Set up your Console organization

NetApp Console local deployment

NetApp
August 10, 2026

Table of Contents

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

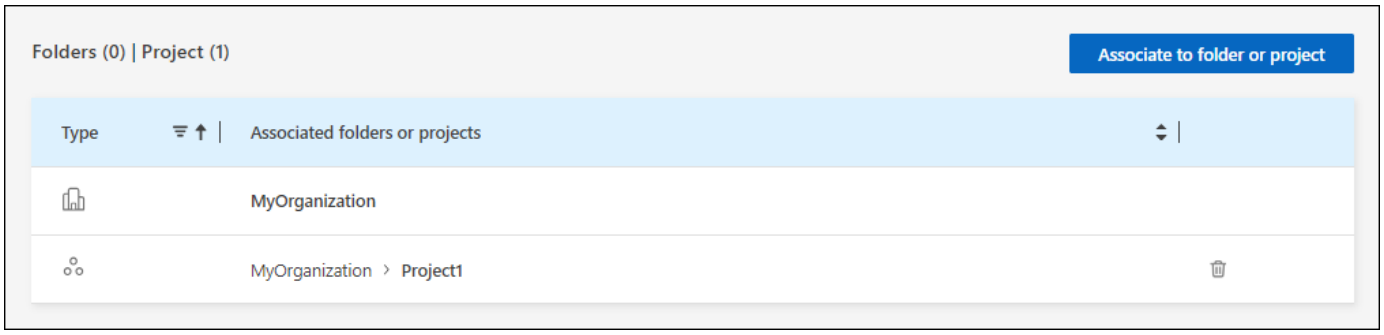
Verify which fleets or folders a resource is associated with.

> 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

Task	Federation admin	Federation viewer
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

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
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
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:					

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
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

Feature and action	Backup and recovery super admin	Backup and recovery backup admin	Backup and recovery restore admin	Backup and recovery viewer
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
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

Copyright information

Trademark information