Data services roles

NetApp Console setup and administration

NetApp
January 27, 2026

Table of Contents

Data services roles

NetApp Backup and Recovery roles in NetApp Console

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

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
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
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

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
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

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

NetApp Disaster Recovery roles in NetApp Console

You can assign the following roles to users to provide them access to NetApp Disaster Recovery within the Console. Disaster 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.

Disaster Recovery uses the following roles:

- **Disaster recovery admin**: Perform any actions.
- **Disaster recovery failover admin**: Perform failover and migrations.
- **Disaster recovery application admin**: Create replication plans. Modify replication plans. Start test failovers.
- **Disaster recovery viewer**: View information only.

The following table indicates the actions that each role can perform.

Feature and action	Disaster recovery admin	Disaster recovery failover admin	Disaster recovery application admin	Disaster recovery viewer
View dashboard and all tabs	Yes	Yes	Yes	Yes
Start free trial	Yes	No	No	No
Initiate discovery of workloads	Yes	No	No	No
View license information	Yes	Yes	Yes	Yes
Activate license	Yes	No	Yes	No
On the Sites tab:				
View sites	Yes	Yes	Yes	Yes
Add, modify, or delete sites	Yes	No	No	No
On the Replication plans tab:				
View replication plans	Yes	Yes	Yes	Yes
View replication plan details	Yes	Yes	Yes	Yes
Create or modify replication plans	Yes	Yes	Yes	No
Create reports	Yes	No	No	No

Feature and action	Disaster recovery admin	Disaster recovery failover admin	Disaster recovery application admin	Disaster recovery viewer
View snapshots	Yes	Yes	Yes	Yes
Perform failover tests	Yes	Yes	Yes	No
Perform failovers	Yes	Yes	No	No
Perform failbacks	Yes	Yes	No	No
Perform migrations	Yes	Yes	No	No
On the Resource groups tab:				
View resource groups	Yes	Yes	Yes	Yes
Create, modify, or delete resource groups	Yes	No	Yes	No
On the Job Monitoring tab:				
View jobs	Yes	No	Yes	Yes
Cancel jobs	Yes	Yes	Yes	No

Ransomware Resilience access roles for NetApp Console

Ransomware Resilience roles provide users access to NetApp Ransomware Resilience. Ransomware Resilience supports the following roles:

Baseline roles

- Ransomware Resilience admin - Configure Ransomware Resilience settings; investigate and respond to encryption alerts
- Ransomware Resilience viewer - View encryption incidents, reports, and discovery settings

User behavior activity roles

Suspicious user activity detection alerts provide visibility into data such as file activity events; these alerts include file names and file actions (such as Read, Write, Delete, Rename) performed by the user. To limit the visibility of this data, only users with these roles can manage or view these alerts.

- Ransomware Resilience user behavior admin - Activate suspicious user activity detection, investigate and respond to suspicious user activity alerts
- Ransomware Resilience user behavior viewer - View suspicious user activity alerts

User behavior roles are not standalone roles; they are designed to be added to Ransomware Resilience admin or viewer roles. For more information, see User behavior roles.

Consult the following tables for detailed descriptions of each role.

Baseline roles

The following table describes the actions available to the Ransomware Resilience admin and viewer roles.

Feature and action	Ransomware Resilience admin	Ransomware Resilience viewer
View dashboard and all tabs	Yes	Yes
On dashboard, update recommendation status	Yes	No
Start free trial	Yes	No
Initiate discovery of workloads	Yes	No
Initiate rediscovery of workloads	Yes	No
On the Protect tab:		
Add, modify, or delete protection plans for *encryption* policies	Yes	No
Protect workloads	Yes	No
Identify exposure to sensitive data with Data Classification	Yes	No
List protection plans and details	Yes	Yes
List protection groups	Yes	Yes
View protection group details	Yes	Yes
Create, edit, or delete protection groups	Yes	No
Download data	Yes	Yes
On the Alerts tab:		
View encryption alerts and alert details	Yes	Yes
Edit encryption incident status	Yes	No
Mark encryption alert for recovery	Yes	No
View encryption incident details	Yes	Yes

Feature and action	Ransomware Resilience admin	Ransomware Resilience viewer
Dismiss or resolve encryption incidents	Yes	No
Get full list of impacted files in encryption event	Yes	No
Download encryption event alerts data	Yes	Yes
Block user (with Workload Security agent configuration)	Yes	No
On the Recover tab:		
Download impacted files from encryption event	Yes	No
Restore workload from encryption event	Yes	No
Download recovery data from encryption event	Yes	Yes
Download reports from encryption event	Yes	Yes
On the Settings tab:		
Add or modify backup destinations	Yes	No
List backup destinations	Yes	Yes
View connected SIEM targets	Yes	Yes
Add or modify SIEM targets	Yes	No
Configure readiness drill	Yes	No
Start, reset, or edit readiness drill	Yes	No
Review readiness drill status	Yes	Yes
Update discovery configuration	Yes	No
View discovery configuration	Yes	Yes
On the Reports tab:		
Download reports	Yes	Yes

User behavior roles

To configure suspicious user behavior settings and respond to alerts, a user must have the Ransomware Resilience user behavior admin role. To only view suspicious user behavior alerts, a user should have the Ransomware Resilience user behavior viewer role.

User behavior roles should be conferred on users with existing Ransomware Resilience admin or viewer priviliges who need access to suspicious user activity settings and alerts. A user with the Ransomware Resilience admin role, for example, should receive the Ransomware Resilience user behavior admin role to configure user activity agents and block or unblock users. The Ransomware Resilience user behavior admin role should not be conferred on a Ransomware Resilience viewer.

To activate suspicious user activity detection, you must have the Console Organization admin role.

The following table describes the actions available to the Ransomware Resilience user behavior admin and viewer roles.

Feature and action	Ransomware Resilience user behavior admin	Ransomware Resilience user behavior viewer
On the Settings tab:		
Create, modify, or delete user activity agent	Yes	No
Create or delete user directory connector	Yes	No
Pause or resume data collector	Yes	No
Run data breach readiness drill	Yes	No
On the Protect tab:		
Add, modify, or delete protection plans for *suspicious user behavior* policies	Yes	No
On the Alerts tab:		
View user activity alerts and alert details	Yes	Yes
Edit user activity incident status	Yes	No
Mark user activity alert for recovery	Yes	No
View user activity incident details	Yes	Yes
Dismiss or resolve user activity incidents	Yes	No
Get full list of impacted files by suspicious user	Yes	Yes

Feature and action	Ransomware Resilience user behavior admin	Ransomware Resilience user behavior viewer
Download user activity event alerts data	Yes	Yes
Block or unblock user	Yes	No
On the Recover tab:		
Download impacted files for user activity event	Yes	No
Restore workload from user activity event	Yes	No
Download recovery data from user activity event	Yes	Yes
Download reports from user activity event	Yes	Yes

Copyright information

Trademark information