Install and set up

NetApp Console local deployment

NetApp
August 10, 2026

Table of Contents

Install and set up

Quick start for setting up NetApp Console local deployment

After you install NetApp Console local deployment, set up your organization so that the right teams can securely manage the right storage resources. Use this checklist to plan your structure, organize resources, add members, configure integrations, and enable data services.

Required access roles

Super admin or Organization admin. Learn about access roles.

1 Install NetApp Console local deployment

- Review the installation workflow to understand the deployment process. Learn about the installation workflow for NetApp Console local deployment.
- Install NetApp Console local deployment in your vCenter. Install NetApp Console local deployment.

2 Plan your organization

- Learn how folders and fleets organize your resources. Learn about folders and fleets.
- Understand how role-based access control (RBAC) grants members the access they need. Learn about role-based access control in NetApp Console local deployment.
- Review the identity and access management workflow. Get started with IAM for fleet and resource management.

3 Set up your organization

- Add your storage systems to NetApp Console local deployment. Add storage systems.
- Create the folder and fleet hierarchy that matches your business structure. Create folders and fleets.
- Associate resources with the correct folders and fleets. Associate resources to folders and fleets.
- Add members and assign their initial roles. Add members and assign roles.

4 Configure integrations and services

- Integrate with Active Directory so that directory users can access the Console local deployment. Integrate with Active Directory.
- Connect your large language model (LLM) to enable the Console assistant and AI-assisted management. Connect your LLM.
- Configure how the Console local deployment delivers notifications. Configure notification delivery.

5 Set up NetApp Backup and Recovery

- Obtain a license for NetApp Backup and Recovery. You can skip this step if you do not want access to advanced Backup and Recovery services.
- Add the NetApp Backup and Recovery license to NetApp Console local deployment. Add the license to NetApp Console local deployment.
- Grant users access to NetApp Backup and Recovery.

Install NetApp Console

Install NetApp Console local deployment using an OVA in vCenter

You use an OVA to install a NetApp Console local deployment in your VCenter. THe OVA download or URL is available through the NetApp Support site.

Prepare to install NetApp Console local deployment

Before installation, make sure your VM host meets the requirements and the NetApp Console local deployment can access the internet and targeted networks. To use NetApp data services such as NetApp Backup and Recovery, create cloud provider credentials for the NetApp Console local deployment to perform actions on your behalf.

Review NetApp Console local deployment host requirements

Make sure your host machine meets installation requirements before installing NetApp Console local deployment.

- CPU: 16 cores or 16 vCPUs
- RAM: 64 GB
- Disk space: 596 GB (thick provisioning recommended)
- vSphere 7.0u3 or higher, with virtual hardware version 19 or higher

Install NetApp Console local deployment in a vCenter environment rather than directly on an ESXi host.

Set up network access for the NetApp Console local deployment

NetApp Console local deployment uses fixed address space for inter-service communication. The IP range 10.42.0.0/16 and 10.43.0.0/16 are used for the internal network. Before deploying Console local deployment, ensure these IP ranges are not assigned to other VMs, DHCP scopes, DNS records, or load balancer VIP pools on the VLANs made available to the Console local deployment.

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

Install NetApp Console local deployment in your VCenter environment

NetApp supports installing NetApp Console local deployment in your VCenter environment. The OVA file includes a pre-configured VM image that you can deploy in your VMware environment.

Download the OVA or copy the URL

Download the OVA.

1. Download the Console local deployment software from the NetApp Support Site.

Deploy NetApp Console local deployment in your VCenter

Log into your VCenter environment to deploy Console local deployment.

Steps

1. Upload the self-signed certificate to your trusted certificates if your environment requires it. You can replace this certificate after installation.
2. Deploy the OVA from the content library or local system.

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

3. Complete the Deploy OVF Template wizard to deploy the Console.
4. Select a name and folder for the VM, then select **Next**.
5. Select a compute resource, then select **Next**.
6. Review the details of the template, then select **Next**.
7. Accept the license agreement, then select **Next**.
8. Choose the type of proxy configuration you want to use: explicit proxy, transparent proxy, or no proxy.
9. Select the datastore where you want to deploy the VM, then select **Next**. Be sure it meets host requirements.
10. Select the network to which you want to connect the VM, then select **Next**. Ensure the network is IPv4 and has outbound internet access to the required endpoints.
11. in the **Customize template** window, complete the following fields:
    - **Proxy information**
      - If you selected explicit proxy, enter the proxy server hostname or IP address and port number, as well as the username, password.
      - If you selected transparent proxy, upload the respective certificate.
    - **Virtual Machine Configuration**
      - **Skip config check**: This check box is unchecked by default which means the NetApp Console local deployment runs a configuration check to validate network access.
        - NetApp recommends leaving this box unchecked so that the installation includes a configuration check of the NetApp Console local deployment. The Configuration check validates that the NetApp Console local deployment has network access to the required endpoints. If it deployment fails because of connectivity issues, you can access the validation report and logs from the NetApp Console local deployment host. In some cases, if you are confident that the NetApp Console local deployment has network access, you can choose to skip the check.

- **Maintenance password**: Set the password for the `maint` user that allows access to the NetApp Console local deployment maintenance console.
- **NTP servers**: Specify one or more NTP servers for time synchronization.
- **Hostname**: Set the hostname for this VM. It must not include the search domain. For example, an FQDN of console10.searchdomain.company.com should be entered as console10.
- **Primary DNS**: Specify the primary DNS server to use for name resolution.
- **Secondary DNS**: Specify the secondary DNS server to use for name resolution.
- Search domains: Specify the search domain name to use when resolving the hostname. For example, if the FQDN is console10.searchdomain.company.com, then enter searchdomain.company.com.
- **IPv4 address**: The IP address that is mapped to the hostname.
- **IPv4 subnet mask**: The subnet mask for the IPv4 address.
- **IPv4 gateway address**: The gateway address for the IPv4 address.

12. Select **Next**.
13. Review the details in the **Ready to complete** window, select **Finish**.

    The vSphere task bar shows the progress as the NetApp Console local deployment is deployed.

14. Power on the VM.

Plan your Console organization

Get started with identity and access in NetApp Console local deployment

In NetApp Console local deployment, set up your folder and fleet hierarchy, add members and starting permissions, and add and place resources in the correct fleets so the right teams can access and manage them.

Required access roles

Super admin, Organization admin, or Folder or fleet admin. Learn about access roles.

You need the **Organization admin** or **Super admin** role to complete initial setup. After setup, manage resources, member access, and fleet access as your organization changes.

Add or discover resources

Add systems to Console local deployment. During initial setup, systems are typically added while the default fleet is selected.

Learn how to create or discover resources:

- On-premises ONTAP clusters

Create your folder and fleet hierarchy

Create additional fleets and folders that match your business hierarchy.

Learn how to organize your resources with folders and fleets.

3 Associate resources with the correct fleets

Adding or discovering a system in Console local deployment automatically associates the resource with the currently selected fleet. To make a system available to the right teams, associate it with the appropriate fleets in your hierarchy.

- Learn how to manage resources in folders and fleets.

4 Add members and assign starting permissions

Add members and assign them roles at the organization, folder, or fleet level based on what they manage.

Learn how to manage members and their permissions.

After initial setup

After initial setup is complete, manage access and resource placement as your organization changes:

- Manage resources in folders and fleets
- Manage member access across fleets and folders (member-centric)
- Manage who can access a specific fleet or folder (fleet-centric)
- Delete folders and fleets when no longer needed

Related information

- Learn about identity and access management in NetApp Console
- Learn about the API for identity and access

Learn about folders and fleets in NetApp Console local deployment

In NetApp Console local deployment, use folders and storage fleets to organize your NetApp resources and control access according to your business structure—by location, department, or workload type.

Use this page for hierarchy strategy and fleet design patterns. For a complete IAM model of members, roles, and resource scope, Learn about identity and access management in NetApp Console local deployment.

You organize resources in a hierarchy: the organization is at the top, then folders (which can contain other folders or fleets), and then fleets, which contain storage systems. Assign access roles at the organization, folder, or fleet level so users have the right access to resources.

ⓘ You must have the Organization admin or Folder or fleet admin role to manage folders and fleets in the NetApp Console local deployment.

Organizational components

The organizational components—organization, folders, and fleets—form a hierarchy that determines how resources are grouped and how access is delegated.

Organization

An organization is the top level of the NetApp Console local deployment hierarchy and typically represents your company. Your organization consists of folders, fleets, members, roles, and resources. Resources are associated with fleets, and members are assigned roles at the organization, folder, or fleet level.

Folders

Folders group related fleets to organize them by location, site, or business unit. You can't associate storage systems directly with folders, but assigning a member a role at the folder level gives them access to all fleets in that folder.

Organization admins can add a resource to a folder to delegate the task of associating the resource with fleets to a Folder or fleet admin. Associate resources with folders and fleets.

Fleets

Fleets group storage systems. Assign resources to fleets and grant members access at the fleet level. Resources can belong to multiple fleets. Members with fleet access can manage the resources in that fleet.

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

Learn how to create folders and storage fleets.

Resources

A resource is a storage system that the Console local deployment is aware of and that can be assigned to a fleet. Associate a resource with a fleet so that users with access to the fleet can manage the resource.

For example, you might associate an ONTAP cluster with one fleet or with all fleets in your organization. How you associate a resource depends on your organization's needs.

Learn how to associate resources with fleets.

Members and roles

Members are the users and service accounts in your organization. Roles define what actions they can perform and at what level of the hierarchy—organization, folder, or fleet.

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.

Users with the Organization admin role can add new members to your organization. All users (including service accounts and Active Directory users) must be explicitly added and granted at least one role in order to access Console local deployment.

Learn how to add members to your organization.

Access roles

The Console local deployment 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 fleet. The role that you select gives a member permission to the resources in the

selected part of the hierarchy.

The NetApp Console local deployment provides granular roles that adhere to the principle of least privilege, which means access roles are designed to give members access to only what they need.

Users can have multiple roles as their duties expand.

Role inheritance

When you assign a role at the organization or folder level, the child folders, fleets, and resources beneath it inherit that role, so your folder and fleet design determines how broadly each assignment applies.

Learn about role inheritance in NetApp Console local deployment.

Organization design examples

The right organizational structure depends on the size of your organization and how your teams are organized. The following examples show how different organizations can use the folder and fleet hierarchy to manage access effectively.

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 fleets (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
- **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) > Fleets per region
- **Platform roles**:
  - 1 Organization admin: Global oversight and policy management
  - 3 Folder or fleet admins: Regional control (one per region)
  - 1 Federation admin: Corporate directory service integration
- **Storage roles by region**:
  - Storage admin: Discover and manage storage systems in assigned regions
  - Storage viewer: Monitor storage resources across regions
  - System health specialist: Manage storage health without system modifications

- **Benefits**: Enhanced security through role segregation, regional autonomy, and compliance with local regulations

Departmental specialization strategy

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

Example: TechCorp (mid-size technology company)

- **Structure**: Organization > Department folders (IT, Security, Development) > Fleet-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
- **Benefits**: Tailored access control, improved operational efficiency, and clear accountability for specialized tasks

Next steps

- Create folders and storage fleets
- Associate resources with folders and fleets
- Manage fleet access assignments
- Monitor or audit Console local deployment actions

Learn about role-based access control in NetApp Console local deployment

Manage user access to NetApp Console local deployment with role-based access control (RBAC), assigning predefined roles at the organization, folder, or fleet level. Each role grants specific permissions that define what actions users can perform within their assigned scope.

NetApp designs Console local deployment roles with least-privilege, so each role includes only the permissions needed for its tasks. This approach enhances security by limiting access to what each member requires.

After you organize resources into folders and fleets, assign organization members a role or roles for specific folders or fleets, that allow them to perform only their responsibilities.

For example, you can assign a member the Backup and Recovery admin role for a specific fleet level, allowing them to perform Backup and Recovery operations for resources within that fleet, without granting them broader access to the entire organization. This same user can be granted the role for several fleets within your organization.

You can assign members multiple roles for the same scope or different scopes, depending on their responsibilities. For example, a smaller organization might assign the same member both Storage admin and Backup and Recovery admin roles at the organization level, while a larger organization might have different members assigned to each role at the fleet level.

Types of Console organization members

NetApp Console local deployment supports the following types of members:

- *Users*: Individual users can either be local users you add to NetApp Console local deployment who use local credentials or directory users who authenticate through your integrated Active Directory or LDAP service. Both types of users can be assigned roles in NetApp Console local deployment to access resources.
- *Service accounts*: Non-human accounts that applications or services use to interact with NetApp Console local deployment through APIs. You can add service accounts directly to your Console local deployment organization.

Learn how to add members to your organization.

Predefined roles in NetApp Console local deployment

NetApp Console local deployment includes predefined roles that you can assign to organization members. Each role includes permissions that specify what actions a member can do within their assigned scope (organization, folder, or fleet).

NetApp Console local deployment roles use least-privilege principles that ensure members have only the permissions needed for their tasks, and categorizes roles by the type of access they provide:

- Platform roles: Provide Console local deployment administration permissions
- Data services roles: Provide permissions for managing specific data services, such as Ransomware Resilience and Backup and Recovery
- Application roles: Provide permissions for managing storage as well as audit Console local deployment events and alerts

You can assign multiple roles to a member based on their responsibilities. For example, you might assign a member both the Storage admin role and the Backup and Recovery admin role for a specific fleet.

To choose access for a member, match the role category to the member's responsibilities, then assign the role at the scope (organization, folder, or fleet) that matches how broadly the member should have that access. Learn about how different organizations structure roles and scope in NetApp Console local deployment.

Learn about the predefined roles that you can assign to members in NetApp Console local deployment.

How role inheritance works

When you assign a role at the organization or folder level, that role is inherited by the child scopes within that part of the hierarchy. This means that organization-level roles apply across the organization, folder-level roles apply to all child folders and fleets in that folder, and fleet-level roles apply only to the resources in that fleet.

Use the scope that matches the access you want the member to keep. For example, assign a role at the folder level when the member needs the same access across several fleets in one region. Assign the role at the fleet level when the member should access only one fleet.

You can't override inherited access at a lower scope. If a member inherits a role from the organization or from a folder, change that assignment at the higher scope where you originally granted it.

Learn about folders and fleets in NetApp Console local deployment.
Manage member access.
Manage fleet access assignments.

Set up your Console organization

Add folders and fleets to your NetApp Console local deployment organization

Create folders and fleets to match your business structure, control access, and organize resources in NetApp Console local deployment.

Required access roles

Super admin, Organization admin, or Folder or fleet admin. Learn about access roles.

NetApp Console local deployment creates one default fleet when you create an organization. You can add more fleets and group them with folders. Learn about the resource hierarchy in NetApp Console.

Using folders and fleets to organize resources

Folders and fleets are the two building blocks you use to shape your organization into something that matches how your teams actually work. For example, one folder per region with a production and a development fleet inside each.

- Folders group related fleets and support delegated administration and role inheritance.
- Fleets are where you associate resources for management and how you grant users operational access.

You can create folders and fleets first and add resources and member access later. This lets you plan your resource hierarchy before adding users and resources in Console local deployment. If your structure is already defined, you can add resources and assign access when you create the fleet. You can update fleets at any time.

For example, put production clusters in a Production fleet and test clusters in a Test fleet, and grant each team access only to the fleet they own.

Folders

Folders organize fleets by business structure, such as business unit, region, or team. You can nest folders to mirror your organization.

Roles assigned at a folder level are inherited by child folders and fleets. You can also use a folder to delegate fleet assignment tasks to a Folder or fleet admin for that part of the hierarchy.

Members work in fleets, not folders. A resource associated only with a folder is not manageable by members until it is associated with a fleet.

For example, a regional enterprise could use folders to organize ONTAP storage by business unit and workload. It might create a top-level folder for North America, subfolders for Production and Development, and fleets for ONTAP clusters that host SAP, VMware, and backup volumes. Storage admins assigned to the North America folder inherit access to all child fleets, while application teams get access only to the fleets they manage.

Fleets

Associate resources with fleets so members can manage them. A fleet can exist directly under the organization or inside a folder.

For example, a healthcare company uses ONTAP storage in separate production and development fleets. The

production fleet runs clinical apps and patient record databases, while the development fleet supports testing and validation. This separation protects live data, enforces tighter production access, supports auditability and least-privilege controls, and lets dev teams work without impacting patient-facing workloads.

Users navigate between assigned fleets on the **Systems** page to manage the resources associated with each fleet.

Add a folder or fleet

Add a fleet whenever you need a new boundary for resources and member access, and add a folder when you want to group related fleets and delegate their administration. For example, add a `Production` folder containing a `Production-US-East` fleet and a `Production-EU-West` fleet, then assign a regional lead the Folder or fleet admin role on just their fleet.

You can create up to seven hierarchy levels.

You can add resources and assign member access when you create a fleet or folder, or you can do it later.

Steps

1. Select **Administration > Identity and access**.
2. Select **Organization**.
3. From the **Organization** page, select **Add folder or fleet**.
4. Select **Folder** or **Fleet**.
5. In **Name and location**: Enter a name and choose a location for the folder or fleet.

1. Optional: Expand the **Resources** section to associate resources with the fleet or folder.
   a. Mark the check box next to the resource you want to associate and then select **Associate with the fleet**. If you haven't added systems to Console local deployment yet, you can do this step later.

   > Members can't access resources in a folder until those resources are assigned to a fleet.

2. Optional: Expand the **Access** section to assign access to members. Select **Add a member** to assign access and a role. By default, the user who creates the fleet has access to it.

   Learn about access roles.

3. Select **Add**.

Rename a folder or fleet

Rename a folder or fleet as needed. Renaming does not affect associated resources or member access.

Steps

1. From the **Organization** page, navigate to a fleet or folder in the table, select ••• and then select **Edit folder** or **Edit fleet**.
2. On the **Edit** page, enter a new name and select **Apply**.

Delete a folder or fleet

Delete folders and fleets you no longer need, such as after team restructuring or fleet completion.

Before you delete a folder or fleet, complete the following checks:

- Verify that the folder or fleet does not contain resources. Learn how to remove resource associations.
- Review members who still have access to the folder or fleet. View member access assignments.
- Remove or update member access as needed. Modify member access assignments.
- If you are deleting a fleet, move resources to the target fleet first. Learn how to move resources between fleets.

Steps

1. From the **Organization** page, navigate to a fleet or folder in the table, select ••• and then select **Delete**.
2. Confirm that you want to delete the folder or fleet.

Manage fleets and folders in NetApp Console local deployment

After initial setup, you can do the following:

- **Manage resource associations for folders and fleets**: Learn how to associate resources with fleets and folders.
- **View or update access for one folder or fleet**: Learn how to grant users access to fleets.
- **Manage one member across multiple folders and fleets**: Learn how to manage member access.
- **Add additional members and assign starting permissions**: Learn how to manage members and permissions.

Related information

- Learn about identity and access in NetApp Console
- Get started with identity and access in NetApp Console
- Manage fleet access assignments
- Learn about the identity and access API

Add storage systems to NetApp Console local deployment

Add storage systems to NetApp Console local deployment to enable monitoring, inventory management, and administration of your storage infrastructure. After a storage system is added, Console local deployment discovers the system and begins collecting information that can be used for monitoring and management tasks.

Before you begin, ensure that you have the required permissions to add storage systems and that the storage system is reachable from Console local deployment.

Steps

1. Select **Storage > Management**.
2. From the Scope drop-down list, select the fleet to which you want to add a storage system.
3. Select **Add system**.
4. Enter the required storage system details, including connection information and credentials.
5. Review the information you entered and select **Add**.

The storage system is added to the selected fleet. Console local deployment begins discovering and monitoring the system. Depending on the environment and network connectivity, it might take several minutes for the system to appear as fully managed.

You can also add a storage system from the **Administration > Identity and access** page by selecting **Add system** and providing the required system information.

Manage resources in folders and fleets in NetApp Console local deployment

Manage resource access in NetApp Console local deployment by associating resources with the correct folder or fleet, which controls which teams can access and manage them.

Required access roles

Super admin, Organization admin, or Folder or fleet admin. Learn about access roles.

Place resources where the right teams can manage them, move them when ownership changes, and remove associations when they are no longer needed.

A *resource* is an entity that Console local deployment recognizes, such as a storage resource or a Backup and Recovery workload.

Console resource types

Console local deployment supports both storage resources and Backup and Recovery workloads. Associate either resource type with a fleet to control access and management.

Storage resources

Storage resources are the most common type of resource in your organization. When you add a storage system to Console local deployment, associate it with a fleet so the appropriate teams can access and manage it. For example, after adding an ONTAP cluster, associate it with the `Production-US-East` fleet.

Backup and Recovery workloads

Backup and Recovery workloads are also considered resources. You can assign member permissions to access Backup and Recovery workloads by associating the workloads with fleets. For example, assign a member access to a Backup and Recovery workload by associating it with a fleet the member can access and granting the appropriate Backup and Recovery role.

View the resources in your organization

View the resources in your organization to find a specific resource and see which fleets or folders it is associated with. If you haven't created any folders or fleets, all resources are associated with the default fleet directly under the organization.

Steps

1. Select **Administration > Identity and access**.
2. Select **Resources**.
3. Select **Advanced Search & Filtering**.
4. Use the available options to find a resource:
   - **Search by resource name**: Enter a text string and select **Add**.
   - **Platform**: Select one or more platforms, such as Amazon Web Services.

- **Resources**: Select one or more resources, such as Cloud Volumes ONTAP.
- **Organization, folder, or fleet**: Select the entire organization, a specific folder, or a specific fleet.

5. Select **Search**.

Associate a resource with a folder or fleet

Associate a resource with a fleet or folder so the appropriate teams can manage it. For example, after adding an ONTAP cluster, associate it with the `Production-US-East` fleet so the regional Storage admins for that fleet can manage it.

> Users with the Organization admin role can add resources to a folder to delegate fleet association tasks to the Folder or fleet admin for that folder. Associate a resource with a folder.

Steps

1. From the **Resources** page, navigate to a resource in the table, select ••• and then select **Associate to a folder or fleet**.
2. Select a folder or fleet and then select **Accept**.
3. To associate an additional folder or fleet, select **Add folder or fleet** and then select the folder or fleet.

   Note that you can only select from the folders and fleets for which you have admin permissions.

4. Select **Associate resources**.
   - If you associated the resource with fleets, members who have permissions for those fleets now have the ability to access the resource from the Console.
   - If you associated the resource with a folder, a *Folder or fleet admin* can now access the resource and associate it with a fleet within the folder. Associate a resource with a folder.

View the folders and fleets associated with a resource

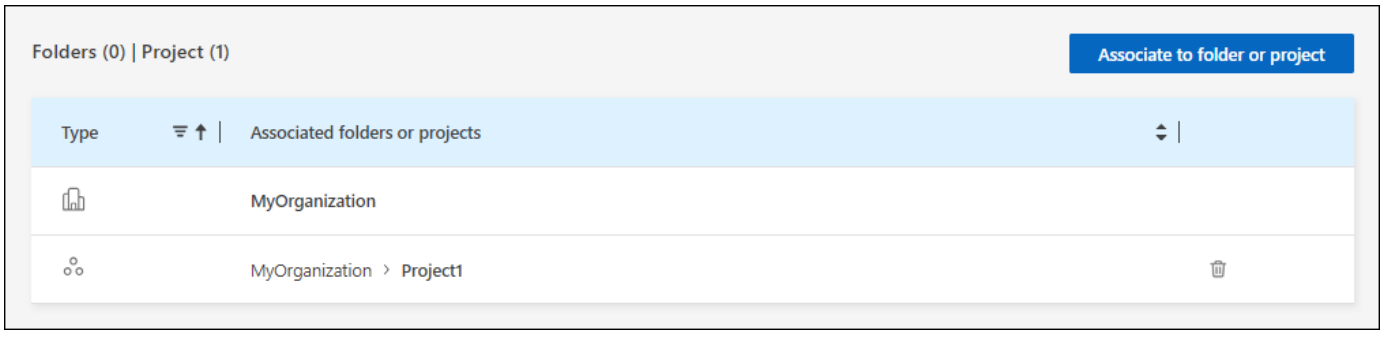
Verify which fleets or folders a resource is associated with.

> To see which members have access to the resource, review the members assigned to the associated folder or fleet. Manage fleet access assignments.

Steps

1. From the **Resources** page, navigate to a resource in the table, select ••• and then select **View details**.

The following example shows a resource that is associated with one fleet.



To see which members have access to the resource, review the associated folder or fleet.

Manage fleet access assignments.
Manage member access.

Remove a resource from a folder or fleet

Remove a resource's association with a folder or fleet to prevent members from managing it there.

To remove a storage system from the entire organization, go to the **Systems** page and remove the system.

Steps

1. From the **Resources** page, navigate to a resource in the table, select ••• and then select **View details**.
2. To remove a resource from a folder or fleet, select next to the folder or fleet.
3. Select **Delete** to remove the association.

Move a resource between fleets

Move a resource from one fleet to another by removing its association with the current fleet and then associating it with the target fleet.

Access to the resource changes as soon as the association changes. If possible, complete both steps in one maintenance window.

Steps

1. From the **Resources** page, navigate to a resource in the table, select ••• and then select **View details**.
2. Select next to the current fleet and select **Delete**.
3. Select **Add folder or fleet**.
4. Select the target fleet and select **Accept**.
5. Select **Associate resources**.

Related information

- Learn about identity and access in NetApp Console
- Get started with identity and access in NetApp Console
- Manage fleet access assignments after moving resources
- Learn about the API for identity and access

Add members to your NetApp Console local deployment organization

Add members to your NetApp Console local deployment organization and assign roles to grant access at the organization, folder, or fleet level for users, service accounts, and directory users.

Required access roles

Super admin, Organization admin, or Folder or fleet admin (for folders and fleets that they are administering).

Learn about access roles.

Before you begin

- Create the folder and fleet hierarchy that matches your organization. Learn how to organize your resources with folders and fleets.
- Associate resources with the correct fleets before you assign member access. Learn how to manage resources in folders and fleets.
- If you are adding a directory user, integrate your directory service first. Learn how to integrate with your directory service.

Understand how access is granted in NetApp Console local deployment

NetApp Console uses role-based access control (RBAC) to manage permissions. Assign roles to members to provide the required access. Each role defines allowed actions for specific resources.

Note the following about granting access in NetApp Console local deployment:

- You must explicitly add each user to your organization and assign at least one role before that user can access resources.
- A role that you assign at the organization or folder level is inherited by child scopes, so choose the assignment scope carefully to give the member access only where needed. Learn about role inheritance in NetApp Console local deployment.

Add members to your organization

NetApp Console supports three types of members: user accounts, directory users, and service accounts.

> You must first configure an email server to use with Console local deployment before you can add users. Learn how to configure an email server.

Directory users authenticate through your integrated directory service, but you must still add each directory user individually and assign roles in Console local deployment. Create service accounts directly in the Console.

All members must have at least one role explicitly assigned to them in order to access Console local deployment.

When adding a member, choose the organization, folder, or fleet where the member needs access and assign the starting role or roles they need.

Add a user account

You must have the Organization admin or Folder or fleet admin role to add a user to an organization, folder, or fleet so they can access resources.

Steps

1. Select **Administration > Identity and access**.
2. Select **Members**.
3. Select **Add a member**.
4. For **Member Type**, keep **User** selected.

5. For **User's email**, enter the user's email address that is associated with the login that they created.
6. Use the **Select an organization, folder, or fleet** section to choose where the member needs access.

   Note the following:

   - You can select only the folders and fleets for which you have permissions.
   - When you select an organization or folder, you grant the member permissions to all its contents.
   - You can only assign the **Organization admin** role at the organization level.
7. **Select a category** then select a **Role** that gives the member the starting permissions they need for the organization, folder, or fleet you selected.

   Learn about access roles.
8. To give access to more folders, fleets, or roles, select **Add role**, choose the folder, fleet, or role category, and select a role.
9. Select **Add**.

   The Console emails instructions to the user.

Add a service account

Add a service account when you need to automate tasks or connect securely to Console APIs. After you create the account, copy its client ID and client secret for the integration that will use it.

Steps

1. Select **Administration > Identity and access**.
2. Select **Members**.
3. Select **Add a member**.
4. For **Member Type**, select **Service account**.
5. Enter a name for the service account.
6. Use the **Select an organization, folder, or fleet** section to choose where the service account needs access.

   Note the following:

   - You can only select from the folders and fleets for which you have permissions.
   - Selecting an organization or folder grants the member permissions to all its contents.
   - You can only assign the **Organization admin** role at the organization level.
7. Select a **Category** then select a **Role** that gives the service account the starting permissions it needs for the organization, folder, or fleet you selected.

   Learn about access roles.
8. To give access to more folders, fleets, or roles, select **Add role**, choose the folder, fleet, or role category, and select a role.
9. Download or copy the client ID and client secret.

   The Console shows the client secret only once. Copy it securely; you can recreate it later if you lose it.

10. Select **Close**.

Add a directory user to your organization

Add a user from your integrated directory service and grant their first roles. For example, add a new storage engineer from Active Directory and assign the Storage admin role on the `Production-US-East` fleet so they can work in that fleet.

You must first configure your directory service before you can add directory users. Learn how to integrate with your directory service.

Steps

1. Select **Administration > Identity and access**.
2. Select **Members**.
3. Select **Add a member**.
4. For **Member Type**, select **Directory user**.
5. For **User's email**, enter the email address of the directory user that you want to add. This email address must match the email address associated with the user's login in your directory.
6. Use the **Select an organization, folder, or fleet** section to choose where the directory user needs access.

   Note the following:

   - You can only select from the folders and fleets for which you have permissions.
   - Selecting an organization or folder grants the member permissions to all its contents.
   - You can only assign the **Organization admin** role at the organization level.
7. Select a **Category** then select a **Role** that gives the directory user the starting permissions they need for the organization, folder, or fleet you selected.

   Learn about access roles.
8. To give the user additional access to other folders, fleets, or roles, select **Add role**, choose the folder or fleet, role category, and select a role.

Access roles

NetApp Console local deployment access roles

Identity and access management (IAM) in NetApp Console local deployment provides predefined roles that you can assign to the members of your organization across different levels of your resource hierarchy. Before you assign these roles, you should understand the permissions that each role includes. Roles fall into the following categories: platform, application, and data service.

Platform roles

Platform roles grant NetApp Console local deployment administration permissions, including role assignment and user management. The Console local deployment has several platform roles.

Platform role	Responsibilities
Organization admin	Allows a user unrestricted access to all fleets and folders within an organization, add members to any fleet or folder, as well as perform any task and use any data service that does not have an explicit role associated with it. Users with this role manage your organization by creating folders and fleets, assigning roles, adding users, and managing systems if they have the proper credentials.
Folder or fleet admin	Allows a user unrestricted access to assigned fleets and folders. Can add members to folders or fleets they manage, as well as perform any task and use any data service or application on resources within the folder or fleet they are assigned.
Federation admin	Allows a user to create and manage directory service federations with the Console so users can authenticate with their existing directory credentials.
Federation viewer	Allows a user to view existing directory service federations with the Console. Cannot create or manage federations.
Super admin	Gives the user all of admin roles. This role is designed for smaller organizations that may not need to distribute Console responsibilities across multiple users.
Super viewer	Gives the user all viewer roles. This role is designed for smaller organizations that may not need to distribute Console responsibilities across multiple users.

Application roles

The following is a list of roles in the application category. Each role grants specific permissions within its designated scope. Users without the required application or platform role cannot access the respective application.

Application role	Responsibilities
Operation support analyst	Provides access to alerts and monitoring tools such as the Audit page.
Storage admin	Administer storage health and governance functions, discover storage resources, as well as modify and delete existing systems.
Storage viewer	View storage health and governance functions, as well as view previously discovered storage resources. Cannot discover, modify, or delete existing storage systems.
System health specialist	Administer storage and health and governance functions, all permissions of the Storage admin except cannot modify or delete existing systems.

Data service roles

The following is a list of roles in the data service category. Each role grants specific permissions within its designated scope. Users who do not have the required data service role or a platform role will be unable to access the data service.

Data service role	Responsibilities
Backup and recovery super admin	Perform any actions in NetApp Backup and Recovery.
Backup and recovery admin	Perform backups to local snapshots, replicate to secondary storage, and back up to object storage.
Backup and recovery restore admin	Restore workloads in the Backup and Recovery.
Backup and recovery clone admin	Clone applications and data in the Backup and Recovery.
Backup and recovery viewer	View Backup and Recovery information.
Classification viewer	Allows users to view NetApp Data Classification scan results. Users with this role can view compliance information and generate reports for resources that they have permission to access. These users can't enable or disable scanning of volumes, buckets, or database schemas. Data Classification does not have an admin role.
SnapCenter admin	Provides the ability to back up snapshots from on-premises ONTAP clusters using NetApp Backup and Recovery for applications. A member who has this role can complete the following actions: * Complete any action from Backup and Recovery > Applications * Manage all systems in the fleets and folders for which they have permissions * Use all NetApp Console services SnapCenter does not have a viewer role.

Related links

- Learn about NetApp Console identity and access management
- Get started with identity and access in NetApp Console
- Add members and assign roles in a NetApp Console organization
- Learn about the API for NetApp Console IAM

NetApp Console local deployment platform access roles

Assign platform roles to users to grant permissions to manage the NetApp Console local deployment, assign roles, add users, create fleets, and manage user authentication.

Example for organization roles for a large multi-national organization

XYZ Corporation organizes data storage access by region—North America, Europe, and Asia-Pacific—providing regional control with centralized oversight.

The **Organization admin** in XYZ Corporation's Console local deployment creates an initial organization and separate folders for each region. The **Folder or fleet admin** for each region organizes fleets (with associated resources) within the region's folder.

Regional admins with the **Folder or fleet admin** role actively manage their folders by adding resources and users. These regional admins can also add, remove, or rename folders and fleets they manage. The **Organization admin** inherits permissions for any new resources, maintaining visibility of storage usage across

the entire organization.

Within the same organization, one user is assigned the **Federation admin** role to manage the federation of the organization with their corporate IdP. This user can add or remove federated organizations, but cannot manage users or resources within the organization. The **Organization admin** assigns a user the **Federation viewer** role to check federation status and view federated organizations.

The following tables indicate the actions that each Console local deployment platform role can perform.

Organization administration roles

Task	Organization admin	Folder or fleet admin
Create, modify or delete systems from the Console local deployment (add or discover systems)	Yes	Yes
Create folders and fleets, including deleting	Yes	No
Rename existing folders and fleets	Yes	Yes
Assign roles and add users	Yes	Yes
Associate resources with folders and fleets	Yes	Yes
Register for support and submit cases through the Console	Yes	Yes
Use data services that are not associated with an explicit access role	Yes	Yes
View the Audit page and notifications	Yes	Yes

Federation roles

Task	Federation admin	Federation viewer
Create and update directory service integrations	Yes	No
View federations and their details	Yes	Yes

Super admin and viewer roles

The **Super admin** role provides full access to manage Console features, storage, and data services. This role suits those overseeing administration and governance. In contrast, the **Super viewer** role offers read-only access, ideal for auditors or stakeholders who need visibility without making changes.

Organizations should use **Super admin** access sparingly to minimize security risks and align with the principle of least privilege. Most organizations should assign fine-grained roles with only the necessary permissions to reduce risk and improve auditability.

Example for super roles

ABC Corporation has a small team of five that leverages the NetApp Console for data services and storage management. Instead of distributing multiple roles, they assign the **Super admin** role to two senior team members who handle all administrative tasks, including user management and resource configuration. The remaining three team members are assigned the **Super viewer** role, allowing them to monitor storage health and data service status without the ability to modify settings.

Role	Inherited roles
Super admin	• Organization admin • Folder or fleet admin • Backup and recovery super admin • Storage admin
Super viewer	• Organization viewer • Backup viewer • Storage viewer

Operational support analyst access role in NetApp Console local deployment

In NetApp Console local deployment, you can assign the Operational support analyst role to users to provide them access to alerts and monitoring.

Operational support analyst

Task	Can perform
View storage systems	Yes
View the Audit page and notifications	Yes
View, download, and configure alerts	Yes

Storage access roles for NetApp Console local deployment

You can assign the following roles to users to provide them access to the storage management features in NetApp Console local deployment. You can assign users an administrative role to manage storage or a viewer role for monitoring.

Administrators can assign storage roles to users for the following storage resources and features:

Storage resources:

- On-premises ONTAP clusters

Console services and features:

- Storage health functions

Example for storage roles in NetApp Console local deployment

XYZ Corporation, a multinational company, has a large team of storage engineers and storage administrators. They allow this team to manage storage assets for their regions while limiting access to core Console local deployment tasks like user management and license management.

Within a team of 12, two users are given the **Storage viewer** role which allows them to monitor the storage resources associated with the Console local deployment fleets they are assigned to. The remaining nine are given the **Storage admin** role which includes the ability to manage software updates, access ONTAP System Manager through the Console local deployment, as well as discover storage resources (add systems). One person on the team is given the **System health specialist** role so they can manage the health of the storage resources in their region, but not modify or delete any systems. This person can also perform software updates on the storage resources for fleets they are assigned.

The organization has two additional users with the **Organization admin** role who can manage all aspects of the Console local deployment, including user management and license management, as well as several users with the **Folder or fleet admin** role who can perform Console local deployment administration tasks for the folders and fleets they are assigned to.

The following table shows the actions each storage role performs.

Feature and action	Storage admin	System health specialist	Storage viewer
Storage Management:			
Discover new resources (add systems)	Yes	Yes	No
View added systems	Yes	Yes	No
Delete systems from the Console	Yes	No	No
Modify systems	Yes	No	No
System manager access			
May enter credentials	Yes	Yes	No

NetApp Backup and Recovery roles in NetApp Console local deployment

In NetApp Console local deployment, you can assign the following roles to users to provide them access to NetApp Backup and Recovery within the Console. Backup and Recovery roles give you the flexibility to assign users a role specific to the tasks they need to accomplish within your organization. How you assign roles depends on your own business and storage management practices.

The service uses the following roles that are specific to NetApp Backup and Recovery.

- **Backup and recovery super admin**: Perform any actions in NetApp Backup and Recovery.
- **Backup and recovery backup admin**: Perform backups to local snapshots, replicate to secondary storage, and back up to object storage actions in NetApp Backup and Recovery.
- **Backup and recovery restore admin**: Restore workloads using NetApp Backup and Recovery.
- **Backup and recovery clone admin**: Clone applications and data using NetApp Backup and Recovery.
- **Backup and recovery viewer**: View information in NetApp Backup and Recovery, but not perform any actions.

For details about all NetApp Console access roles, see the Console setup and administration documentation.

Roles used for common actions

The following table indicates the actions that each NetApp Backup and Recovery role can perform for all workloads.

Feature and action	Backup and recovery super admin	Backup and recovery backup admin	Backup and recovery restore admin	Backup and recovery clone admin	Backup and recovery viewer
Add, edit, or delete hosts	Yes	No	No	No	No
Install plugins	Yes	No	No	No	No
Add credentials (host, instance, vCenter)	Yes	No	No	No	No
View dashboard and all tabs	Yes	Yes	Yes	Yes	Yes
Start free trial	Yes	No	No	No	No
Initiate discovery of workloads	No	Yes	Yes	Yes	No
View license information	Yes	Yes	Yes	Yes	Yes
Activate license	Yes	No	No	No	No
View hosts	Yes	Yes	Yes	Yes	Yes
Schedules:					
Activate schedules	Yes	Yes	Yes	Yes	No
Suspend schedules	Yes	Yes	Yes	Yes	No
Policies and protection:					
View protection plans	Yes	Yes	Yes	Yes	Yes
Create, modify, or delete protection plans	Yes	Yes	No	No	No
Restore workloads	Yes	No	Yes	No	No
Create, split, or delete clones	Yes	No	No	Yes	No

Feature and action	Backup and recovery super admin	Backup and recovery backup admin	Backup and recovery restore admin	Backup and recovery clone admin	Backup and recovery viewer
Create, modify, or delete policy	Yes	Yes	No	No	No
Reports:					
View reports	Yes	Yes	Yes	Yes	Yes
Create reports	Yes	Yes	Yes	Yes	No
Delete reports	Yes	No	No	No	No
Import from SnapCenter and manage host:					
View imported SnapCenter data	Yes	Yes	Yes	Yes	Yes
Import data from SnapCenter	Yes	Yes	No	No	No
Manage (migrate) host	Yes	Yes	No	No	No
Configure settings:					
Configure log directory	Yes	Yes	Yes	No	No
Associate or remove instance credentials	Yes	Yes	Yes	No	No
Buckets:					
View buckets	Yes	Yes	Yes	Yes	Yes
Create, edit, or delete bucket	Yes	Yes	No	No	No

Roles used for workload-specific actions

The following table indicates the actions that each NetApp Backup and Recovery role can perform for specific workloads.

Kubernetes workloads

This table indicates the actions that each NetApp Backup and Recovery role can perform for actions specific to Kubernetes workloads.

Feature and action	Backup and recovery super admin	Backup and recovery backup admin	Backup and recovery restore admin	Backup and recovery viewer
View clusters, namespaces, storage classes, and API resources	Yes	Yes	Yes	Yes
Add new Kubernetes clusters	Yes	Yes	No	No
Update cluster configurations	Yes	No	No	No
Remove clusters from management	Yes	No	No	No
View applications	Yes	Yes	Yes	Yes
Create and define new applications	Yes	Yes	No	No
Update application configurations	Yes	Yes	No	No
Remove applications from management	Yes	Yes	No	No
View protected resources and backup status	Yes	Yes	Yes	Yes
Create backups and protect applications with policies	Yes	Yes	No	No
Unprotect apps and delete backups	Yes	Yes	No	No
View recovery points and resource viewer results	Yes	Yes	Yes	Yes
Restore applications from recovery points	Yes	No	Yes	No
View Kubernetes backup policies	Yes	Yes	Yes	Yes
Create Kubernetes backup policies	Yes	Yes	Yes	No
Update backup policies	Yes	Yes	Yes	No
Delete backup policies	Yes	Yes	Yes	No
View execution hooks and hook sources	Yes	Yes	Yes	Yes

Feature and action	Backup and recovery super admin	Backup and recovery backup admin	Backup and recovery restore admin	Backup and recovery viewer
Create execution hooks and hook sources	Yes	Yes	Yes	No
Update execution hooks and hook sources	Yes	Yes	Yes	No
Delete execution hooks and hook sources	Yes	Yes	Yes	No
View execution hook templates	Yes	Yes	Yes	Yes
Create execution hook templates	Yes	Yes	Yes	No
Update execution hook templates	Yes	Yes	Yes	No
Delete execution hook templates	Yes	Yes	Yes	No
View workload summary and analytics dashboards	Yes	Yes	Yes	Yes
View StorageGRID buckets and storage targets	Yes	Yes	Yes	Yes

Configure Console integrations and services

Integrate NetApp Console local deployment with Active Directory

Integrate NetApp Console local deployment with Active Directory for directory-backed sign-in and user lookup. Use your directory service to authenticate users, then assign access to those users in NetApp Console local deployment.

Required access roles

Super admin or Organization admin. Learn about access roles.

When you integrate with Active Directory, Console local deployment authenticates users through your existing directory. After you add a directory user, assign Console access roles to control what that user can access.

Active Directory integration also helps you meet compliance requirements by applying your existing controls, audit trails, and policies to Console local deployment access.

- Active Directory integration does not create federated groups, does not synchronize directory-group assignments, and does not automatically grant access. Administrators still add directory users to the organization and assign roles in Console local deployment.
- Only one Active Directory integration is supported at a time. Once an integration is configured, the **Add integration** button is disabled. To switch to a different directory, disable or delete the existing integration first.
- Directory users do not configure or use multi-factor authentication (MFA). Console local deployment supports MFA only for local users. Learn how to manage member security settings.

Before you begin

Before you integrate with Active Directory, confirm that you have:

- An Active Directory domain and credentials that can query the directory
- The LDAP server address and the base distinguished name (DN) for the directory tree
- Network access from Console local deployment to your LDAP server on port 389 (LDAP) or 636 (LDAPS)
- SSL/TLS certificates, if you plan to use LDAPS

Steps

1. Select **Administration > Identity and access**.
2. Select **Directory services** to open the Federations page.
3. Select **Add integration**.
4. Enter the connection details for your Active Directory server:
   - A descriptive name for the integration.
   - The **LDAP host**: hostname or IP address of your LDAP server. For multiple servers, enter the primary.
   - The port: 389 for LDAP or 636 for LDAPS.
   - The **Connection timeout** in milliseconds. The default is 1000 ms.
5. Select **Use SSL/TLS** to use LDAPS. Confirm that your LDAP server supports LDAPS and that the Console can access the required certificates.
6. Test the connection. If it fails, check the LDAP host, port, network connectivity, and SSL/TLS certificates.
7. After the test succeeds, enter the directory and user details:
   - **Base DN binding**: Enter the Bind DN for the LDAP/AD account this app will use to connect to the directory, and enter the Bind credential (password) for that account. Console uses these details to bind to LDAP and validate the connection.
   - **User DN**: a user account with permission to query the directory. For example, `CN=ldap-reader,OU=Service Accounts,DC=example,DC=com`.
8. Select **Add** to save the integration.

After you finish

After you save the integration, add directory users to your organization and assign roles. You must configure and enable at least one Active Directory integration before you can add directory users. Learn how to add directory users and assign roles.

Disable or enable an Active Directory integration

Disable an integration to temporarily suspend directory-backed authentication without deleting the configuration. When you disable a directory service, directory users cannot sign in through the directory.

Steps

1. Select **Administration > Identity and access**.
2. Select **Directory services** to open the Federations page.
3. In the integrations list, locate the integration and select the action menu for that row.
4. Select **Disable** to suspend the integration, or **Enable** to restore it.

Delete an Active Directory integration

Delete an integration to permanently remove the directory service configuration. Before deleting, review any warnings about directory users that are linked to the integration, as their access will be affected.

Steps

1. Select **Administration > Identity and access**.
2. Select **Directory services** to open the Federations page.
3. In the integrations list, locate the integration and select the action menu for that row.
4. Select **Delete** and confirm the deletion.

Connect your LLM and enable the NetApp Console assistant in NetApp Console local deployment

Connect your large language model (LLM) to NetApp Console local deployment to enable the Console assistant and AI-assisted storage management.

This documentation regarding connecting an LLM to the Console assistant to enable AI features is provided as a technology preview. With this preview offering, NetApp reserves the right to modify offering details, contents, and timeline before General Availability.

Required access roles

Super admin or Organization admin. Learn about access roles.

After setup, users open the Console assistant from the dashboard and choose an access mode:

- In **Read only** mode, the assistant answers questions and provides guidance without making changes.
- In **Read/write** mode, the assistant can act on storage infrastructure. It shows details for review and confirmation before each change. For asynchronous operations, such as volume creation, it creates a job that users can check from the assistant.

To connect your LLM, select a provider path, enter endpoint details and API key, and then select a model in **Administration > AI Tools**. Assistant actions stay within your storage policies and role-based access controls.

Gather what you need before you connect an LLM

Before you connect your LLM, gather the following:

- Your provider type decision: OpenAI or OpenAI-compatible. Learn about provider choices.
- A valid API key for the provider path you select.
- The endpoint URL for your provider path.
- Your proxy or gateway URL, if your organization requires one.
- Your user name or single sign-on (SSO) ID for the LLM provider account, if required.
- Network access from Console local deployment to the selected endpoint.
- Storage classes and role-based access controls for the assistant actions you plan to allow.

For supported model details, see Learn about supported LLM providers and models in NetApp Console local deployment.

Connect an LLM to NetApp Console local deployment

Enter provider settings, API key, and model to connect your LLM to Console local deployment.

Steps

1. Log in to the NetApp Console local deployment.
2. Select **Administration > AI Tools**.
3. Select the menu, and then select **Edit**.
4. In **Provider type**, select a provider type.

   Learn about LLM integration in NetApp Console local deployment.

5. If prompted for a provider endpoint, enter the endpoint URL for the provider path you selected.
6. Enter the proxy or gateway URL and credentials.
7. In the **User name** field, enter your user name or SSO ID if your provider path requires it.
8. In the **API key** field, paste the API key from your selected provider path.
9. Select a model from the list.
10. Review the configuration, and then select **Save**.

    If save or test fails, verify the provider type, endpoint URL, API key, and selected model, and then try again.

Troubleshoot your LLM integration.

Verify that LLM integration works

After you save the configuration, verify assistant availability and behavior.

Steps

1. Confirm that the **Console assistant** button appears on the NetApp Console local deployment dashboard.
2. Open the assistant in **Read only** mode and run a basic query.
3. Open the assistant in **Read/write** mode and confirm that storage-changing actions require user confirmation before execution.
4. Verify that the users who need action workflows have the required role-based access controls.

After you complete validation, users can open the Console assistant from the dashboard and describe tasks in

plain language. For usage examples and end-user workflows, see Use the NetApp Console assistant.

Protect credentials and monitor LLM usage

- Use a dedicated API key for Console local deployment integration when possible.
- Rotate API keys according to your organization policy.
- Restrict who can edit AI Tools settings to required admin roles only.
- Monitor provider-side API usage and alerts to track abnormal activity or cost spikes.

Troubleshoot LLM integration in NetApp Console local deployment

Use this quick triage flow to diagnose and resolve common LLM integration issues in NetApp Console local deployment.

> This documentation regarding connecting an LLM to the Console assistant to enable AI features is provided as a technology preview. With this preview offering, NetApp reserves the right to modify offering details, contents, and timeline before General Availability.

If you have not completed setup, see Connect your LLM and enable the NetApp Console assistant.

Triage LLM integration issues quickly

1. Validate AI Tools configuration in **Administration > AI Tools**.

   Confirm provider type, endpoint URL, API key, selected model, and outbound network access.

2. Validate assistant availability on the dashboard.

   Confirm the **Console assistant** button appears for expected users and organizations.

3. Validate runtime behavior.

   Run a simple read-only request and confirm provider endpoint reachability, model availability, and provider service health.

Troubleshoot by symptom

Symptom	Likely cause	What to check	Next action
Save or test fails in AI Tools	Configuration or connectivity mismatch	Provider type, endpoint URL, API key format, selected model, and outbound access	Correct the value that fails validation and save again
Console assistant button is missing	Unhealthy integration status, org mismatch, or RBAC mismatch	Successful AI Tools save, integration status, current organization, and expected access role	Refresh the session and verify with a known-good admin account

Symptom	Likely cause	What to check	Next action
Assistant opens but request fails	Provider or runtime path issue	Endpoint reachability, model availability on that endpoint, provider limits, and temporary provider status	Retry after fixing endpoint/model mismatch or provider-side limit issues
Assistant response is slow or inconsistent	Prompt size, endpoint performance, or network/proxy instability	Short prompt test, provider service health, and network/proxy stability	Use a shorter prompt, try another supported model, and stabilize network or proxy routing

Respond to LLM credential exposure or misuse

If you suspect API key exposure or unauthorized use:

1. Revoke the existing API key in your provider system.
2. Create a new API key.
3. Update the key in **Administration > AI Tools**.
4. Verify successful reconnection with a read-only assistant test.

Set up notification delivery channels in NetApp Console local deployment

In NetApp Console local deployment, you can set up multiple channels for alert notifications, including email and webhooks.

Required access roles

Super admin or Organization admin. Learn about access roles.

By default, Console local deployment displays notifications through its built-in notification system. Configuring additional delivery channels lets you receive notifications in the way that best fits your workflow.

You can send all notifications through the same channels or use different channels for different notification types. For example, you might send urgent storage alerts through email while routing other alert traffic to a third-party monitoring tool through a webhook.

After you set up notification delivery channels, you can configure notification rules and assign them to different channels. Learn how to configure notification rules.

Configure an email server

When you configure an email server, Console local deployment sends notifications, alerts, and user invitations through it. Console local deployment supports SMTP email servers, which can be your existing corporate email server or a third-party email service.

Steps

1. Select **Administration > Console**.
2. Select **Configuration** to open the System configurations page.
3. In the **Email server** section, select **Configure**.
4. Enter the connection details for your email server:

- Add a sender name and a sender email address.
- The **SMTP host**: hostname or IP address of your SMTP server. For multiple servers, enter the primary.
- Select the connection protocol from the **Connection security** dropdown list. The port is configured for you and is read-only: 25 for SMTP with STARTTLS, or 465 for SMTPS.

  SMTPS (port 465) establishes an encrypted connection immediately and is recommended for security-sensitive environments. STARTTLS (port 25) upgrades from an unencrypted connection and may fall back to unencrypted transmission if the encryption negotiation fails.

5. Select **Test email** to send a test email to a recipient you specify.
6. After the test succeeds, select **Save** to save the configuration.

   If the test fails, re-verify the settings you entered and double-check that Console local deployment has network access to the email server.

Update an email server configuration

You can update an existing email server configuration if you want to use a different email server.

Steps

1. Select **Administration > Console**.
2. Select **Configuration** to open the System configurations page.
3. In the **Email server** section, select **Configure**.
4. Select **Clear fields** to clear the existing configuration.
5. Enter the new connection details for your email server.
6. Select **Test email** to send a test email to a recipient you specify.
7. After the test succeeds, select **Save** to save the new configuration.

   If the test fails, re-verify the settings you entered and double-check that Console local deployment has network access to the email server.

Remove an email server configuration

You can remove the email server configuration if you no longer want Console local deployment to send emails.

Steps

1. Select **Administration > Console**.
2. Select **Configuration** to open the Systems configuration page.
3. In the **Email server** section, select **Configure**.
4. Select **Clear fields** to clear the existing configuration.
5. Select **Save** to save the cleared configuration, which removes the email server configuration from Console local deployment.

Configure a webhook

Set up webhooks to send notifications from Console local deployment to other tools or services. You can configure multiple webhooks, each pointing to a different endpoint. For example, one for a SIEM and another

for an on-call paging service.

After you create a webhook, users with the Storage admin role can assign it to specific alert rules. For example, they can send critical alerts to email while sending all alerts to a third-party monitoring tool through a webhook.

> Console local deployment does not enforce access control on webhook endpoints. Any user or system that can reach the endpoint URL receives the alert data. Ensure that access to the receiving application is restricted to authorized users through that application's own access controls.

Before you begin

Confirm that Console local deployment can reach the receiving application over the network, and gather the endpoint URL, HTTP method, and any authentication or certificate details required by that application.

Steps

1. Select **Administration > Console**.
2. Select **Configuration** to open the System configurations page.
3. In the **Webhook integration** section, select **Configure**.
4. Enter the required details for the webhook:
   - A descriptive name for the webhook.
   - The Endpoint URL provided by the receiving application.
   - HTTP method
   - Optional: A self-signed certificate in PEM format.
   - Any required headers or secrets (authentication credentials).
   - The format to use when sending the webhook. JSON and OTEL (OpenTelemetry) are supported.

     Use JSON for general-purpose webhooks and custom REST endpoints. Use OTEL for observability platforms that natively consume OpenTelemetry signals, such as Grafana or other OpenTelemetry-compatible collectors.
5. Select **Test webhook** to test the webhook connection and ensure that Console local deployment can successfully send messages to the receiving application.
6. After the test succeeds, select **Save** to create the webhook.

   After you save the webhook, it is available for users to select where webhooks are supported, such as Alert delivery options. Learn how to create alert rules and assign webhooks for alert delivery.

Copyright information

Trademark information