP, create cloud provider credentials for the Console agent to perform actions on your behalf.

## Review Console agent host requirements

Make sure your host machine meets installation requirements before installing the Console agent.



Install the agent in a vCenter environment rather than directly on an ESXi host.

## Set up network access for the Console agent

Work with your network administrator to ensure the Console agent has outbound access to the required endpoints and connections to targeted networks.

## Connections to target networks

The Console agent requires a network connection to the location where you're planning to create and manage systems. 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 Console agent must have an outbound internet connection to contact specific endpoints.

## Endpoints contacted from computers when using the web-based NetApp Console

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

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

## Endpoints contacted from the Console agent

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

The endpoints listed below are all CNAME entries.



You can't manage resources in Google Cloud with an Console agent installed on your premises. To manage Google Cloud resources, install an agent in Google Cloud.

## AWS

When the Console agent is installed on-premises, it needs network access to the following AWS endpoints in order to manage NetApp systems (such as Cloud Volumes ONTAP) deployed in AWS.

### Endpoints contacted from the Console agent

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

The endpoints listed below are all CNAME entries.

Endpoints	Purpose
AWS services (amazonaws.com): <ul style="list-style-type: none"><li>• CloudFormation</li><li>• Elastic Compute Cloud (EC2)</li><li>• Identity and Access Management (IAM)</li><li>• Key Management Service (KMS)</li><li>• Security Token Service (STS)</li><li>• Simple Storage Service (S3)</li></ul>	To manage AWS resources. The endpoint depends on your AWS region. <a href="#">Refer to AWS documentation for details</a>
https://mysupport.netapp.com	To obtain licensing information and to send AutoSupport messages to NetApp support.
https://signin.b2c.netapp.com	To update NetApp Support Site (NSS) credentials or to add new NSS credentials to the NetApp Console.
https://api.bluexp.netapp.com https://netapp-cloud-account.auth0.com https://netapp-cloud-account.us.auth0.com https://console.netapp.com https://components.console.bluexp.netapp.com https://cdn.auth0.com	To provide features and services within the NetApp Console.

Endpoints	Purpose
<a href="https://bluexpinfraprod.eastus2.data.azurecr.io">https://bluexpinfraprod.eastus2.data.azurecr.io</a> <a href="https://bluexpinfraprod.azurecr.io">https://bluexpinfraprod.azurecr.io</a>	<p>To obtain images for Console agent upgrades.</p> <ul style="list-style-type: none"> <li>When you deploy a new agent, the validation check tests connectivity to current endpoints. If you use xref:./previous endpoints, the validation check fails. To avoid this failure, skip the validation check.</li> </ul> <p>Although the previous endpoints are still supported, NetApp recommends updating your firewall rules to the current endpoints as soon as possible. <a href="#">Learn how to update your endpoint list.</a></p> <ul style="list-style-type: none"> <li>When you update to the current endpoints in your firewall, your existing agents will continue to work.</li> </ul>

## Azure

When the Console agent is installed on-premises, it needs network access to the following Azure endpoints in order to manage NetApp systems (such as Cloud Volumes ONTAP) deployed in Azure.

Endpoints	Purpose
<a href="https://management.azure.com">https://management.azure.com</a> <a href="https://login.microsoftonline.com">https://login.microsoftonline.com</a> <a href="https://blob.core.windows.net">https://blob.core.windows.net</a> <a href="https://core.windows.net">https://core.windows.net</a>	To manage resources in Azure public regions.
<a href="https://management.chinacloudapi.cn">https://management.chinacloudapi.cn</a> <a href="https://login.chinacloudapi.cn">https://login.chinacloudapi.cn</a> <a href="https://blob.core.chinacloudapi.cn">https://blob.core.chinacloudapi.cn</a> <a href="https://core.chinacloudapi.cn">https://core.chinacloudapi.cn</a>	To manage resources in Azure China regions.
<a href="https://mysupport.netapp.com">https://mysupport.netapp.com</a>	To obtain licensing information and to send AutoSupport messages to NetApp support.
<a href="https://signin.b2c.netapp.com">https://signin.b2c.netapp.com</a>	To update NetApp Support Site (NSS) credentials or to add new NSS credentials to the NetApp Console.
<a href="https://api.bluexp.netapp.com">https://api.bluexp.netapp.com</a> <a href="https://netapp-cloud-account.auth0.com">https://netapp-cloud-account.auth0.com</a> <a href="https://netapp-cloud-account.us.auth0.com">https://netapp-cloud-account.us.auth0.com</a> <a href="https://console.netapp.com">https://console.netapp.com</a> <a href="https://components.console.bluexp.netapp.com">https://components.console.bluexp.netapp.com</a> <a href="https://cdn.auth0.com">https://cdn.auth0.com</a>	To provide features and services within the NetApp Console.

Endpoints	Purpose
<a href="https://bluexpinfraprod.eastus2.data.azurecr.io">https://bluexpinfraprod.eastus2.data.azurecr.io</a> <a href="https://bluexpinfraprod.azurecr.io">https://bluexpinfraprod.azurecr.io</a>	<p>To obtain images for Console agent upgrades.</p> <ul style="list-style-type: none"> <li>When you deploy a new agent, the validation check tests connectivity to current endpoints. If you use xref:./previous endpoints, the validation check fails. To avoid this failure, skip the validation check.</li> </ul> <p>Although the previous endpoints are still supported, NetApp recommends updating your firewall rules to the current endpoints as soon as possible. <a href="#">Learn how to update your endpoint list.</a></p> <ul style="list-style-type: none"> <li>When you update to the current endpoints in your firewall, your existing agents will continue to work.</li> </ul>

## 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 Console agent, unless you initiate it or if it 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, the Console automatically configures those systems to use a proxy server that's included with the Console agent. The only requirement is to ensure that the Console agent's security group allows inbound connections over port 3128. You'll need to open this port after you deploy the Console agent.

## Enable NTP

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



## Create Console agent cloud permissions for AWS or Azure

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



You can't manage resources in Google Cloud with a Console agent installed on your premises. If you want to manage Google Cloud resources, you need to install an agent in Google Cloud.

## AWS

For on-premises Console agents, provide AWS permissions by adding IAM user access keys.

Use IAM user access keys for on-premises Console agents; IAM roles are not supported for on-premises Console agents.

### 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 Console agent](#).
  - c. Finish the remaining steps to create the policy.

Depending on the NetApp data 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 Console agent](#).

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 the NetApp Console after you install the Console agent.

### Result

You should now have IAM user access keys with the required permissions. After you install the Console agent, associate these credentials with the Console agent from the Console.

## Azure

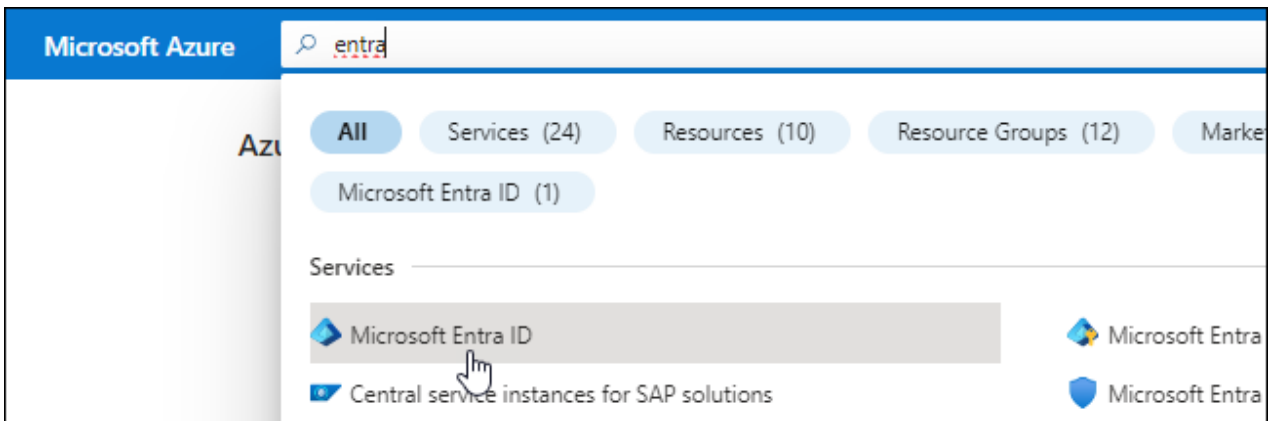
When the Console agent is installed on-premises, you need to give the Console agent Azure permissions by setting up a service principal in Microsoft Entra ID and getting the Azure credentials that the Console agent needs.

### 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 the NetApp Console).
  - **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 Console agent](#) 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.

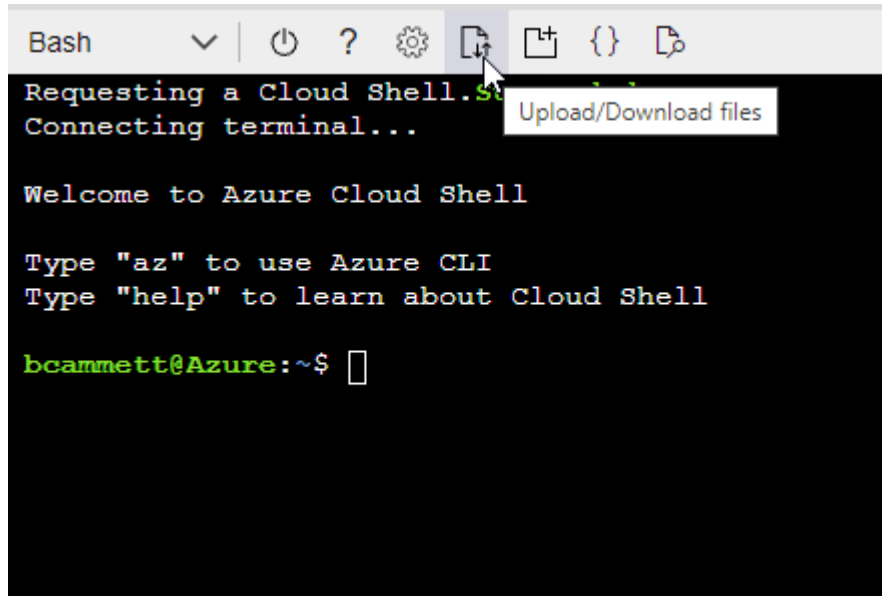
#### Example

```
"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 Console Operator that you can assign to the Console agent 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 **Console 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 Console agent.

If you want to deploy Cloud Volumes ONTAP from multiple Azure subscriptions, then you must bind the service principal to each of those subscriptions. In the NetApp Console, you can 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

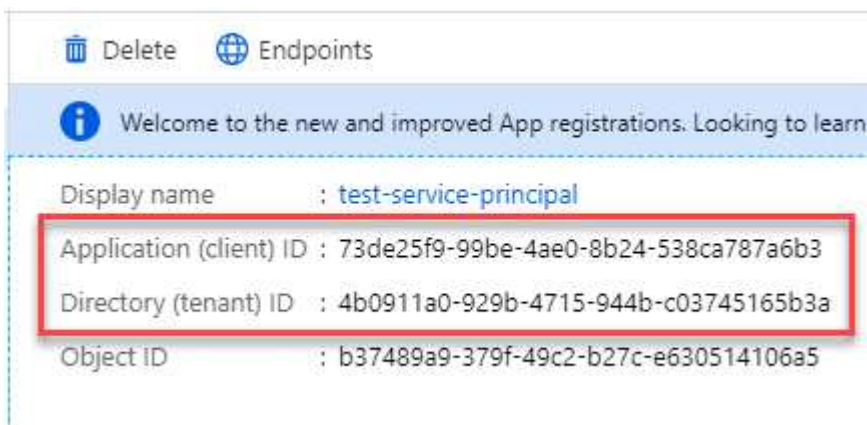


user\_impersonation

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 the Console, you need to provide the application (client) ID and the directory (tenant) ID for the application. The Console 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

Install a Console agent in your VCenter environment

NetApp supports installing the Console agent in your VCenter environment. The OVA file includes a pre-configured VM image that you can deploy in your VMware environment. A file download or URL deployment is available directly from the NetApp Console. It includes the Console agent software and a self-signed certificate.

Download the OVA or copy the URL

Download the OVA or copy the OVA URL directly from the NetApp Console.

- 1. Select **Administration > Agents**.
- 2. On the **Overview** page, select **Deploy agent > On-Premises**.
- 3. Select **With OVA**.
- 4. Choose to either download the OVA or copy the URL to use in VCenter.

Deploy the agent in your VCenter

Log into your VCenter environment to deploy the agent.

Steps

- 1. Upload the self-signed certificate to your trusted certificates if your environment requires it. You replace this certificate after installation.[Learn how to replace the self-signed certificate.](#)
- 2. Deploy the OVA from the content library or local system.

From the local system	From the content library
a. Right-click and select <b>Deploy OVF template....</b>	a. Go to your content library and select the Console agent OVA.
b. Choose the OVA file from the URL or browse to its location, then select <b>Next</b> .	b. Select <b>Actions &gt; New VM from this template</b>

- 3. Complete the Deploy OVF Template wizard to deploy the Console agent.
- 4. Select a name and folder for the VM, then select **Next**.
- 5. Select a compute resource, then select **Next**.
- 6. Review the details of the template, then select **Next**.
- 7. Accept the license agreement, then select **Next**.
- 8. Choose the type of proxy configuration you want to use: explicit proxy, transparent proxy, or no proxy.



9. Select the datastore where you want to deploy the VM, then select **Next**. Be sure it meets host requirements.
10. Select the network to which you want to connect the VM, then select **Next**. Ensure the network is IPv4 and has outbound internet access to the required endpoints.
11. In the **Customize template** window, complete the following fields:
  - **Proxy information**
    - If you selected explicit proxy, enter the proxy server hostname or IP address and port number, as well as the username, password.
    - If you selected transparent proxy, upload the respective certificate.
  - **Virtual Machine Configuration**
    - **Skip config check:** This check box is unchecked by default which means the agent runs a configuration check to validate network access.
      - NetApp recommends leaving this box unchecked so that the installation includes a configuration check of the agent. The Configuration check validates that the agent has network access to the required endpoints. If deployment fails because of connectivity issues, you can access the validation report and logs from the agent host. In some cases, if you are confident that the agent has network access, you can choose to skip the check. For example, if you are still using the [previous endpoints](#) used for agent upgrades, the validation fails with an error. To avoid this, mark the check box to install without a validation check. [Learn how to update your endpoint list](#).
    - **Maintenance password:** Set the password for the `maint` user that allows access to the agent maintenance console.
    - **NTP servers:** Specify one or more NTP servers for time synchronization.
    - **Hostname:** Set the hostname for this VM. It must not include the search domain. For example, an FQDN of `console10.searchdomain.company.com` should be entered as `console10`.
    - **Primary DNS:** Specify the primary DNS server to use for name resolution.
    - **Secondary DNS:** Specify the secondary DNS server to use for name resolution.
    - **Search domains:** Specify the search domain name to use when resolving the hostname. For example, if the FQDN is `console10.searchdomain.company.com`, then enter `searchdomain.company.com`.
    - **IPv4 address:** The IP address that is mapped to the hostname.
    - **IPv4 subnet mask:** The subnet mask for the IPv4 address.
    - **IPv4 gateway address:** The gateway address for the IPv4 address.
12. Select **Next**.
13. Review the details in the **Ready to complete** window, select **Finish**.

The vSphere task bar shows the progress as the Console agent is deployed.

14. Power on the VM.



If the deployment fails, you can access the validation report and logs from the agent host. [Learn how to troubleshoot installation issues](#).

## Register the Console agent with NetApp Console

Log into the Console and associate the Console agent with your organization. How you log in depends on the mode in which you are using Console. If you are using the Console in standard mode, you log in through the SaaS website. If you are using the Console in restricted or private mode, you log in locally from the Console agent host.

### Steps

1. Open a web browser and enter the Console agent host URL:

The Console host URL can be a localhost, a private IP address, or a public IP address, depending on the configuration of the host. For example, if the Console agent 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 Console agent host.

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

Restricted mode isn't supported when the Console agent is installed on-premises.

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

## Add cloud provider credentials to the Console

After you install and set up the Console agent, add your cloud credentials so that the Console agent 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 the Console.

### Steps

1. Select **Administration > Credentials**.
2. Select **Organization credentials**.
3. Select **Add Credentials** and follow the steps in the wizard.
  - a. **Credentials Location**: Select \*Amazon Web Services > Agent.
  - 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**.

You can now go to the [NetApp Console](#) to start using the Console agent.

## 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 the Console agent.

### Steps

1. Select **Administration > Credentials**.
2. Select **Add Credentials** and follow the steps in the wizard.
  - a. **Credentials Location**: Select **Microsoft Azure > Agent**.
  - 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

The Console agent now has the permissions that it needs to perform actions in Azure on your behalf. You can now go to the [NetApp Console](#) to start using the Console agent.

## 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:

- NetApp Backup and Recovery
- Cloud Volumes ONTAP
- NetApp Cloud Tiering
- NetApp Ransomware Resilience
- NetApp Disaster Recovery

NetApp Data Classification is enabled through your subscription, but there is no charge for using classification.

**Before you begin**

You must have already deployed a Console agent in order to subscribe to data services. You need to associate a marketplace subscription to the cloud credentials connected to a Console agent.

## AWS

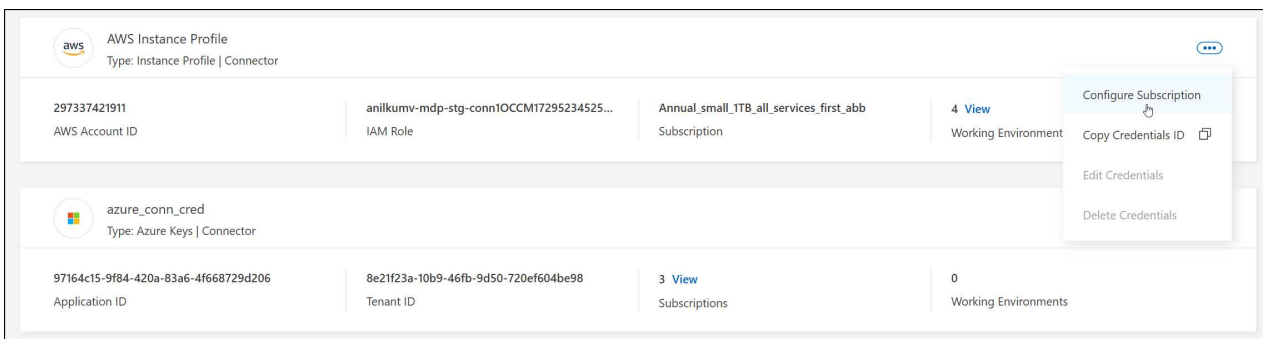
The following video shows the steps to subscribe to NetApp Intelligent Services from the AWS Marketplace:

### [Subscribe to NetApp Intelligent Services from the AWS Marketplace](#)

#### Steps

1. Select **Administration > \*Credentials**.
2. Select **Organization credentials**.
3. Select the action menu for a set of credentials that are associated with a Console agent and then select **Configure Subscription**.

You must select credentials that are associated with a Console agent. You can't associate a marketplace subscription with credentials that are associated with the NetApp Console.



4. To associate the credentials with an existing subscription, select the subscription from the down-down list and select **Configure**.
5. 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 NetApp Console.

- d. From the **Subscription Assignment** page:
  - Select the Console 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.

The Console 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. Select **Administration > \*Credentials**.
2. Select **Organization credentials**.
3. Select the action menu for a set of credentials that are associated with a Console agent and then select **Configure Subscription**.

You must select credentials that are associated with a Console agent. You can't associate a marketplace subscription with credentials that are associated with the NetApp Console.

4. To associate the credentials with an existing subscription, select the subscription from the down-down list and select **Configure**.
5. 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 the NetApp Console.

- e. From the **Subscription Assignment** page:
  - Select the Console 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.

The Console 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**.

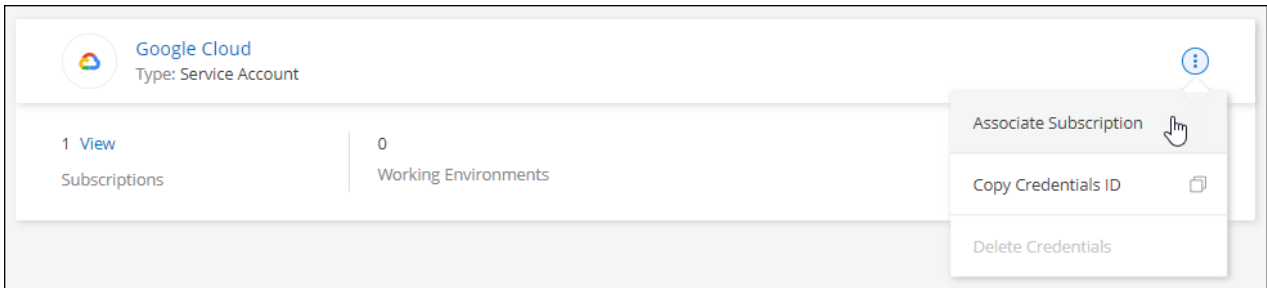
The following video shows the steps to subscribe from the Azure Marketplace:

[Subscribe to NetApp Intelligent Services from the Azure Marketplace](#)

## Google Cloud

### Steps

1. Select **Administration > \*Credentials**.
2. Select **Organization credentials**.
3. Select the action menu for a set of credentials that are associated with a Console agent and then select **Configure Subscription**.  
+new screenshot needed (TS)



4. 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**.

Google Cloud Project

OCCM-Dev ▼

Subscription

● GCP subscription for staging ▼

---

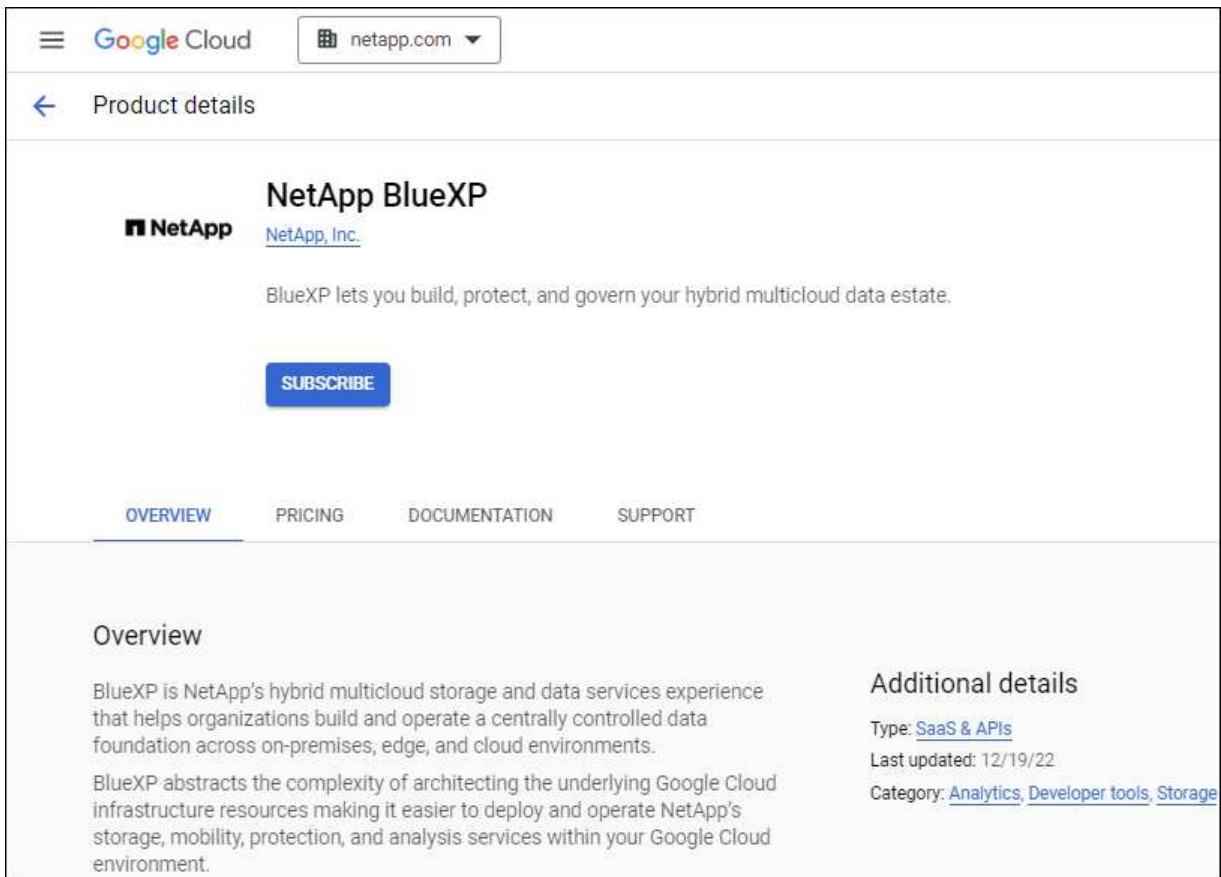
Add Subscription

5. 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 NetApp Console 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 Console organization or account. The process of linking a subscription isn't complete until you are redirected from this page and then sign in to the Console.



Your order request has been sent to NetApp, Inc.



Your new subscription to the Cloud Manager 1 month plan for Cloud Manager for Cloud Volumes ONTAP requires your registration with NetApp, Inc.. After NetApp, Inc. approves your request, your subscription will be active and you will begin getting charged. This processing time will depend on the vendor, and you should reach out to NetApp, Inc. directly with any questions related to signup.

[VIEW ORDERS](#)

[REGISTER WITH NETAPP, INC.](#)

f. Complete the steps on the **Subscription Assignment** page:



If someone from your organization has already has a marketplace subscription from your billing account, then you will be redirected to [the Cloud Volumes ONTAP page within NetApp Console](#) instead. If this is unexpected, contact your NetApp sales team. Google enables only one subscription per Google billing account.

- Select the Console 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.

The Console 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.

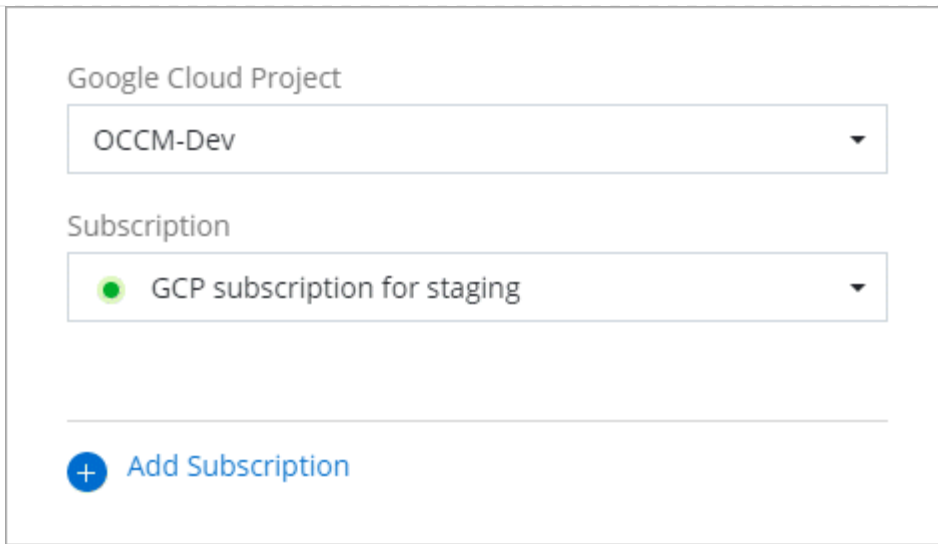
For all other organizations or accounts, you'll need to manually associate the subscription by repeating these steps.

- Select **Save**.

The following video shows the steps to subscribe from the Google Cloud Marketplace:

[Subscribe from the Google Cloud Marketplace](#)

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



The screenshot shows a configuration window 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 status indicator. Below these dropdowns 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 (standard mode)

Now that you've logged in and set up NetApp Console in standard mode, users can create and discover storage systems and use NetApp data services.



If you installed a Console agent in AWS, Microsoft Azure, or Google Cloud, then the Console automatically discovers information about the Amazon S3 buckets, Azure Blob storage, or Google Cloud Storage buckets in the location where the agent is installed. These systems are automatically added to the **Systems** page.

For help, go to the [home page for the NetApp Console documentation](#) to view the NetApp Console documentation.

#### Related information

[NetApp Console deployment modes](#)

## Get started with restricted mode

### Getting started workflow (restricted mode)

Get started with the NetApp Console in restricted mode by preparing your environment and deploying the Console agent.

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 [Console agents](#) and [deployment modes](#).

1

### Prepare for deployment

<https://raw.githubusercontent.com/NetAppDocs/console-setup-admin-internal/blob/main/media/screenshot-canvas.png>

- 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 Console agent instance after you deploy it.

2

### Deploy the Console agent

- a. Install the Console agent from your cloud provider's marketplace or by manually installing the software on your own Linux host.
- b. Set up the NetApp Console by opening a web browser and entering the Linux host's IP address.
- c. Provide the Console agent 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 NetApp Backup and Recovery, Cloud Volumes ONTAP, NetApp Cloud Tiering, NetApp Ransomware Resilience and NetApp Disaster Recovery. NetApp Data Classification is included with your subscription at no additional cost.

## Prepare for deployment in restricted mode

Prepare your environment before you deploy NetApp Console in restricted mode. You need to review host requirements, prepare networking, set up permissions, and more.

### Step 1: Understand how restricted mode works

Understand how the NetApp Console works in restricted mode before starting.

Use the browser-based interface available locally from the installed NetApp Console agent. You can't access the NetApp Console from the web-based console that's provided through the SaaS layer.

In addition, not all Console features and NetApp data services are available.

[Learn how restricted mode works.](#)

### Step 2: Review installation options

In restricted mode, you can only install the Console agent in the cloud. The following installation options are available:

- From the AWS Marketplace
- From the Azure Marketplace
- Manually installing the Console agent on your own Linux host running in AWS, Azure, or Google Cloud

### Step 3: Review host requirements

A host must meet specific OS, RAM, and port requirements to run the Console agent.

When you deploy the Console agent 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 Console agent is not supported on a host that is shared with other applications. The host must be a dedicated host. The host can be of any architecture that meets the following size requirements:

- CPU: 8 cores or 8 vCPUs
- RAM: 32 GB
- Disk space: 165 GB is recommended for the host, with the following partition requirements:
  - `/opt`: 120 GiB of space must be available

The agent uses `/opt` to install the `/opt/application/netapp` directory and its contents.

- `/var`: 40 GiB of space must be available

The Console agent 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.

#### Hypervisor

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

#### Operating system and container requirements

The Console agent is supported with the following operating systems when using the Console in standard mode or restricted mode. A container orchestration tool is required before you install the agent.

Operating system	Supported OS versions	Supported agent versions	Required container tool	SELinux a
Red Hat Enterprise Linux	9.1 to 9.4 8.6 to 8.10 <ul style="list-style-type: none"> <li>English language versions only.</li> <li>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 agent installation.</li> </ul>	3.9.50 or later with the Console in standard mode or restricted mode	Podman version 4.6.1 or 4.9.4  <a href="#">View Podman configuration requirements.</a>	Supported in enforcing mode or permissive mode <ul style="list-style-type: none"> <li>Management of Cloud Volumes ONTAP systems is NOT supported by agents that have SELinux enabled on the operating system.</li> </ul>
Ubuntu	24.04 LTS	3.9.45 or later with the NetApp Console in standard mode or restricted mode	Docker Engine 23.06 to 28.0.0.	Not supported
	22.04 LTS	3.9.50 or later	Docker Engine 23.0.6 to 28.0.0.	Not supported

### 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 Console agent 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

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

## Disk space in /var

20 GiB of space must be available

The Console agent 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

To manually install the Console agent, prepare the host by installing Podman or Docker Engine.

Depending on your operating system, either Podman or Docker Engine is required before installing the agent.

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

[View the supported Podman versions.](#)

- Docker Engine is required for Ubuntu.

[View the supported Docker Engine versions.](#)

## Example 5. Steps

### Podman

Follow these steps to install and configure Podman:

- 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
- If using Red Hat Enterprise Linux 8, verify that your Podman version is using Aardvark DNS instead of CNI



Adjust the aardvark-dns port (default: 53) after installing the agent to avoid DNS port conflicts. 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.

You can obtain Podman 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 supported Podman versions](#).

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 supported Podman versions](#).

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.

6. If using Red Hat Enterprise:

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
```

7. 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.

8. If using Red Hat Enterprise Linux 8, verify that your Podman version is using NetAvark with Aardvark DNS instead of CNI.

a. Check to see if your networkBackend is set to CNI by running the following command:

```
podman info | grep networkBackend
```

b. If the networkBackend is set to CNI, you'll need to change it to netavark.

c. Install netavark and aardvark-dns using the following command:

```
dnf install aardvark-dns netavark
```

d. Open the `/etc/containers/containers.conf` file and modify the `network_backend` option to use "netavark" instead of "cni".

If `/etc/containers/containers.conf` doesn't exist, make the configuration changes to



```
/usr/share/containers/containers.conf.
```

#### 9. Restart podman.

```
systemctl restart podman
```

#### 10. Confirm networkBackend is now changed to "netavark" using the following command:

```
podman info | grep networkBackend
```

### Docker Engine

Follow the documentation from Docker to install Docker Engine.

#### Steps

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

Follow the steps to install a supported Docker Engine version. Do not install the latest version, as it is unsupported by the Console.

##### 2. Verify that Docker is enabled and running.

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

### Step 5: Prepare network access

Set up network access so the Console agent can manage resources in your public cloud. In addition to having a virtual network and subnet for the Console agent, you need to ensure that the following requirements are met.

#### Connections to target networks

Ensure the Console agent has a network connection to the storage locations. 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 NetApp Console

In restricted mode, users access the Console from the Console agent VM. The Console agent contacts a few endpoints to complete data management tasks. These endpoints are contacted from a user's computer when completing specific actions from the Console.



Console agents previous to version 4.0.0 need additional endpoints. If you upgraded to 4.0.0 or later, you can remove the old endpoints from your allow list. [Learn more about the required network access for versions previous to 4.0.0.](#)

+

Endpoints	Purpose
<a href="https://api.bluelxp.netapp.com">https://api.bluelxp.netapp.com</a> <a href="https://netapp-cloud-account.auth0.com">https://netapp-cloud-account.auth0.com</a> <a href="https://netapp-cloud-account.us.auth0.com">https://netapp-cloud-account.us.auth0.com</a> <a href="https://console.netapp.com">https://console.netapp.com</a> <a href="https://components.console.bluelxp.netapp.com">https://components.console.bluelxp.netapp.com</a> <a href="https://cdn.auth0.com">https://cdn.auth0.com</a>	To provide features and services within the NetApp Console.
<a href="https://cdn.auth0.com">https://cdn.auth0.com</a> <a href="https://services.cloud.netapp.com">https://services.cloud.netapp.com</a>	Your web browser connects to these endpoints for centralized user authentication through the NetApp Console.

### Outbound internet access for day-to-day operations

The Console agent's network location must have outbound internet access. It needs to be able to reach the SaaS services of the NetApp Console as well as endpoints within your respective public cloud environment.

Endpoints	Purpose
<b>AWS environments</b>	
AWS services (amazonaws.com): <ul style="list-style-type: none"> <li>• CloudFormation</li> <li>• Elastic Compute Cloud (EC2)</li> <li>• Identity and Access Management (IAM)</li> <li>• Key Management Service (KMS)</li> <li>• Security Token Service (STS)</li> <li>• Simple Storage Service (S3)</li> </ul>	To manage AWS resources. The endpoint depends on your AWS region. <a href="#">Refer to AWS documentation for details</a>
<b>Azure environments</b>	
<a href="https://management.azure.com">https://management.azure.com</a> <a href="https://login.microsoftonline.com">https://login.microsoftonline.com</a> <a href="https://blob.core.windows.net">https://blob.core.windows.net</a> <a href="https://core.windows.net">https://core.windows.net</a>	To manage resources in Azure public regions.
<a href="https://management.usgovcloudapi.net">https://management.usgovcloudapi.net</a> <a href="https://login.microsoftonline.us">https://login.microsoftonline.us</a> <a href="https://blob.core.usgovcloudapi.net">https://blob.core.usgovcloudapi.net</a> <a href="https://core.usgovcloudapi.net">https://core.usgovcloudapi.net</a>	To manage resources in Azure Government regions.
<a href="https://management.chinacloudapi.cn">https://management.chinacloudapi.cn</a> <a href="https://login.chinacloudapi.cn">https://login.chinacloudapi.cn</a> <a href="https://blob.core.chinacloudapi.cn">https://blob.core.chinacloudapi.cn</a> <a href="https://core.chinacloudapi.cn">https://core.chinacloudapi.cn</a>	To manage resources in Azure China regions.
<b>Google Cloud environments</b>	

Endpoints	Purpose
<a href="https://www.googleapis.com/compute/v1/">https://www.googleapis.com/compute/v1/</a> <a href="https://compute.googleapis.com/compute/v1">https://compute.googleapis.com/compute/v1</a> <a href="https://cloudresourcemanager.googleapis.com/v1/projects">https://cloudresourcemanager.googleapis.com/v1/projects</a> <a href="https://www.googleapis.com/compute/beta">https://www.googleapis.com/compute/beta</a> <a href="https://storage.googleapis.com/storage/v1">https://storage.googleapis.com/storage/v1</a> <a href="https://www.googleapis.com/storage/v1">https://www.googleapis.com/storage/v1</a> <a href="https://iam.googleapis.com/v1">https://iam.googleapis.com/v1</a> <a href="https://cloudkms.googleapis.com/v1">https://cloudkms.googleapis.com/v1</a> <a href="https://www.googleapis.com/deploymentmanager/v2/projects">https://www.googleapis.com/deploymentmanager/v2/projects</a>	To manage resources in Google Cloud.
<b>NetApp Console endpoints</b>	
<a href="https://mysupport.netapp.com">https://mysupport.netapp.com</a>	To obtain licensing information and to send AutoSupport messages to NetApp support.
<a href="https://signin.b2c.netapp.com">https://signin.b2c.netapp.com</a>	To update NetApp Support Site (NSS) credentials or to add new NSS credentials to the NetApp Console.
<a href="https://api.bluexp.netapp.com">https://api.bluexp.netapp.com</a> <a href="https://netapp-cloud-account.auth0.com">https://netapp-cloud-account.auth0.com</a> <a href="https://netapp-cloud-account.us.auth0.com">https://netapp-cloud-account.us.auth0.com</a> <a href="https://console.netapp.com">https://console.netapp.com</a> <a href="https://components.console.bluexp.netapp.com">https://components.console.bluexp.netapp.com</a> <a href="https://cdn.auth0.com">https://cdn.auth0.com</a>	To provide features and services within the NetApp Console.
<a href="https://bluexpinfraprod.eastus2.data.azurecr.io">https://bluexpinfraprod.eastus2.data.azurecr.io</a> <a href="https://bluexpinfraprod.azurecr.io">https://bluexpinfraprod.azurecr.io</a>	<p>To obtain images for Console agent upgrades.</p> <ul style="list-style-type: none"> <li>When you deploy a new agent, the validation check tests connectivity to current endpoints. If you use <a href="#">xref:./previous endpoints</a>, the validation check fails. To avoid this failure, skip the validation check.</li> </ul> <p>Although the previous endpoints are still supported, NetApp recommends updating your firewall rules to the current endpoints as soon as possible. <a href="#">Learn how to update your endpoint list.</a></p> <ul style="list-style-type: none"> <li>When you update to the current endpoints in your firewall, your existing agents will continue to work.</li> </ul>

## Public IP address in Azure

If you want to use a public IP address with the Console agent VM in Azure, the IP address must use a Basic SKU to ensure that the Console uses this public IP address.

If you use a Standard SKU IP address instead, then the Console uses the *private* IP address of the Console agent, instead of the public IP. If the machine that you're using to access the Console doesn't have access to that private IP address, then actions from the 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 Console agent, unless you initiate it or if it 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, the Console automatically configures those systems to use a proxy server that's included with the Console agent. The only requirement is to ensure that the Console agent's security group allows inbound connections over port 3128. You'll need to open this port after you deploy the Console agent.

### Enable NTP

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

If you're planning to create a Console agent from your cloud provider's marketplace, implement this networking requirement after you create the Console agent.

## **Step 6: Prepare cloud permissions**

The Console agent requires permissions from your cloud provider to deploy Cloud Volumes ONTAP in a virtual network and to use NetApp data services. You need to set up permissions in your cloud provider and then associate those permissions with the Console agent.

To view the required steps, choose the authentication option to use for your cloud provider.

## AWS IAM role

Use an IAM role to provide the Console agent with permissions.

If you're creating the Console agent from the AWS Marketplace, you are prompted to select that IAM role when you launch the EC2 instance.

If you're manually installing the Console agent on your own Linux host, 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 Console agent](#).
  - 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 Console agent EC2 instance.

## AWS access key

Set up permissions and an access key for an IAM user. You'll need to provide the Console with the AWS access key after you install the Console agent and set up the Console.

### 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 Console agent](#).
  - c. Finish the remaining steps to create the policy.

Depending on the NetApp data services that you plan 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 Console agent](#).

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 the NetApp Console after you install the Console agent.

### Azure role

Create an Azure custom role with the required permissions. You'll assign this role to the Console agent 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 the NetApp Console.

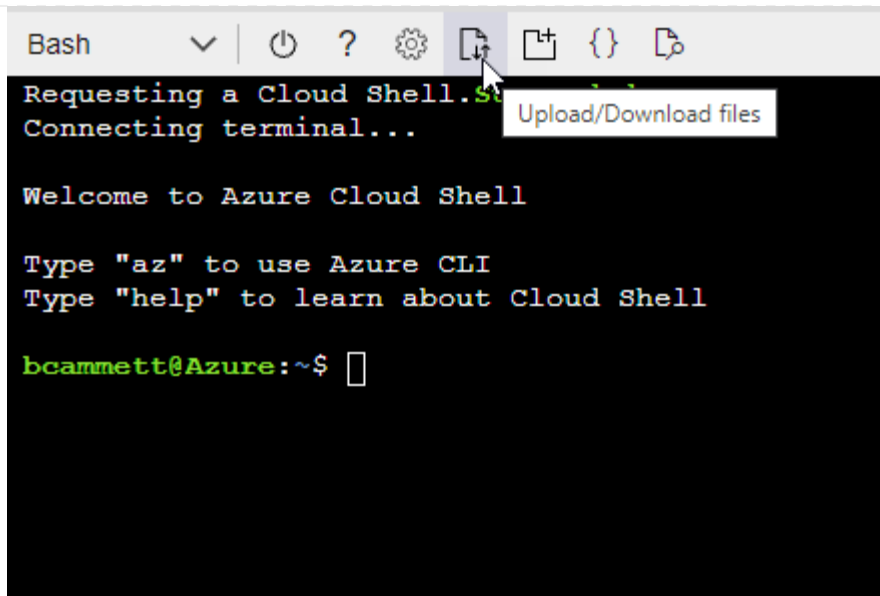
### Example

```
"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
```

### Azure service principal

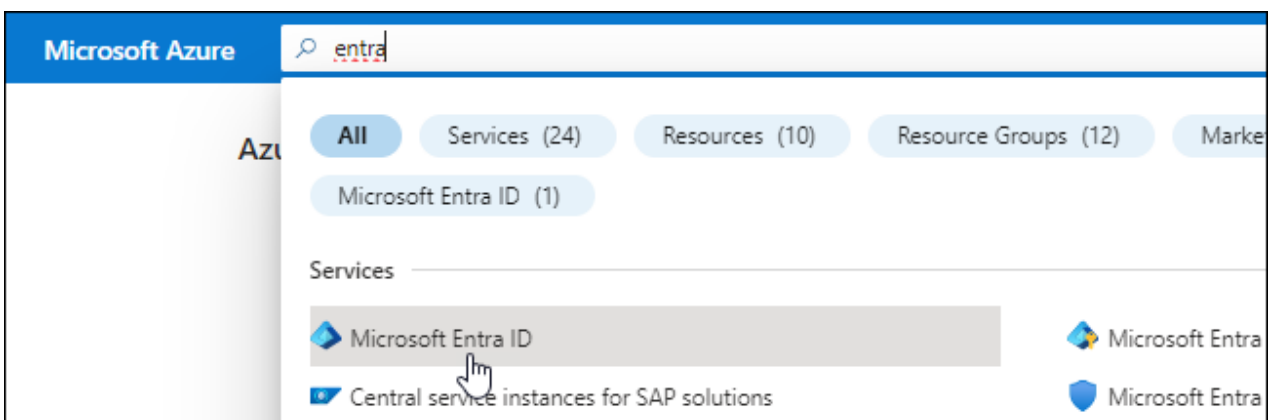
Create and set up a service principal in Microsoft Entra ID and obtain the Azure credentials that the Console needs. You need to provide the Console with these credentials after you install the Console agent.

### 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 the NetApp Console).
- **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](#)

- Copy the contents of the [custom role permissions for the Console agent](#) and save them in a JSON file.
- 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.

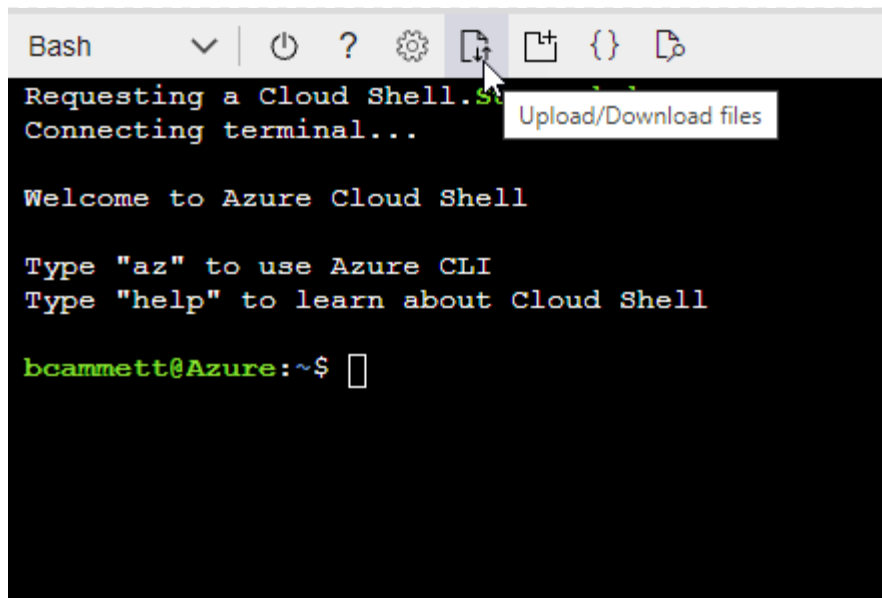
### Example

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

- 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 Console Operator that you can assign to the Console agent 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 **Console 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 Console agent.

If you want to deploy Cloud Volumes ONTAP from multiple Azure subscriptions, then you must bind the service principal to each of those subscriptions. In the NetApp Console, you can 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

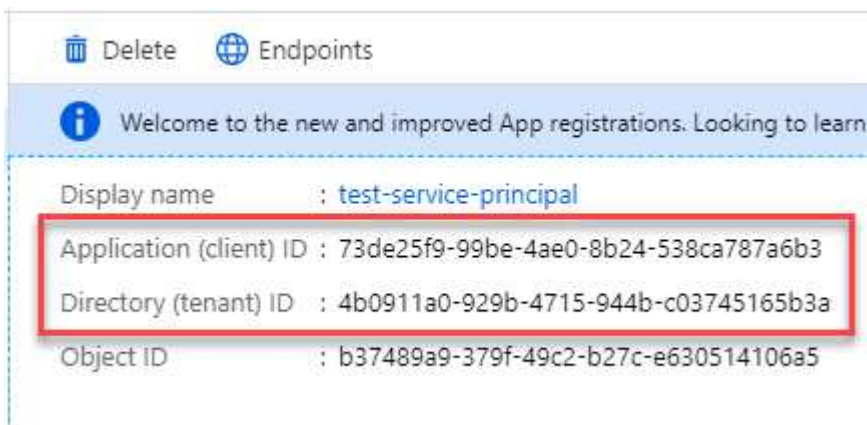


user\_impersonation

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 the Console, you need to provide the application (client) ID and the directory (tenant) ID for the application. The Console 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.

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

## Result

Your service principal is now set up 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 the Console 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 Console agent VM instance.

## Steps

1. Create a custom role in Google Cloud:
  - a. Create a YAML file that includes the permissions defined in the [Console agent policy for Google Cloud](#).
  - b. From Google Cloud, activate cloud shell.
  - c. Upload the YAML file that includes the required permissions for the Console agent.
  - 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 Console agent 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 NetApp Backup and Recovery with customer-managed encryption keys (CMEK))

## Deploy the Console agent in restricted mode

Deploy the Console agent in restricted mode so that you can use the NetApp Console with limited outbound connectivity. To get started, install the Console agent, set up the Console by accessing the user interface that's running on the Console agent, and then provide the cloud permissions that you previously set up.

### Step 1: Install the Console agent

Install the Console agent from your cloud provider's marketplace or manually on a 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 Console agent.

[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 [NetApp Console agent 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**.

Use the EC2 Console to launch the instance and attach an IAM role. This is not possible with 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 Console agent 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 Console agent 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 Console agent.
- **Summary:** Review the summary and select **Launch instance**.

## Result

AWS launches the software with the specified settings. The Console agent instance and software run in approximately five minutes.

## What's next?

Set up the NetApp Console.

## AWS Gov Marketplace

### Before you begin

You should have the following:

- A VPC and subnet that meets networking requirements.

[Learn about networking requirements](#)

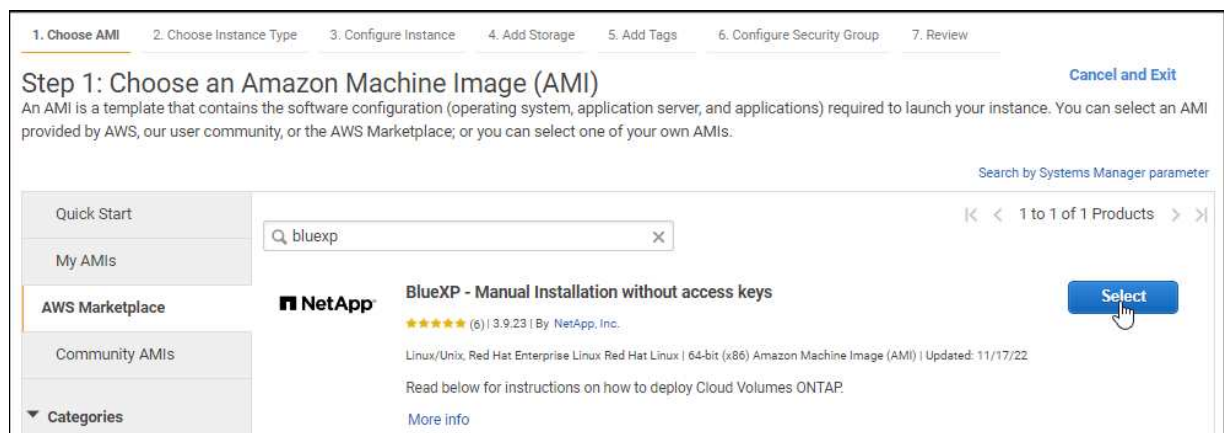
- An IAM role with an attached policy that includes the required permissions for the Console agent.

[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 NetApp Console agent offering in the AWS Marketplace.
  - a. Open the EC2 service and select **Launch instance**.
  - b. Select **AWS Marketplace**.
  - c. Search for NetApp Console 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	1	<a href="#">Launch into Auto Scaling Group</a>
Purchasing option	<input type="checkbox"/> Request Spot instances	
Network	vpc-a76d91c2   VPC4QA (default)	<a href="#">Create new VPC</a>
Subnet	subnet-39536c13   QASubnet1   us-east-1b 155 IP Addresses available	<a href="#">Create new subnet</a>
Auto-assign Public IP	Enable	
Placement group	<input type="checkbox"/> Add instance to placement group	
Capacity Reservation	Open	<a href="#">Create new Capacity Reservation</a>
IAM role	Cloud_Manager	<a href="#">Create new IAM role</a>
CPU options	<input type="checkbox"/> Specify CPU options	
Shutdown behavior	Stop	
Enable termination protection	<input checked="" type="checkbox"/> Protect against accidental termination	
Monitoring	<input type="checkbox"/> Enable CloudWatch detailed monitoring <a href="#">Additional charges apply.</a>	

- **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 Console agent instance: SSH, HTTP, and HTTPS.
- **Review:** Review your selections and select **Launch**.

## Result

AWS launches the software with the specified settings. The Console agent instance and software run in approximately five minutes.

## What's next?

Set up the Console.

## Azure Gov 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 Console agent.

### [Learn how to set up Azure permissions](#)

#### Steps

1. Go to the NetApp Console agent 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 Console agent can perform optimally with either HDD or SSD disks.
- **Public IP:** If you want to use a public IP address with the Console agent VM, the IP address must use a Basic SKU to ensure that the Console uses this public IP address.

If you use a Standard SKU IP address instead, then the Console uses the *private* IP address of the Console agent, instead of the public IP. If the machine that you're using to access the Console doesn't have access to that private IP address, then actions from the Console will fail.

[Azure documentation: Public IP SKU](#)

- **Network security group:** The Console agent 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 Console agent 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 Console agent software should be running in approximately five minutes.

## What's next?

Set up the NetApp Console.

## Manual install

### Before you begin

You should have the following:

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

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

- 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 Console agent. If you need to set a certificate for a transparent proxy server, you must use the Maintenance Console after installation. Learn more about the [Agent Maintenance Console](#).

- You need to disable the configuration check that verifies outbound connectivity during installation. The manual install fails if this check is not disabled. [Learn how to disable configuration checks for manual installations](#).
- Depending on your operating system, either Podman or Docker Engine is required before you install the Console agent.

## About this task

The installer that is available on the NetApp Support Site might be an earlier version. After installation, the Console agent 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 fails.

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

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

3. Assign permissions to run the script.

```
chmod +x NetApp_Console_Agent_Cloud_<version>
```

Where <version> is the version of the Console agent that you downloaded.

4. If installing in a Government Cloud environment, disable the configuration checks. [Learn how to disable configuration checks for manual installations.](#)
5. Run the installation script.

```
./NetApp_Console_Agent_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:

```
./NetApp_Console_Agent_Cloud_v4.0.0--proxy  
https://user:password@10.0.0.30:8080/ --cacert  
/tmp/cacert/certificate.cer
```

`--proxy` configures the Console agent 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.
- The Console agent 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 Console agent 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 Console agent host:

+

```
./NetApp_Console_Agent_Cloud_v4.0.0 --cacert  
/tmp/cacert/certificate.cer
```

1. If you used Podman, you'll need to adjust the aardvark-dns port.
  - a. SSH to the Console agent 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 Console agent virtual machine.

### Result

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

### What's next?

Set up the NetApp Console.

## Step 2: Set up NetApp Console

When you access the console for the first time, you are prompted to choose an organization for the Console agent and need to enable restricted mode.

### Before you begin

The person who sets up the Console agent must log in to the Console using a login that doesn't already belong to a Console organization.

If your login is associated with another organization, you'll need to sign up with a new 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 Console agent instance and enter the following URL of the Console agent you installed.
2. Sign up or log in to the NetApp Console.
3. After you're logged in, set up the Console:
  - a. Enter a name for the Console agent.
  - b. Enter a name for a new Console organization.
  - 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 the account is created. You can't enable restricted mode later and you can't disable it later.

If you deployed the Console agent 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.

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

### Result

The Console agent is now installed and set up with your Console organization. All users need to access the Console using the IP address of the Console agent instance.

### What's next?

Provide the Console with the permissions that you previously set up.

### Step 3: Provide permissions to NetApp Console

If you deployed the Console agent from the Azure Marketplace or if you manually installed the Console agent software, you need to provide the permissions that you previously set up.

These steps don't apply if you deployed the Console agent 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 Console agent.

These steps apply only if you manually installed the Console agent in AWS. For AWS Marketplace deployments, you already associated the Console agent instance with an IAM role that includes the required permissions.

#### Steps

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

### AWS access key

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

#### Steps

1. Select **Administration > Credentials**.
2. Select **Organization credentials**.
3. Select **Add Credentials** and follow the steps in the wizard.
  - a. **Credentials Location**: Select \*Amazon Web Services > Agent.
  - 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**.

### Azure role

Go to the Azure portal and assign the Azure custom role to the Console agent 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 the NetApp Console 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 **Console Operator** role and select **Next**.



Console Operator is the default name provided in the 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 Console agent virtual machine was created, under **Managed identity**, choose **Virtual machine**, and then select the Console agent 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.

### Azure service principal

Provide the NetApp Console with the credentials for the Azure service principal that you previously setup.

#### Steps

1. Select **Administration > Credentials**.
2. Select **Add Credentials** and follow the steps in the wizard.
  - a. **Credentials Location**: Select **Microsoft Azure > Agent**.
  - 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

the NetApp Console 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 Console agent VM.

#### Steps

1. Go to the Google Cloud portal and assign the service account to the Console agent 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 Console agent role to that project. You'll need to repeat this step for each project.

## 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:

- NetApp Backup and Recovery
- Cloud Volumes ONTAP
- NetApp Cloud Tiering
- NetApp Ransomware Resilience
- NetApp Disaster Recovery

NetApp Data Classification is enabled through your subscription, but there is no charge for using classification.

**Before you begin**

You must have already deployed a Console agent in order to subscribe to data services. You need to associate a marketplace subscription to the cloud credentials connected to a Console agent.

## AWS

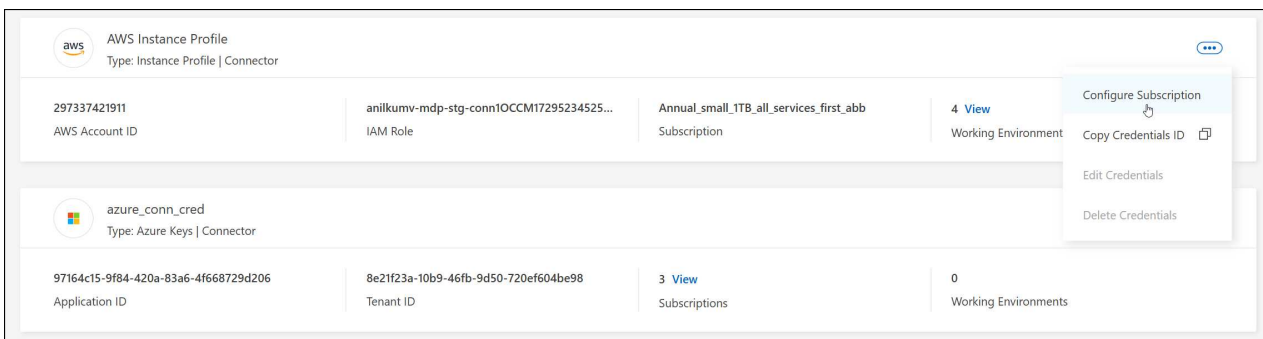
The following video shows the steps to subscribe to NetApp Intelligent Services from the AWS Marketplace:

### [Subscribe to NetApp Intelligent Services from the AWS Marketplace](#)

#### Steps

1. Select **Administration > \*Credentials**.
2. Select **Organization credentials**.
3. Select the action menu for a set of credentials that are associated with a Console agent and then select **Configure Subscription**.

You must select credentials that are associated with a Console agent. You can't associate a marketplace subscription with credentials that are associated with the NetApp Console.



4. To associate the credentials with an existing subscription, select the subscription from the down-down list and select **Configure**.
5. 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 NetApp Console.

- d. From the **Subscription Assignment** page:
  - Select the Console 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.

The Console 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. Select **Administration > \*Credentials**.
2. Select **Organization credentials**.
3. Select the action menu for a set of credentials that are associated with a Console agent and then select **Configure Subscription**.

You must select credentials that are associated with a Console agent. You can't associate a marketplace subscription with credentials that are associated with the NetApp Console.

4. To associate the credentials with an existing subscription, select the subscription from the down-down list and select **Configure**.
5. 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 the NetApp Console.

- e. From the **Subscription Assignment** page:
  - Select the Console 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.

The Console 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**.

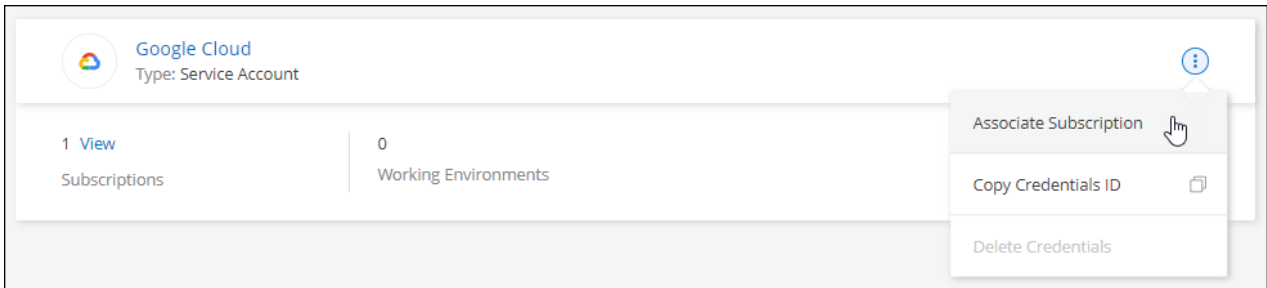
The following video shows the steps to subscribe from the Azure Marketplace:

[Subscribe to NetApp Intelligent Services from the Azure Marketplace](#)

## Google Cloud

### Steps

1. Select **Administration > \*Credentials**.
2. Select **Organization credentials**.
3. Select the action menu for a set of credentials that are associated with a Console agent and then select **Configure Subscription**.  
+new screenshot needed (TS)



4. 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**.

Google Cloud Project

OCCM-Dev

Subscription

GCP subscription for staging

Add Subscription

5. 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 NetApp Console 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 console. At the top, there's a navigation bar with the Google Cloud logo and a dropdown menu showing 'netapp.com'. Below this is a breadcrumb trail with 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.' A prominent blue 'SUBSCRIBE' button is centered. Below the button is a horizontal menu with links for 'OVERVIEW' (which is underlined), 'PRICING', 'DOCUMENTATION', and 'SUPPORT'. 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 of the overview is an 'Additional details' section with the following information: 'Type: [SaaS & APIs](#)', 'Last updated: 12/19/22', and 'Category: [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 Console organization or account. The process of linking a subscription isn't complete until you are redirected from this page and then sign in to the Console.

Your order request has been sent to NetApp, Inc.



Your new subscription to the Cloud Manager 1 month plan for Cloud Manager for Cloud Volumes ONTAP requires your registration with NetApp, Inc.. After NetApp, Inc. approves your request, your subscription will be active and you will begin getting charged. This processing time will depend on the vendor, and you should reach out to NetApp, Inc. directly with any questions related to signup.

[VIEW ORDERS](#)

[REGISTER WITH NETAPP, INC.](#)

f. Complete the steps on the **Subscription Assignment** page:



If someone from your organization has already has a marketplace subscription from your billing account, then you will be redirected to [the Cloud Volumes ONTAP page within NetApp Console](#) instead. If this is unexpected, contact your NetApp sales team. Google enables only one subscription per Google billing account.

- Select the Console 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.

The Console 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.

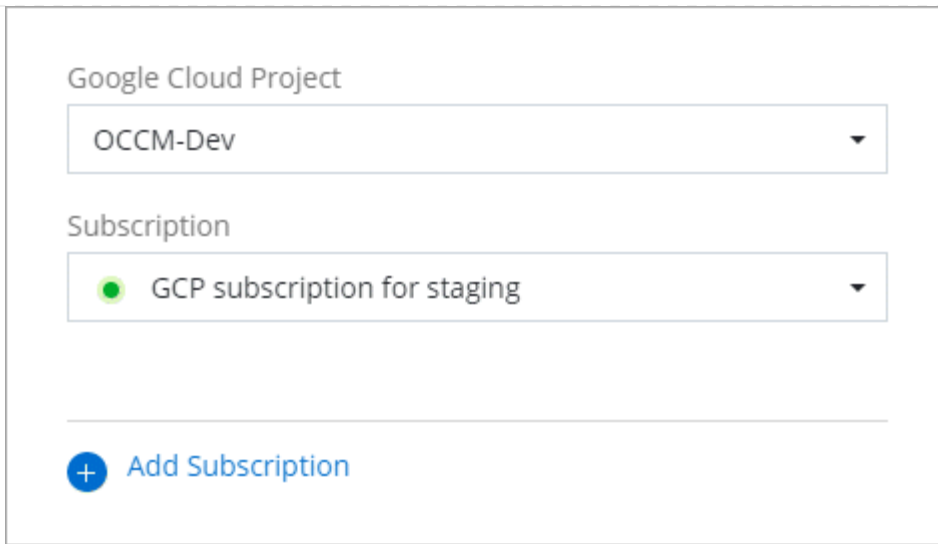
For all other organizations or accounts, you'll need to manually associate the subscription by repeating these steps.

- Select **Save**.

The following video shows the steps to subscribe from the Google Cloud Marketplace:

[Subscribe from the Google Cloud Marketplace](#)

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



The screenshot shows a configuration panel 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 small green circle icon. Below these dropdowns is a horizontal line, and then a blue circular button with a white plus sign followed by 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 NetApp Console in restricted mode, you can start using the 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

[NetApp Console deployment modes](#)

## Get started with BlueXP legacy interface (private mode)



## Getting started workflow (BlueXP private mode)

BlueXP private mode (legacy BlueXP interface) 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. NetApp continues to support these environments with the legacy BlueXP interface.

[PDF documentation for BlueXP private mode](#)

### Features and data services supported with private mode

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

Note that some services might be supported with limitations.

Product area	BlueXP service or feature	Private mode
<b>Working environments</b>  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
	Amazon S3	No
	Azure Blob	No
	Azure NetApp Files	No
	Cloud Volumes ONTAP	Yes
	Google Cloud NetApp Volumes	No
	Google Cloud Storage	No
	On-premises ONTAP clusters	Yes
	E-Series	No
	StorageGRID	No

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

# Use NetApp Console

## Log in to the NetApp Console

How you log in to the NetApp Console depends on which deployment mode that you're using.

You are automatically logged out after 24 hours or if you close your browser.

[Learn about Console deployment modes.](#)

## Standard mode

After you sign up to the NetApp Console, 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 NetApp Console using one of the following options:

- Your existing NetApp Support Site (NSS) credentials
- A NetApp Console account 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 set up identity federation.](#)

### Steps

1. Open a web browser and go to the [NetApp 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 to manage your hybrid multi-cloud infrastructure.

## Restricted mode

When you use the Console in restricted mode, you need to log in to the the Console from the user interface that runs locally on the agent.

### About this task

The Console supports logging in with one of the following options when in restricted mode:

- A NetApp Console 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.](#)

### Steps

1. Open a web browser and enter the IP address where the agent is installed.
2. Enter your user name and password to log in.

# View metrics on the NetApp Console Home page

Monitoring the health of your storage estate ensures that you are aware of issues with storage protection and can take steps to resolve them. Using the NetApp Console Home page, view a status of your backups and restores from NetApp Backup and Recovery and the number of workloads that are at risk for a ransomware attack or protected as indicated by NetApp Ransomware Resilience. You can review the storage capacity for individual clusters and Cloud Volumes ONTAP, ONTAP alerts, storage performance capacity per cluster or Cloud Volumes ONTAP system, the different types of licenses you have, and more.

All panes on the Home page show data at the organization level. The Storage capacity and Storage performance panes show systems associated with projects that the user can access based on IAM permissions.

The system refreshes the data on the Home page every five minutes. Caching may cause the data on this page to differ from real values for up to 15 minutes.



Accurate metrics on the Home page require appropriately sized and configured Console agents.

## Required NetApp Console roles

Each pane in the Home page requires different user roles:

- **Storage capacity pane:** Ability to see the NetApp Console Systems page
- **ONTAP alerts pane:** Folder or project admin, Operations Support Analyst, Organization admin, Organization viewer, Super admin, Super viewer
- **Storage performance capacity pane:** Ability to see the NetApp Console Systems page
- **Licenses and subscriptions pane:** Folder or project admin, Organization admin, Organization viewer, Super admin, Super viewer
- **Ransomware Resilience pane:** Folder or project admin, Organization admin, Ransomware protection admin, Ransomware protection viewer, Super admin, Super viewer
- **Backup and Recovery pane:** Backup and recovery backup admin, Backup and recovery super admin, Backup and recovery backup viewer, Backup and recovery clone admin, Folder or project admin, Organization admin, Backup and recovery restore admin, Super admin, Super viewer

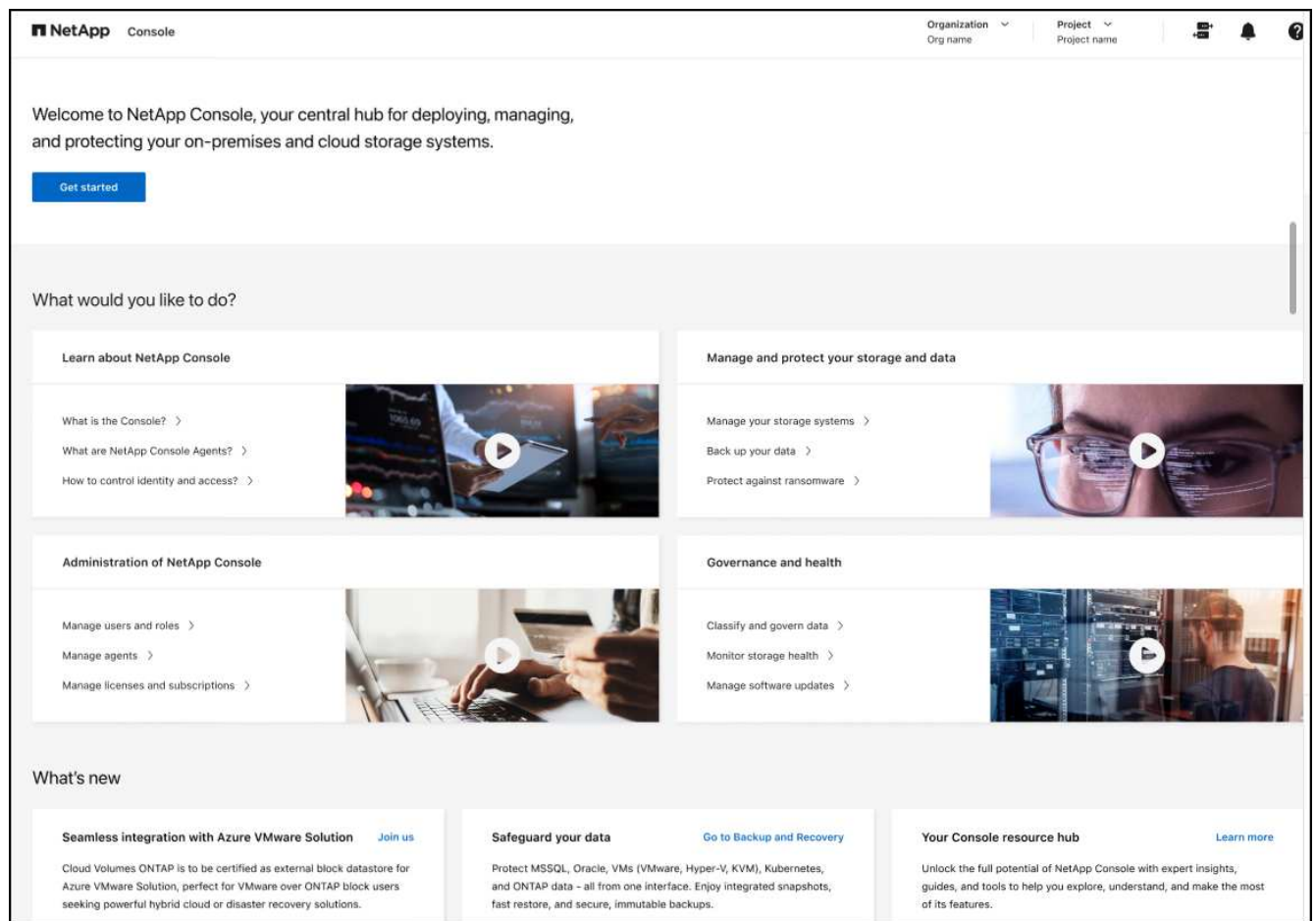
If you do not have permissions to access a pane, the pane displays a message indicating you lack permissions to use it.

[Learn about NetApp Console access roles..](#)

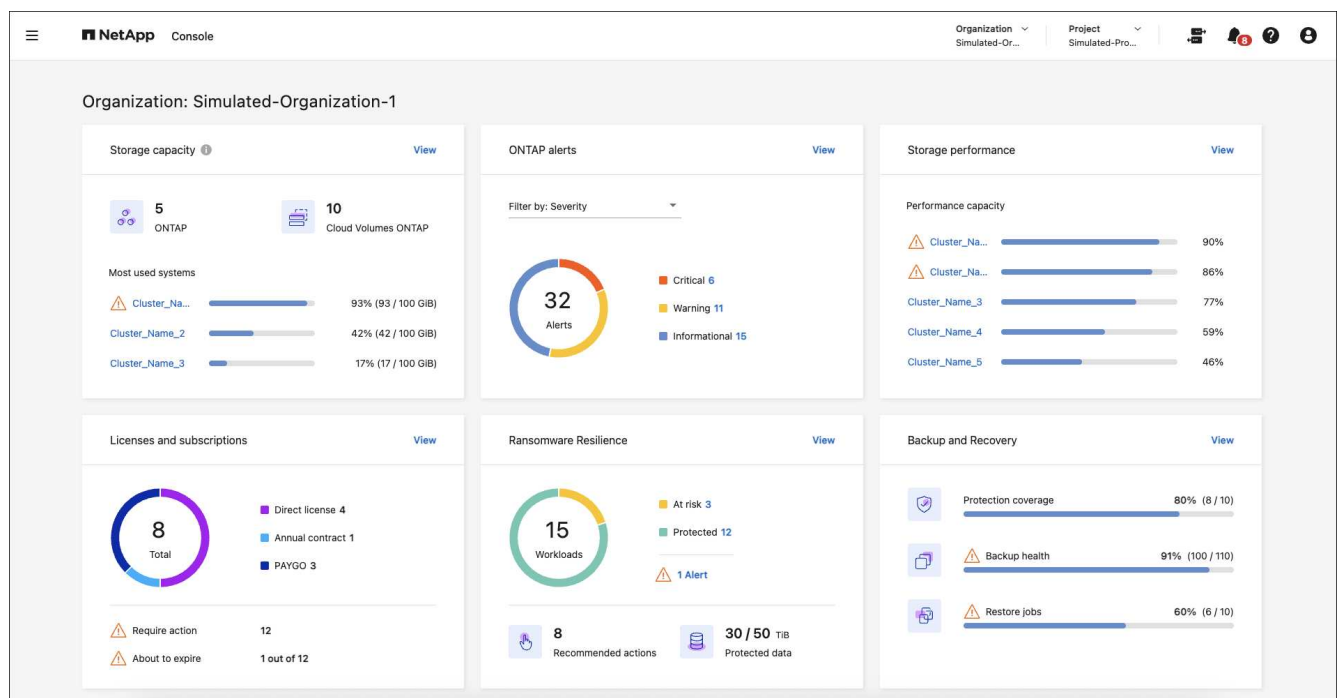
### Steps

1. From the NetApp Console menu, select **Home**.

If you have the Organization admin role and no agent or storage systems are set up, the Home page displays getting started information.



If you already set up the NetApp Console, at least one Console agent is enabled, and at least one cluster or Cloud Volumes ONTAP system has been added on that agent, the Home page shows metrics about your storage environment.



## Enable metrics to appear on the Home page

You can see metrics on the Home page when the following conditions are met:

- You are logged into a SaaS instance of the NetApp Console.
- You belong to an organization with existing storage resources (agent and cluster or Cloud Volumes ONTAP system).
- At least one Console agent is enabled.
- At least one cluster or Cloud Volumes ONTAP system has been added on that agent.

To enable metrics to appear on the Home page, complete the following tasks:

- Enable at least one Console agent.
- Add at least one cluster or one Cloud Volumes ONTAP using that agent.

## View the overall storage capacity

The Storage capacity pane provides the following information across ONTAP clusters and Cloud Volumes ONTAP systems:

- Number of ONTAP systems discovered in the Console
- Number of Cloud Volumes ONTAP systems discovered in the Console
- Capacity usage per cluster

The order of the clusters or Cloud Volumes ONTAP systems is based on the amount of capacity used. The cluster or system with the highest capacity appears first for easy identification.

Warning indicators show for clusters at 80% capacity, with data updating every five minutes.



If you have multiple projects, you might see different data in the Storage capacity pane compared to the Systems page. This is because the Systems page shows information based on the project level, whereas the Storage capacity pane shows information at the organization level. Also, the data on this pane might differ from real values for a maximum of 15 minutes because the data is cached for that duration to optimize performance.

### Steps

1. From the NetApp Console menu, review the Storage capacity pane.
2. In the Storage capacity pane, select **View** to go to the Console Systems page.
3. On the Systems page, select the project containing the cluster you want to view.
4. On the Systems page, select a cluster to view more details about that cluster.

## View ONTAP alerts

View issues or potential risks in your NetApp on-premises ONTAP environments. You can see some non-EMS alerts and some EMS alerts.

The data updates every 5 minutes.

You can see ONTAP alerts with these severities:

- Critical
- Warning
- Informational

You can see ONTAP alerts for these impact areas:

- Capacity
- Performance
- Protection
- Availability
- Security



Caching optimizes performance, but may cause the data on this pane to differ from actual values for up to 15 minutes.

## Systems supported

- An on-premises ONTAP NAS or SAN system is supported.
- Cloud Volumes ONTAP systems are not supported.

## Data sources supported

View alerts regarding certain events that occur in ONTAP. They are a combination of EMS and metric-based alerts.

For details about ONTAP alerts, refer to [About ONTAP alerts](#).

For a list of alerts that you might see, refer to [View potential risks in ONTAP storage](#).

## Steps

1. From the NetApp Console menu, review the ONTAP alerts pane.
2. Optionally, filter the alerts by selecting the severity level or change the filter to show alerts based on impact area.
3. In the ONTAP alerts pane, select **View** to go to the Console Alerts page.

## View storage performance capacity

Review the storage performance capacity used per cluster or Cloud Volumes ONTAP system to determine how performance capacity, latency, and IOPS are impacting your workloads. For example, you might find that you need to shift workloads to minimize latency and maximize IOPS and throughput for your critical workloads.

The system arranges clusters and systems by performance capacity, listing the highest capacity first for easy identification.



Caching optimizes performance, but may cause the data on this pane to differ from actual values for up to 15 minutes.

## Steps

1. From the NetApp Console menu, review the Storage performance pane.



2. In the Storage performance pane, select **View** to go to a Performance page that lists all the clusters and Cloud Volumes ONTAP systems data for performance capacity, IOPS, and latency.
3. Select a cluster to view its details in System Manager.

## View the licenses and subscriptions that you have

Review the following information on the Licenses and subscriptions pane:

- The total number of licenses and subscriptions that you have.
- The number of each type of license and subscription that you have (direct license, annual contract, or PAYGO).
- The number of licenses and subscriptions that are active, require action, or nearing expiration.
- The system displays indicators next to the license types that require action or are nearing expiration.

The data refreshes every 5 minutes.



Caching optimizes performance, but may cause the data on this pane to differ from actual values for up to 15 minutes.

### Steps

1. From the NetApp Console menu, review the Licenses and subscriptions pane.
2. In the Licenses and subscriptions pane, select **View** to go to the Console Licenses and subscriptions page.

## View Ransomware Resilience status

Find out if workloads are at risk of ransomware attacks or protected with the NetApp Ransomware Resilience data service. You can review the total amount of data that is protected, view the number of recommended actions, and view the number of alerts related to ransomware protection.

The data refreshes every 5 minutes and matches the data shown in the NetApp Ransomware Resilience Dashboard.

[Learn about NetApp Ransomware Resilience.](#)

### Steps

1. From the NetApp Console menu, review the Ransomware Resilience pane.
2. Do one of the following in the Ransomware Resilience pane:
  - Select **View** to go to the NetApp Ransomware Resilience Dashboard. For details, refer to [Monitor workload health using the NetApp Ransomware Resilience Dashboard](#).
  - Review "Recommended actions" in the NetApp Ransomware Resilience Dashboard. For details, refer to [Review protection recommendations on the NetApp Ransomware Resilience Dashboard](#).
  - Select the alerts link to review alerts in NetApp Ransomware Resilience Alerts page. For details, refer to [Handle detected ransomware alerts with NetApp Ransomware Resilience](#).

## View Backup and Recovery status

Review the overall status of your backups and restores from NetApp Backup and Recovery. You can see the number of protected and unprotected resources. You can also see the percentage of backups and restore operations for protection of your workloads. A higher percentage indicates improved data protection.

The data refreshes every 5 minutes.



Caching optimizes performance, but may cause the data on this pane to differ from actual values for up to 15 minutes.

### Steps

1. From the NetApp Console menu, review the Backup and Recovery pane.
2. Select **View** to go to the NetApp Backup and Recovery Dashboard. For details, refer to [NetApp Backup and Recovery documentation](#).

## Manage your NetApp Console user settings

You can modify your Console profile including change your password, enable multi-factor authentication (MFA), and see who your Console administrator is.

Within the Console, 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 Console display name that is used to identify you 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 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 improve security by requiring a second verification method.

Users who use 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 used for 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 Console administrator for help.

#### Steps

1. Select the profile icon in the upper right corner of the 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, the Console prompts you to enter a one-time code from your authentication app each time you log in.

## 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 the 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 login, 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 Organization administrator to reset your MFA configuration.

### Steps

1. Select the profile icon in the upper right corner of the 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 the Console. 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 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 the Console to display in dark mode.

### Steps

1. Select the profile icon in the upper right corner of the Console to view the User settings panel.
2. Move the **Dark theme** slider to enable it.

# Administer NetApp Console

## Identity and access management

### Learn about NetApp Console identity and access management

Identity and access management (IAM) within the NetApp Console 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 Console deployment modes](#)

### How IAM works

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.

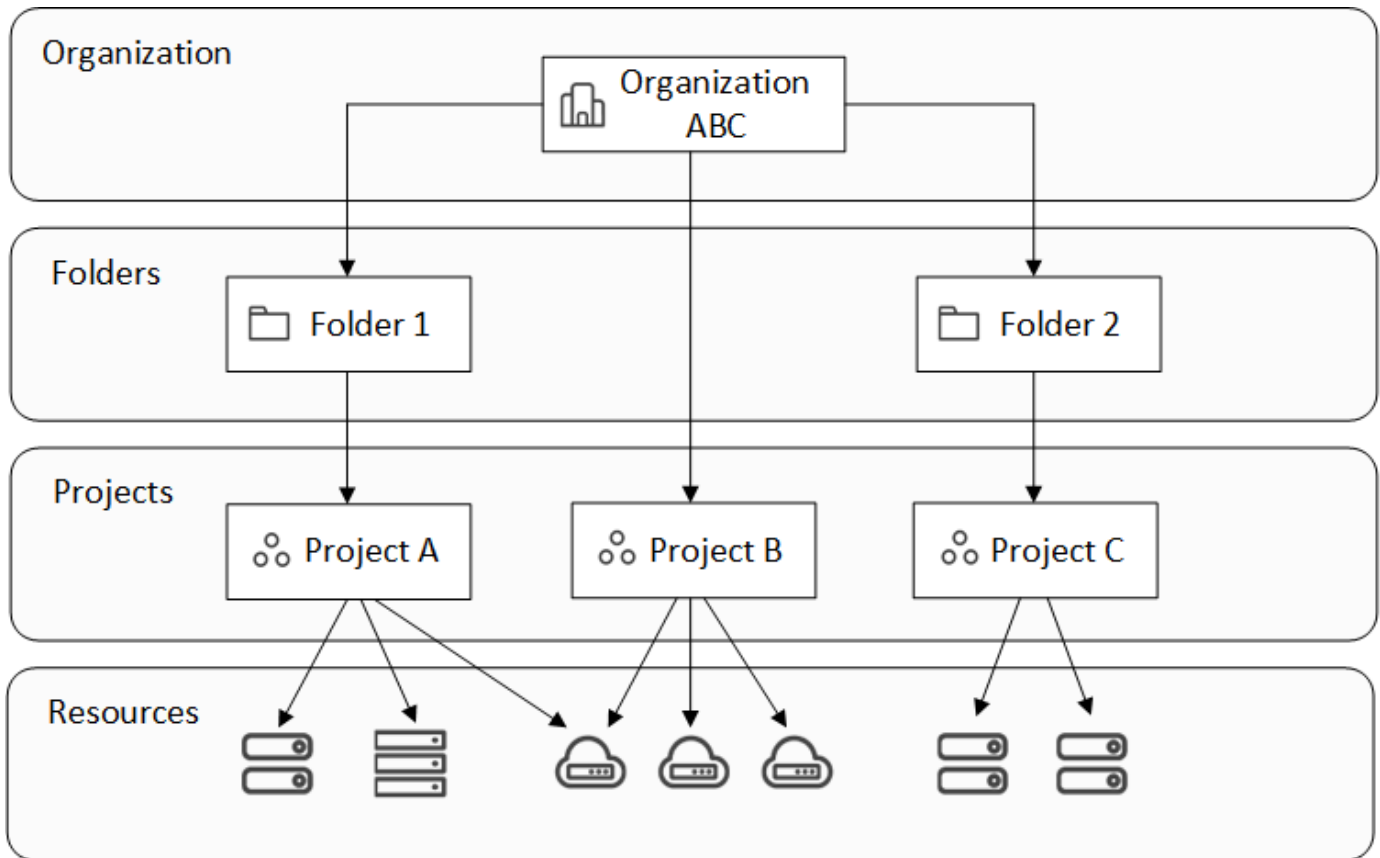
When using IAM, you manage the following components:

- The organization
- Folders
- Projects
- Resources
- Members
- Roles and permissions
- Console agents

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 the Console IAM system and typically represents your company. Your organization consists of folders, projects, members, roles, and resources. Agents 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).

You can organize folders to contain projects, other folders, or both. They are optional.

## Projects

A *project* represents a workspace in the Console that organization members access from the **Systems** page 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 system that you created or discovered in the Console.

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.



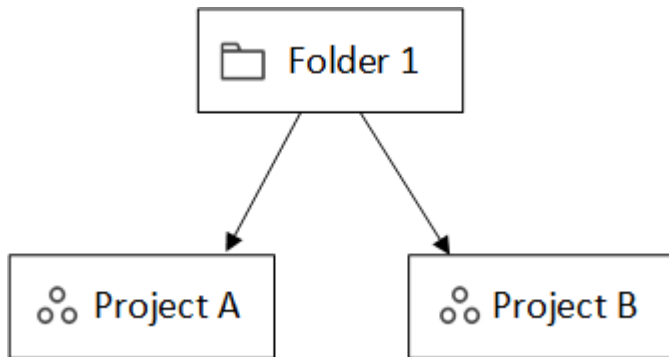
Agents can also be associated with more than one project. [Learn more about using agents with IAM.](#)

### When to associate a resource with a folder

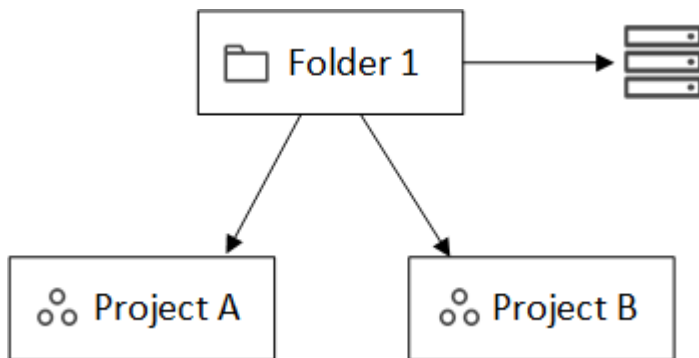
You also have the option to associate a resource with a folder, but this is optional and meets the needs of a specific use case.

An *Organization administrator* can associate a resource with a folder so a *Folder or project administrator* can link it to the appropriate projects in the folder.

For example, let's say you have a folder that contains two projects:

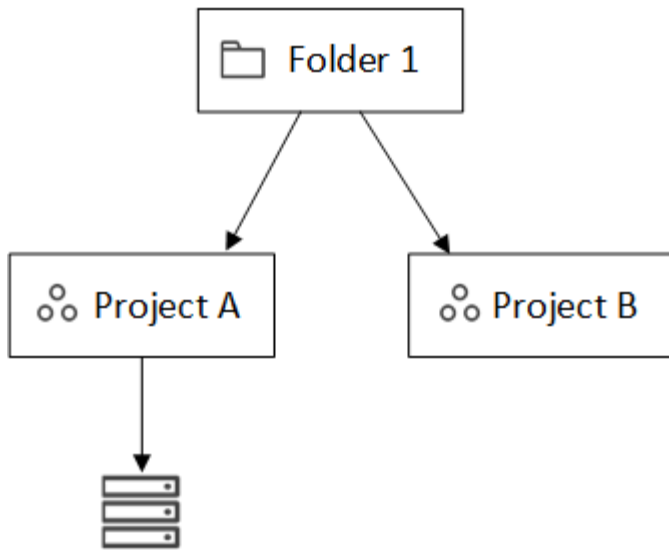


The *Organization admin* can associate a resource with the folder:



Associating a resource with a folder does not 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 (the Console 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

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 roles at a hierarchy level restricts access to the resources and services a member needs.

### 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

The Console provides access roles that you can assign to the members of your organization.

[Learn about access roles.](#)

## Console agents

When an *Organization admin* creates a Console agent, the Console automatically associates that agent with the organization and the currently selected project. The *Organization admin* automatically has access to that agent from anywhere in the organization. But if you have other members in your organization with different roles, those members can only access that agent from the project in which it was created, unless you associate that agent with other projects.

You make a Console agent available for another project in these cases:

- You want to allow members in your organization to use an existing agent to create or discover additional systems in another project
- You associated an existing resource with another project and that resource is managed by a Console agent

If a resource that you associate with an additional project is discovered using a Console agent then you also need to associate the agent with the project that the resource is now associated with. Otherwise, the agent and its associated resource aren't accessible from the **Systems** page by members who don't have the *Organization admin* role.

You can create an association from the **Agents** page within the Console IAM:

- Associate a Console agent with a project

When you associate a Console agent with a project, that agent is accessible from the **Systems** page when viewing the project.

- Associate a Console agent with a folder

Associating a Console agent with a folder doesn't automatically make that agent accessible from all projects in the folder. Organization members can't access a Console agent from a project until you associate the agent with that specific project.

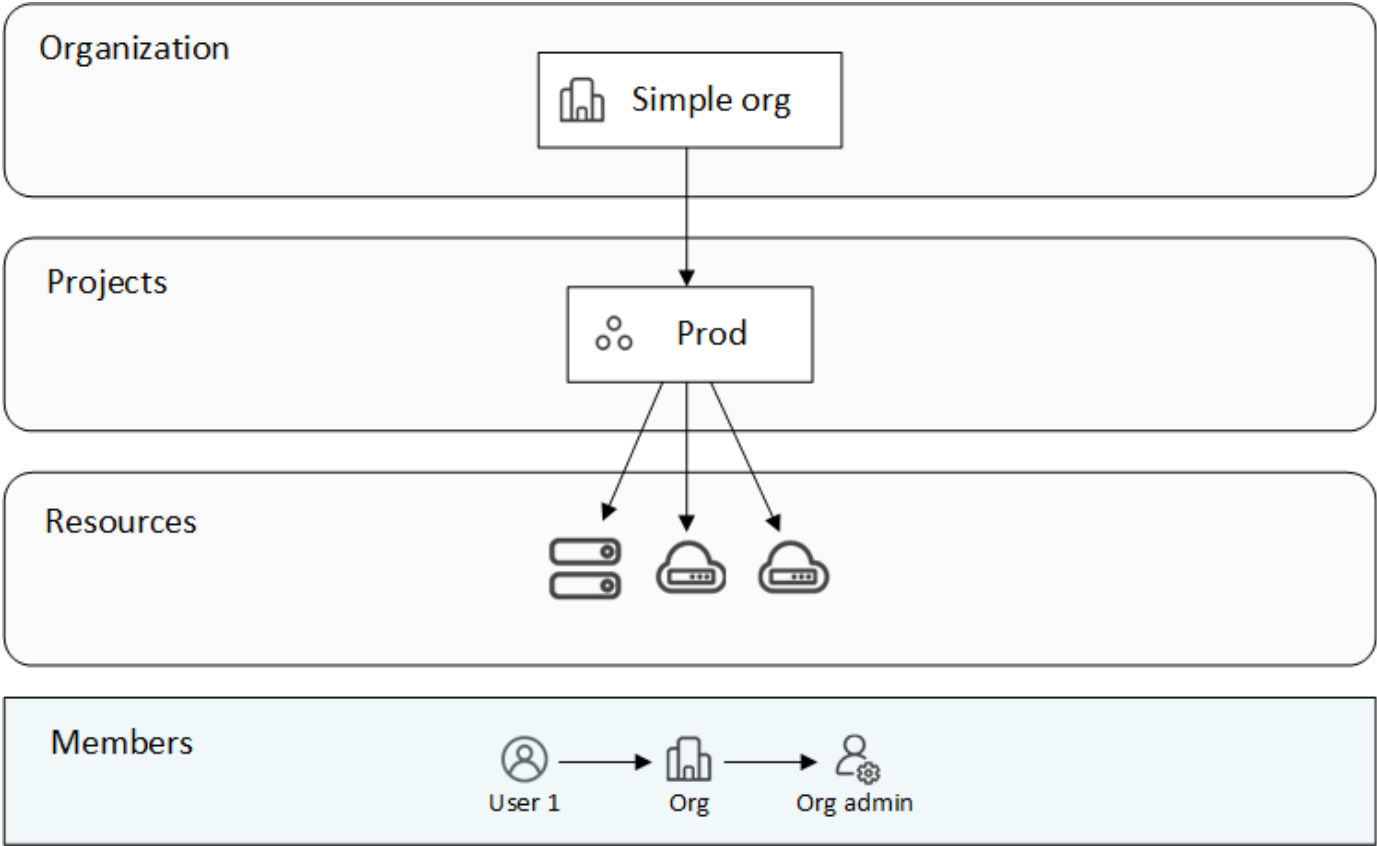
An *Organization admin* might associate a Console agent with a folder so that the *Folder or project admin* can make the decision to associate that agent with the appropriate projects that reside in the folder.

**IAM examples**

These examples demonstrate how you might set up your organization.

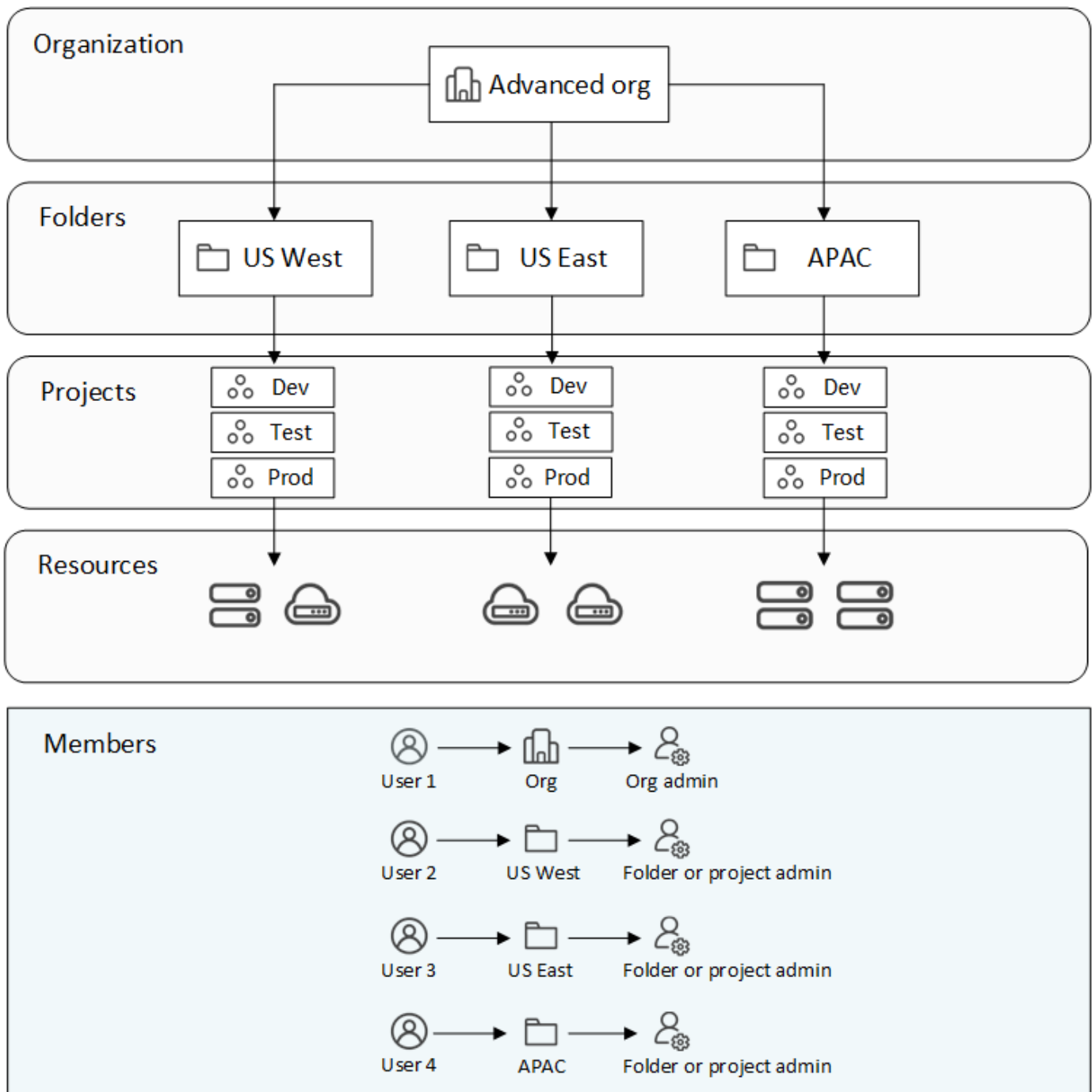
**Simple organization**

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 IAM

The following examples describe how you might use IAM to manage your Console 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 IAM in NetApp Console](#)
- [Organize your resources in NetApp Console with folders and projects](#)
- [Manage NetApp Console members and their permissions](#)
- [Manage the resource hierarchy in your NetApp Console organization](#)
- [Associate agents with folders and projects](#)
- [Switch between NetApp Console projects and organizations](#)
- [Rename your NetApp Console organization](#)
- [Monitor or audit IAM activity](#)
- [NetApp Console access roles](#)
- [Learn about the API for NetApp Console IAM](#)

## Get started with identity and access in NetApp Console

When you sign up for the NetApp Console, you're prompted to create a new organization. The organization includes one member (an Organization admin) and one default project. To set up 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 identity and access for your entire organization. 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 organization. The order may vary based 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

Link user accounts to your organization and assign 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 (systems) to the Console. Organization members manage systems 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

Adding or discovering a system in the Console automatically associates the resource with the currently selected project. To make that resource available to another project in your organization, associate it with the respective project. If a Console agent is used to manage the resource, associate the Console agent with the respective project.

- [Learn how to manage your organization's resource hierarchy.](#)
- [Learn how to associate a Console agent with a folder or project.](#)

#### Related information

- [Learn about identity and access management in NetApp Console](#)
- [Learn about the API for identity and access](#)

## Organize your NetApp Console resources with folders and projects

Within the NetApp Console, you organize your NetApp resources using projects and folders. A *project* represents a workspace in the Console 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 organization, it includes a single project. Add projects to manage resources and folders to group related projects.

Your organization's resource hierarchy can have up to seven levels, with folders nested six levels deep and projects at the seventh.

#### Steps

1. Select **Administration > Identity and access**.
2. Select **Organization**.
3. From the **Organization** page, select **Add folder or project**.
4. Select **Folder** or **Project**.

5. 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 be directly under the organization or inside 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.

[Learn when to 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.

Select **Add a member** to assign access and a role to additional members. A role defines the permissions that members have for the folder or project.

[Learn about access roles.](#)

6. Select **Add**.

### 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

Delete folders and projects you no longer need.

#### Before you begin

- Ensure the folder or project has no associated resources. [Learn how to disassociate resources.](#)
- Make sure the folder or project has no associated resources.

#### 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

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 to 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)

Learn more about user roles

Add a member

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. Update member permissions at the higher hierarchy level to change access. 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 identity and access in NetApp Console](#)
- [Get started with identity and access](#)
- [Learn about the identity and access API](#)

## Add members and service accounts to NetApp Console

Within the Console, you can add users and service accounts 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 (user or service account) to perform specific actions at a specific level of the resource hierarchy.

You need one of the following roles to manage users and permissions:

- 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. [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. Applications use service accounts to perform API tasks without human intervention. A person typically uses a user account to log in and manage resources.

Users must sign up for the NetApp Console before you can add them to an organization or assign them a role. You create service accounts directly from the Console.

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.

### Add a user account

Although users sign up for the NetApp Console on their own, they need to be explicitly added to an organization or to specific folders or projects to access resources in the Console.

#### Steps

1. Direct the user to visit [NetApp Console](#) to sign up.

Once users sign up, they complete the **Sign up** page, check their email, and log in. If the Console 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 organization.

[Learn how to sign up for the NetApp Console.](#)

2. Select **Administration > Identity and access**.
3. Select **Members**.
4. Select **Add a member**.
5. For **Member Type**, keep **User** selected.
6. For **User's email**, enter the user's email address that is associated with the login that they created.
7. Use the **Select an organization, folder, or project** section to 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 permissions.
  - Selecting an organization or folder grants the member permissions to all its contents.
  - You can only assign the **Organization admin** role at the organization level.
8. **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.

[Learn about access roles.](#)

9. Optional: Select an additional role or project. If you want to provide access to additional folders or projects within your organization or grant the user additional roles in the selected area, select **Add role**, specify another folder or project or a different role category and then choose a role.
10. Select **Add**.

The Console sends the user an email with instructions.

### Add a service account

You can automate tasks and integrate with Console APIs securely with service accounts. When you create a service account, choose between two authentication methods: using a client ID and secret, or using JWT (JSON Web Token) authentication. The client ID and secret method suits simple setups, while JWT authentication offers stronger security for automated or cloud-native environments. Choose the option that best fits your security needs and how you plan to use the Console.

If you want to use JWT authentication, have your public key or certificate ready to use.

### Steps

1. Select **Administration > Identity and access**.
2. Select **Members**.
3. Select **Add a member**.
4. For **Member Type**, select **Service account**.
5. Enter a name for the service account.
6. If you want to use JWT authentication, select **Use private key JWT authentication** and upload your public RSA key or certificate. Skip this step if you want to use a client ID and secret instead.

Your X.509 certificate. It must be in PEM, CRT, or CER format.

7. Use the **Select an organization, folder, or project** section to 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 permissions.
  - Selecting an organization or folder grants the member permissions to all its contents.
  - You can only assign the **Organization admin** role at the organization level.
8. 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.

[Learn about access roles.](#)

9. Optional: Select an additional role or project. If you want to provide access to additional folders or projects within your organization or grant the user additional roles in the selected area, select **Add role**, specify another folder or project or a different role category and then choose a role.
10. If you didn't choose to use JWT authentication, download or copy the client ID and client secret. The Console shows the client secret only once. Copy it securely; you can recreate it later if needed.
11. If you chose JWT authentication, download or copy the client ID and JWT audience. This information is shown only once and cannot be retrieved later.
12. Select **Close**.

### View organization members

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 Console 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. Select **Administration > Identity and access**.
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.

The system removes the member's permissions but keeps their Console 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 you lose them or need to update them.

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. Select **Administration > Identity and access**.
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.  
The client secret displays only once. Copy or download it and store it securely.

### Manage a user's multi-factor authentication (MFA)

If a user loses access to their MFA device, you can either remove or disable their MFA configuration.

Users must reconfigure MFA at login after removal. 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.

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 manage a user's multi-factor authentication, you must have an email address in the same domain as the affected user.

#### Steps

1. Select **Administration > Identity and access**.
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 **Manage multi-factor authentication**.

4. Choose whether to remove or to disable the user's MFA configuration.