



Access roles

NetApp Console local deployment

NetApp
August 10, 2026

Table of Contents

- Access roles 1
 - NetApp Console local deployment access roles 1
 - Platform roles 1
 - Application roles 1
 - Data service roles 2
 - Related links 2
 - NetApp Console local deployment platform access roles 3
 - Organization administration roles 3
 - Federation roles 3
 - Super admin and viewer roles 4
 - Operational support analyst access role in NetApp Console local deployment 4
 - Operational support analyst 4
 - Storage access roles for NetApp Console local deployment 5
 - NetApp Backup and Recovery roles in NetApp Console local deployment 6
 - Roles used for common actions 6
 - Roles used for workload-specific actions 8

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

Task	Can perform
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

Feature and action	Storage admin	System health specialist	Storage viewer
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

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 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
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

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
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

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

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

Copyright © 2026 NetApp, Inc. All Rights Reserved. Printed in the U.S. No part of this document covered by copyright may be reproduced in any form or by any means—graphic, electronic, or mechanical, including photocopying, recording, taping, or storage in an electronic retrieval system—without prior written permission of the copyright owner.

Software derived from copyrighted NetApp material is subject to the following license and disclaimer:

THIS SOFTWARE IS PROVIDED BY NETAPP “AS IS” AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, WHICH ARE HEREBY DISCLAIMED. IN NO EVENT SHALL NETAPP BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

NetApp reserves the right to change any products described herein at any time, and without notice. NetApp assumes no responsibility or liability arising from the use of products described herein, except as expressly agreed to in writing by NetApp. The use or purchase of this product does not convey a license under any patent rights, trademark rights, or any other intellectual property rights of NetApp.

The product described in this manual may be protected by one or more U.S. patents, foreign patents, or pending applications.

LIMITED RIGHTS LEGEND: Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (b)(3) of the Rights in Technical Data -Noncommercial Items at DFARS 252.227-7013 (FEB 2014) and FAR 52.227-19 (DEC 2007).

Data contained herein pertains to a commercial product and/or commercial service (as defined in FAR 2.101) and is proprietary to NetApp, Inc. All NetApp technical data and computer software provided under this Agreement is commercial in nature and developed solely at private expense. The U.S. Government has a non-exclusive, non-transferrable, nonsublicensable, worldwide, limited irrevocable license to use the Data only in connection with and in support of the U.S. Government contract under which the Data was delivered. Except as provided herein, the Data may not be used, disclosed, reproduced, modified, performed, or displayed without the prior written approval of NetApp, Inc. United States Government license rights for the Department of Defense are limited to those rights identified in DFARS clause 252.227-7015(b) (FEB 2014).

Trademark information

NETAPP, the NETAPP logo, and the marks listed at <http://www.netapp.com/TM> are trademarks of NetApp, Inc. Other company and product names may be trademarks of their respective owners.