NetApp Console

NetApp Console setup and administration

NetApp
January 13, 2026

Inhalt

NetApp Console

Erfahren Sie mehr über die Zugriffsrollen der NetApp Console

Das Identitäts- und Zugriffsmanagement (IAM) in der NetApp Console bietet vordefinierte Rollen, die Sie den Mitgliedern Ihrer Organisation auf verschiedenen Ebenen Ihrer Ressourcenhierarchie zuweisen können. Bevor Sie diese Rollen zuweisen, sollten Sie sich über die Berechtigungen im Klaren sein, die jede Rolle umfasst. Rollen fallen in die folgenden Kategorien: Plattform, Anwendung und Datendienst.

Plattformrollen

Plattformrollen gewähren Administratorberechtigungen für die NetApp Console , einschließlich Rollenzuweisung und Benutzerverwaltung. Die Konsole hat mehrere Plattformrollen.

Plattformrolle	Aufgaben
"Organisationsadministrator"	Ermöglicht einem Benutzer uneingeschränkten Zugriff auf alle Projekte und Ordner innerhalb einer Organisation, das Hinzufügen von Mitgliedern zu Projekten oder Ordnern sowie das Ausführen beliebiger Aufgaben und die Verwendung beliebiger Datendienste, denen keine explizite Rolle zugeordnet ist. Benutzer mit dieser Rolle verwalten Ihre Organisation, indem sie Ordner und Projekte erstellen, Rollen zuweisen, Benutzer hinzufügen und Systeme verwalten, wenn sie über die entsprechenden Anmeldeinformationen verfügen. Dies ist die einzige Zugriffsrolle, die Konsolenagenten erstellen kann.
"Ordner- oder Projektadministrator"	Ermöglicht einem Benutzer uneingeschränkten Zugriff auf zugewiesene Projekte und Ordner. Kann Mitglieder zu Ordnern oder Projekten hinzufügen, die sie verwalten, sowie beliebige Aufgaben ausführen und beliebige Datendienste oder Anwendungen auf Ressourcen innerhalb des ihnen zugewiesenen Ordners oder Projekts verwenden. Ordner- oder Projektadministratoren können keine Konsolenagenten erstellen.
"Föderationsadministrator"	Ermöglicht einem Benutzer das Erstellen und Verwalten von Föderationen mit der Konsole, wodurch Single Sign-On (SSO) ermöglicht wird.
"Föderationsbetrachter"	Ermöglicht einem Benutzer, vorhandene Föderationen mit der Konsole anzuzeigen. Föderationen können nicht erstellt oder verwaltet werden.
"Partnerschaftsadministrator"	Ermöglicht einem Benutzer, Partnerschaften zu erstellen und zu verwalten.
"Partnerschafts-Viewer"	Ermöglicht einem Benutzer, bestehende Partnerschaften anzuzeigen. Partnerschaften können nicht erstellt oder verwaltet werden.
"Super-Admin"	Gibt dem Benutzer eine Teilmenge von Administratorrollen. Diese Rolle ist für kleinere Organisationen gedacht, die die Konsolenverantwortlichkeiten möglicherweise nicht auf mehrere Benutzer verteilen müssen.

Plattformrolle	Aufgaben
"Super Viewer"	Gibt dem Benutzer eine Teilmenge der Viewer-Rollen. Diese Rolle ist für kleinere Organisationen gedacht, die die Konsolenverantwortlichkeiten möglicherweise nicht auf mehrere Benutzer verteilen müssen.

Anwendungsrollen

Nachfolgend finden Sie eine Liste der Rollen in der Anwendungskategorie. Jede Rolle gewährt innerhalb ihres festgelegten Umfangs spezifische Berechtigungen. Benutzer ohne die erforderliche Anwendungs- oder Plattformrolle können nicht auf die jeweilige Anwendung zugreifen.

Anwendungsrolle	Aufgaben
"Google Cloud NetApp Volumes Administrator"	Benutzer mit der Rolle „Google Cloud NetApp Volumes“ können Google Cloud NetApp Volumes erkennen und verwalten.
"Google Cloud NetApp Volumes Viewer"	Benutzer mit der Benutzerrolle „Google Cloud NetApp Volumes“ können Google Cloud NetApp Volumes anzeigen.
"Keystone -Administrator"	Benutzer mit der Keystone Administratorrolle können Serviceanfragen erstellen. Ermöglicht Benutzern, Nutzung, Ressourcen und Administratordetails innerhalb des Keystone Mandanten, auf den sie zugreifen, zu überwachen und anzuzeigen.
"Keystone -Viewer"	Benutzer mit der Keystone Viewer-Rolle KÖNNEN KEINE Serviceanfragen erstellen. Ermöglicht Benutzern die Überwachung und Anzeige von Verbrauch, Anlagen und Verwaltungsinformationen innerhalb des Keystone Mandanten, auf den sie zugreifen.
ONTAP Mediator-Setup-Rolle	Dienstkonten mit der Setup-Rolle „ONTAP Mediator“ können Dienstanfragen erstellen. Diese Rolle ist in einem Dienstkonto erforderlich, um eine Instanz des"ONTAP Cloud Mediator" .
"Betriebsunterstützungsanalyst"	Bietet Zugriff auf Warn- und Überwachungstools und die Möglichkeit, Supportfälle einzugeben und zu verwalten.
"Speicheradministrator"	Verwalten Sie Speicherintegritäts- und Governance-Funktionen, ermitteln Sie Speicherressourcen und ändern und löschen Sie vorhandene Systeme.
"Speicheranzeige"	Zeigen Sie Speicherintegrität und Governance-Funktionen an und zeigen Sie zuvor erkannte Speicherressourcen an. Vorhandene Speichersysteme können nicht erkannt, geändert oder gelöscht werden.
"Systemintegritätsspezialist"	Verwalten Sie Speicher-, Integritäts- und Governance-Funktionen. Alle Berechtigungen des Speicheradministrators sind zulässig, außer dass er vorhandene Systeme nicht ändern oder löschen kann.

Datendienstrollen

Nachfolgend finden Sie eine Liste der Rollen in der Kategorie Datendienste. Jede Rolle gewährt innerhalb ihres festgelegten Umfangs spezifische Berechtigungen. Benutzer, die nicht über die erforderliche Datendienstrolle oder Plattformrolle verfügen, können nicht auf den Datendienst zugreifen.

Datendienstrolle	Aufgaben
"Superadministrator für Backup und Wiederherstellung"	Führen Sie beliebige Aktionen in NetApp Backup and Recovery durch.
"Backup- und Wiederherstellungsadministrator"	Führen Sie Sicherungen auf lokalen Snapshots durch, replizieren Sie auf sekundären Speicher und sichern Sie auf Objektspeicher.
"Administrator für die Wiederherstellung von Backup und Wiederherstellung"	Stellen Sie Workloads in Backup und Recovery wieder her.
"Backup- und Wiederherstellungsklon-Administrator"	Klonen Sie Anwendungen und Daten in der Sicherung und Wiederherstellung.
"Backup- und Wiederherstellungs-Viewer"	Informationen zur Sicherung und Wiederherstellung anzeigen.
"Disaster Recovery-Administrator"	Führen Sie alle Aktionen im NetApp Disaster Recovery -Dienst aus.
"Disaster Recovery-Failover-Administrator"	Führen Sie Failover und Migrationen durch.
"Disaster Recovery-Anwendungsadministrator"	Erstellen Sie Replikationspläne, ändern Sie Replikationspläne und starten Sie Test-Failover.
"Disaster Recovery-Viewer"	Nur Informationen anzeigen.
Klassifizierungsanzeige	Ermöglicht Benutzern das Anzeigen der Scanergebnisse der NetApp Data Classification . Benutzer mit dieser Rolle können Compliance-Informationen anzeigen und Berichte für Ressourcen erstellen, auf die sie Zugriffsberechtigung haben. Diese Benutzer können das Scannen von Volumes, Buckets oder Datenbankschemata weder aktivieren noch deaktivieren. Die Klassifizierung hat keine Administratorrolle.
"Ransomware-Resilienz-Administrator"	Verwalten Sie Aktionen auf den Registerkarten „Schützen“, „Warnungen“, „Wiederherstellen“, „Einstellungen“ und „Berichte“ von NetApp Ransomware Resilience.
"Ransomware Resilience-Viewer"	Zeigen Sie Arbeitslastdaten und Warndaten an, laden Sie Wiederherstellungsdaten herunter und laden Sie Berichte in Ransomware Resilience herunter.
"Ransomware Resilience-Benutzerverhaltensadministrator"	Konfigurieren, verwalten und zeigen Sie die Erkennung, Warnungen und Überwachung verdächtigen Benutzerverhaltens in Ransomware Resilience an.
"Ransomware Resilience-Benutzerverhaltensanzeige"	Zeigen Sie Warnungen und Einblicke zu verdächtigem Benutzerverhalten in Ransomware Resilience an.
SnapCenter -Administrator	Bietet die Möglichkeit, Snapshots von lokalen ONTAP Clustern mithilfe von NetApp Backup and Recovery für Anwendungen zu sichern. Ein Mitglied mit dieser Rolle kann die folgenden Aktionen ausführen: * Alle Aktionen unter „Sicherung und Wiederherstellung > Anwendungen“ ausführen * Alle Systeme in den Projekten und Ordnern verwalten, für die es Berechtigungen hat * Alle NetApp Console verwenden SnapCenter hat keine Viewer-Rolle.

Weiterführende Links

- "Erfahren Sie mehr über die Identitäts- und Zugriffsverwaltung der NetApp Console"
- "Erste Schritte mit NetApp Console IAM"
- "Verwalten Sie NetApp Console Mitglieder und ihre Berechtigungen"
- "Erfahren Sie mehr über die API für NetApp Console IAM"

Plattformzugriffsrollen für die NetApp Console

Weisen Sie Benutzern Plattformrollen zu, um ihnen Berechtigungen zum Verwalten der NetApp Console, zum Zuweisen von Rollen, zum Hinzufügen von Benutzern, zum Erstellen von Konsolenagenten und zum Verwalten von Föderationen zu erteilen.

Beispiel für Organisationsrollen für eine große multinationale Organisation

Die XYZ Corporation organisiert den Datenspeicherzugriff nach Regionen – Nordamerika, Europa und Asien-Pazifik – und bietet regionale Kontrolle mit zentraler Aufsicht.

Der **Organisationsadministrator** in der Konsole der XYZ Corporation erstellt eine anfängliche Organisation und separate Ordner für jede Region. Der **Ordner- oder Projektadministrator** für jede Region organisiert Projekte (mit zugehörigen Ressourcen) innerhalb des Ordners der Region.

Regionale Administratoren mit der Rolle **Ordner- oder Projektadministrator** verwalten ihre Ordner aktiv, indem sie Ressourcen und Benutzer hinzufügen. Diese regionalen Administratoren können auch von ihnen verwaltete Ordner und Projekte hinzufügen, entfernen oder umbenennen. Der **Organisationsadministrator** erbt Berechtigungen für alle neuen Ressourcen und behält so die Übersicht über die Speichernutzung in der gesamten Organisation.

Innerhalb derselben Organisation wird einem Benutzer die Rolle **Föderationsadministrator** zugewiesen, um die Föderation der Organisation mit ihrem Unternehmens-IdP zu verwalten. Dieser Benutzer kann föderierte Organisationen hinzufügen oder entfernen, kann jedoch keine Benutzer oder Ressourcen innerhalb der Organisation verwalten. Der **Organisationsadministrator** weist einem Benutzer die Rolle **Föderationsbetrachter** zu, um den Föderationsstatus zu überprüfen und föderierte Organisationen anzuzeigen.

Die folgenden Tabellen zeigen die Aktionen, die jede Konsolenplattformrolle ausführen kann.

Rollen in der Organisationsverwaltung

Aufgabe	Organisationsadministrator	Ordner- oder Projektadministrator
Agenten erstellen	Ja	Nein
Erstellen, Ändern oder Löschen von Systemen über die Konsole (Hinzufügen oder Erkennen von Systemen)	Ja	Ja
Erstellen von Ordnern und Projekten, einschließlich Löschen	Ja	Nein
Vorhandene Ordner und Projekte umbenennen	Ja	Ja
Rollen zuweisen und Benutzer hinzufügen	Ja	Ja

Aufgabe	Organisationsadministrator	Ordner- oder Projektadministrator
Ressourcen mit Ordnern und Projekten verknüpfen	Ja	Ja
Agenten Ordnern und Projekten zuordnen	Ja	Nein
Agenten aus Ordnern und Projekten entfernen	Ja	Nein
Agenten verwalten (Zertifikate, Einstellungen usw. bearbeiten)	Ja	Nein
Verwalten Sie Anmeldeinformationen unter „Verwaltung > Anmeldeinformationen“.	Ja	Ja
Erstellen, Verwalten und Anzeigen von Föderationen	Ja	Nein
Registrieren Sie sich für den Support und reichen Sie Fälle über die Konsole ein	Ja	Ja
Verwenden Sie Datendienste, die keiner expliziten Zugriffsrolle zugeordnet sind	Ja	Ja
Anzeigen der Audit-Seite und Benachrichtigungen	Ja	Ja

Föderationsrollen

Aufgabe	Föderationsadministrator	Föderationsbetrachter
Erstellen einer Föderation	Ja	Nein
Verifizieren einer Domäne	Ja	Nein
Hinzufügen einer Domäne zu einem Verbund	Ja	Nein
Deaktivieren und Löschen von Föderationen	Ja	Nein
Testverbände	Ja	Nein
Verbände und deren Details anzeigen	Ja	Ja

Partnerschaftsrollen

Aufgabe	Partnerschaftsadministrator	Partnerschafts-Viewer
Kann eine Partnerschaft schaffen	Ja	Nein
Zuweisen von Rollen zu Partnermitgliedern	Ja	Nein
Kann Mitglieder zu einer Partnerschaft hinzufügen	Ja	Nein
Kann Details zur Organisationspartnerschaft anzeigen	Ja	Ja

Superadministrator- und Viewer-Rollen

Die Rolle **Superadministrator** bietet vollständigen Zugriff auf die Verwaltung von Konsolenfunktionen, Speicher und Datendiensten. Diese Rolle eignet sich für Personen, die für die Verwaltung und Governance zuständig sind. Im Gegensatz dazu bietet die Rolle „Super Viewer“ schreibgeschützten Zugriff, ideal für Prüfer

oder Stakeholder, die Einblick benötigen, ohne Änderungen vorzunehmen.

Organisationen sollten den **Superadministrator**-Zugriff sparsam verwenden, um Sicherheitsrisiken zu minimieren und das Prinzip der geringsten Privilegien einzuhalten. Die meisten Organisationen sollten fein abgestufte Rollen mit nur den erforderlichen Berechtigungen zuweisen, um das Risiko zu verringern und die Überprüfbarkeit zu verbessern.

Beispiel für Superrollen

ABC Corporation verfügt über ein kleines fünfköpfiges Team, das die NetApp Console für Datendienste und Speicherverwaltung nutzt. Anstatt mehrere Rollen zu verteilen, weisen sie die Rolle des **Superadministrators** zwei leitenden Teammitgliedern zu, die alle Verwaltungsaufgaben übernehmen, einschließlich Benutzerverwaltung und Ressourcenkonfiguration. Den übrigen drei Teammitgliedern wird die Rolle „Super Viewer“ zugewiesen, die es ihnen ermöglicht, die Speicherintegrität und den Status des Datendienstes zu überwachen, ohne die Möglichkeit zu haben, Einstellungen zu ändern.

Rolle	Geerbte Rollen
Super-Admin	• Organisationsadministrator • Ordner- oder Projektadministrator • Föderationsadministrator • Partnerschaftsadministrator • Ransomware-Resilienz-Administrator • Notfallwiederherstellungsadministrator • Backup-Superadministrator • Speicheradministrator • Keystone -Administrator • Google Cloud NetApp Volumes Administrator
Super Viewer	• Organisationsanzeige • Föderationsbetrachter • Partnerschafts-Viewer • Ransomware Resilience-Viewer • Disaster Recovery-Viewer • Backup-Viewer • Speicheranzeige • Keystone -Viewer • Google Cloud NetApp Volumes Viewer

Anwendungsrollen

Google Cloud NetApp Volumes -Rollen in der NetApp Console

Sie können Benutzern die folgende Rolle zuweisen, um ihnen Zugriff auf die Google Cloud NetApp Volumes in der NetApp Console zu gewähren.

Google Cloud NetApp Volumes verwendet die folgende Rolle:

- * Google Cloud NetApp Volumes Administrator*: Entdecken und verwalten Sie Google Cloud NetApp Volumes in der Konsole.
- * Google Cloud NetApp Volumes Viewer*: Google Cloud NetApp Volumes in der Konsole anzeigen.

Keystone -Zugriffsrollen in der NetApp Console

Keystone -Rollen bieten Zugriff auf die Keystone Dashboards und ermöglichen Benutzern das Anzeigen und Verwalten ihres Keystone Abonnements. Es gibt zwei Keystone -Rollen: Keystone -Administrator und Keystone Viewer. Der Hauptunterschied zwischen den beiden Rollen besteht in den Aktionen, die sie in Keystone ausführen können. Die Keystone Administratorrolle ist die einzige Rolle, die Serviceanfragen erstellen oder Abonnements ändern darf.

Beispiel für Keystone -Rollen in der NetApp Console

Bei der XYZ Corporation sind vier Speicheringenieure aus verschiedenen Abteilungen damit beschäftigt, die Keystone Abonnementinformationen anzuzeigen. Obwohl alle diese Benutzer das Keystone Abonnement überwachen müssen, darf nur der Teamleiter Serviceanfragen stellen. Drei Teammitglieder erhalten die Rolle „Keystone -Viewer“, während der Teamleiter die Rolle „Keystone Administrator“ erhält, sodass es einen Kontrollpunkt für die Serviceanfragen des Unternehmens gibt.

Die folgende Tabelle zeigt die Aktionen, die jede Keystone -Rolle ausführen kann.

Funktion und Aktion	Keystone -Administrator	Keystone -Viewer
Zeigen Sie die folgenden Registerkarten an: Abonnement, Assets, Monitor und Verwaltung	Ja	Ja
* Keystone -Abonnementseite*:		
Abonnements anzeigen	Ja	Ja
Abonnements ändern oder verlängern	Ja	Nein
* Keystone -Asset-Seite*:		
Assets anzeigen	Ja	Ja
Verwalten von Assets	Ja	Nein
* Keystone -Warnseite*:		

Funktion und Aktion	Keystone -Administrator	Keystone -Viewer
Warnungen anzeigen	Ja	Ja
Verwalten von Warnungen	Ja	Nein
Erstellen Sie Benachrichtigungen für sich selbst	Ja	Ja
* Licenses and subscriptions*:		
Kann Lizenzen und Abonnements anzeigen	Ja	Ja
* Keystone -Berichtsseite*:		
Berichte herunterladen	Ja	Ja
Berichte verwalten	Ja	Ja
Berichte für sich selbst erstellen	Ja	Ja
Serviceanfragen:		
Serviceanfragen erstellen	Ja	Nein
Zeigen Sie Serviceanfragen an, die von einem beliebigen Benutzer innerhalb der Organisation erstellt wurden	Ja	Ja

Zugriffsrolle „Operational Support Analyst“ für die NetApp Console

Sie können Benutzern die Rolle des Operational Support Analyst zuweisen, um ihnen Zugriff auf Warnmeldungen und Überwachungsfunktionen zu gewähren. Benutzer mit dieser Rolle können auch Supportfälle eröffnen.

Analyst für operative Unterstützung

Aufgabe	Kann durchführen
Verwalten Sie Ihre eigenen Benutzeranmeldeinformationen unter „Einstellungen > Anmeldeinformationen“.	Ja
Erkannte Ressourcen anzeigen	Ja
Registrieren Sie sich für den Support und reichen Sie Fälle über die Konsole ein	Ja
Anzeigen der Audit-Seite und Benachrichtigungen	Ja

Aufgabe	Kann durchführen
Anzeigen, Herunterladen und Konfigurieren von Warnungen	Ja

Speicherzugriffsrollen für die NetApp Console

Sie können Benutzern die folgenden Rollen zuweisen, um ihnen Zugriff auf die Speicherverwaltungsfunktionen in der NetApp Console zu gewähren. Sie können Benutzern eine Administratorrolle zum Verwalten des Speichers oder eine Viewer-Rolle zum Überwachen zuweisen.

Diese Rollen sind über die NetApp Console Partnerschafts-API nicht verfügbar.

Administratoren können Benutzern Speicherrollen für die folgenden Speicherressourcen und -funktionen zuweisen:

Speicherressourcen:

- On-Premises- ONTAP -Cluster
- StorageGRID
- E-Series

Konsolendienste und -funktionen:

- Digitaler Berater
- Software-Updates
- Lebenszyklusplanung
- Nachhaltigkeit

Beispiel für Speicherrollen in der NetApp Console

XYZ Corporation, ein multinationales Unternehmen, verfügt über ein großes Team von Speicheringenieuren und Speicheradministratoren. Sie ermöglichen diesem Team die Verwaltung von Speicherressourcen für ihre Regionen und beschränken gleichzeitig den Zugriff auf zentrale Konsolenaufgaben wie Benutzerverwaltung, Agentenerstellung und Lizenzverwaltung.

Innerhalb eines 12-köpfigen Teams erhalten zwei Benutzer die Rolle „Speicherbetrachter“, die es ihnen ermöglicht, die Speicherressourcen zu überwachen, die mit den ihnen zugewiesenen Konsolenprojekten verknüpft sind. Den restlichen neun wird die Rolle „Storage-Admin“ zugewiesen, die die Möglichkeit umfasst, Software-Updates zu verwalten, über die Konsole auf ONTAP System Manager zuzugreifen und Speicherressourcen zu ermitteln (Systeme hinzuzufügen). Einer Person im Team wird die Rolle „Systemintegritätsspezialist“ zugewiesen, damit sie die Integrität der Speicherressourcen in ihrer Region verwalten, aber keine Systeme ändern oder löschen kann. Diese Person kann auch Software-Updates auf den Speicherressourcen für die ihr zugewiesenen Projekte durchführen.

Die Organisation verfügt über zwei weitere Benutzer mit der Rolle **Organisationsadministrator**, die alle Aspekte der Konsole verwalten können, einschließlich Benutzerverwaltung, Agentenerstellung und Lizenzverwaltung, sowie mehrere Benutzer mit der Rolle **Ordner- oder Projektadministrator**, die Konsolenverwaltungsaufgaben für die ihnen zugewiesenen Ordner und Projekte ausführen können.

Die folgende Tabelle zeigt die Aktionen, die jede Speicherrolle ausführt.

Funktion und Aktion	Speicheradministrator	Systemintegritätsspezialist	Speicheranzeige
Speicherverwaltung:			
Neue Ressourcen entdecken (Systeme erstellen)	Ja	Ja	Nein
Erkannte Systeme anzeigen	Ja	Ja	Nein
Systeme aus der Konsole löschen	Ja	Nein	Nein
Systeme ändern	Ja	Nein	Nein
Agenten erstellen	Nein	Nein	Nein
Digitaler Berater			
Alle Seiten und Funktionen anzeigen	Ja	Ja	Ja
* Licenses and subscriptions*			
Alle Seiten und Funktionen anzeigen	Nein	Nein	Nein
Software-Updates			
Zielseite und Empfehlungen anzeigen	Ja	Ja	Ja
Überprüfen Sie mögliche Versionsempfehlungen und Hauptvorteile	Ja	Ja	Ja
Anzeigen von Updatedetails für einen Cluster	Ja	Ja	Ja
Führen Sie vor dem Update Prüfungen durch und laden Sie den Upgrade-Plan herunter	Ja	Ja	Ja
Installieren Sie Softwareupdates	Ja	Ja	Nein
Lebenszyklusplanung			
Überprüfen des Kapazitätsplanungsstatus	Ja	Ja	Ja
Nächste Aktion auswählen (Best Practice, Stufe)	Ja	Nein	Nein
Verteilen Sie kalte Daten in den Cloud-Speicher und geben Sie Speicherplatz frei	Ja	Ja	Nein
Erinnerungen einrichten	Ja	Ja	Ja
Nachhaltigkeit			

Funktion und Aktion	Speicheradministrator	Systemintegritätsspezialist	Speicheranzeige
Dashboard und Empfehlungen anzeigen	Ja	Ja	Ja
Berichtsdaten herunterladen	Ja	Ja	Ja
Prozentsatz der CO2-Minderung bearbeiten	Ja	Ja	Nein
Empfehlungen zur Fehlerbehebung	Ja	Ja	Nein
Empfehlungen aufschieben	Ja	Ja	Nein
Systemmanager-Zugriff			
Darf Anmeldeinformationen eingeben	Ja	Ja	Nein
Referenzen			
Benutzeranmeldeinformationen	Ja	Ja	Nein

Datendienstrollen

NetApp Backup and Recovery -Rollen in der NetApp Console

Sie können Benutzern die folgenden Rollen zuweisen, um ihnen Zugriff auf NetApp Backup and Recovery innerhalb der Konsole zu gewähren. Mithilfe von Sicherungs- und Wiederherstellungsrollen können Sie Benutzern flexibel eine Rolle zuweisen, die speziell auf die Aufgaben zugeschnitten ist, die sie in Ihrem Unternehmen erledigen müssen. Wie Sie Rollen zuweisen, hängt von Ihren eigenen Geschäfts- und Speicherverwaltungspraktiken ab.

Der Dienst verwendet die folgenden Rollen, die spezifisch für NetApp Backup and Recovery sind.

- **Superadministrator für Backup und Wiederherstellung**: Führen Sie beliebige Aktionen in NetApp Backup and Recovery aus.
- **Backup- und Recovery-Backup-Administrator**: Führen Sie Sicherungen auf lokalen Snapshots durch, replizieren Sie auf sekundären Speicher und sichern Sie Aktionen auf Objektspeicher in NetApp Backup and Recovery.
- **Backup- und Recovery-Wiederherstellungsadministrator**: Stellen Sie Workloads mit NetApp Backup and Recovery wieder her.
- **Backup- und Recovery-Klonadministrator**: Klonen Sie Anwendungen und Daten mit NetApp Backup and Recovery.
- **Backup- und Recovery-Viewer**: Informationen in NetApp Backup and Recovery anzeigen, aber keine Aktionen ausführen.

Einzelheiten zu allen NetApp Console finden Sie unter "die Dokumentation zur Einrichtung und Verwaltung der Konsole" .

Für allgemeine Aktionen verwendete Rollen

Die folgende Tabelle zeigt die Aktionen, die jede NetApp Backup and Recovery -Rolle für alle Workloads ausführen kann.

Funktion und Aktion	Superadministrator für Backup und Wiederherstellung	Backup- und Wiederherstellungs-Backup-Administrator	Administrator für die Wiederherstellung von Backup und Wiederherstellung	Backup- und Wiederherstellungsklon-Administrator	Backup- und Wiederherstellungs-Viewer
Hosts hinzufügen, bearbeiten oder löschen	Ja	Nein	Nein	Nein	Nein
Plugins installieren	Ja	Nein	Nein	Nein	Nein
Anmeldeinformationen hinzufügen (Host, Instanz, vCenter)	Ja	Nein	Nein	Nein	Nein
Dashboard und alle Registerkarten anzeigen	Ja	Ja	Ja	Ja	Ja
Kostenlose Testversion starten	Ja	Nein	Nein	Nein	Nein
Ermittlung von Workloads initiieren	Nein	Ja	Ja	Ja	Nein
Lizenzinformationen anzeigen	Ja	Ja	Ja	Ja	Ja
Lizenz aktivieren	Ja	Nein	Nein	Nein	Nein
Hosts anzeigen	Ja	Ja	Ja	Ja	Ja
Zeitpläne:					
Zeitpläne aktivieren	Ja	Ja	Ja	Ja	Nein
Zeitpläne aussetzen	Ja	Ja	Ja	Ja	Nein
Richtlinien und Schutz:					
Schutzpläne anzeigen	Ja	Ja	Ja	Ja	Ja
Erstellen, Ändern oder Löschen von Schutzplänen	Ja	Ja	Nein	Nein	Nein
Wiederherstellen von Workloads	Ja	Nein	Ja	Nein	Nein

Funktion und Aktion	Superadministrator für Backup und Wiederherstellung	Backup- und Wiederherstellungs-Backup-Administrator	Administrator für die Wiederherstellung von Backup und Wiederherstellung	Backup- und Wiederherstellungsklon-Administrator	Backup- und Wiederherstellungs-Viewer
Erstellen, Teilen oder Löschen von Klonen	Ja	Nein	Nein	Ja	Nein
Richtlinie erstellen, ändern oder löschen	Ja	Ja	Nein	Nein	Nein
Berichte:					
Berichte anzeigen	Ja	Ja	Ja	Ja	Ja
Erstellen von Berichten	Ja	Ja	Ja	Ja	Nein
Berichte löschen	Ja	Nein	Nein	Nein	Nein
Von SnapCenter importieren und Host verwalten:					
Importierte SnapCenter -Daten anzeigen	Ja	Ja	Ja	Ja	Ja
Daten aus SnapCenter importieren	Ja	Ja	Nein	Nein	Nein
Host verwalten (migrieren)	Ja	Ja	Nein	Nein	Nein
Einstellungen konfigurieren:					
Konfigurieren des Protokollverzeichnisses	Ja	Ja	Ja	Nein	Nein
Instanzanmeldeinformationen zuordnen oder entfernen	Ja	Ja	Ja	Nein	Nein
Eimer:					
Buckets anzeigen	Ja	Ja	Ja	Ja	Ja
Bucket erstellen, bearbeiten oder löschen	Ja	Ja	Nein	Nein	Nein

Für Workload-spezifische Aktionen verwendete Rollen

Die folgende Tabelle zeigt die Aktionen, die jede NetApp Backup and Recovery -Rolle für bestimmte Workloads ausführen kann.

Kubernetes-Workloads

Diese Tabelle zeigt die Aktionen, die jede NetApp Backup and Recovery -Rolle für Aktionen ausführen kann, die spezifisch für Kubernetes-Workloads sind.

Funktion und Aktion	Superadministrator für Backup und Wiederherstellung	Backup- und Wiederherstellungs-Backup-Administrator	Administrator für die Wiederherstellung von Backup und Wiederherstellung	Backup- und Wiederherstellungs-Viewer
Cluster, Namespaces, Speicherklassen und API-Ressourcen anzeigen	Ja	Ja	Ja	Ja
Neue Kubernetes-Cluster hinzufügen	Ja	Ja	Nein	Nein
Aktualisieren von Clusterkonfigurationen	Ja	Nein	Nein	Nein
Entfernen von Clustern aus der Verwaltung	Ja	Nein	Nein	Nein
Anwendungen anzeigen	Ja	Ja	Ja	Ja
Erstellen und Definieren neuer Anwendungen	Ja	Ja	Nein	Nein
Aktualisieren von Anwendungskonfigurationen	Ja	Ja	Nein	Nein
Entfernen von Anwendungen aus der Verwaltung	Ja	Ja	Nein	Nein
Anzeigen geschützter Ressourcen und Sicherungsstatus	Ja	Ja	Ja	Ja
Erstellen Sie Backups und schützen Sie Anwendungen mit Richtlinien	Ja	Ja	Nein	Nein
Schutz von Apps aufheben und Backups löschen	Ja	Ja	Nein	Nein
Anzeigen von Wiederherstellungspunkten und Ressourcen-Viewer-Ergebnissen	Ja	Ja	Ja	Ja

Funktion und Aktion	Superadministrator für Backup und Wiederherstellung	Backup- und Wiederherstellungs-Backup-Administrator	Administrator für die Wiederherstellung von Backup und Wiederherstellung	Backup- und Wiederherstellungs-Viewer
Wiederherstellen von Anwendungen aus Wiederherstellungspunkten	Ja	Nein	Ja	Nein
Kubernetes-Sicherungsrichtlinien anzeigen	Ja	Ja	Ja	Ja
Erstellen von Kubernetes-Sicherungsrichtlinien	Ja	Ja	Ja	Nein
Aktualisieren der Sicherungsrichtlinien	Ja	Ja	Ja	Nein
Löschen von Sicherungsrichtlinien	Ja	Ja	Ja	Nein
Ausführungs-Hooks und Hook-Quellen anzeigen	Ja	Ja	Ja	Ja
Erstellen Sie Ausführungs-Hooks und Hook-Quellen	Ja	Ja	Ja	Nein
Aktualisieren von Ausführungs-Hooks und Hook-Quellen	Ja	Ja	Ja	Nein
Ausführungs-Hooks und Hook-Quellen löschen	Ja	Ja	Ja	Nein
Vorlagen für Ausführungs-Hooks anzeigen	Ja	Ja	Ja	Ja
Erstellen von Ausführungs-Hook-Vorlagen	Ja	Ja	Ja	Nein
Aktualisieren von Ausführungs-Hook-Vorlagen	Ja	Ja	Ja	Nein
Ausführungs-Hook-Vorlagen löschen	Ja	Ja	Ja	Nein
Übersicht über die Arbeitslast und Analyse-Dashboards anzeigen	Ja	Ja	Ja	Ja

Funktion und Aktion	Superadministrator für Backup und Wiederherstellung	Backup- und Wiederherstellungs-Backup-Administrator	Administrator für die Wiederherstellung von Backup und Wiederherstellung	Backup- und Wiederherstellungs-Viewer
StorageGRID -Buckets und Speicherziele anzeigen	Ja	Ja	Ja	Ja

NetApp Disaster Recovery Rollen in der NetApp Console

Sie können Benutzern die folgenden Rollen zuweisen, um ihnen Zugriff auf NetApp Disaster Recovery innerhalb der Konsole zu gewähren. Mithilfe von Disaster Recovery-Rollen können Sie Benutzern flexibel Rollen zuweisen, die speziell auf die Aufgaben zugeschnitten sind, die sie in Ihrer Organisation erledigen müssen. Wie Sie Rollen zuweisen, hängt von Ihren eigenen Geschäfts- und Speicherverwaltungspraktiken ab.

Disaster Recovery verwendet die folgenden Rollen:

- **Notfallwiederherstellungsadministrator**: Führen Sie alle Aktionen aus.
- **Disaster Recovery Failover-Administrator**: Führen Sie Failover und Migrationen durch.
- **Administrator der Notfallwiederherstellungsanwendung**: Erstellen Sie Replikationspläne. Replikationspläne ändern. Starten Sie Test-Failover.
- **Disaster Recovery Viewer**: Nur Informationen anzeigen.

Die folgende Tabelle zeigt die Aktionen, die jede Rolle ausführen kann.

Funktion und Aktion	Notfallwiederherstellungsadministrator	Administrator für Notfallwiederherstellungs-Failover	Administrator der Notfallwiederherstellungsanwendung	Disaster Recovery-Viewer
Dashboard und alle Registerkarten anzeigen	Ja	Ja	Ja	Ja
Kostenlose Testversion starten	Ja	Nein	Nein	Nein
Ermittlung von Workloads initiieren	Ja	Nein	Nein	Nein
Lizenzinformationen anzeigen	Ja	Ja	Ja	Ja
Lizenz aktivieren	Ja	Nein	Ja	Nein
Auf der Registerkarte „Sites“:				
Websites anzeigen	Ja	Ja	Ja	Ja

Funktion und Aktion	Notfallwiederherstellungsadministrator	Administrator für Notfallwiederherstellungs-Failover	Administrator der Notfallwiederherstellungsanwendung	Disaster Recovery-Viewer
Hinzufügen, Ändern oder Löschen von Sites	Ja	Nein	Nein	Nein
Auf der Registerkarte Replikationspläne:				
Replikationspläne anzeigen	Ja	Ja	Ja	Ja
Anzeigen von Replikationsplandetails	Ja	Ja	Ja	Ja
Erstellen oder Ändern von Replikationsplänen	Ja	Ja	Ja	Nein
Erstellen von Berichten	Ja	Nein	Nein	Nein
Snapshots anzeigen	Ja	Ja	Ja	Ja
Durchführen von Failover-Tests	Ja	Ja	Ja	Nein
Durchführen von Failovers	Ja	Ja	Nein	Nein
Failbacks durchführen	Ja	Ja	Nein	Nein
Migrationen durchführen	Ja	Ja	Nein	Nein
Auf der Registerkarte „Ressourcengruppen“:				
Anzeigen von Ressourcengruppen	Ja	Ja	Ja	Ja
Erstellen, Ändern oder Löschen von Ressourcengruppen	Ja	Nein	Ja	Nein
Auf der Registerkarte „Jobüberwachung“:				
Jobs anzeigen	Ja	Nein	Ja	Ja
Aufträge abbrechen	Ja	Ja	Ja	Nein

Ransomware Resilience-Zugriffsrollen für die NetApp Console

Ransomware Resilience-Rollen bieten Benutzern Zugriff auf NetApp Ransomware Resilience. Ransomware Resilience unterstützt die folgenden Rollen:

Basisrollen

- Ransomware-Resilience-Administrator – Konfigurieren Sie die Ransomware-Resilience-Einstellungen;

untersuchen Sie Verschlüsselungswarnungen und reagieren Sie darauf.

- Ransomware Resilience Viewer – Anzeigen von Verschlüsselungsvorfällen, Berichten und Erkennungseinstellungen

Aktivitätsrollen für Benutzerverhalten"Erkennung verdächtiger Benutzeraktivitäten" Warnungen bieten Einblick in Daten wie Dateiaktivitätsereignisse. Diese Warnungen umfassen Dateinamen und vom Benutzer ausgeführte Dateiaktionen (wie Lesen, Schreiben, Löschen, Umbenennen). Um die Sichtbarkeit dieser Daten einzuschränken, können nur Benutzer mit diesen Rollen diese Warnungen verwalten oder anzeigen.

- Ransomware Resilience-Benutzerverhaltensadministrator – Aktivieren Sie die Erkennung verdächtiger Benutzeraktivitäten, untersuchen Sie verdächtige Benutzeraktivitäten und reagieren Sie auf Warnungen zu verdächtigen Benutzeraktivitäten
- Ransomware Resilience-Benutzerverhaltensanzeige – Anzeigen von Warnungen zu verdächtigen Benutzeraktivitäten

Benutzerverhaltensrollen sind keine eigenständigen Rollen. Sie sind dafür vorgesehen, den Administrator- oder Viewer-Rollen von Ransomware Resilience hinzugefügt zu werden. Weitere Informationen finden Sie unter Benutzerverhaltensrollen.

Ausführliche Beschreibungen der einzelnen Rollen finden Sie in den folgenden Tabellen.

Basisrollen

In der folgenden Tabelle werden die Aktionen beschrieben, die den Administrator- und Viewer-Rollen von Ransomware Resilience zur Verfügung stehen.

Funktion und Aktion	Ransomware-Resilienz-Administrator	Ransomware Resilience-Viewer
Dashboard und alle Registerkarten anzeigen	Ja	Ja
Aktualisieren Sie den Empfehlungsstatus auf dem Dashboard	Ja	Nein
Kostenlose Testversion starten	Ja	Nein
Ermittlung von Workloads initiieren	Ja	Nein
Neuermittlung von Workloads einleiten	Ja	Nein
Auf der Registerkarte „Schützen“:		
Hinzufügen, Ändern oder Löschen von Schutzplänen für _Verschlüsselungs_richtlinien	Ja	Nein
Workloads schützen	Ja	Nein
Identifizieren Sie die Gefährdung sensibler Daten mit der Datenklassifizierung	Ja	Nein
Listen Sie Schutzpläne und Details auf	Ja	Ja

Funktion und Aktion	Ransomware-Resilienz-Administrator	Ransomware Resilience-Viewer
Auflisten von Schutzgruppen	Ja	Ja
Anzeigen von Schutzgruppendetails	Ja	Ja
Erstellen, Bearbeiten oder Löschen von Schutzgruppen	Ja	Nein
Daten herunterladen	Ja	Ja
Auf der Registerkarte „Warnungen“:		
Anzeigen von Verschlüsselungswarnungen und Warnungsdetails	Ja	Ja
Verschlüsselungsvorfallstatus bearbeiten	Ja	Nein
Verschlüsselungsalarm zur Wiederherstellung markieren	Ja	Nein
Details zum Verschlüsselungsvorfall anzeigen	Ja	Ja
Verschlüsselungsvorfälle verwerfen oder beheben	Ja	Nein
Vollständige Liste der betroffenen Dateien im Verschlüsselungsereignis abrufen	Ja	Nein
Daten zu Verschlüsselungsereigniswarnungen herunterladen	Ja	Ja
Benutzer blockieren (mit Workload Security-Agent-Konfiguration)	Ja	Nein
Auf der Registerkarte „Wiederherstellen“:		
Herunterladen der betroffenen Dateien vom Verschlüsselungsereignis	Ja	Nein
Workload nach Verschlüsselungsereignis wiederherstellen	Ja	Nein
Wiederherstellungsdaten aus dem Verschlüsselungsereignis herunterladen	Ja	Ja
Laden Sie Berichte vom Verschlüsselungsereignis herunter	Ja	Ja
Auf der Registerkarte „Einstellungen“:		
Hinzufügen oder Ändern von Sicherungszielen	Ja	Nein
Auflisten der Sicherungsziele	Ja	Ja
Verbundene SIEM-Ziele anzeigen	Ja	Ja

Funktion und Aktion	Ransomware-Resilienz-Administrator	Ransomware Resilience-Viewer
SIEM-Ziele hinzufügen oder ändern	Ja	Nein
Bereitschaftsübung konfigurieren	Ja	Nein
Bereitschaftsübung starten, zurücksetzen oder bearbeiten	Ja	Nein
Status der Bereitschaftsübung überprüfen	Ja	Ja
Aktualisieren der Erkennungskonfiguration	Ja	Nein
Anzeigen der Erkennungskonfiguration	Ja	Ja
Auf der Registerkarte „Berichte“:		
Berichte herunterladen	Ja	Ja

Benutzerverhaltensrollen

Um Einstellungen für verdächtiges Benutzerverhalten zu konfigurieren und auf Warnungen zu reagieren, muss ein Benutzer über die Administratorrolle „Ransomware Resilience-Benutzerverhalten“ verfügen. Um nur Warnungen zu verdächtigem Benutzerverhalten anzuzeigen, sollte ein Benutzer über die Rolle „Ransomware Resilience-Benutzerverhaltensanzeiger“ verfügen.

Benutzerverhaltensrollen sollten Benutzern mit vorhandenen Ransomware Resilience-Administrator- oder Viewer-Berechtigungen zugewiesen werden, die Zugriff auf Folgendes benötigen:"Einstellungen und Warnungen bei verdächtigen Benutzeraktivitäten" . Ein Benutzer mit der Administratorrolle „Ransomware Resilience“ sollte beispielsweise die Administratorrolle „Ransomware Resilience-Benutzerverhalten“ erhalten, um Benutzeraktivitäts-Agenten zu konfigurieren und Benutzer zu sperren oder die Sperrung aufzuheben. Die Administratorrolle für das Benutzerverhalten von Ransomware Resilience sollte keinem Ransomware Resilience-Viewer übertragen werden.

Um die Erkennung verdächtiger Benutzeraktivitäten zu aktivieren, müssen Sie über die Administratorrolle der Konsolenorganisation verfügen.

In der folgenden Tabelle werden die Aktionen beschrieben, die für die Administrator- und Viewer-Rollen des Benutzerverhaltens von Ransomware Resilience verfügbar sind.

Funktion und Aktion	Ransomware Resilience-Benutzerverhaltensadministrator	Ransomware Resilience-Benutzerverhaltensanzeige
Auf der Registerkarte „Einstellungen“:		
Erstellen, Ändern oder Löschen eines Benutzeraktivitätsagenten	Ja	Nein
Benutzerverzeichnis-Connector erstellen oder löschen	Ja	Nein

Funktion und Aktion	Ransomware Resilience-Benutzerverhaltensadministrator	Ransomware Resilience-Benutzerverhaltensanzeige
Datensammler anhalten oder fortsetzen	Ja	Nein
Führen Sie eine Übung zur Vorbereitung auf Datenschutzverletzungen durch	Ja	Nein
Auf der Registerkarte „Schützen“:		
Hinzufügen, Ändern oder Löschen von Schutzplänen für Richtlinien zu *verdächtigem Benutzerverhalten*	Ja	Nein
Auf der Registerkarte „Warnungen“:		
Anzeigen von Benutzeraktivitätswarnungen und Warnungsdetails	Ja	Ja
Bearbeiten des Vorfallstatus für Benutzeraktivitäten	Ja	Nein
Benutzeraktivitätswarnung zur Wiederherstellung markieren	Ja	Nein
Details zum Vorfall mit Benutzeraktivität anzeigen	Ja	Ja
Abweisen oder Lösen von Vorfällen im Zusammenhang mit Benutzeraktivitäten	Ja	Nein
Vollständige Liste der betroffenen Dateien nach verdächtigem Benutzer abrufen	Ja	Ja
Laden Sie Ereigniswarnungsdaten zu Benutzeraktivitäten herunter	Ja	Ja
Benutzer blockieren oder entsperren	Ja	Nein
Auf der Registerkarte „Wiederherstellen“:		
Herunterladen betroffener Dateien für Benutzeraktivitätsereignisse	Ja	Nein
Wiederherstellen der Arbeitslast aus dem Benutzeraktivitätsereignis	Ja	Nein
Laden Sie Wiederherstellungsdaten aus dem Benutzeraktivitätsereignis herunter	Ja	Ja
Laden Sie Berichte zum Benutzeraktivitätsereignis herunter	Ja	Ja