Datendienstrollen

NetApp Console setup and administration

NetApp
January 13, 2026

Inhalt

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

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
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
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

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 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
Wiederherstellen von Anwendungen aus Wiederherstellungspunkten	Ja	Nein	Ja	Nein

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
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
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
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

Funktion und Aktion	Notfallwiederherstellungsadministrator	Administrator für Notfallwiederherstellungs-Failover	Administrator der Notfallwiederherstellungsanwendung	Disaster Recovery-Viewer
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
Auflisten von Schutzgruppen	Ja	Ja
Anzeigen von Schutzgruppendetails	Ja	Ja
Erstellen, Bearbeiten oder Löschen von Schutzgruppen	Ja	Nein
Daten herunterladen	Ja	Ja

Funktion und Aktion	Ransomware-Resilienz-Administrator	Ransomware Resilience-Viewer
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
SIEM-Ziele hinzufügen oder ändern	Ja	Nein
Bereitschaftsübung konfigurieren	Ja	Nein
Bereitschaftsübung starten, zurücksetzen oder bearbeiten	Ja	Nein
Status der Bereitschaftsübung überprüfen	Ja	Ja

Funktion und Aktion	Ransomware-Resilienz-Administrator	Ransomware Resilience-Viewer
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
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

Funktion und Aktion	Ransomware Resilience-Benutzerverhaltensadministrator	Ransomware Resilience-Benutzerverhaltensanzeige
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