# Benutzerzugriff und Sicherheit verwalten

NetApp Console setup and administration

NetApp
February 11, 2026

# Inhalt

# Benutzerzugriff und Sicherheit verwalten

## Erfahren Sie mehr über die rollenbasierte Zugriffskontrolle (RBAC) der NetApp Console .

Verwalten Sie den Benutzerzugriff auf die NetApp Console mit rollenbasierter Zugriffskontrolle (RBAC), indem Sie vordefinierte Rollen auf Organisations-, Ordner- oder Projektebene zuweisen. Jede Rolle gewährt spezifische Berechtigungen, die definieren, welche Aktionen Benutzer innerhalb ihres zugewiesenen Bereichs ausführen können.

NetApp entwirft Konsolenrollen nach dem Prinzip der minimalen Berechtigungen, sodass jede Rolle nur die Berechtigungen enthält, die für ihre Aufgaben erforderlich sind. Dieser Ansatz erhöht die Sicherheit, indem der Zugriff auf das beschränkt wird, was jedes Mitglied benötigt.

Nachdem Sie die Ressourcen in Ordnern und Projekten organisiert haben, weisen Sie den Organisationsmitgliedern eine oder mehrere Rollen für bestimmte Ordner oder Projekte zu, die es ihnen ermöglichen, nur ihre jeweiligen Verantwortlichkeiten wahrzunehmen.

Beispielsweise können Sie einem Mitglied die Administratorrolle für Ransomware-Resilienz auf einer bestimmten Projektebene zuweisen, sodass dieses Mitglied Ransomware-Resilienzmaßnahmen für Ressourcen innerhalb dieses Projekts durchführen kann, ohne ihm einen umfassenderen Zugriff auf die gesamte Organisation zu gewähren. Diesem Benutzer kann die Rolle für mehrere Projekte innerhalb Ihrer Organisation zugewiesen werden.

Sie können Benutzern je nach ihren Verantwortlichkeiten mehrere Rollen für denselben oder für verschiedene Verantwortungsbereiche zuweisen. In einer kleineren Organisation könnte beispielsweise ein und derselbe Benutzer sowohl die Aufgaben der Ransomware-Resilienz als auch der Datensicherung und -wiederherstellung auf Organisationsebene verwalten, während in einer größeren Organisation auf Projektebene unterschiedliche Benutzer den einzelnen Rollen zugeordnet sein könnten.

### Arten von Konsolenorganisationsmitgliedern

In einer NetApp Console Organisation gibt es drei Arten von Mitgliedern: * *Benutzerkonten*: Einzelne Benutzer, die sich bei der NetApp Console anmelden, um Ressourcen zu verwalten. Benutzer müssen sich bei der NetApp Console registrieren, bevor sie einer Organisation hinzugefügt werden können. * *Servicekonten*: Nicht-menschliche Konten, die von Anwendungen oder Diensten verwendet werden, um über APIs mit der NetApp Console zu interagieren. Sie können Dienstkonten direkt zu Ihrer Konsolenorganisation hinzufügen. * *Verbundene Gruppen*: Gruppen, die von Ihrem Identitätsanbieter (IdP) synchronisiert werden und es Ihnen ermöglichen, den Zugriff für mehrere Benutzer gemeinsam zu verwalten. Jeder Benutzer innerhalb einer föderierten Gruppe muss sich bei der NetApp Console registriert haben und Ihrer Organisation mit einer Zugriffsrolle hinzugefügt worden sein, bevor er auf die der Gruppe zugewiesenen Ressourcen zugreifen kann.

"Erfahren Sie, wie Sie Mitglieder zu Ihrer Organisation hinzufügen."

### Vordefinierte Rollen in der NetApp Console

Die NetApp Console enthält vordefinierte Rollen, die Sie Organisationsmitgliedern zuweisen können. Jede Rolle beinhaltet Berechtigungen, die festlegen, welche Aktionen ein Mitglied innerhalb seines zugewiesenen Bereichs (Organisation, Ordner oder Projekt) durchführen kann.

Die NetApp Console -Rollen verwenden das Prinzip der minimalen Berechtigungen, um sicherzustellen, dass

Mitglieder nur über die für ihre Aufgaben erforderlichen Berechtigungen verfügen, und kategorisieren die Rollen nach der Art des Zugriffs, den sie gewähren:

- Plattformrollen: Konsolenadministrationsberechtigungen bereitstellen
- Datendienstrollen: Berechtigungen für die Verwaltung spezifischer Datendienste wie Ransomware-Resilienz und Datensicherung und -wiederherstellung bereitstellen.
- Anwendungsrollen: Berechtigungen für die Speicherverwaltung sowie für die Überwachung von Konsolenereignissen und -warnungen bereitstellen.

Sie können einem Mitglied mehrere Rollen entsprechend seinen Verantwortlichkeiten zuweisen. Beispielsweise könnten Sie einem Mitglied für ein bestimmtes Projekt sowohl die Administratorrolle für Ransomware-Resilienz als auch die Administratorrolle für Datensicherung und -wiederherstellung zuweisen.

"Erfahren Sie mehr über die in der NetApp Console verfügbaren vordefinierten Rollen."Die

# Mitgliederzugriffe in der NetApp Console verwalten

Verwalten Sie den Mitgliederzugriff in Ihrer Console-Organisation. Weisen Sie Rollen zu, um Berechtigungen festzulegen. Mitglieder werden entfernt, wenn sie das Unternehmen verlassen.

**Erforderliche Zugriffsrollen**

Super-Admin, Organisations-Admin oder Ordner- bzw. Projekt-Admin (für die von ihnen verwalteten Ordner und Projekte). Link:reference-iam-predefined-roles.html[Erfahren Sie mehr über Zugriffsrollen].

Sie können Zugriffsrollen projekt- oder ordnerbasiert zuweisen. Weisen Sie beispielsweise einem Benutzer eine Rolle für zwei bestimmte Projekte zu oder weisen Sie die Rolle auf Ordnerebene zu, um einem Benutzer die Administratorrolle für Ransomware-Resilienz für alle Projekte in einem Ordner zu geben.

Fügen Sie Ihre Ordner und Projekte hinzu, bevor Sie Benutzern Zugriffsrechte zuweisen. "Erfahren Sie, wie Sie Ordner und Projekte hinzufügen."

## Verstehen Sie, wie der Zugriff in der NetApp Console gewährt wird.

Die NetApp Console verwendet ein rollenbasiertes Zugriffskontrollmodell (RBAC) zur Verwaltung von Benutzerberechtigungen. Sie können Mitgliedern vordefinierte Rollen einzeln oder über föderierte Gruppen zuweisen. Sie können Dienstkonten und Verbundgruppen Rollen hinzufügen und zuweisen. Jede Rolle definiert, welche Aktionen ein Mitglied an den zugehörigen Ressourcen durchführen kann.

Beachten Sie Folgendes bezüglich der Zugriffsgewährung in der NetApp Console:

- Alle Benutzer müssen sich zunächst bei der NetApp Console registrieren, bevor ihnen Zugriff auf Ressourcen gewährt werden kann.
- Sie müssen jedem Benutzer in der Konsole explizit eine Rolle zuweisen, bevor er auf Ressourcen zugreifen kann, selbst wenn er Mitglied einer Verbundgruppe ist, der eine Rolle zugewiesen wurde.
- Sie können Dienstkonten direkt über die Konsole hinzufügen und ihnen Rollen zuweisen.

**Verwendung der Rollenvererbung**

Wenn Sie in der NetApp Console eine Rolle auf Organisations-, Ordner- oder Projektebene zuweisen, wird diese Rolle automatisch an alle Ressourcen innerhalb des ausgewählten Bereichs vererbt. Beispielsweise

gelten Rollen auf Ordnerebene für alle darin enthaltenen Projekte, während Rollen auf Projektebene für alle Ressourcen innerhalb dieses Projekts gelten.

## Organisationsmitglieder anzeigen

Um zu verstehen, welche Ressourcen und Berechtigungen einem Mitglied zur Verfügung stehen, können Sie die dem Mitglied auf verschiedenen Ebenen der Ressourcenhierarchie Ihrer Organisation zugewiesenen Rollen anzeigen."Erfahren Sie, wie Sie mithilfe von Rollen den Zugriff auf Konsolenressourcen steuern."

**Schritte**

1. Wählen Sie **Verwaltung > Identität und Zugriff**.
2. Wählen Sie **Mitglieder** aus.

   In der Tabelle **Mitglieder** sind die Mitglieder Ihrer Organisation aufgelistet.
3. Navigieren Sie auf der Seite **Mitglieder** zu einem Mitglied in der Tabelle, wählen Sie ••• und wählen Sie dann **Details anzeigen**.

## Einem Mitglied zugewiesene Rollen anzeigen

Sie können überprüfen, welche Rollen ihnen aktuell zugewiesen sind.

Wenn Sie die Rolle „Ordner- oder Projektadministrator“ haben, werden auf der Seite alle Mitglieder der Organisation angezeigt. Sie können jedoch nur die Mitgliedsberechtigungen für die Ordner und Projekte anzeigen und verwalten, für die Sie über Berechtigungen verfügen. "Erfahren Sie mehr über die Aktionen, die ein Ordner- oder Projektadministrator ausführen kann." .

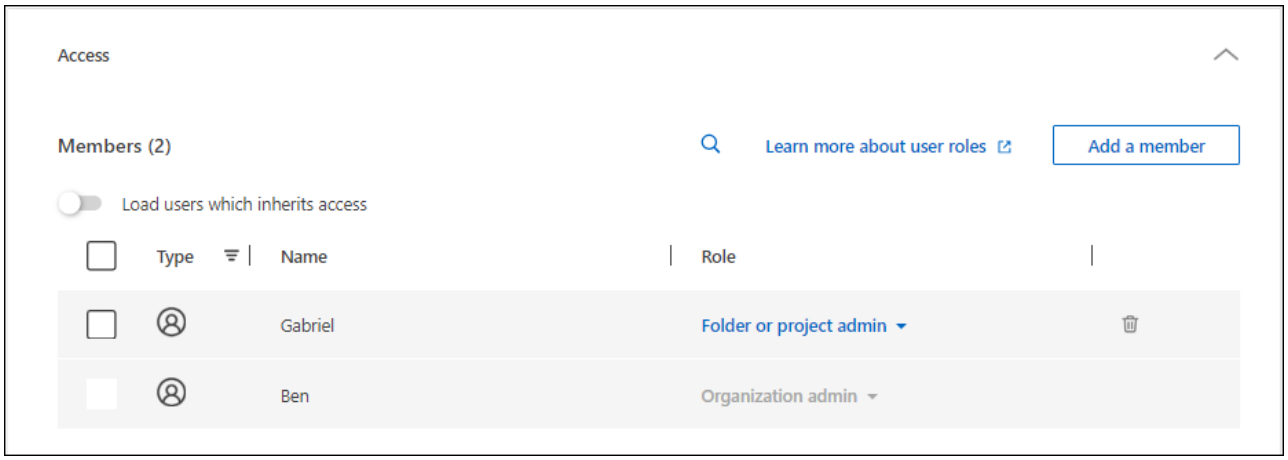
1. Navigieren Sie auf der Seite **Mitglieder** zu einem Mitglied in der Tabelle und wählen Sie es aus. ••• und wählen Sie dann **Details anzeigen**.
2. Erweitern Sie in der Tabelle die jeweilige Zeile für die Organisation, den Ordner oder das Projekt, in dem Sie die zugewiesene Rolle des Mitglieds anzeigen möchten, und wählen Sie in der Spalte **Rolle** die Option **Anzeigen** aus.

## Anzeigen von Mitgliedern, die einem Ordner oder Projekt zugeordnet sind

Sie können die Mitglieder anzeigen, die Zugriff auf einen bestimmten Ordner oder ein bestimmtes Projekt haben.

**Schritte**

1. Wählen Sie **Verwaltung > Identität und Zugriff**.
2. Wählen Sie **Organisation** aus.
3. Navigieren Sie auf der Seite **Organisation** zu einem Projekt oder Ordner in der Tabelle, wählen Sie ••• und wählen Sie dann **Ordner bearbeiten** oder **Projekt bearbeiten**.
   - Wählen Sie **Zugriff** aus, um die Mitglieder anzuzeigen, die Zugriff auf den Ordner oder das Projekt haben.




## Mitgliederzugriff zuweisen oder ändern

Nach der Registrierung eines Benutzers bei der NetApp Console können Sie ihn Ihrer Organisation hinzufügen und ihm eine Rolle zuweisen, um ihm Zugriff auf Ressourcen zu gewähren. "Erfahren Sie, wie Sie Mitglieder zu Ihrer Organisation hinzufügen."

Sie können die Zugriffsrechte eines Mitglieds anpassen, indem Sie nach Bedarf Rollen hinzufügen oder entfernen.

## Einem Mitglied eine Zugriffsrolle hinzufügen

Normalerweise weisen Sie eine Rolle zu, wenn Sie ein Mitglied zu Ihrer Organisation hinzufügen, Sie können sie jedoch jederzeit aktualisieren, indem Sie Rollen entfernen oder hinzufügen.

Sie können einem Benutzer eine Zugriffsrolle für Ihre Organisation, Ihren Ordner oder Ihr Projekt zuweisen.

Mitglieder können innerhalb desselben Projekts und in verschiedenen Projekten mehrere Rollen innehaben. Kleinere Organisationen weisen beispielsweise alle verfügbaren Zugriffsrollen demselben Benutzer zu, während größere Organisationen ihre Benutzer mit spezialisierteren Aufgaben betrauen. Alternativ könnten Sie auch einem Benutzer die Administratorrolle für Ransomware-Resilienz auf Organisationsebene zuweisen. In diesem Beispiel könnte der Benutzer Ransomware-Resilienzmaßnahmen für alle Projekte innerhalb seiner Organisation durchführen.

Ihre Zugriffsrollenstrategie sollte mit der Art und Weise übereinstimmen, wie Sie Ihre NetApp -Ressourcen organisiert haben.

**Schritte**

1. Wählen Sie **Verwaltung > Identität und Zugriff**.
2. Wählen Sie **Mitglieder** aus.
3. Wählen Sie einen der Mitglieder-Tabs aus: **Benutzer**, **Dienstkonten** oder **Verbundgruppen**.
4. Wählen Sie das Aktionsmenü ••• neben dem Mitglied, dem Sie eine Rolle zuweisen möchten, und wählen Sie **Rolle hinzufügen** aus.
5. Um eine Rolle hinzuzufügen, führen Sie die Schritte im Dialogfeld aus:
   - **Wählen Sie eine Organisation, einen Ordner oder ein Projekt aus**: Wählen Sie die Ebene Ihrer Ressourcenhierarchie aus, für die das Mitglied Berechtigungen haben soll.

     Wenn Sie die Organisation oder einen Ordner auswählen, verfügt das Mitglied über Berechtigungen für

alles, was sich innerhalb der Organisation oder des Ordners befindet.

- **Kategorie auswählen**: Wählen Sie eine Rollenkategorie. "Informationen zu Zugriffsrollen" .
- Wählen Sie eine **Rolle**: Wählen Sie eine Rolle, die dem Mitglied Berechtigungen für die Ressourcen erteilt, die mit der von Ihnen ausgewählten Organisation, dem Ordner oder dem Projekt verknüpft sind.
- **Rolle hinzufügen**: Wenn Sie Zugriff auf zusätzliche Ordner oder Projekte innerhalb Ihrer Organisation gewähren möchten, wählen Sie **Rolle hinzufügen**, geben Sie einen weiteren Ordner oder ein weiteres Projekt oder eine weitere Rollenkategorie an und wählen Sie dann eine Rollenkategorie und eine entsprechende Rolle aus.

6. Wählen Sie **Neue Rollen hinzufügen**.

## Ändern der einem Mitglied zugewiesenen Rolle

Ändern Sie die Rollen eines Mitglieds, um dessen Zugriffsrechte zu aktualisieren.

Benutzern muss mindestens eine Rolle zugewiesen sein. Sie können einem Benutzer nicht alle Rollen entziehen. Wenn Sie alle Rollen entfernen müssen, müssen Sie den Benutzer aus Ihrer Organisation löschen.

**Schritte**

1. Wählen Sie **Verwaltung > Identität und Zugriff**.
2. Wählen Sie **Mitglieder** aus.
3. Wählen Sie einen der Mitglieder-Tabs aus: **Benutzer**, **Dienstkonten** oder **Verbundgruppen**.
4. Navigieren Sie auf der Seite **Mitglieder** zu einem Mitglied in der Tabelle, wählen Sie ••• und wählen Sie dann **Details anzeigen**.
5. Erweitern Sie in der Tabelle die jeweilige Zeile für die Organisation, den Ordner oder das Projekt, in dem Sie die zugewiesene Rolle des Mitglieds ändern möchten, und wählen Sie in der Spalte **Rolle Anzeigen** aus, um die diesem Mitglied zugewiesenen Rollen anzuzeigen.
6. Sie können eine vorhandene Rolle für ein Mitglied ändern oder eine Rolle entfernen.
   a. Um die Rolle eines Mitglieds zu ändern, wählen Sie **Ändern** neben der Rolle, die Sie ändern möchten. Sie können eine Rolle nur in eine Rolle innerhalb derselben Rollenkategorie ändern. Sie können beispielsweise von einer Datendienstrolle zu einer anderen wechseln. Bestätigen Sie die Änderung.
   b. Um die Rolle eines Mitglieds aufzuheben, wählen Sie aus 🗑 neben der Rolle, um die jeweilige Rolle vom Mitglied zu entfernen. Sie werden aufgefordert, die Entfernung zu bestätigen.

## Entfernen eines Mitglieds aus Ihrer Organisation

Entfernen Sie ein Mitglied, wenn es Ihre Organisation verlässt.

Wenn Sie ein Mitglied entfernen, entzieht das System ihm die Konsolenberechtigungen, behält aber seine Konsolen- und NetApp -Support-Site-Konten bei.

**Verbandsmitglieder**

- Verbundbenutzer verlieren automatisch den Zugriff auf die NetApp Console, wenn sie von Ihrem Identitätsanbieter entfernt werden. Sie sollten sie aber trotzdem aus Ihrer Console-Organisation entfernen, um Ihre Mitgliederliste aktuell zu halten.
- Wenn Sie einen Benutzer aus einer Verbundgruppe in Ihrem Identitätsanbieter entfernen, verliert er den mit dieser Gruppe verbundenen Konsolenzugriff. Sie behalten jedoch weiterhin alle Zugriffsrechte, die mit einer ihnen in der Konsole explizit zugewiesenen Rolle verbunden sind.

**Schritte**

1. Wählen Sie **Verwaltung > Identität und Zugriff**.
2. Wählen Sie **Mitglieder** aus.
3. Wählen Sie einen der Mitglieder-Tabs aus: **Benutzer**, **Dienstkonten** oder **Verbundgruppen**.
4. Navigieren Sie auf der Seite **Mitglieder** zu einem Mitglied in der Tabelle, wählen Sie ••• Wählen Sie dann **Benutzer löschen**.
5. Bestätigen Sie, dass Sie das Mitglied aus Ihrer Organisation entfernen möchten.

# Benutzersicherheit

Sichern Sie den Benutzerzugriff auf Ihre NetApp Console -Organisation durch die Verwaltung der Sicherheitseinstellungen der Mitglieder. Sie können Benutzerpasswörter zurücksetzen, die Multi-Faktor-Authentifizierung (MFA) verwalten und die Anmeldeinformationen für Dienstkonten neu erstellen.

**Erforderliche Zugriffsrollen**

Super-Admin, Organisations-Admin oder Ordner- bzw. Projekt-Admin (für die von ihnen verwalteten Ordner und Projekte). Link:reference-iam-predefined-roles.html[Erfahren Sie mehr über Zugriffsrollen].

## Benutzerpasswörter zurücksetzen (nur für lokale Benutzer)

Organisationsadministratoren können die Passwörter lokaler Benutzer nicht zurücksetzen. Sie können die Benutzer jedoch anweisen, ihre Passwörter selbst zurückzusetzen.

Weisen Sie den Benutzer an, sein Passwort auf der Anmeldeseite der Konsole zurückzusetzen, indem er **Passwort vergessen?** auswählt.

Diese Option steht Benutzern in einer föderierten Organisation nicht zur Verfügung.

## Verwalten der Multi-Faktor-Authentifizierung (MFA) eines Benutzers

Wenn ein Benutzer den Zugriff auf sein MFA-Gerät verliert, können Sie seine MFA-Konfiguration entweder entfernen oder deaktivieren.

Die Multi-Faktor-Authentifizierung ist nur für lokale Benutzer verfügbar. Verbundbenutzer können MFA nicht aktivieren.

Nach der Deaktivierung müssen die Nutzer die Multi-Faktor-Authentifizierung (MFA) bei der nächsten Anmeldung erneut einrichten. Wenn der Benutzer vorübergehend den Zugriff auf sein MFA-Gerät verliert, kann

er sich mit seinem gespeicherten Wiederherstellungscode anmelden.

Wenn sie ihren Wiederherstellungscode nicht haben, deaktivieren Sie MFA vorübergehend, um die Anmeldung zu ermöglichen. Wenn Sie MFA für einen Benutzer deaktivieren, wird es nur für acht Stunden deaktiviert und dann automatisch wieder aktiviert. Dem Benutzer ist während dieser Zeit eine Anmeldung ohne MFA gestattet. Nach Ablauf der acht Stunden muss der Benutzer MFA verwenden, um sich anzumelden.

Um die Multi-Faktor-Authentifizierung eines Benutzers zu verwalten, müssen Sie über eine E-Mail-Adresse in derselben Domäne wie der betroffene Benutzer verfügen.

**Schritte**

1. Wählen Sie **Verwaltung > Identität und Zugriff**.
2. Wählen Sie **Mitglieder** aus.

   In der Tabelle **Mitglieder** sind die Mitglieder Ihrer Organisation aufgelistet.
3. Navigieren Sie auf der Seite **Mitglieder** zu einem Mitglied in der Tabelle, wählen Sie ••• und wählen Sie dann **Multi-Faktor-Authentifizierung verwalten**.
4. Wählen Sie, ob die MFA-Konfiguration des Benutzers entfernt oder deaktiviert werden soll.

## Erstellen Sie die Anmeldeinformationen für ein Dienstkonto neu

Sie können neue Zugangsdaten für einen Dienst erstellen, falls Sie diese verlieren oder aktualisieren müssen.

Durch das Erstellen neuer Anmeldeinformationen werden die alten gelöscht. Die alten Zugangsdaten können nicht verwendet werden.

**Schritte**

1. Wählen Sie **Verwaltung > Identität und Zugriff**.
2. Wählen Sie **Mitglieder** aus.
3. Navigieren Sie in der Tabelle **Mitglieder** zu einem Dienstkonto, wählen Sie ••• und wählen Sie dann **Geheimnisse neu erstellen**.
4. Wählen Sie **Neu erstellen**.
5. Laden Sie die Client-ID und das Client-Geheimnis herunter oder kopieren Sie sie.

   Die Konsole zeigt das Client-Geheimnis nur einmal an. Stellen Sie sicher, dass Sie die Datei kopieren oder herunterladen und sicher aufbewahren.