Plan your Console organization

NetApp Console local deployment

NetApp
August 10, 2026

Table of Contents

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.

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.

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.

Copyright information

Trademark information