Get started

NetApp Console setup and administration

NetApp
January 27, 2026

Table of Contents

Get started

Learn the basics

Learn about NetApp Console

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

It is available as a service (SaaS) platform or a self-hosted option that you can install in your sovereign cloud. It provides storage management, data mobility, data protection, and data analysis and control. Management capabilities are provided through a web-based console and APIs.

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

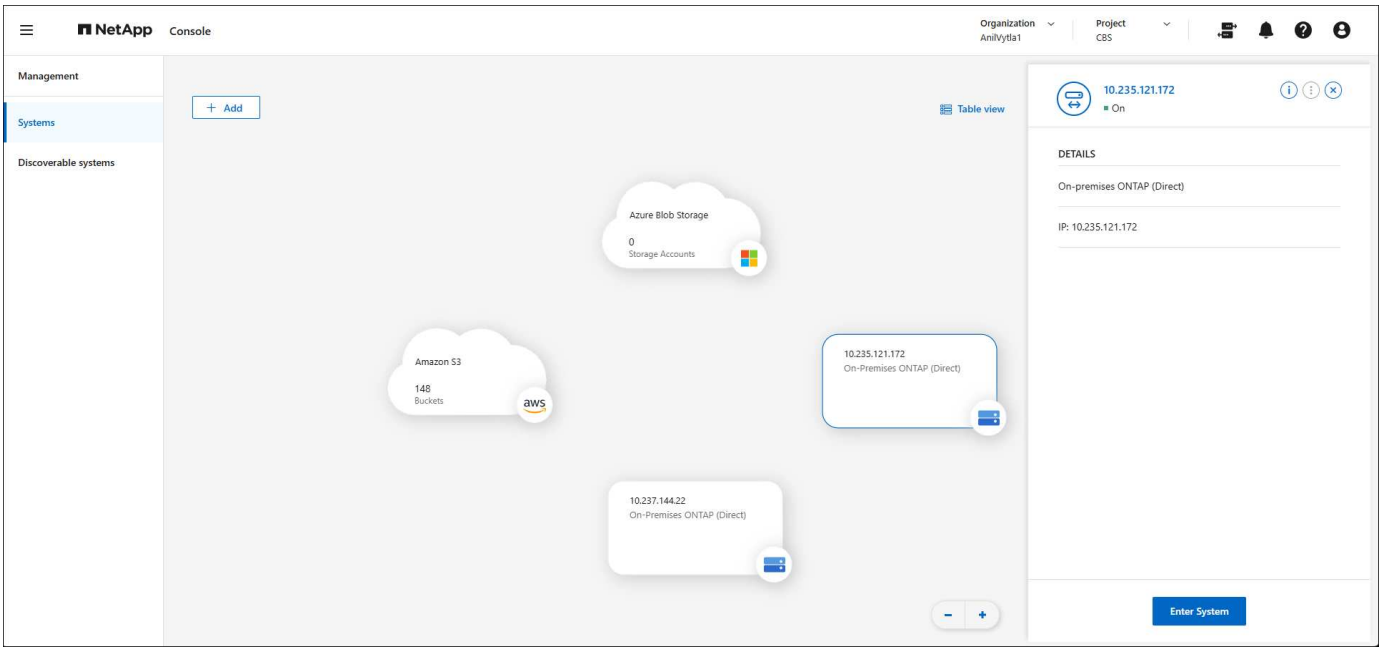
- E-Series systems
- ONTAP clusters
- StorageGRID systems

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-premisesand 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.

SaaS versus sovereign cloud deployment

You can start using NetApp Console by signing up for the SaaS offering or deploying it in your sovereign cloud. When you deploy NetApp Console in a sovereign cloud, NetApp limits outbound connectivity to meet your organization's security and compliance requirements. Not all features and services are available when the Console is deployed in a sovereign cloud.

NetApp continues to offer BlueXP for sites that want no outbound connectivity. BlueXP can be installed on your network with no outbound connectivity. 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 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

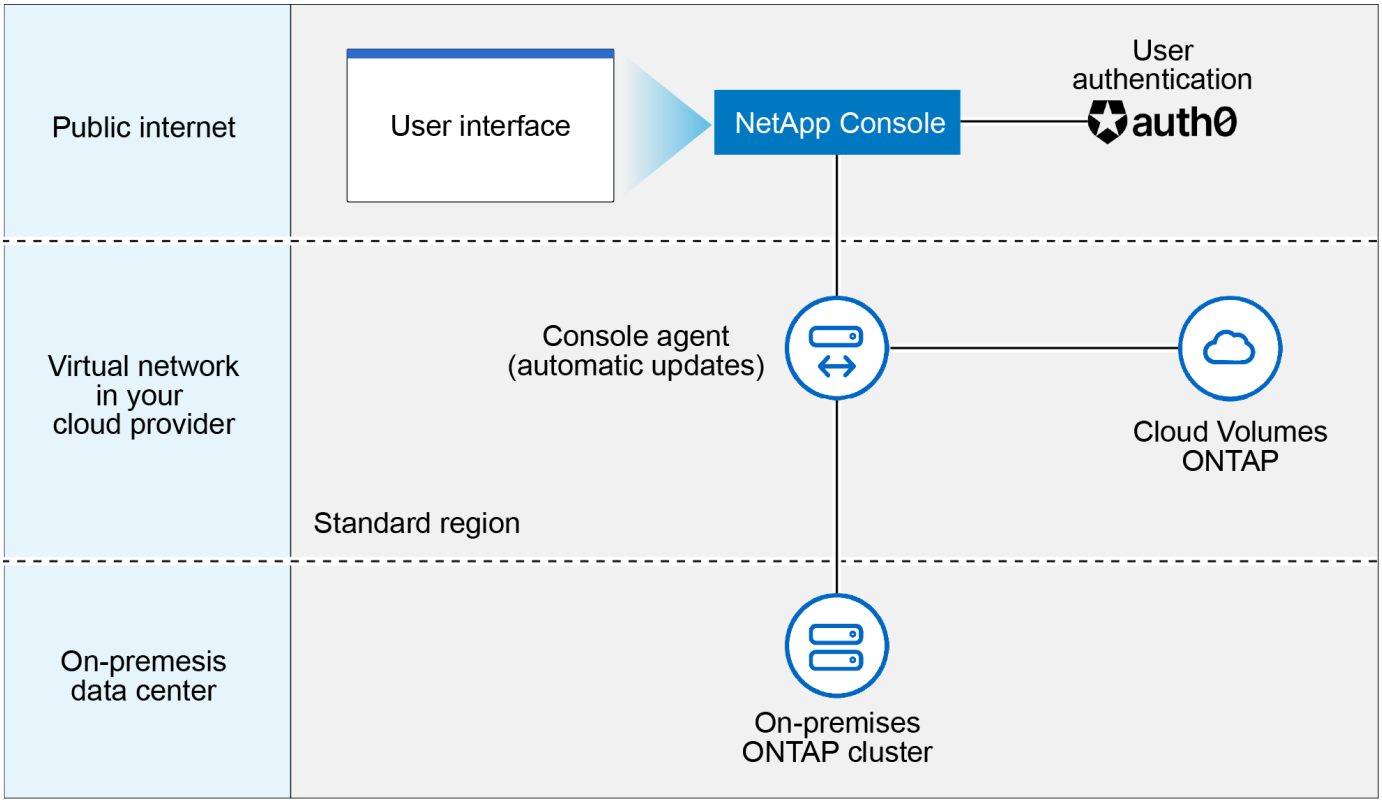
The following table provides a comparison of the NetApp console.

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

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.bluexp.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.

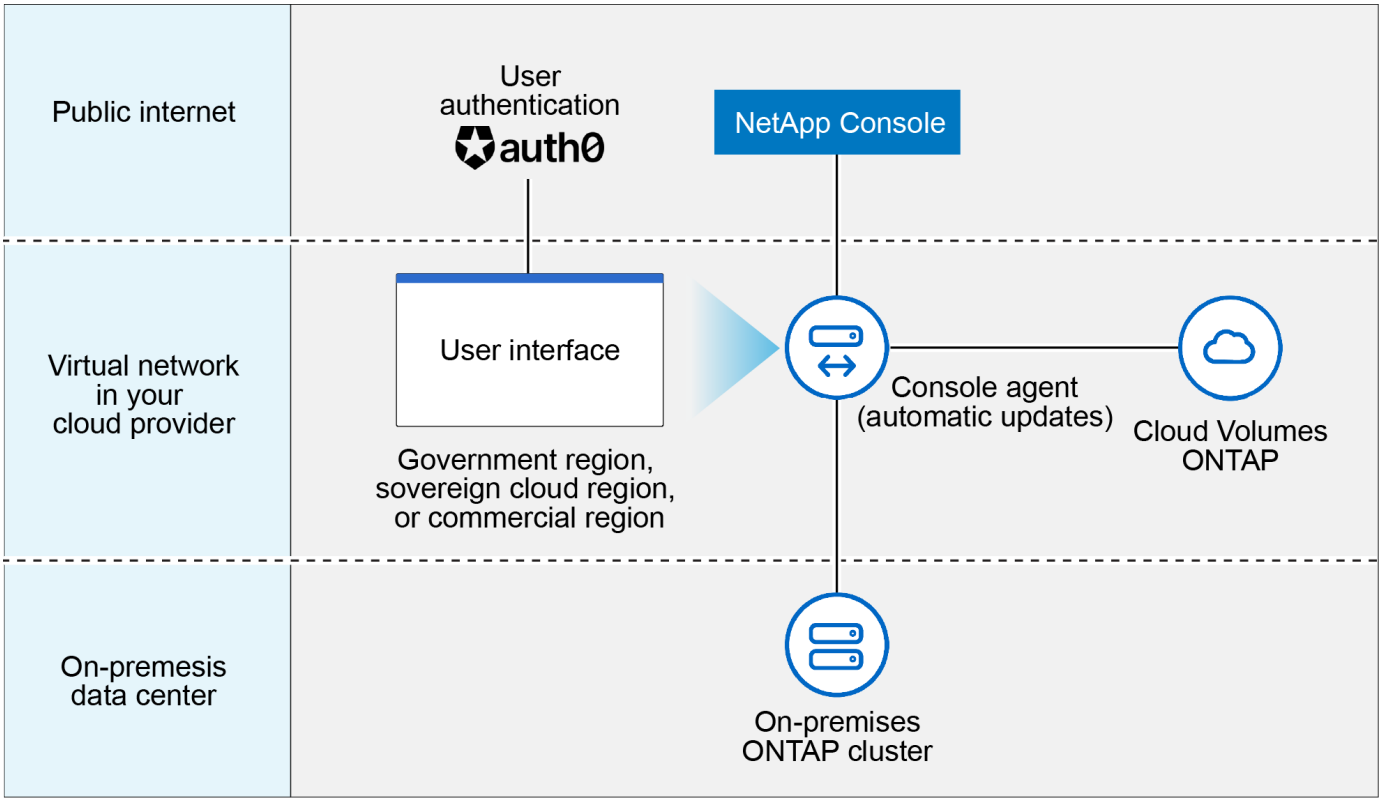
How to get started with standard mode

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 us 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. View the list of supported backup destinations for ONTAP data 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

Supported services	Notes
Licenses and subscriptions	You can access license and subscription information with the supported licensing options listed below for restricted mode.
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
Storage 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
Data Services	NetApp Backup and recovery	Yes View the list of supported backup destinations for ONTAP volume data
	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

Manage NSS credentials associated with NetApp Console

Associate a NetApp Support Site account with your Console organization to enable key workflows for storage management. These NSS credentials are associated with the entire organization.

The Console also supports associating one NSS account per user account. Learn how to manage user-level credentials.

Overview

Associating NetApp Support Site credentials with your specific Console account serial number is required to enable the following tasks:

- Deploying Cloud Volumes ONTAP when you bring your own license (BYOL)

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

- Registering pay-as-you-go Cloud Volumes ONTAP systems

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

- Upgrading Cloud Volumes ONTAP software to the latest release

These credentials are associated with your specific Console account serial number. Users can access these credentials from **Support > NSS Management**.

Add an NSS account

You can add and manage your NetApp Support Site accounts for use with the Console from the Support Dashboard within the Console.

When you have added your NSS account, the Console uses this information for things like license downloads, software upgrade verification, and future support registrations.

You can associate multiple NSS accounts with your organization; however, you cannot have customer accounts and partner accounts within the same organization.

NetApp uses Microsoft Entra ID as the identity provider for authentication services specific to support and licensing.

Steps

1. In **Administration > Support**.
2. Select **NSS Management**.
3. Select **Add NSS Account**.
4. Select **Continue** to be redirected to a Microsoft login page.
5. At the login page, provide your NetApp Support Site registered email address and password.

   Upon successful login, NetApp will store the NSS user name.

   This is a system-generated ID that maps to your email. On the **NSS Management** page, you can display your email from the ••• menu.

   - If you ever need to refresh your login credential tokens, there is also an **Update Credentials** option in the ••• menu.

     Using this option prompts you to log in again. Note that the token for these accounts expire after 90 days. A notification will be posted to alert you of this.

What's next?

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

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

Update NSS credentials

For security reasons, you must update your NSS credentials every 90 days. You'll be notified in the Console notification center if your NSS credential has expired. Learn about the Notification Center.

Expired credentials can disrupt the following, but are not limited to:

- License updates, which mean you won't be able to take advantage of newly purchased capacity.
- Ability to submit and track support cases.

Additionally, you can update the NSS credentials associated with your organization if you want to change the NSS account associated with your organization. For example, if the person associated with your NSS account has left your company.

Steps

1. In **Administration > Support**.
2. Select **NSS Management**.
3. For the NSS account that you want to update, select ••• and then select **Update Credentials**.
4. When you're prompted, select **Continue** to be redirected to a Microsoft login page.

   NetApp uses Microsoft Entra ID as the identity provider for authentication services related to support and licensing.

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

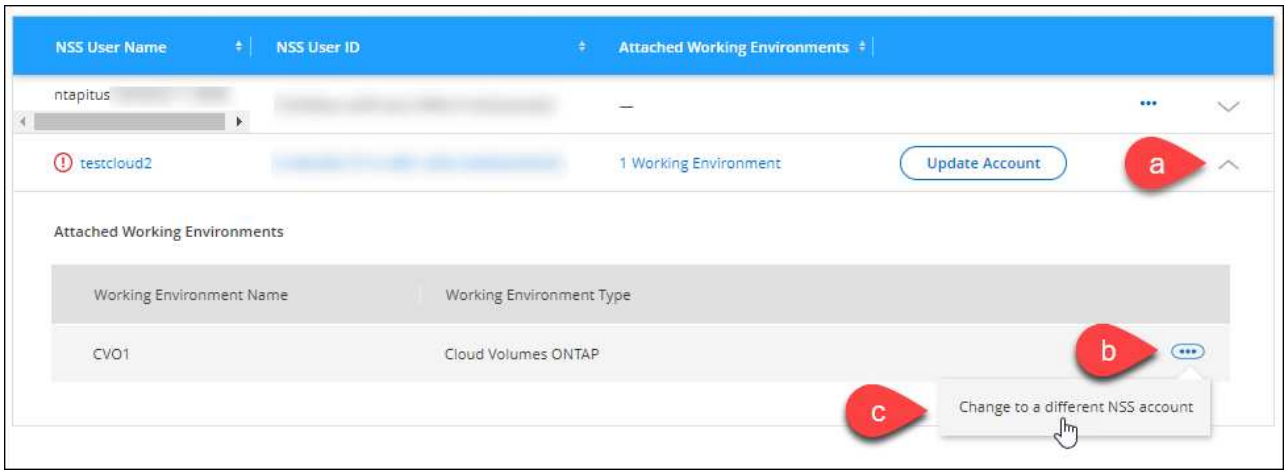
Attach a system to a different NSS account

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

You must first have associated the account with the Console.

Steps

1. In **Administration > Support**.
2. Select **NSS Management**.
3. Complete the following steps to change the NSS account:
   a. Expand the row for the NetApp Support Site account that the system is currently associated with.
   b. For the system that you want to change the association for, select •••
   c. Select **Change to a different NSS account**.



   d. Select the account and then select **Save**.

Display the email address for an NSS account

For security, the email address associated with an NSS account is not displayed by default. You can view the email address and associated user name for an NSS account.

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

Steps

1. In **Administration > Support**.
2. Select **NSS Management**.
3. For the NSS account that you want to update, select ••• and then select **Display Email Address**. You can use the copy button to copy the email address.

Remove an NSS account

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

You can't delete an account that is currently associated with a Cloud Volumes ONTAP system. You first need to attach those systems to a different NSS account.

Steps

1. In **Administration > Support**.
2. Select **NSS Management**.
3. For the NSS account that you want to delete, select ••• and then select **Delete**.
4. Select **Delete** to confirm.

Learn about NetApp Console agents

You use a Console agent to connect NetApp Console to your infrastructure and securely orchestrate storage solutions across AWS, Azure, Google Cloud, or on-premises environments, as well as use data protection services.

A Console agent enables you to:

- Orchestrate storage management tasks from the NetApp Console such as provisioning Cloud Volumes ONTAP, setting up storage volumes, using data classification, and more.
- Authenticate using your cloud provider's IAM roles for subscription billing integration
- Use advanced data services (NetApp Backup and Recovery, NetApp Disaster Recovery, NetApp Ransomware Resilience, and NetApp Cloud Tiering)
- Use the Console in restricted mode.

If you don't need advanced orchestration or data protection, you can centrally manage on-premises ONTAP clusters and cloud-native storage services without deploying an agent. Monitoring and data mobility tools are also available.

The following table shows which features and services you can use with and without a Console agent.

	Available with agent	Available without agent
Supported Storage systems:		

	Available with agent	Available without agent
Amazon FSx for ONTAP	Yes (discovery and management features)	Yes (discovery only)
Amazon S3 storage	Yes	No
Azure Blob storage	Yes	Yes
Azure NetApp Files	Yes	Yes
Cloud Volumes ONTAP	Yes	No
E-Series systems	Yes	No
Google Cloud NetApp Volumes	Yes	Yes
Google Cloud storage buckets	Yes	No
StorageGRID systems	Yes	No
On-premises ONTAP cluster (advanced management and discovery)	Yes (advanced management and discovery)	No (basic discovery only)
Available storage management services:		
Alerts	Yes	No
Automation hub	Yes	Yes
Digital Advisor (Active IQ)	Yes	No
License and subscription management	Yes	No
Economic efficiency	Yes	No
Home page dashboard metrics	Yes[2]	No
Lifecycle planning	Yes	No[1]
Sustainability	Yes	No
Software updates	Yes	Yes
NetApp Workloads	Yes	Yes

	Available with agent	Available without agent
Available data services:		
NetApp Backup and Recovery	Yes	No
Data Classification	Yes	No
NetApp Cloud Tiering	Yes	No
NetApp Copy and Sync	Yes	No
NetApp Disaster Recovery	Yes	No
NetApp Ransomware Resilience	Yes	No
NetApp Volume Caching	Yes	No

[1] You can view Lifecycle planning without a Console agent, but a Console agent is required to initiate actions.

[2] Accurate metrics on the Home page require appropriately sized and configured Console agents.

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.

- Learn about NetApp Console deployment modes
- Get started with NetApp Console in standard mode
- Get started with NetApp Console in restricted mode

Cloud provider permissions

You need specific permissions to create the Console agent directly from the NetApp Console and another set of permissions for the Console agent 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.

When you install your agent in the cloud, 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 gent 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 identity and access management

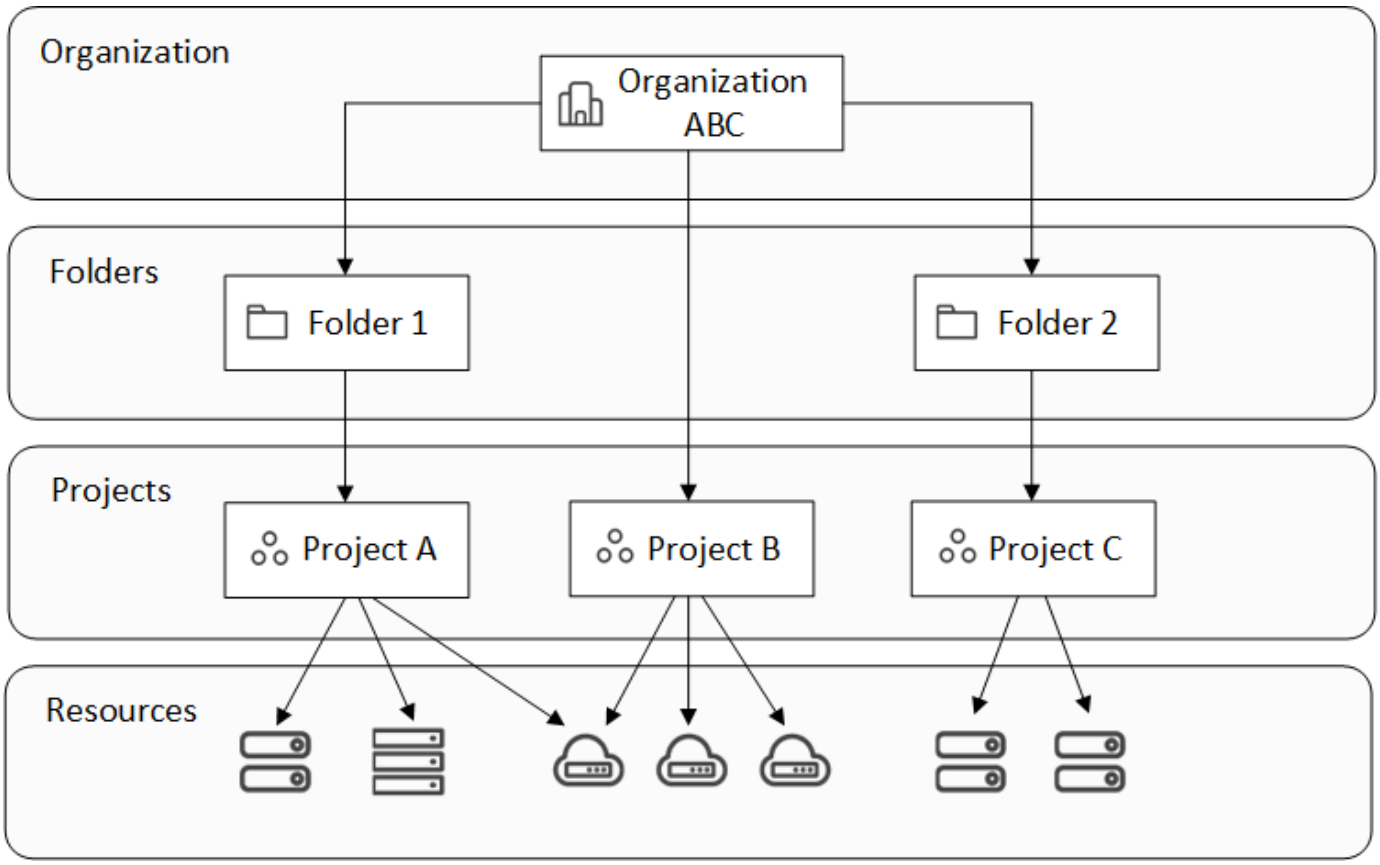
Use NetApp Console's Identity and Access Management (IAM) to organize your NetApp resources and control access according to your business structure—by location, department, or project.

Resources are arranged hierarchically: the organization is at the top, followed by folders (which can contain other folders or projects), and then projects, which contain storage systems, workloads, and agents.

Assign role-based access control (RBAC) permissions to members at the organization, folder, or project level to ensure users have the appropriate access to resources.

You must have the *Super admin*, *Organization admin* , or *Folder or project admin* roles to manage IAM in NetApp Console.

The following image illustrates this hierarchy at a basic level.



]

Identity and access management components

Within NetApp Console, you organize your storage resources using three main components: organizational components, resource components, and user access components.

Projects and folders within your organization

Within your IAM structure, you work with three organizational components are organizations, projects, and folders. You can grant users access by assigning them roles at any of these levels.

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.

Projects

A *project* is used to provide access to a storage resource. You must assign a resources to project before anyone can access them. You can assign multiple resources to a single project and you can also have multiple projects. You then assign users permissions to the project to give them access to the resources within it.

For example, you can associate an on-premises ONTAP system with a single project or with all projects in your organization, depending on your needs.

Learn how to add projects to your organization.

Folders

Group related projects in *folders* to organize them by location, site, or business unit. You can't associate resources directly with folders, but assigning a user a role at the folder level gives them access to all projects in that folder.

Learn how to add folders to your organization.

Resources

Resources include storage systems, Keystone subscriptions, as well as Console agents.

+
You must associate a resource with a project before anyone can access it.

+

For example, you might associate a Cloud Volumes ONTAP system with one project or with all projects in your organization. How you associate a resource depends on your organization's needs.

+

Learn how to associate resources to projects.

Storage systems and Keystone subscriptions

Storage systems are the primary resources that you manage in NetApp Console. NetApp Console supports management of both on-premises and cloud storage systems. You must add a storage system to a project before anyone can access it.

Storage systems are automatically associated with the project where they are added, but you can also associate them with other projects or folders from the **Resources** page.

Keystone subscriptions are also resources that you can associate with projects in order to grant users access to the subscription in NetApp Console.

Console agents

Organization admins create Console agents to manage storage systems and enable NetApp data services. Agents are initially tied to the project where they are created, but admins can add them to other projects or folders from the Agents page.

Associating an agent with a project enables management of resources in that project, while associating an agent with a folder lets folder or project admins decide which projects should use the agent. Agents must be linked to specific projects to provide management capabilities.

Learn how to associate agents with projects.

Members and roles

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.

You need to add members to your organization after they sign up for NetApp Console. Once added, you can assign them roles to provide access to resources. You can manually add service accounts from within the Console or automate their creation and management through the NetApp Console IAM API.

Learn how to add members to your organization.

Access roles

The Console provides access roles that you can assign to the members of your organization.

When you associate a member with a role, you can grant that role for 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.

NetApp Console provides granular roles that adhere to the principles of "least privilege" which means access roles are designed to give users access to only that that they need

This means users may have multiple roles assigned to them as their duties expand.

Learn about access roles.

IAM strategy examples

Small organization strategy

For organizations with fewer than 50 users and centralized storage management, consider a simplified approach using Super admin and Super viewer roles.

Example: ABC Corporation (5-person team)

- **Structure:** Single organization with 3 projects (Production, Development, Backup)
- **Roles:**
  - 2 senior members: **Super admin** role for full administrative access
  - 3 team members: **Super viewer** role for monitoring without modification rights
- **Agent strategy:** Single agent associated with all projects for shared resource access
- **Benefits:** Simplified administration, reduced role complexity, suitable for teams requiring broad access

Multi-regional enterprise strategy

For large organizations with regional operations and specialized teams, implement a hierarchical approach with folders representing geographical or business unit boundaries.

Example: XYZ Corporation (multinational company)

- **Structure:** Organization > Regional folders (North America, Europe, Asia-Pacific) > Project folders per region
- **Platform roles:**
  - 1 **Organization admin**: Global oversight and policy management
  - 3 **Folder or project admins**: Regional control (one per region)
  - 1 **Federation admin**: Corporate identity provider integration
- **Storage roles by region:**
  - 9 **Storage admin**: Discover and manage storage systems in assigned regions
  - 2 **Storage viewer**: Monitor storage resources across regions
  - 1 **System health specialist**: Manage storage health without system modifications

- **Data service roles:**
  - **Backup and Recovery admin**: Per-project based on backup responsibilities
  - **Ransomware Resilience admin**: Security team monitoring across projects
- **Agent strategy:** Regional agents associated with appropriate geographical projects
- **Benefits:** Enhanced security through role segregation, regional autonomy, and compliance with local regulations

Departmental specialization strategy

For organizations with specialized teams requiring specific data service access, use targeted role assignments based on functional responsibilities.

Example: TechCorp (mid-size technology company)

- **Structure:** Organization > Department folders (IT, Security, Development) > Project-specific resources
- **Specialized roles:**
  - Security team: **Ransomware Resilience admin** and **Classification viewer** roles
  - Backup team: **Backup and Recovery super admin** for comprehensive backup operations
  - Development team: **Storage admin** for test environment management
  - Compliance team: **Operation support analyst** for monitoring and support case management
- **Agent strategy:** Agents linked to departmental projects based on resource ownership
- **Benefits:** Tailored access control, improved operational efficiency, and clear accountability for specialized tasks

Next steps with IAM in NetApp Console

- Get started with IAM in NetApp Console
- Monitor or audit IAM activity
- Learn about the API for NetApp Console IAM

Get started with NetApp Console (Saas)

Getting started workflow (SaaS)

Get started with the NetApp Console (SaaS) by preparing networking for the Console, signing up and creating an account, and using the Console assistant to set up initial functionality.

You access a web-based console that is hosted as a Software-as-a-service (SaaS) product from NetApp. You can use the Console to manage your hybrid cloud storage environment and use NetApp data services.

Prepare networking for using the NetApp console

Ensure computers accessing the NetApp console have network access to the required endpoints.

Learn how to prepare networking for the NetApp console.

2 Sign up and create an organization

Go to the NetApp console and sign up. If prompted to create an organization and you think an organization already exists for your company, close the dialog box and tell your organization administrator. If there isn't currently an Organization administrator for your company, you can claim this role. Learn how to contact an organization administrator.

At this point, you're logged in and can use the NetApp assistant to start configuring the Console. To begin, associate your NetApp Support account and a Console agent to enable full functionality.

If you choose not to use the NetApp assistant or install a Console agent, you 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 Associate your NetApp Support Site (NSS) account

Associating your NetApp Support Site (NSS) account with the Console enables you to manage your licenses and subscriptions more easily as well as access support resources directly from the Console.

4 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

5 Add a storage system to the Console

Within the NetApp Console, you can add or discover storage systems to manage your hybrid cloud storage environment. Use the NetApp assistant to add your first storage system.

If you install 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.

- Learn how to discover an ONTAP system
- Learn how to discover a StorageGRID system
- Learn how to discover an E-Series system

6 Subscribe to NetApp Intelligent Services (optional)

Sign up for NetApp Intelligent Services through your cloud provider for hourly (PAYGO) or annual billing. A subscription includes NetApp Backup and Recovery, Cloud Volumes ONTAP, NetApp Cloud Tiering, NetApp Ransomware Resilience, NetApp Disaster Recovery, and NetApp Data Classification.

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)
- Console agents you install on-premises or in the cloud. Console agents.

With 4.0.0, 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 NetApp Console and Console agents

Each agent you deploy and each computer that accesses the NetApp Console must have connections to the endpoints listed below.

Console agents that are deployed in your cloud provider need access to endpoints respective to that cloud provider.

Endpoints	Purpose
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://support.netapp.com	To obtain licensing information and to send AutoSupport messages to NetApp support as well as to receive software updates for Cloud Volumes ONTAP.
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
https://bluexpinfraprod.eastus2.data.azurecr.io https://bluexpinfraprod.azurecr.io	To obtain images for Console agent upgrades. • When you deploy a new agent, the validation check tests connectivity to current endpoints. If you use previous endpoints, the validation check fails. To avoid this failure, skip the validation check. Although the previous endpoints are still supported, NetApp recommends updating your firewall rules to the current endpoints as soon as possible. Learn how to update your endpoint list. • When you update to the current endpoints in your firewall, your existing agents will continue to work.

Cloud provider endpoints contacted the Console agent

Console agents must have access to additional endpoints if they are deployed in your cloud provider.

Set up cloud provider 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

Data services endpoints contacted by the Console agent

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

Endpoints for Workloads

The Console agent must be able to access the following endpoint for NetApp Workloads.

Endpoints	Purpose
https://api.workloads.netapp.com	The web-based console contacts this endpoint to interact with the Workload Factory APIs to manage and operate FSx for ONTAP-based workloads.

Sign up or log in to NetApp Console

To use the Console, sign up or log in with your NetApp Support Site credentials, or create a NetApp Console login. If you are the first from your company to sign up, you create a new organization as the administrator. If your company already has an organization, sign up or log in with your existing NetApp Support Site credentials or company single-sign-on (SSO).

Sign up for NetApp Console as the initial organization administrator

If your company doesn't have a NetApp Console organization, sign up to create one. The first user becomes the organization administrator and manages user accounts and permissions. You can update roles and add more administrators later.

Steps

1. Open a web browser and go to the NetApp Console
2. If you have a NetApp Support Site account, enter the email address associated with your account directly on the **Log in** page.

   The Console signs you up as part of this initial login with your NetApp Support Site credentials.

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**.

      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.

      Verify your email address to complete sign up.

4. After you log in, review and accept the End User License Agreement.
5. On the **Welcome** page, create an organization.
6. Select **Let's Start**.

+ As a first-time user and organization administrator, you follow a guided process to add storage resources, create a Console agent, and more. Learn about using the Console Assistant.

Next steps

As an administrator, after you complete the steps included in the Console Assistant, you should plan your identity and access strategy, add users to your organization, and assign roles. Learn about identity and access management for NetApp Console

Sign up or login to NetApp Console when an organization already exists

If your company already has a NetApp Console organization, sign up or log in to access it. Your sign-up or log-in method depends on whether your company uses identity federation or has NetApp Support Site credentials. If not, create a NetApp Console log-in.

Steps

1. Open a web browser and go to the NetApp Console

2. If you have a NetApp Support Site account or if your company has set up single sign-on (SSO), enter your associated email address or SSO credentials on the **Log in** page. Follow the prompts to complete login.

   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**.

      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.

      Verify your email address to complete sign up.

4. After you log in, review and accept the End User License Agreement.
5. If the system prompts you to create an organization, close the dialog box and tell a Console admin so they can add you to your Console organization and give you access. Learn how to contact an organization administrator.

Next steps

After you are given access to your organization, you can start managing storage and using the data services that you are assigned.

Get started using the NetApp Console assistant

If you are a first-time user of the NetApp Console (SaaS) 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.

By default, the NetApp Console displays the Console assistant on the Home page for first-time users who have the Organization admin role. It remains available until you complete the mandatory tasks of creating a Console agent and adding a system.

Use the assistant to complete these tasks, which provide the minimal set up for your NetApp Console environment:

- Add a NetApp Support Site (NSS) account.

  Learn how to add an NSS account.

- Connect to your storage estate by deploying a Console agent.

  Learn how to install a Console agent on-premises.

- Manage a storage system by adding or discovering a cluster

- Add a marketplace subscription or PAYGO license.

  Learn how to add licenses and subscriptions.

- Review data services information.

Get started with NetApp Console (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.

Prepare for deployment

a. Prepare a dedicated Linux host that meets requirements for CPU, RAM, disk space, container orchestration tool, and more.

b. Set up networking that provides access to the target networks, outbound internet access for manual installations, and outbound internet for day-to-day access.

c. Set up permissions in your cloud provider so that you can associate those permissions with the Console agent instance after you deploy it.

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.

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 requires a dedicated host. Any architecture is supported if it meets these 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 Podman or Docker are architected to create the containers within this directory. Specifically, they will create containers in the `/var/lib/containers/storage` directory and `/var/lib/docker` for Docker. External mounts or symlinks do not work for this space.

AWS EC2 instance type

An instance type that meets CPU and RAM requirements. NetApp recommends t3.2xlarge.

Azure VM size

An instance type that meets CPU and RAM requirements. NetApp recommends Standard_D8s_v3.

Google Cloud machine type

An instance type that meets CPU and RAM requirements. NetApp recommends n2-standard-8.

The Console agent is supported in Google Cloud on a VM instance with an OS that supports Shielded VM features

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				
	9.6 • English language versions only. • 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.	4.0.0 or later with the Console in standard mode or restricted mode	Podman version 5.4.0 with podman-compose 1.5.0. View Podman configuration requirements.	Supported in enforcing mode or permissive mode

Operating system	Supported OS versions	Supported agent versions	Required container tool	SELinux
	9.1 to 9.4 • English language versions only. • 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.	3.9.50 or later with the Console in standard mode or restricted mode	Podman version 4.9.4 with podman-compose 1.5.0. View Podman configuration requirements.	Supported in enforcing mode or permissive mode
	8.6 to 8.10 • English language versions only. • 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.	3.9.50 or later with the Console in standard mode or restricted mode	Podman version 4.6.1 or 4.9.4 with podman-compose 1.0.6. View Podman configuration requirements.	Supported in enforcing mode or permissive mode
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

Operating system	Supported OS versions	Supported agent versions	Required container tool	SELinux
	22.04 LTS	3.9.50 or later	Docker Engine 23.0.6 to 28.0.0.	Not supported

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 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, verify that your Podman version is using Netavark 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.

   a. For Red Hat Enterprise Linux 9.6:

   ```
   sudo dnf install podman-5:<version>
   ```

   Where <version> is the supported version of Podman that you're installing. View the supported Podman versions.

   b. For Red Hat Enterprise Linux 9.1 to 9.4:

   ```
   sudo dnf install podman-4:<version>
   ```

   Where <version> is the supported version of Podman that you're installing. View the supported Podman versions.

   c. For Red Hat Enterprise Linux 8:

   ```
   sudo dnf install podman-4:<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.

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

6. If using Red Hat Enterprise 9:

   a. Install the EPEL repository package.

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

   a. Install podman-compose package 1.5.0.

```
sudo dnf install podman-compose-1.5.0
```

7. If using Red Hat Enterprise Linux 8:

   a. Install the EPEL repository package.

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

   b. 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.

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

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

```
podman info | grep networkBackend
```

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

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

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

iv. 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`.

v. Restart podman.

```
systemctl restart podman
```

vi. 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
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://cdn.auth0.com https://services.cloud.netapp.com	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.

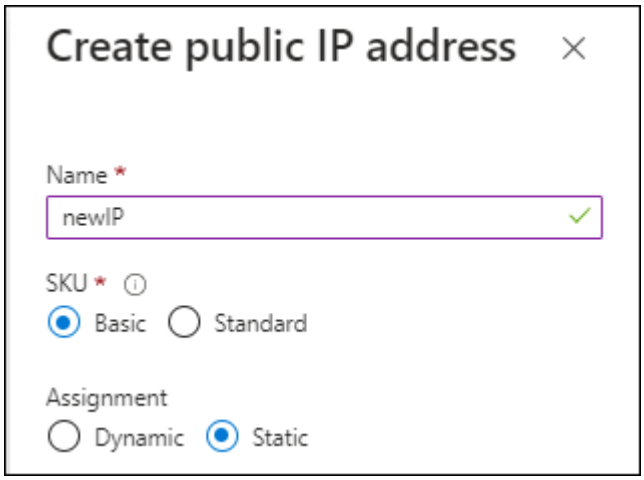
Endpoints	Purpose
AWS environments	
AWS services (amazonaws.com): • CloudFormation • Elastic Compute Cloud (EC2) • Identity and Access Management (IAM) • Key Management Service (KMS) • Security Token Service (STS) • Simple Storage Service (S3)	To manage AWS resources. The endpoint depends on your AWS region. Refer to AWS documentation for details
Amazon FsX for NetApp ONTAP: • api.workloads.netapp.com	The web-based console contacts this endpoint to interact with the Workload Factory APIs to manage and operate FSx for ONTAP based workloads.
Azure environments	

Endpoints	Purpose
https://management.azure.com https://login.microsoftonline.com https://blob.core.windows.net https://core.windows.net	To manage resources in Azure public regions.
https://management.usgovcloudapi.net https://login.microsoftonline.us https://blob.core.usgovcloudapi.net https://core.usgovcloudapi.net	To manage resources in Azure Government regions.
https://management.chinacloudapi.cn https://login.chinacloudapi.cn https://blob.core.chinacloudapi.cn https://core.chinacloudapi.cn	To manage resources in Azure China regions.
Google Cloud environments	
https://www.googleapis.com/compute/v1/ https://compute.googleapis.com/compute/v1 https://cloudresourcemanager.googleapis.com/v1/projects https://www.googleapis.com/compute/beta https://storage.googleapis.com/storage/v1 https://www.googleapis.com/storage/v1 https://iam.googleapis.com/v1 https://cloudkms.googleapis.com/v1 https://config.googleapis.com/v1/projects	To manage resources in Google Cloud.
NetApp Console endpoints	
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://support.netapp.com	To obtain licensing information and to send AutoSupport messages to NetApp support as well as to receive software updates for Cloud Volumes ONTAP.
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
https://bluexpinfraprod.eastus2.data.azurecr.io https://bluexpinfraprod.azurecr.io	To obtain images for Console agent upgrades. • When you deploy a new agent, the validation check tests connectivity to current endpoints. If you use previous endpoints, the validation check fails. To avoid this failure, skip the validation check. Although the previous endpoints are still supported, NetApp recommends updating your firewall rules to the current endpoints as soon as possible. Learn how to update your endpoint list. • When you update to the current endpoints in your firewall, your existing agents will continue to work.

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

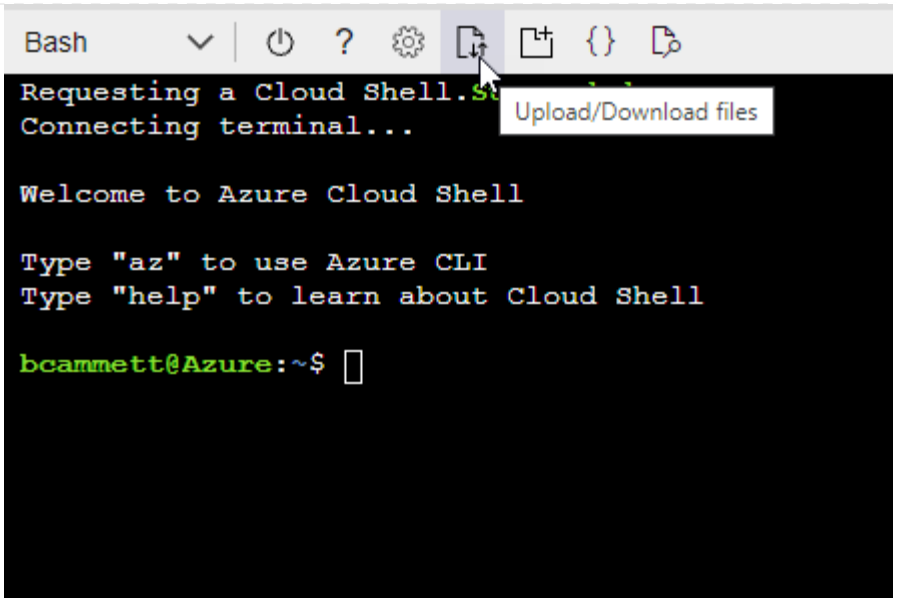
   ```
   "AssignableScopes": [
   "/subscriptions/d333af45-0d07-4154-943d-c25fbzzzzzzz",
   "/subscriptions/54b91999-b3e6-4599-908e-416e0zzzzzzz",
   "/subscriptions/398e471c-3b42-4ae7-9b59-ce5bbzzzzzzz"
   ]
   ```

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 agent_Policy.json
```

Azure service principal

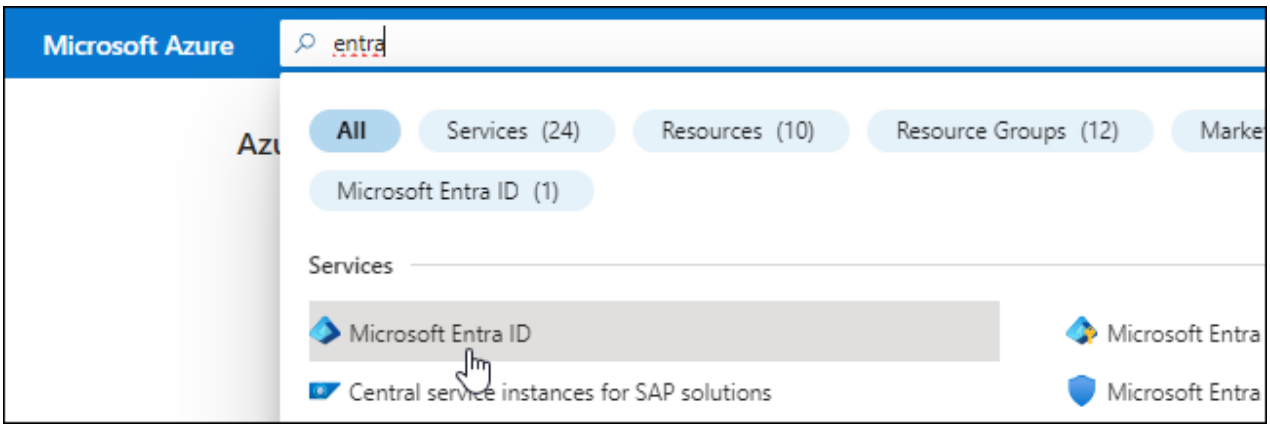
Create and set up a service principal in Microsoft Entra ID and obtain the Azure credentials that the Console needs. You need to provide the Console with these credentials after you install the Console agent.

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

   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.

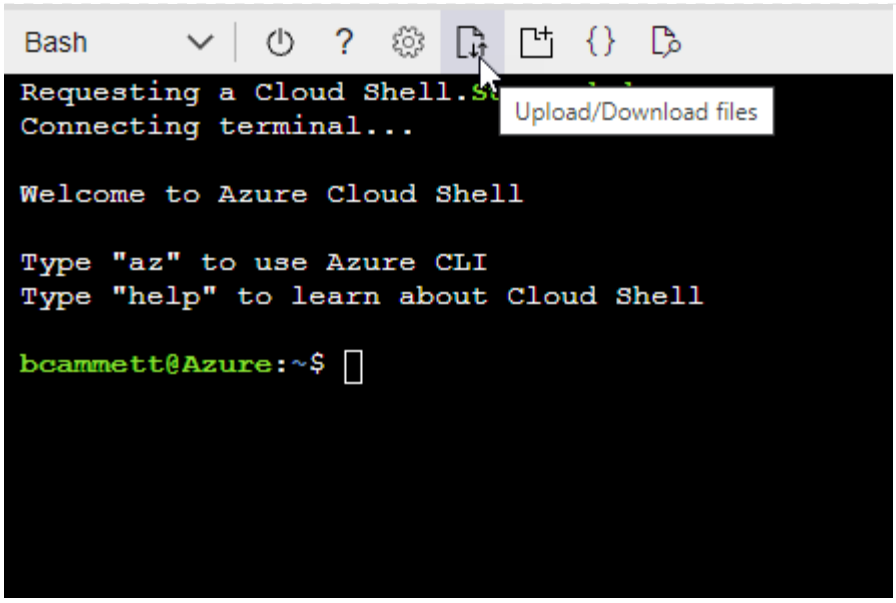
      Example

      ```
      "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.

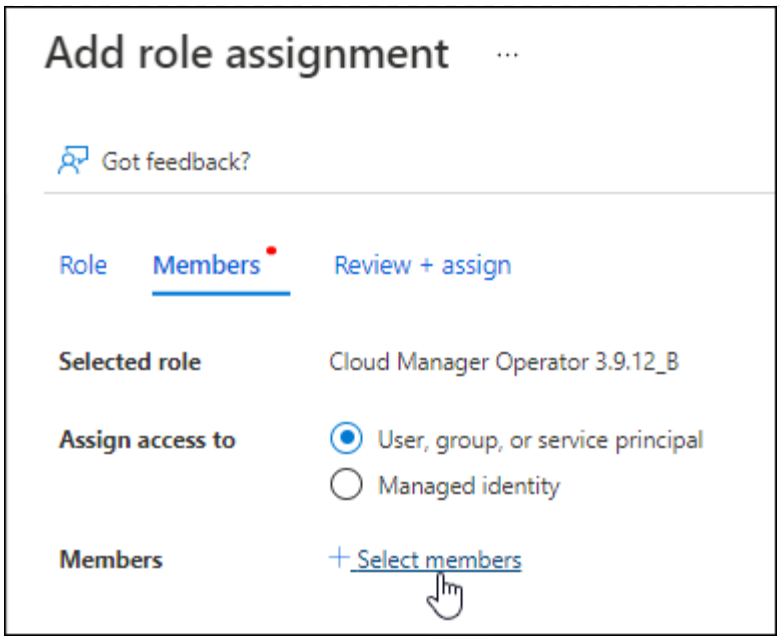


- Use the Azure CLI to create the custom role:

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

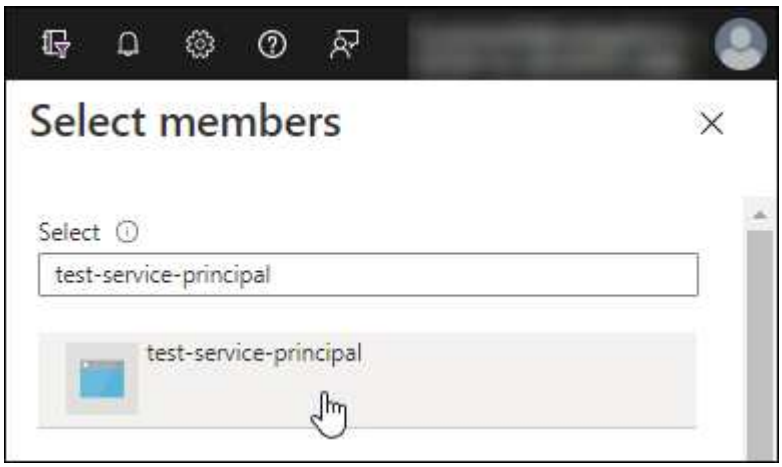
You should now have a custom role called Console Operator that you can assign to the Console agent virtual machine.

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**.

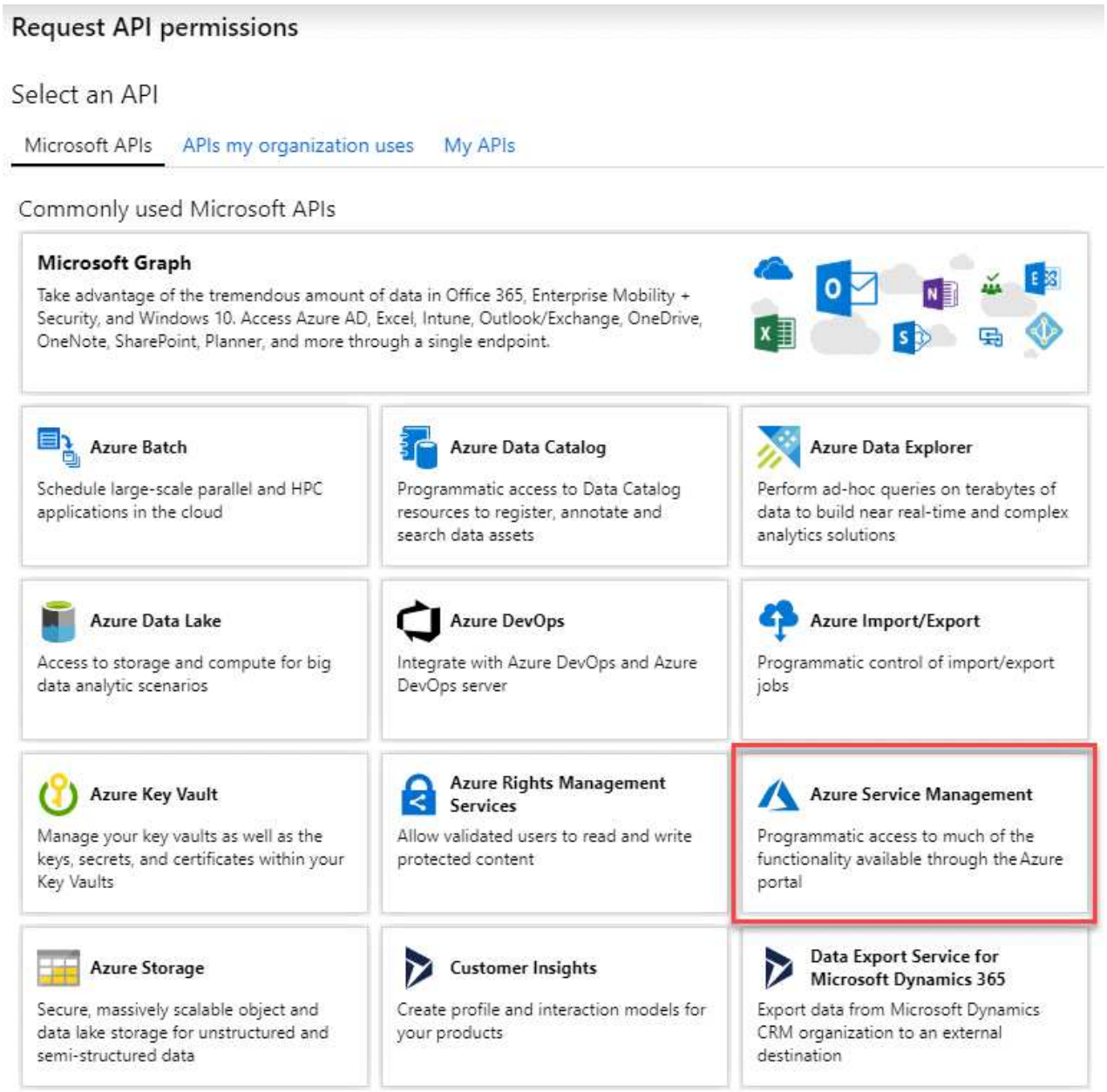
f. Select **Review + assign**.

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

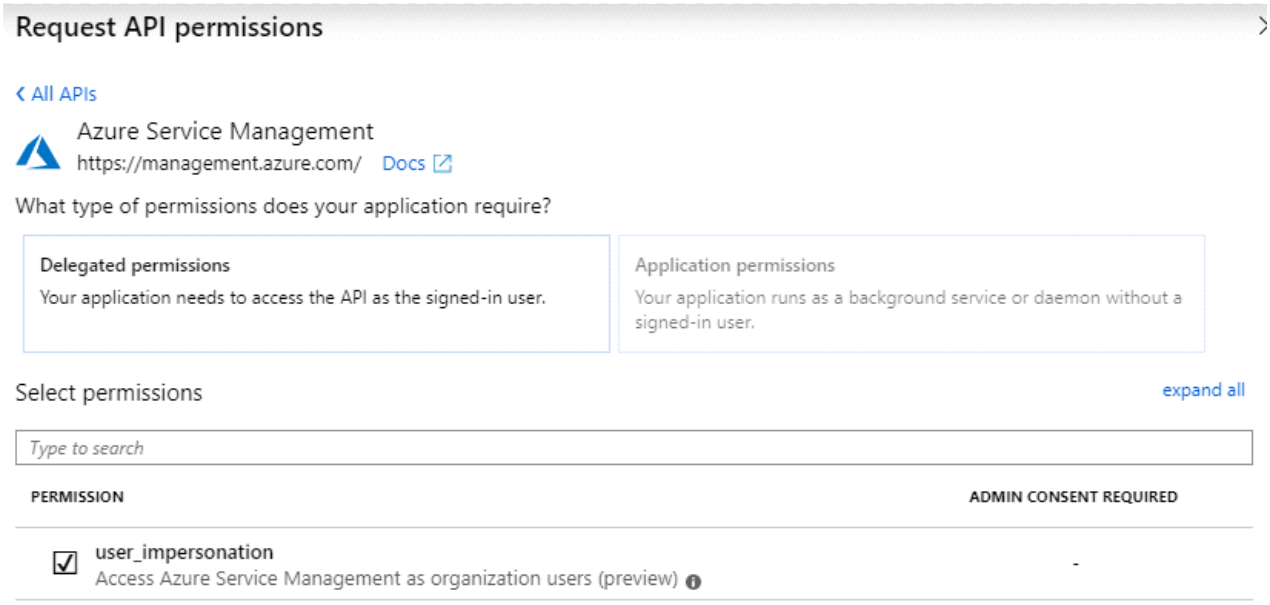
If you want to deploy Cloud Volumes ONTAP from multiple Azure subscriptions, then you must bind the service principal to each of those subscriptions. In the NetApp Console, you can select the subscription that you want to use when deploying Cloud Volumes ONTAP.

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**.

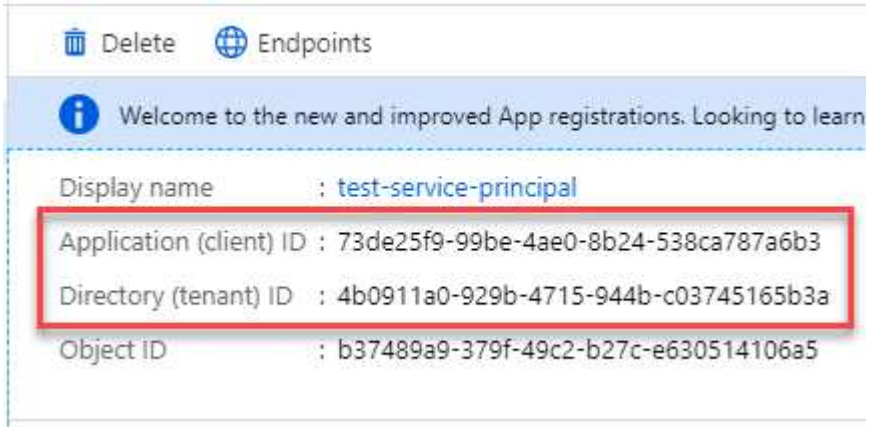


4. Select **Access Azure Service Management as organization users** and then select **Add permissions**.



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.

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 "agent" at the project level:

      ```
      gcloud iam roles create agent --project=myproject
      --file=agent.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

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 Infrastructure Manager API
- 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.

You need to have prepared your environment before you install the Console agent. You can install from the AWS Marketplace, from the Azure Marketplace, or manually on your own Linux host running in AWS, Azure, or Google Cloud.

AWS Commercial Marketplace

Before you begin

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 agent.

  Review agent 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 deploys in approximately five minutes.

What's next?

Set up the NetApp Console.

AWS Gov Marketplace

Before you begin

Have the following:

- A VPC and subnet that meets networking requirements.

  Learn about networking requirements

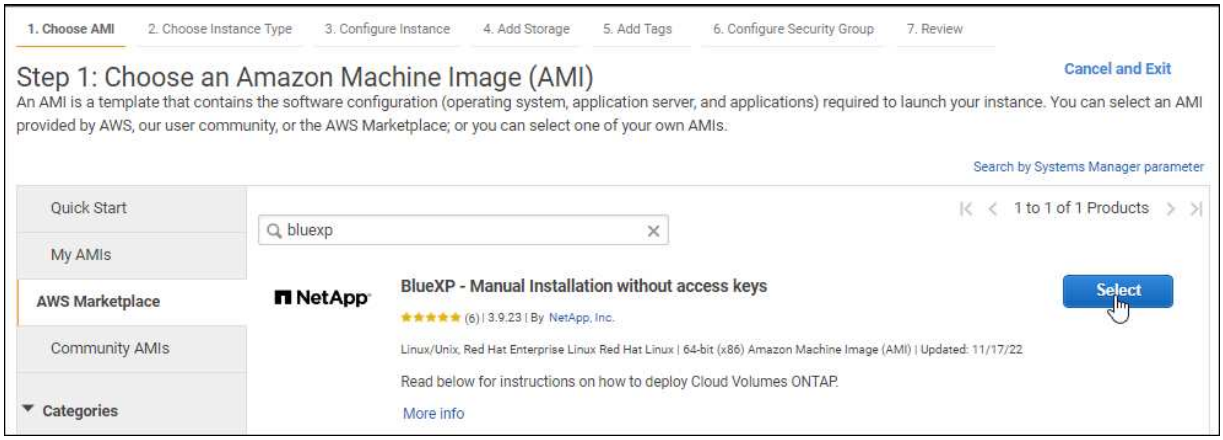
- An IAM role with an attached policy that includes the required permissions for the Console agent.

  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.

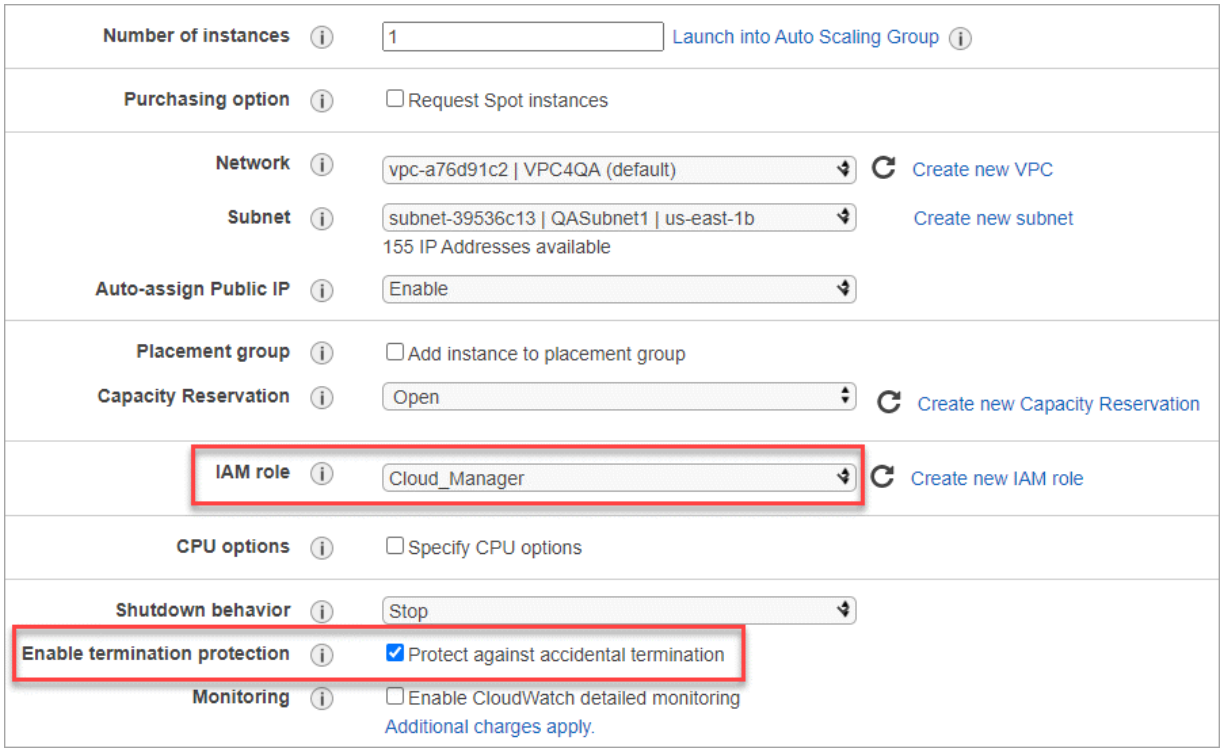


   d. Select **Continue**.

2. Follow the prompts to set up and start 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.



   - **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 deploys 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.

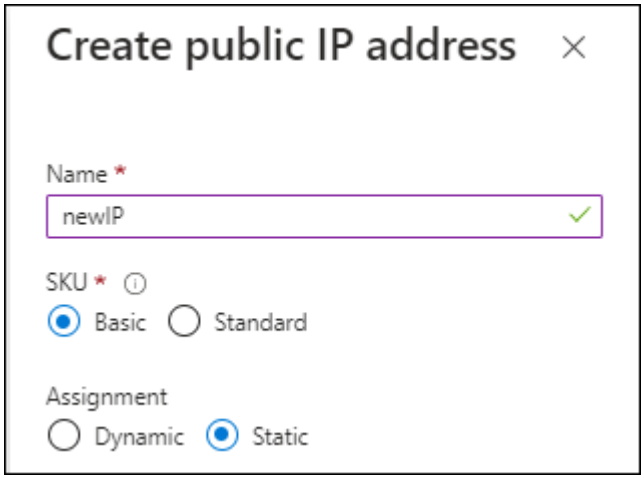
  Learn how to set up Azure permissions

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**: To use a public IP address with the Console agent VM, select a Basic SKU.



   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 you use to access the Console cannot reach the private IP address, the Console does not work.

   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**.

     A managed identity lets the Console agent VM identify itself to Microsoft Entra ID without 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 (must use for Google Cloud)

You can install the Console agent manually on your own Linux host running in AWS, Azure, or Google Cloud.

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

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 and then copy it to the Linux host. You can download it either from the NetApp Console or the NetApp Support site.
   - NetApp Console: Go to **Agents > Management> Deploy agent > On-prem > Manual install**.

     Choose download the agent installer files or a URL to the files.

- NetApp Support Site (needed if you don't already have access to the Console) NetApp Support Site,

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 an explicit proxy during installation. The `--proxy` and `--cacert` parameters are optional and you won't be prompted to add them. If you have an explicit proxy server, you will need to enter the parameters as shown.

If you want to configure a transparent proxy, you can do so after you've installed. Learn about the agent maintenance console

+

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

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
      ```

      For example:

      ```
      # 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
      ```

   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 need to sign up with a new login. Otherwise, you do not 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 the Console agent

If you installed the Console agent from the Azure Marketplace or manually, you need to give the permissions you set up earlier.

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

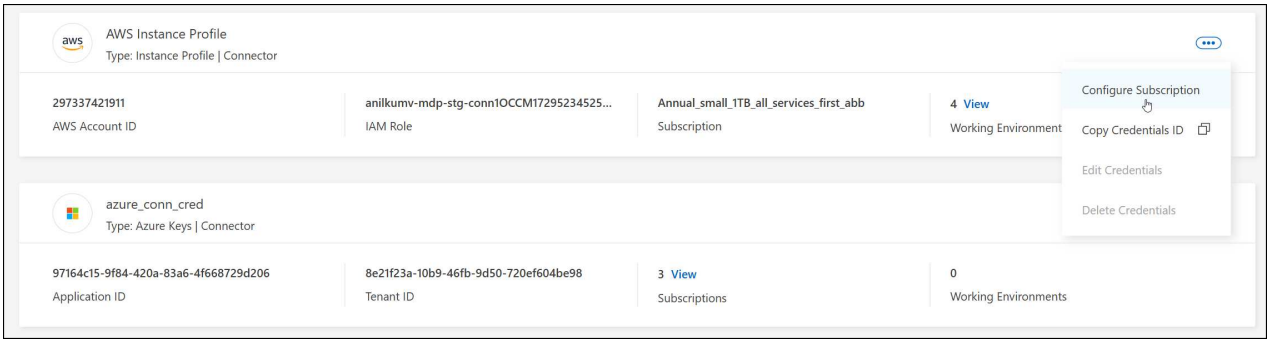
You must have already deployed a Console agent in order to subscribe to data services. You need to associate a marketplace subscription to the cloud credentials connected to a Console agent.

AWS

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.

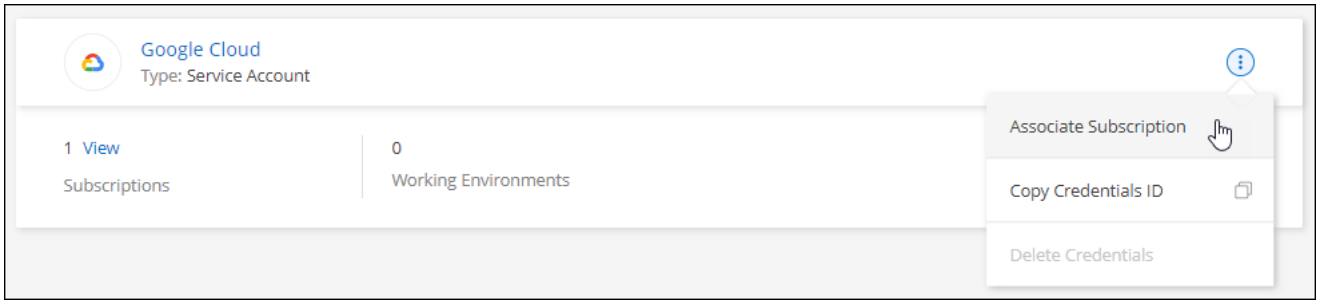
        For all other organizations or accounts, you'll need to manually associate the subscription by repeating these steps.

      - Select **Save**.

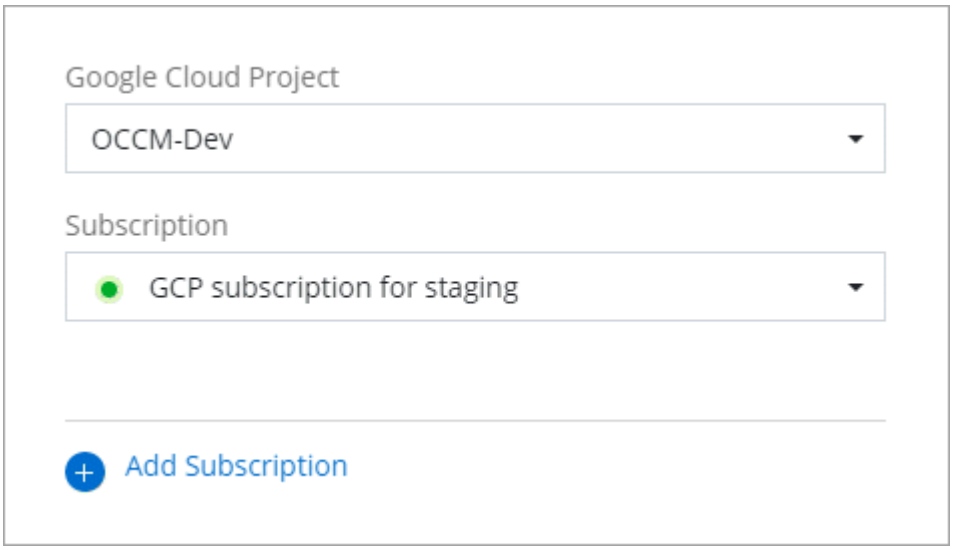
Google Cloud

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**.



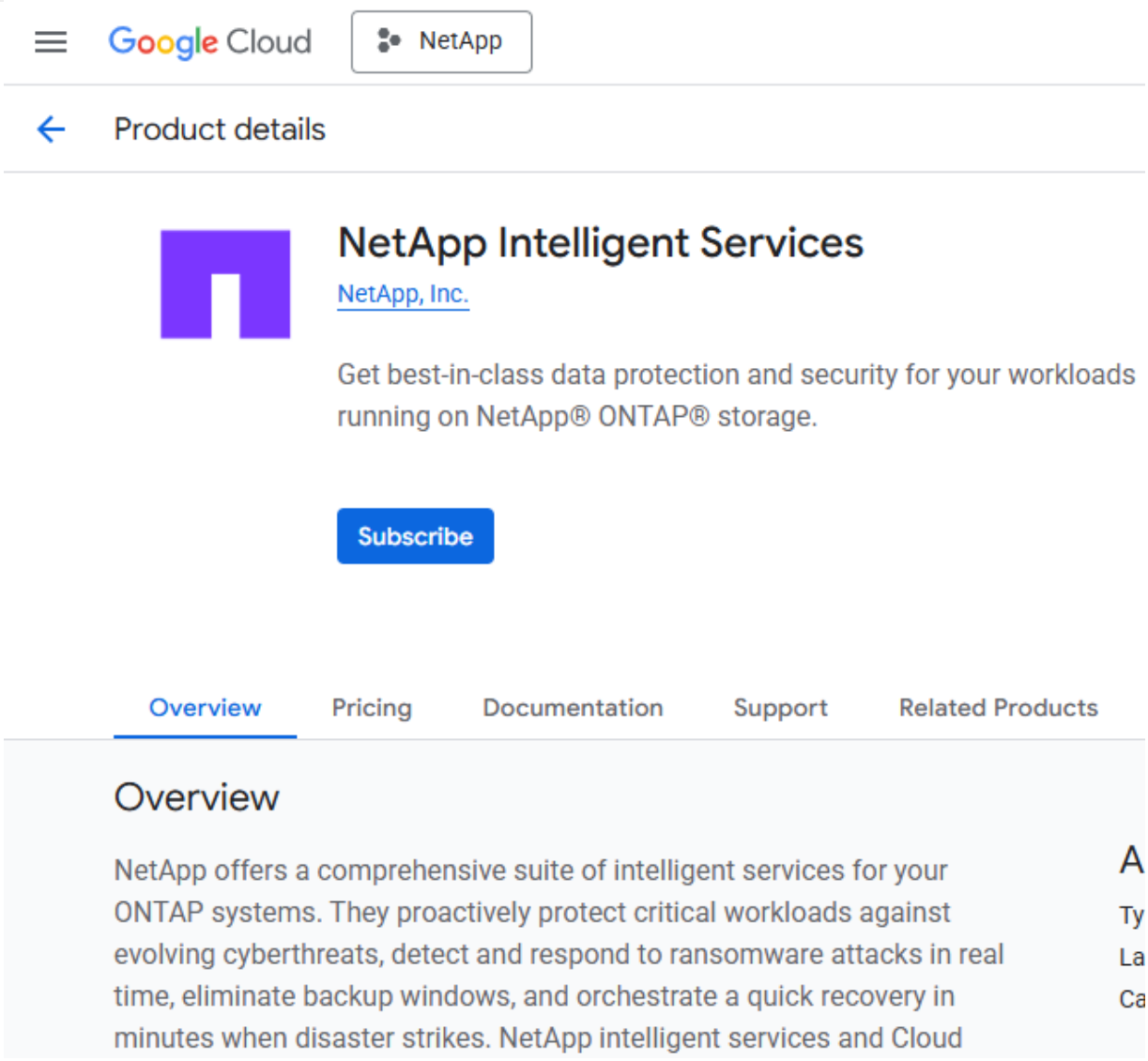
1. To configure an existing subscription with the selected credentials, select a Google Cloud project and subscription from the drop-down list, and then select **Configure**.



2. 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.

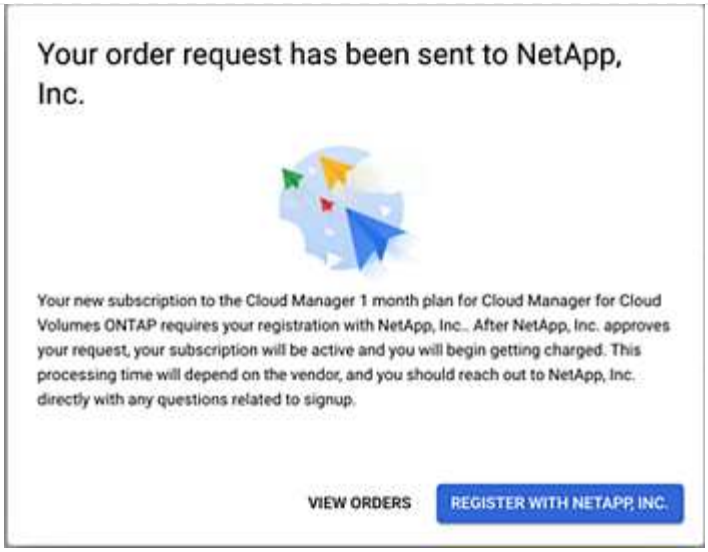


b. Select **Subscribe**.
c. Select the appropriate billing account and agree to the terms and conditions.
d. Select **Subscribe**.

   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.



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.

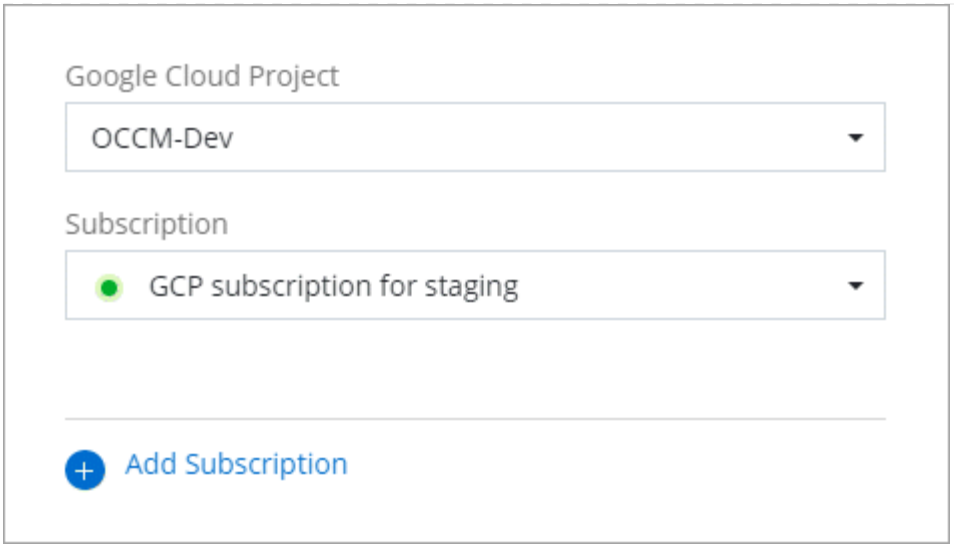
- Select the Console organization that you'd like to associate this subscription with.
- In the **Replace existing subscription** field, choose whether you'd like to automatically replace the existing subscription for one organization with this new subscription.

  The Console replaces the existing subscription for all credentials in the organization 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**.

a. Once this process is complete, navigate back to the Credentials page in the Console and select this new 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 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
Working environments This portion of the table lists support for working environment management from the BlueXP canvas. It does not indicate the supported backup destinations for BlueXP backup and recovery.	Amazon FSx for ONTAP	No
	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 View the list of supported backup destinations for ONTAP volume data
	Classification	Yes
	Copy and sync	No
	Digital advisor	No
	Digital wallet	Yes
	Disaster recovery	No
	Economic efficiency	No
	Ransomware Resilience	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

Copyright information

Trademark information