Identitäts- und Zugriffsverwaltung

NetApp Console setup and administration

NetApp
February 11, 2026

Inhalt

Identitäts- und Zugriffsverwaltung

Erfahren Sie mehr über die Identitäts- und Zugriffsverwaltung der NetApp Console

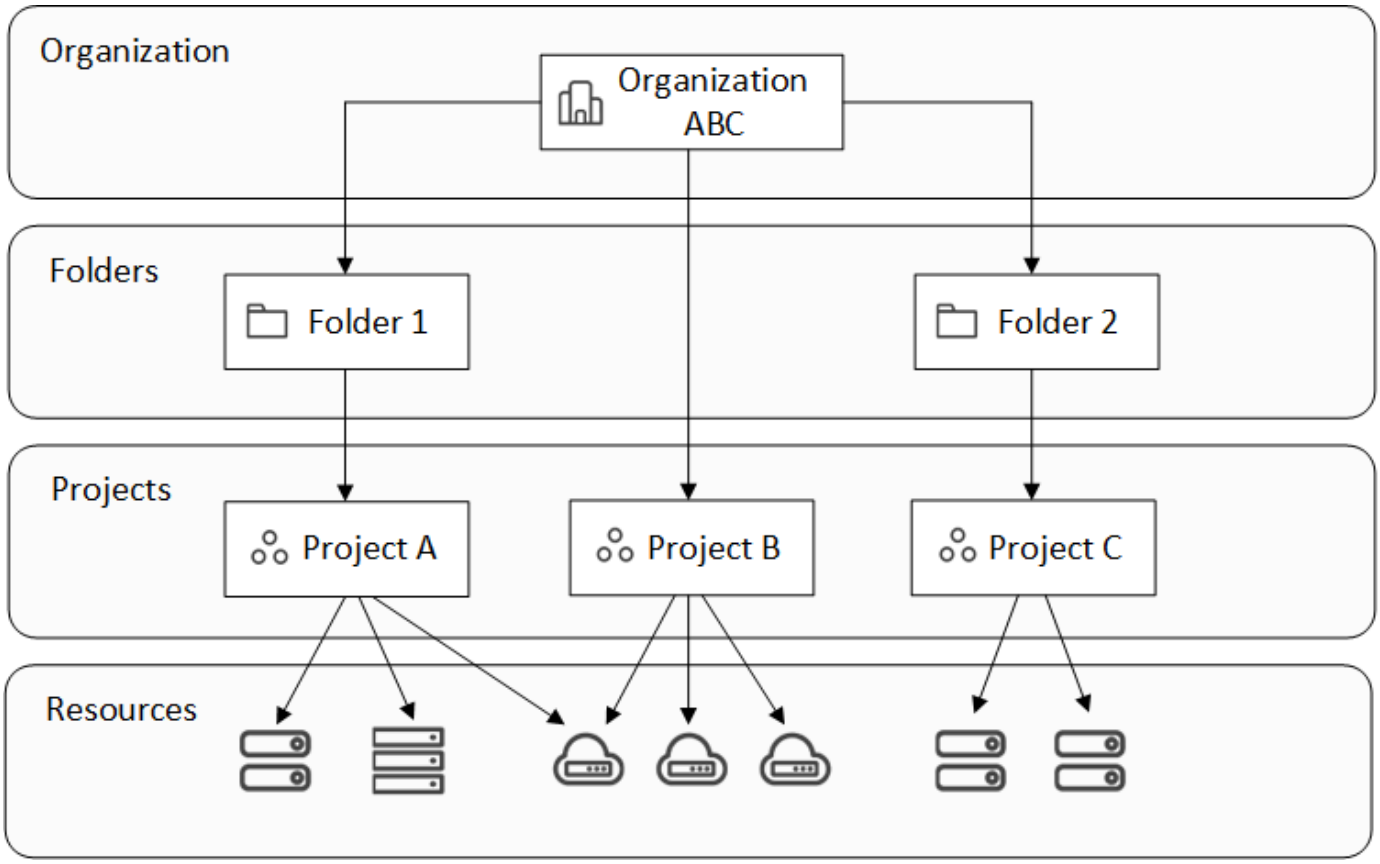
Mit der Identitäts- und Zugriffsverwaltung (IAM) der NetApp Console können Sie Ihre NetApp -Ressourcen organisieren und den Zugriff entsprechend Ihrer Unternehmensstruktur steuern – nach Standort, Abteilung oder Projekt.

Die Ressourcen sind hierarchisch angeordnet: An oberster Stelle steht die Organisation, gefolgt von Ordnern (die weitere Ordner oder Projekte enthalten können) und dann Projekten, die Speichersysteme, Workloads und Agenten enthalten.

Weisen Sie Zugriffsrollen auf Organisations-, Ordner- oder Projektebene zu, damit Benutzer den richtigen Zugriff auf Ressourcen haben.

Sie benötigen die Rollen *Super admin*, *Organization admin* oder *Folder or project admin*, um IAM in der NetApp Console zu verwalten.

Das folgende Bild veranschaulicht diese Hierarchie auf einer grundlegenden Ebene.



]

Komponenten für Identitäts- und Zugriffsmanagement

In der NetApp Console organisieren Sie Ihre Speicherressourcen mithilfe von drei Hauptkomponenten:

Organisationskomponenten, Ressourcenkomponenten und Benutzerzugriffskomponenten.

Projekte und Ordner innerhalb Ihrer Organisation

Innerhalb Ihrer IAM-Struktur arbeiten Sie mit drei Organisationskomponenten: Organisationen, Projekten und Ordnern. Sie können Benutzern Zugriff gewähren, indem Sie ihnen Rollen auf einer dieser Ebenen zuweisen.

Organisation

Eine *Organisation* ist die oberste Ebene des Console IAM-Systems und repräsentiert normalerweise Ihr Unternehmen. Ihre Organisation besteht aus Ordnern, Projekten, Mitgliedern, Rollen und Ressourcen. Agenten sind bestimmten Projekten in der Organisation zugeordnet.

Projekte

Ein *Projekt* dient dazu, Zugriff auf eine Speicherressource zu ermöglichen. Sie müssen Ressourcen einem Projekt zuweisen, bevor jemand darauf zugreifen kann. Sie können einem einzelnen Projekt mehrere Ressourcen zuweisen und Sie können auch mehrere Projekte haben. Anschließend weisen Sie den Benutzern Berechtigungen für das Projekt zu, um ihnen Zugriff auf die darin enthaltenen Ressourcen zu gewähren.

Sie können beispielsweise ein lokales ONTAP System einem einzelnen Projekt oder allen Projekten in Ihrer Organisation zuordnen, je nach Ihren Bedürfnissen.

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

Ordner

Gruppieren Sie verwandte Projekte in Ordnern, um sie nach Standort, Standort oder Geschäftsbereich zu organisieren. Ressourcen können nicht direkt Ordnern zugeordnet werden, aber durch die Zuweisung einer Rolle auf Ordnerebene erhält der Benutzer Zugriff auf alle Projekte in diesem Ordner.

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

Ressourcen

Eine *Ressource* ist eine Entität, die der Console bekannt ist und die einem Projekt zugewiesen werden kann. *Ressourcen* umfassen Speichersysteme, Keystone-Abonnements, einige NetApp Backup and Recovery-Workloads sowie Console-Agenten.

+ Eine Ressource muss einem Projekt zugeordnet werden, bevor jemand darauf zugreifen kann.

+

Beispielsweise können Sie ein Cloud Volumes ONTAP -System einem einzelnen Projekt oder allen Projekten in Ihrer Organisation zuordnen. Wie Sie eine Ressource zuordnen, hängt von den Bedürfnissen Ihrer Organisation ab.

+

"Erfahren Sie, wie Sie Ressourcen Projekten zuordnen."

Speichersysteme und Keystone -Abonnements

Speichersysteme sind die primären Ressourcen, die Sie in NetApp Console verwalten. NetApp Console unterstützt die Verwaltung sowohl lokaler als auch Cloud-Speichersysteme. Sie müssen einem Projekt ein Speichersystem hinzufügen, damit die dem Projekt zugewiesenen Personen darauf zugreifen können.

Speichersysteme

Speichersysteme werden automatisch dem Projekt zugeordnet, in dem sie hinzugefügt werden, aber Sie können sie auf der Seite **Ressourcen** auch anderen Projekten oder Ordnern zuordnen. Sie können FSx for NetApp ONTAP-Speichersysteme nicht Projekten oder Ordnern zuordnen, aber Sie können sie auf der Seite **Systeme** oder unter Workloads einsehen.

Keystone -Abonnements

Keystone -Abonnements sind außerdem Ressourcen, die Sie Projekten zuordnen können, um Benutzern Zugriff auf das Abonnement in der NetApp Console zu gewähren.

Backup and Recovery-Workloads (Oracle und Microsoft SQL Server)

Einige Backup und Recovery Workloads werden ebenfalls als Ressourcen betrachtet. Sie können Benutzern Berechtigungen für den Zugriff auf Backup und

Konsolenagenten

Organisationsadministratoren erstellen Konsolenagenten, um Speichersysteme zu verwalten und NetApp -Datendienste zu aktivieren. Agenten sind zunächst an das Projekt gebunden, in dem sie erstellt wurden. Administratoren können sie jedoch von der Agentenseite aus anderen Projekten oder Ordnern hinzufügen.

Durch die Zuordnung eines Agenten zu einem Projekt wird die Verwaltung von Ressourcen in diesem Projekt ermöglicht, während die Zuordnung eines Agenten zu einem Ordner es Ordner- oder Projektadministratoren erlaubt, zu entscheiden, welche Projekte den Agenten verwenden sollen. Um Managementfunktionen bereitstellen zu können, müssen Agenten bestimmten Projekten zugeordnet werden.

"Erfahren Sie, wie Sie Agenten Projekten zuordnen."

Mitglieder und Rollen

Mitglieder

Mitglieder Ihrer Organisation sind Benutzerkonten oder Dienstkonten. Ein Dienstkonto wird normalerweise von einer Anwendung verwendet, um bestimmte Aufgaben ohne menschliches Eingreifen abzuschließen.

Sie müssen Mitglieder zu Ihrer Organisation hinzufügen, nachdem diese sich bei der NetApp Console angemeldet haben. Sobald sie hinzugefügt wurden, können Sie ihnen Rollen zuweisen, um ihnen Zugriff auf Ressourcen zu gewähren. Sie können Servicekonten manuell über die Konsole hinzufügen oder deren Erstellung und Verwaltung über die NetApp Console IAM API automatisieren.

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

Zugriffsrollen

Die Konsole bietet Zugriffsrollen, die Sie den Mitgliedern Ihrer Organisation zuweisen können.

Wenn Sie einem Mitglied eine Rolle zuweisen, können Sie diese Rolle für die gesamte Organisation, einen bestimmten Ordner oder ein bestimmtes Projekt vergeben. Die von Ihnen ausgewählte Rolle gewährt einem Mitglied Berechtigungen für die Ressourcen im ausgewählten Teil der Hierarchie.

Die NetApp Console bietet differenzierte Rollen, die dem Prinzip der „minimalen Berechtigungen“ folgen. Das bedeutet, dass Zugriffsrollen so gestaltet sind, dass Benutzer nur auf das zugreifen können, was sie benötigen.

Dies bedeutet, dass Benutzern im Zuge der Erweiterung ihrer Aufgaben mehrere Rollen zugewiesen werden können.

"Informationen zu Zugriffsrollen" .

Beispiele für IAM-Strategien

Strategie für kleine Organisationen

Für Organisationen mit weniger als 50 Benutzern und zentralisierter Speicherverwaltung empfiehlt sich ein vereinfachter Ansatz mit den Rollen Super-Administrator und Super-Betrachter.

Beispiel: ABC Corporation (5-köpfiges Team)

- **Struktur:** Einzelne Organisation mit 3 Projekten (Produktion, Entwicklung, Backup)
- **Rollen:**
  - 2 hochrangige Mitglieder: **Super-Admin**-Rolle für vollen administrativen Zugriff
  - 3 Teammitglieder: **Superbeobachter**-Rolle zur Überwachung ohne Änderungsrechte
- **Agentenstrategie:** Ein einziger Agent ist allen Projekten für den gemeinsamen Ressourcenzugriff zugeordnet.
- **Vorteile:** Vereinfachte Administration, reduzierte Rollenkomplexität, geeignet für Teams, die einen breiten Zugriff benötigen

Strategie für ein multiregionales Unternehmen

Bei großen Organisationen mit regionalen Niederlassungen und spezialisierten Teams empfiehlt sich ein hierarchischer Ansatz mit Ordnern, die geografische oder Geschäftsbereichsgrenzen repräsentieren.

Beispiel: XYZ Corporation (multinationales Unternehmen)

- **Struktur:** Organisation > Regionale Ordner (Nordamerika, Europa, Asien-Pazifik) > Projektordner pro Region
- **Plattformrollen:**
  - 1 **Organisationsverwaltung**: Globale Aufsicht und Richtlinienmanagement
  - 3 **Ordner- oder Projektadministratoren**: Regionale Kontrolle (einer pro Region)
  - 1 **Verbandsverwaltung**: Integration des Corporate Identity Providers
- **Speicherrollen nach Region:**
  - 9 **Speicheradministration**: Speichersysteme in zugewiesenen Regionen erkennen und verwalten
  - 2 **Speicheranzeige**: Überwachen Sie Speicherressourcen regionsübergreifend
  - 1 **Systemgesundheitsspezialist**: Speicherzustand ohne Systemänderungen verwalten
- **Rollen im Bereich Datendienste:**
  - **Administrator für Datensicherung und -wiederherstellung**: Projektbezogen basierend auf den Aufgaben im Bereich Datensicherung
  - **Administrator für Ransomware-Resilienz**: Überwachung der Sicherheitsteams in verschiedenen Projekten
- **Agentenstrategie:** Regionale Agenten, die geeigneten geografischen Projekten zugeordnet sind
- **Vorteile:** Erhöhte Sicherheit durch Rollentrennung, regionale Autonomie und Einhaltung lokaler Vorschriften

Strategie der Fachbereichsspezialisierung

Für Organisationen mit spezialisierten Teams, die einen spezifischen Zugriff auf Datendienste benötigen, sollten gezielte Rollenzuweisungen auf der Grundlage funktionaler Verantwortlichkeiten verwendet werden.

Beispiel: TechCorp (mittelständisches Technologieunternehmen)

- **Struktur:** Organisation > Abteilungsordner (IT, Sicherheit, Entwicklung) > Projektspezifische Ressourcen
- **Spezialisierte Rollen:**
  - Sicherheitsteam: **Administrator für Ransomware-Resilienz** und **Klassifizierungsbetrachter** (Rollen)
  - Backup-Team: **Super-Administrator für Backup und Wiederherstellung** für umfassende Backup-Operationen
  - Entwicklungsteam: **Speicheradministrator** für die Testumgebungsverwaltung
  - Compliance-Team: **Analyst für operative Unterstützung** für Überwachung und Fallmanagement
- **Agentenstrategie:** Agenten werden basierend auf der Ressourcenverantwortung Abteilungsprojekten zugeordnet.
- **Vorteile:** Maßgeschneiderte Zugangskontrolle, verbesserte betriebliche Effizienz und klare Verantwortlichkeiten für spezialisierte Aufgaben

Nächste Schritte mit IAM in der NetApp Console

- "Erste Schritte mit IAM in der NetApp Console"
- "Überwachen oder prüfen Sie die IAM-Aktivität"
- "Erfahren Sie mehr über die API für NetApp Console IAM"

Erste Schritte mit Identität und Zugriff in der NetApp Console

Wenn Sie sich für die NetApp Console anmelden, werden Sie aufgefordert, eine neue Organisation zu erstellen. Die Organisation umfasst ein Mitglied (einen Organisationsadministrator) und ein Standardprojekt. Um die Identitäts- und Zugriffsverwaltung (IAM) so einzurichten, dass sie Ihren Geschäftsanforderungen entspricht, müssen Sie die Hierarchie Ihrer Organisation anpassen, zusätzliche Mitglieder hinzufügen, Ressourcen hinzufügen oder ermitteln und diese Ressourcen in Ihrer Hierarchie verknüpfen.

Sie benötigen die Berechtigungen **Organisationsadministrator** oder **Superadministrator**, um Identität und Zugriff für Ihre Organisation zu verwalten. Mit **Ordner- oder Projektadministratorberechtigungen** können Sie nur die Ordner und Projekte verwalten, auf die Sie Zugriff haben.

Befolgen Sie diese Schritte, um eine neue Organisation einzurichten. Die Reihenfolge kann je nach den Anforderungen Ihrer Organisation variieren.

Bearbeiten Sie das Standardprojekt oder fügen Sie es der Hierarchie Ihrer Organisation hinzu

Verwenden Sie das Standardprojekt oder erstellen Sie zusätzliche Projekte und Ordner, die Ihrer Unternehmenshierarchie entsprechen.

"Erfahren Sie, wie Sie Ihre Ressourcen mit Ordnern und Projekten organisieren" .

2 Ordnen Sie Mitglieder Ihrer Organisation zu

Nachdem sich Benutzer bei NetApp Console registriert haben, müssen Sie sie explizit Ihrer Console-Organisation hinzufügen. Sie haben außerdem die Möglichkeit, Ihrer Organisation Servicekonten hinzuzufügen.

"Erfahren Sie, wie Sie Mitglieder und ihre Berechtigungen verwalten" .

3 Ressourcen hinzufügen oder entdecken

Fügen Sie der Konsole Ressourcen (Systeme) hinzu oder ermitteln Sie sie. Mitglieder der Organisation verwalten Systeme innerhalb eines Projekts.

Erfahren Sie, wie Sie Ressourcen erstellen oder entdecken:

- "Amazon FSx for NetApp ONTAP"
- "Azure NetApp Files"
- "Cloud Volumes ONTAP"
- "Systeme der E-Serie"
- "On-Premises- ONTAP -Cluster"
- "StorageGRID"

4 Ressourcen zusätzlichen Projekten zuordnen

Durch das Hinzufügen oder Erkennen eines Systems in der Konsole wird die Ressource automatisch dem aktuell ausgewählten Projekt zugeordnet. Um diese Ressource einem anderen Projekt in Ihrer Organisation zur Verfügung zu stellen, verknüpfen Sie sie mit dem jeweiligen Projekt. Wenn zur Verwaltung der Ressource ein Konsolenagent verwendet wird, ordnen Sie den Konsolenagenten dem jeweiligen Projekt zu.

- "Erfahren Sie, wie Sie die Ressourcenhierarchie Ihres Unternehmens verwalten" .
- "Erfahren Sie, wie Sie einen Konsolenagenten mit einem Ordner oder Projekt verknüpfen" .

Ähnliche Informationen

- "Erfahren Sie mehr über Identitäts- und Zugriffsmanagement in der NetApp Console"
- "Erfahren Sie mehr über die API für Identität und Zugriff"

Richten Sie Ihre Konsolenorganisation ein.

Fügen Sie Ihrer NetApp Console Organisation Ordner und Projekte hinzu.

Fügen Sie Ordner und Projekte hinzu, die Ihrer Unternehmensstruktur entsprechen. Nachdem Sie Ordner und Projekte erstellt haben, können Sie ihnen Ressourcen zuordnen und den Zugriff von Mitgliedern auf diese Projekte verwalten.

Die Konsole erstellt automatisch ein Projekt für Sie, wenn Sie eine neue Organisation anlegen. Die meisten

Organisationen benötigen mehr als ein Projekt sowie Ordner, um die Dinge übersichtlich zu organisieren. "Erfahren Sie mehr über die Ressourcenhierarchie in der NetApp Console."Die

Ressourcen mithilfe von Ordnern und Projekten organisieren

In der NetApp Console enthält eine Organisation Ordner und Projekte, die Ihnen helfen, Ihre Ressourcen zu organisieren. Ordner helfen Ihnen, zusammengehörige Projekte zu gruppieren, und Projekte helfen Ihnen, Ressourcen und den Mitgliederzugriff zu verwalten.

Ordner

Ordner helfen Ihnen, zusammengehörige Projekte zu organisieren. Sie können verschachtelte Ordner erstellen, um verschiedene Ebenen der Struktur Ihrer Organisation darzustellen. Beispielsweise könnten Sie für jede Geschäftseinheit einen Ordner der obersten Ebene erstellen und darin Unterordner für die verschiedenen Teams innerhalb dieser Geschäftseinheit anlegen. Anschließend erstellen Sie Projekte in Ordnern.

Ordner ermöglichen Ihnen außerdem eine effizientere Verwaltung der Mitgliederzugriffe durch Rollenvererbung. Wenn Sie Mitgliedern Rollen auf Ordnerebene zuweisen, erben diese die Berechtigungen für alle untergeordneten Projekte und Ordner.

Ordner sind ein Organisationswerkzeug und für Mitglieder, die keine IAM-Berechtigungen wie z. B. die Rollen Organisationsadministrator, Ordner- oder Projektadministrator oder Superadministrator besitzen, nicht sichtbar. Mitglieder greifen auf Projekte zu, nicht auf Ordner.

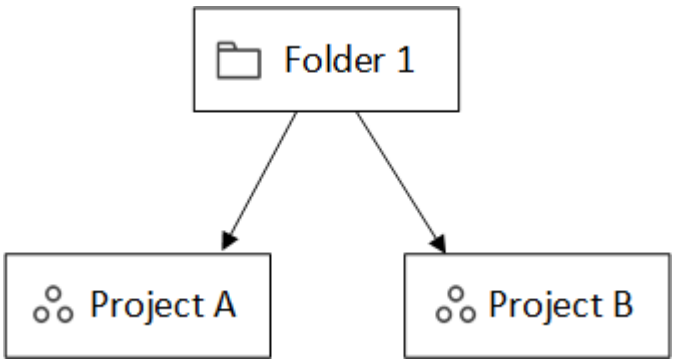
Organisationsadministratoren können administrative Aufgaben delegieren, indem sie Ordner erstellen. Nach dem Erstellen eines Ordners kann ein Organisationsadministrator einem Mitglied die Ordner- oder Projektadministratorrolle für bestimmte Ordner zuweisen. Diese Mitglieder können dann alle Projekte innerhalb dieses Ordners verwalten, ohne Zugriff auf die gesamte Organisation zu haben.

Ordner können andere Ordner oder Projekte als Unterordner haben, aber es können keine Ressourcen direkt mit ihnen verknüpft sein. Ressourcen müssen einem Projekt zugeordnet werden.

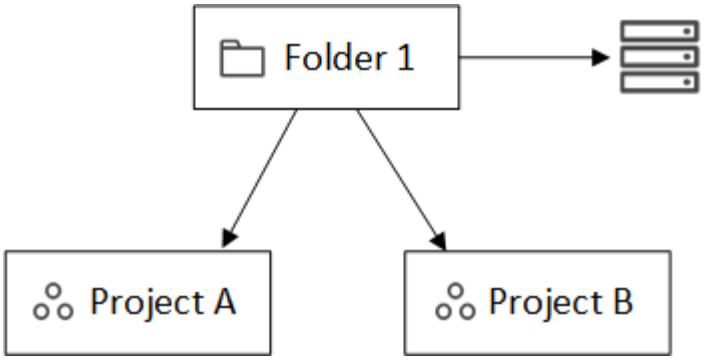
Wann sollte eine Ressource einem Ordner zugeordnet werden?

Ein *Organisationsadministrator* kann eine Ressource mit einem Ordner verknüpfen, sodass ein *Ordner- oder Projektadministrator* sie mit den entsprechenden Projekten im Ordner verknüpfen kann.

Nehmen wir beispielsweise an, Sie haben einen Ordner, der zwei Projekte enthält:

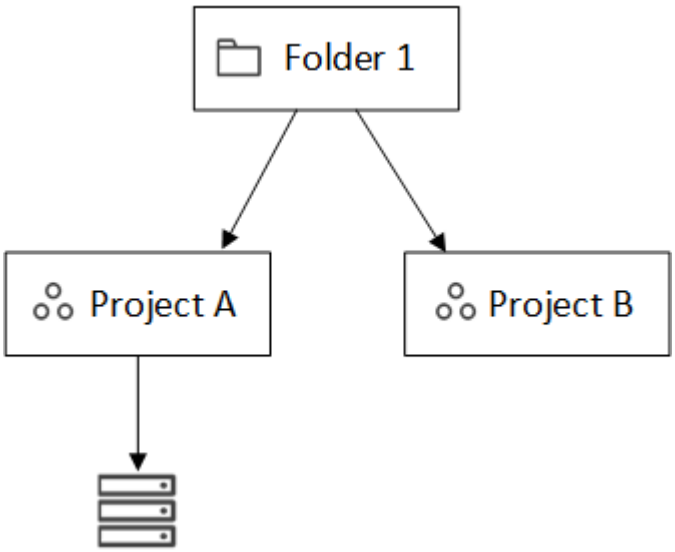


Der *Organisationsadministrator* kann eine Ressource mit dem Ordner verknüpfen:



Durch die Verknüpfung einer Ressource mit einem Ordner wird diese nicht für alle Projekte zugänglich; nur der Ordner- oder Projektadministrator kann sie sehen. Der *Ordner- oder Projektadministrator* entscheidet, welche Projekte darauf zugreifen können und ordnet die Ressource den entsprechenden Projekten zu.

In diesem Beispiel verknüpft der Administrator die Ressource mit Projekt A:



Mitglieder, die über Berechtigungen für Projekt A verfügen, können jetzt auf die Ressource zugreifen.

Projekte

Ordnen Sie Ressourcen Projekten zu, damit die Mitglieder diese verwalten können. Ressourcen müssen einem Projekt zugeordnet werden, damit sie verwaltet und von Benutzern zugänglich gemacht werden können.

Eine Organisation kann ein oder mehrere Projekte haben. Ein Projekt kann sich direkt unter der Organisation oder in einem Ordner befinden. Wenn ein Agent zur Ermittlung von Ressourcen innerhalb eines Projekts verwendet wird, müssen Sie den Agenten auch diesem Projekt zuordnen.

Auf der Seite **Systeme** navigieren die Benutzer zwischen den ihnen zugewiesenen Projekten, um die Ressourcen zu verwalten, die mit jedem Projekt verbunden sind.

Einen Ordner oder ein Projekt hinzufügen

Fügen Sie Projekte hinzu, um Ressourcen zu verwalten, und Ordner, um zusammengehörige Projekte zu gruppieren. Wenn Sie eine neue Organisation erstellen, enthält die Konsole ein Projekt.

Sie können in der Ressourcenstruktur Ihrer Organisation bis zu sieben Ebenen von Ordnern und Projekten erstellen. Erstellen Sie nach Bedarf verschachtelte Ordner, um Ihre Ressourcen zu organisieren.

Schritte

1. Wählen Sie **Verwaltung > Identität und Zugriff**.
2. Wählen Sie **Organisation** aus.
3. Wählen Sie auf der Seite **Organisation** die Option **Ordner oder Projekt hinzufügen** aus.
4. Wählen Sie **Ordner** oder **Projekt**.
5. Ordner- oder Projektdetails eingeben:
   - **Name und Speicherort**: Geben Sie einen Namen ein und wählen Sie einen Speicherort für den Ordner oder das Projekt. Sie können Ordner oder Projekte innerhalb der Organisation oder in einem anderen Ordner ablegen.
   - **Ressourcen**: Wählen Sie die Ressourcen aus, die Sie diesem Ordner oder Projekt zuordnen möchten. Falls Sie der Konsole noch keine Speichersysteme hinzugefügt haben, können Sie diesen Schritt später durchführen.

     Mitglieder können erst dann auf Ressourcen in einem Ordner zugreifen, wenn diese Ressourcen einem Projekt zugewiesen wurden. Verwenden Sie Ordner, um Ressourcen vorübergehend zu speichern, bis Sie die benötigten Projekte erstellt haben. Dies kann dem Organisationsadministrator helfen, die Ressourcenzuweisung an einen Ordner- oder Projektadministrator zu delegieren, der dann Ressourcen den Projekten innerhalb des Ordners zuweist.

   - **Zugriff**: Wählen Sie **Mitglied hinzufügen**, um Zugriffsrechte und eine Rolle zuzuweisen. Sie können jederzeit Mitglieder zum Projekt oder Ordner hinzufügen oder daraus entfernen.

     "Informationen zu Zugriffsrollen" .
6. Wählen Sie **Hinzufügen**.

Umbenennen eines Ordners oder Projekts

Benennen Sie einen Ordner oder ein Projekt nach Bedarf um. Die Umbenennung hat keine Auswirkungen auf zugehörige Ressourcen oder den Mitgliederzugriff.

Schritte

1. 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**.
2. Geben Sie auf der Seite **Bearbeiten** einen neuen Namen ein und wählen Sie **Übernehmen**.

Löschen eines Ordners oder Projekts

Löschen Sie Ordner und Projekte, die Sie nicht mehr benötigen, beispielsweise nach einer Teamumstrukturierung oder nach Projektabschluss.

Bevor Sie einen Ordner oder ein Projekt löschen, vergewissern Sie sich, dass es keine Ressourcen mehr enthält. Erfahren Sie, wie Sie Ressourcen entfernen.

Schritte

1. Navigieren Sie auf der Seite **Organisation** zu einem Projekt oder Ordner in der Tabelle, wählen Sie ••• und

wählen Sie dann **Löschen**.

2. Bestätigen Sie, dass Sie den Ordner oder das Projekt löschen möchten.

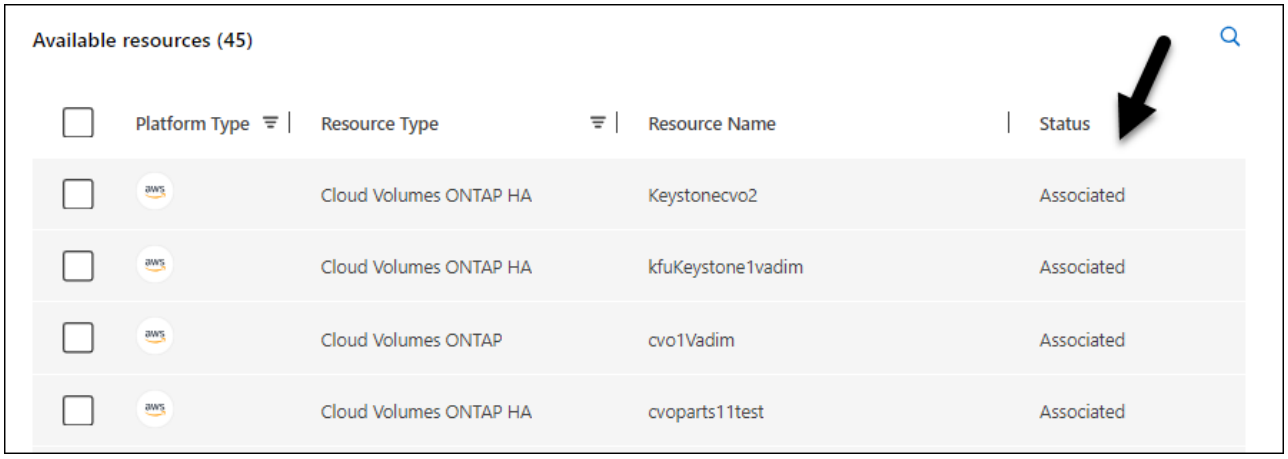
Anzeigen der mit einem Ordner oder Projekt verknüpften Ressourcen

Zeigen Sie an, welche Ressourcen und Mitglieder mit einem Ordner oder Projekt verknüpft sind.

Schritte

1. 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**.

2. Auf der Seite **Bearbeiten** können Sie Details zum ausgewählten Ordner oder Projekt anzeigen, indem Sie die Abschnitte **Ressourcen** oder **Zugriff** erweitern.
   - Wählen Sie **Ressourcen** aus, um die zugehörigen Ressourcen anzuzeigen. In der Tabelle identifiziert die Spalte **Status** die Ressourcen, die mit dem Ordner oder Projekt verknüpft sind.



Ändern Sie die Ressourcen, die einem Ordner oder Projekt zugeordnet sind.

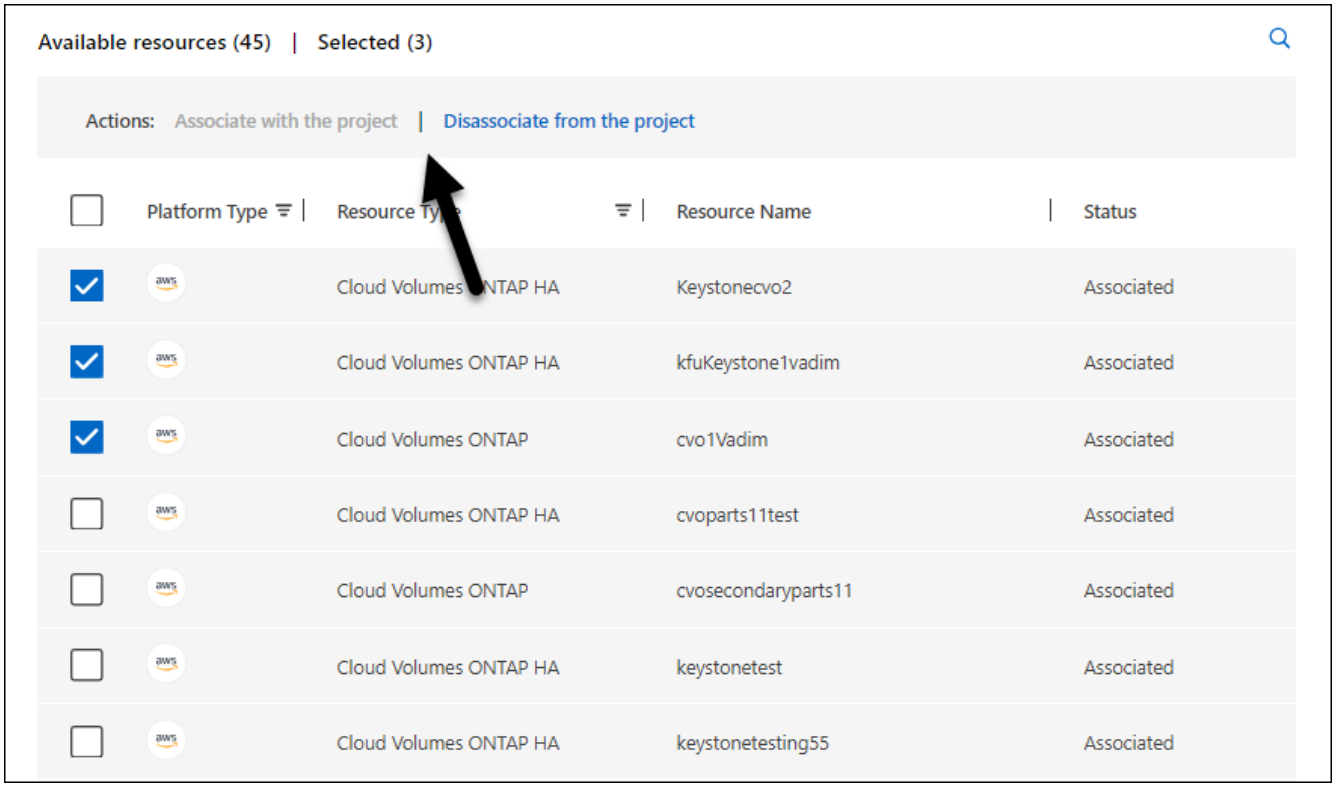
Sie können die einem Ordner oder Projekt zugeordneten Ressourcen ändern, wenn sich die Bedürfnisse Ihrer Organisation ändern.

Schritte

1. 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**.
2. Wählen Sie auf der Seite **Bearbeiten Ressourcen** aus.

   In der Tabelle identifiziert die Spalte **Status** die Ressourcen, die mit dem Ordner oder Projekt verknüpft sind.

3. Wählen Sie die Ressourcen aus, die Sie zuordnen oder deren Zuordnung Sie aufheben möchten.
4. Basierend auf den von Ihnen ausgewählten Ressourcen wählen Sie entweder **Dem Projekt zuordnen** oder **Vom Projekt trennen**.



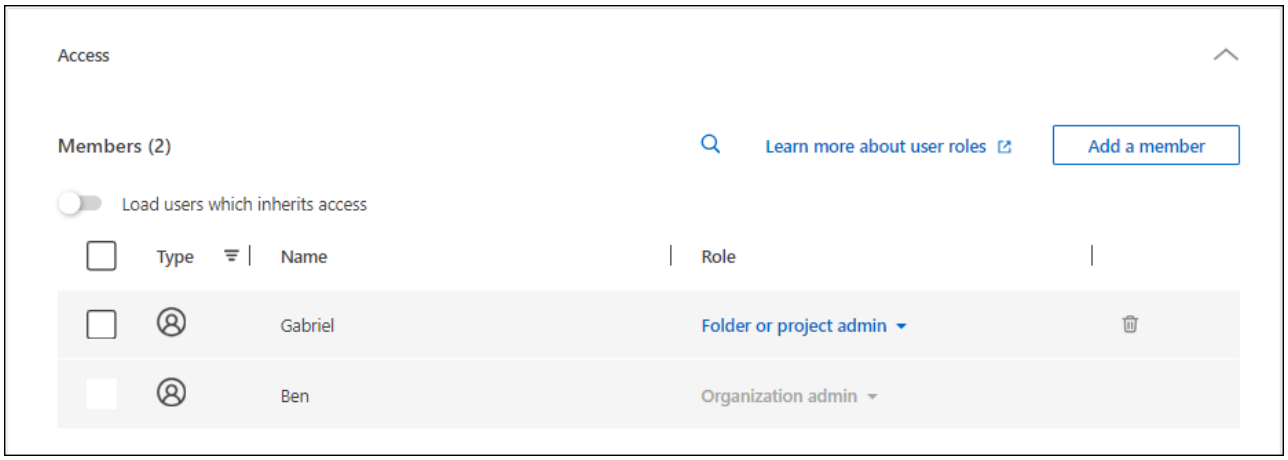
5. Wählen Sie **Übernehmen**.

Anzeigen von Mitgliedern, die einem Ordner oder Projekt zugeordnet sind

Auf der Seite **Organisation** können Sie die Mitglieder anzeigen, die einem Ordner oder Projekt zugeordnet sind.

Schritte

1. 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**.
2. Wählen Sie auf der Seite **Bearbeiten Zugriff** aus, um die Liste der Mitglieder anzuzeigen, die Zugriff auf den ausgewählten Ordner oder das ausgewählte Projekt haben.
   - Wählen Sie **Zugriff** aus, um die Mitglieder anzuzeigen, die Zugriff auf den Ordner oder das Projekt haben.



Ändern des Mitgliederzugriffs auf einen Ordner oder ein Projekt

Ändern Sie die Zugriffsrechte der Mitglieder, um den Ressourcenzugriff zu steuern. Beachten Sie, dass Rollen, die auf Ordnerebene zugewiesen werden, an alle untergeordneten Projekte und Ordner vererbt werden.

Die Zugriffsrechte von Mitgliedern auf niedrigeren Ebenen können nicht geändert werden, wenn sie von der Ordner- oder Organisationsebene übernommen wurden. Ändern Sie die Berechtigungen des Mitglieds auf der höheren Hierarchieebene, um den Zugriff zu ändern. Alternativ können Sie "Verwalten Sie Berechtigungen auf der Seite „Mitglieder““Die

Schritte

1. 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**.
2. Wählen Sie auf der Seite **Bearbeiten Zugriff** aus, um die Liste der Mitglieder anzuzeigen, die Zugriff auf den ausgewählten Ordner oder das ausgewählte Projekt haben.
3. Mitgliederzugriff ändern:
   - **Mitglied hinzufügen**: Wählen Sie das Mitglied aus, das Sie dem Ordner oder Projekt hinzufügen möchten, und weisen Sie ihm eine Rolle zu.
   - **Rolle eines Mitglieds ändern**: Wählen Sie für alle Mitglieder mit einer anderen Rolle als „Organisationsadministrator“ ihre vorhandene Rolle und dann eine neue Rolle aus.
   - **Mitgliederzugriff entfernen**: Sie können den Zugriff von Mitgliedern entfernen, denen für den Ordner oder das Projekt, das Sie gerade anzeigen, eine Rolle definiert ist.
4. Wählen Sie **Übernehmen**.

Ähnliche Informationen

- "Erfahren Sie mehr über Identität und Zugriff in der NetApp Console"
- "Erste Schritte mit Identität und Zugriff"
- "Erfahren Sie mehr über die Identitäts- und Zugriffs-API"

Fügen Sie Ressourcen zu Ordnern und Projekten in der NetApp Console hinzu.

Steuern Sie den Benutzerzugriff auf Ressourcen, indem Sie diese Projekten und Ordnern in Ihrer NetApp Console -Organisation hinzufügen. Benutzern Zugriff auf Projektebene gewähren.

Eine *Ressource* ist eine Entität, die der Konsole bekannt ist, wie beispielsweise eine Speicherressource, ein Konsolenagent oder eine Backup- und Wiederherstellungs-Workload.

Auf der Seite **Ressourcen** in der Konsole können Sie Ressourcen anzeigen und verwalten.

Konsolenressourcentypen

Sie können in Ihrer NetApp Console Organisation verschiedene Ressourcentypen Projekten zuordnen:

Speicherressourcen

Speicherressourcen sind die am häufigsten vorkommende Ressourcenart in Ihrem Unternehmen und umfassen sowohl lokale als auch Cloud-Speichersysteme. Wenn Sie ein Speichersystem zur Konsole hinzufügen, können Sie es einem Ordner oder Projekt hinzufügen. Bis dahin wird es in der Konsole als nicht entdeckt markiert und nicht auf der Seite **Ressourcen** angezeigt.

Konsolenagenten

Wenn Sie einen Console-Agenten zur Erkennung von Speichersystemen verwendet haben, fügen Sie den Agenten demselben Ordner oder Projekt hinzu. Dies ermöglicht es Benutzern, agentenbasierte Funktionen auszuführen, wie z. B. Datendienste oder die native Speicherverwaltung der Konsole. Sie können Agenten über die Seite **Agenten** in der Konsole Ordnern oder Projekten hinzufügen. "Erfahren Sie, wie Sie einen Konsolenagenten mit einem Ordner oder Projekt verknüpfen"Die

Keystone -Abonnements

Wenn Sie in Ihrer Organisation Keystone Abonnements haben, können Sie diese auf der Seite **Ressourcen** einsehen. Sie können Keystone -Abonnements mit Ordnern oder Projekten verknüpfen, um Mitgliedern, die über Berechtigungen für diese Ordner oder Projekte verfügen, Zugriff zu gewähren.

Zeigen Sie die Ressourcen in Ihrer Organisation an

Sie können sowohl entdeckte als auch unentdeckte Ressourcen anzeigen, die mit Ihrer Organisation verknüpft sind. Das System findet Speicherressourcen und markiert sie als nicht entdeckt, bis Sie sie zur Konsole hinzufügen.

Die Konsole schließt Amazon FSx for NetApp ONTAP Ressourcen von der Ressourcenseite aus, da Benutzer sie keiner Rolle zuordnen können. Sie können diese Ressourcen auf der Seite **Systeme** oder unter Workloads einsehen.

Schritte

1. Wählen Sie **Verwaltung > Identität und Zugriff**.
2. Wählen Sie **Ressourcen** aus.
3. Wählen Sie **Erweiterte Suche und Filterung**.
4. Nutzen Sie die verfügbaren Optionen, um eine Ressource zu finden:
   - **Suche nach Ressourcennamen**: Geben Sie eine Textzeichenfolge ein und wählen Sie **Hinzufügen**.
   - **Plattform**: Wählen Sie eine oder mehrere Plattformen aus, beispielsweise Amazon Web Services.
   - **Ressourcen**: Wählen Sie eine oder mehrere Ressourcen aus, beispielsweise Cloud Volumes ONTAP.
   - **Organisation, Ordner oder Projekt**: Wählen Sie die gesamte Organisation, einen bestimmten Ordner oder ein bestimmtes Projekt aus.
5. Wählen Sie **Suchen**.

Zuordnen einer Ressource zu Ordnern und Projekten

Verknüpfen Sie eine Ressource mit einem Ordner oder Projekt, um sie Mitgliedern zur Verfügung zu stellen, die über Berechtigungen für diesen Ordner oder dieses Projekt verfügen.

Schritte

1. Navigieren Sie auf der Seite **Ressourcen** zu einer Ressource in der Tabelle, wählen Sie ••• und wählen Sie dann **Mit Ordnern oder Projekten verknüpfen**.
2. Wählen Sie einen Ordner oder ein Projekt aus und wählen Sie dann **Akzeptieren**.
3. Um einen zusätzlichen Ordner oder ein zusätzliches Projekt zuzuordnen, wählen Sie **Ordner oder Projekt hinzufügen** und wählen Sie dann den Ordner oder das Projekt aus.

   Beachten Sie, dass Sie nur aus den Ordnern und Projekten auswählen können, für die Sie über Administratorberechtigungen verfügen.

4. Wählen Sie **Ressourcen zuordnen**.
   - Wenn Sie die Ressource mit Projekten verknüpft haben, können Mitglieder, die über Berechtigungen für diese Projekte verfügen, jetzt über die Konsole auf die Ressource zugreifen.
   - Wenn Sie die Ressource mit einem Ordner verknüpft haben, kann ein *Ordner- oder Projektadministrator* jetzt auf die Ressource zugreifen und sie mit einem Projekt innerhalb des Ordners verknüpfen. "Informationen zum Verknüpfen einer Ressource mit einem Ordner"Die

Nach Abschluss

Wenn Sie mithilfe eines Konsolenagenten eine Ressource entdecken, verknüpfen Sie den Konsolenagenten mit dem Projekt, um Zugriff zu gewähren. Andernfalls sind der Konsolenagent und die zugehörige Ressource für Mitglieder ohne die Rolle „Organisationsadministrator“ nicht zugänglich.

"Erfahren Sie, wie Sie einen Konsolenagenten mit einem Ordner oder Projekt verknüpfen".

Anzeigen der mit einer Ressource verknüpften Ordner und Projekte

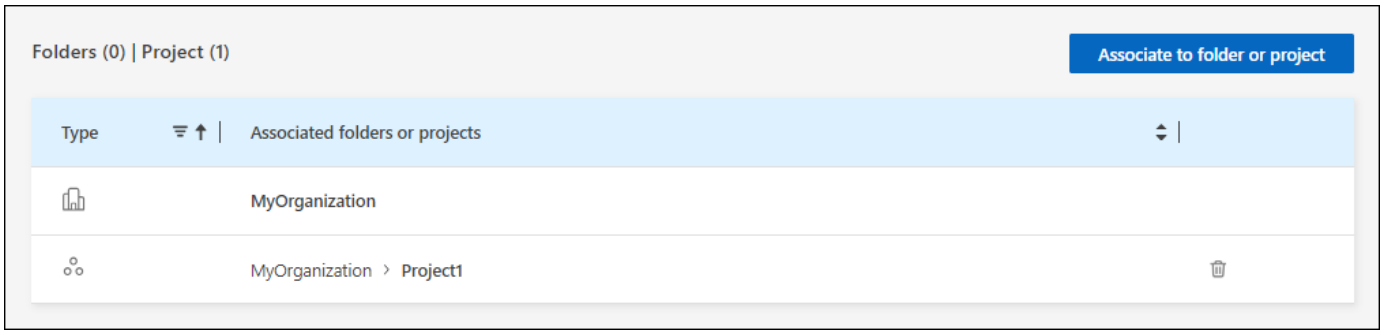
Sie können die Ordner und Projekte anzeigen, die mit einer bestimmten Ressource verknüpft sind.

> Wenn Sie herausfinden möchten, welche Organisationsmitglieder Zugriff auf die Ressource haben, können Sie"Zeigen Sie die Mitglieder an, die Zugriff auf die Ordner und Projekte haben, die mit der Ressource verknüpft sind." .

Schritte

1. Navigieren Sie auf der Seite **Ressourcen** zu einer Ressource in der Tabelle, wählen Sie ••• und wählen Sie dann **Details anzeigen**.

Das folgende Beispiel zeigt eine Ressource, die mit einem Projekt verknüpft ist.



Um zu sehen, welche Organisationsmitglieder Zugriff auf die Ressource haben,"Mitglieder mit Zugriff auf zugehörige Ordner und Projekte anzeigen" Die

Entfernen einer Ressource aus einem Ordner oder Projekt

Um eine Ressource aus einem Ordner oder Projekt zu entfernen, muss ihre Zuordnung aufgehoben werden. Dies verhindert, dass Mitglieder die Ressource in diesem Ordner oder Projekt verwalten können.

Um eine gefundene Ressource aus der gesamten Organisation zu entfernen, gehen Sie zur Seite **Systeme** und entfernen Sie das System.

Schritte

1. Navigieren Sie auf der Seite **Ressourcen** zu einer Ressource in der Tabelle, wählen Sie ••• und wählen Sie dann **Details anzeigen**.
2. Um eine Ressource aus einem Ordner oder Projekt zu entfernen, wählen Sie Folgendes aus: 🗑 neben dem Ordner oder Projekt.
3. Wählen Sie **Löschen**, um die Verknüpfung zu entfernen.

Ähnliche Informationen

- "Erfahren Sie mehr über Identität und Zugriff in der NetApp Console"
- "Erste Schritte mit Identität und Zugriff in der NetApp Console"
- "Erfahren Sie mehr über die API für Identität und Zugriff"

Verknüpfen Sie einen Konsolenagenten mit anderen Ordnern und Projekten

Ordnen Sie Console-Agenten spezifischen Projekten zu, um Ressourcenmanagement und Datenzugriff zu ermöglichen. Für Ressourcen, die über einen Console-Agenten gefunden werden, müssen sowohl die Ressource als auch der Agent den gleichen Projekten zugeordnet sein, damit das Team darauf zugreifen kann.

Super-Administratoren und Organisationsadministratoren können Agenten erstellen und jeden Agenten einem beliebigen Projekt oder Ordner zuordnen. Ordner- oder Projektadministratoren können nur vorhandene Agenten Ordnern und Projekten zuordnen, für die sie die entsprechenden Berechtigungen besitzen. "Erfahren Sie mehr über die Aktionen, die ein Ordner- oder Projektadministrator ausführen kann."Die

Schritte

1. Wählen Sie **Verwaltung > Identität und Zugriff** > **Agenten**.
2. Suchen Sie in der Tabelle den Konsolenagenten, den Sie zuordnen möchten.

Verwenden Sie die Suche über der Tabelle, um einen bestimmten Konsolenagenten zu finden, oder filtern Sie die Tabelle nach Ressourcenhierarchie.

3. Um die mit dem Konsolenagenten verknüpften Ordner und Projekte anzuzeigen, wählen Sie ••• und wählen Sie dann **Details anzeigen**.

   Auf der Seite werden Details zu den Ordnern und Projekten angezeigt, die mit dem Konsolenagenten verknüpft sind.

4. Wählen Sie **Mit Ordner oder Projekt verknüpfen**.
5. Wählen Sie einen Ordner oder ein Projekt aus und wählen Sie dann **Akzeptieren**.
6. Um den Konsolenagenten mit einem zusätzlichen Ordner oder Projekt zu verknüpfen, wählen Sie **Ordner oder Projekt hinzufügen** und wählen Sie dann den Ordner oder das Projekt aus.
7. Wählen Sie **Associate Agent** aus.

Nach Abschluss

Ordnen Sie die Ressourcen des Konsolenagenten denselben Ordnern und Projekten von der Seite **Ressourcen** zu.

"Erfahren Sie, wie Sie eine Ressource mit Ordnern und Projekten verknüpfen" .

Ähnliche Informationen

- "Erfahren Sie mehr über NetApp Console -Agenten"
- "Erfahren Sie mehr über die Identitäts- und Zugriffsverwaltung der NetApp Console"
- "Erste Schritte mit Identität und Zugriff"
- "Erfahren Sie mehr über die API für Identitäts- und Zugriffsverwaltung"

Fügen Sie Ihrer Konsolenorganisation Benutzer hinzu.

Fügen Sie Benutzer zu einer NetApp Console Organisation hinzu

Innerhalb der Konsole gewähren Sie Benutzern Zugriff auf Projekte oder Ordner entsprechend einer Zugriffsrolle. Eine Zugriffsrolle enthält eine Reihe von Berechtigungen, die es einem Mitglied (Benutzer oder Dienstkonto) ermöglichen, bestimmte Aktionen auf der zugewiesenen Ebene der Ressourcenhierarchie durchzuführen.

Erforderliche Zugriffsrollen

Super-Admin, Organisations-Admin oder Ordner- bzw. Projekt-Admin (für die von ihnen verwalteten Ordner und Projekte). "Informationen zu Zugriffsrollen"Die

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

Die NetApp Console verwendet rollenbasierte Zugriffskontrolle (RBAC) zur Verwaltung von Berechtigungen. Weisen Sie Benutzern Rollen einzeln oder über föderierte Gruppen zu. Jede Rolle definiert die zulässigen Aktionen für bestimmte Ressourcen.

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.

Fügen Sie Ihrer Organisation Mitglieder hinzu

Die NetApp Console unterstützt drei Arten von Mitgliedern: Benutzerkonten, Dienstkonten und Verbundgruppen.

Benutzer müssen sich bei der NetApp Console registrieren, bevor Sie sie hinzufügen und ihnen eine Rolle zuweisen können, selbst wenn sie Mitglied einer Verbundgruppe sind. Dienstkonten können direkt in der Konsole erstellt werden.

Alle Mitglieder müssen mindestens eine Rolle explizit zugewiesen bekommen haben, um auf Ressourcen zugreifen zu können.

Beim Hinzufügen eines Mitglieds wählen Sie die Ressourcenebene (Organisation, Ordner oder Projekt) und weisen Sie eine oder mehrere Rollen mit den erforderlichen Berechtigungen zu.

Einen Benutzer hinzufügen

Benutzer registrieren sich für die NetApp Console, aber ein Organisationsadministrator, Ordner- oder Projektadministrator muss sie einer Organisation, einem Ordner oder einem Projekt hinzufügen, damit sie auf Ressourcen zugreifen können.

Bevor Sie beginnen:

Der Benutzer muss sich bereits für die NetApp Console registriert haben. Falls sie sich noch nicht angemeldet haben, leiten Sie sie bitte weiter zu "Registrieren Sie sich für die NetApp Console."

> Wenn Sie einen Benutzer hinzufügen, der Teil einer Verbundgruppe ist, stellen Sie sicher, dass sich der Benutzer bereits bei der NetApp Console registriert hat und ihm explizit eine Rolle in der Console zugewiesen wurde. NetApp empfiehlt, eine minimale Zugriffsrolle wie z. B. „Organisationsbetrachter“ zuzuweisen.

Schritte

1. Wählen Sie **Verwaltung > Identität und Zugriff**.
2. Wählen Sie **Mitglieder** aus.
3. Wählen Sie **Mitglied hinzufügen**.
4. Behalten Sie für **Mitgliedstyp** die Auswahl von **Benutzer** bei.
5. Geben Sie bei **E-Mail des Benutzers** die E-Mail-Adresse des Benutzers ein, die mit der von ihm erstellten Anmeldung verknüpft ist.
6. Verwenden Sie den Abschnitt **Wählen Sie eine Organisation, einen Ordner oder ein Projekt aus**, um die Ebene Ihrer Ressourcenhierarchie auszuwählen, für die das Mitglied Berechtigungen haben soll.

   Beachten Sie Folgendes:

   - Sie können nur die Ordner und Projekte auswählen, für die Sie die entsprechenden Berechtigungen besitzen.

- Wenn Sie eine Organisation oder einen Ordner auswählen, erteilen Sie dem Mitglied Berechtigungen für alle darin enthaltenen Inhalte.
- Sie können die Rolle **Organisationsadministrator** nur auf Organisationsebene zuweisen.

7. **Wählen Sie eine Kategorie** und dann eine **Rolle** aus, die dem Mitglied Berechtigungen für die Ressourcen erteilt, die mit der von Ihnen ausgewählten Organisation, dem Ordner oder dem Projekt verknüpft sind.

   "Informationen zu Zugriffsrollen" .

8. Um Zugriff auf weitere Ordner, Projekte oder Rollen zu gewähren, wählen Sie **Rolle hinzufügen**, wählen Sie die Ordner-, Projekt- oder Rollenkategorie und anschließend eine Rolle aus.
9. Wählen Sie **Hinzufügen**.

   Die Konsole sendet dem Benutzer eine E-Mail mit Anweisungen.

Hinzufügen eines Dienstkontos

Dienstkonten ermöglichen die Automatisierung von Aufgaben und die sichere Verbindung mit Console-APIs. Wählen Sie eine Client-ID und ein Client-Geheimnis für einfache Setups oder JWT (JSON Web Token) für eine höhere Sicherheit in automatisierten oder Cloud-nativen Umgebungen. Wählen Sie die Methode, die Ihren Sicherheitsanforderungen entspricht.

Bevor Sie beginnen:

Bereiten Sie für die JWT-Authentifizierung Ihren öffentlichen Schlüssel oder Ihr Zertifikat vor.

Schritte

1. Wählen Sie **Verwaltung > Identität und Zugriff**.
2. Wählen Sie **Mitglieder** aus.
3. Wählen Sie **Mitglied hinzufügen**.
4. Wählen Sie für **Mitgliedstyp Dienstkonto** aus.
5. Geben Sie einen Namen für das Dienstkonto ein.
6. Um die JWT-Authentifizierung zu verwenden, wählen Sie **Private-Key-JWT-Authentifizierung verwenden** und laden Sie Ihren öffentlichen RSA-Schlüssel oder Ihr Zertifikat hoch. Überspringen, falls Client-ID und Client-Geheimnis verwendet werden.

   Ihr X.509-Zertifikat. Es muss im PEM-, CRT- oder CER-Format vorliegen.

   a. Richten Sie Ablaufbenachrichtigungen für Ihr Zertifikat ein. Sie haben die Wahl zwischen sieben Tagen oder 30 Tagen. Ablaufbenachrichtigungen werden per E-Mail versendet und Benutzern mit der Rolle „Super-Admin“ oder „Org-Admin“ in der Konsole angezeigt.

7. Verwenden Sie den Abschnitt **Wählen Sie eine Organisation, einen Ordner oder ein Projekt aus**, um die Ebene Ihrer Ressourcenhierarchie auszuwählen, für die das Mitglied Berechtigungen haben soll.

   Beachten Sie Folgendes:

   - Sie können nur aus den Ordnern und Projekten auswählen, für die Sie Berechtigungen haben.
   - Durch die Auswahl einer Organisation oder eines Ordners erhält das Mitglied Zugriff auf alle Inhalte.
   - Sie können die Rolle **Organisationsadministrator** nur auf Organisationsebene zuweisen.

8. Wählen Sie eine **Kategorie** und anschließend eine **Rolle** aus, die dem Mitglied Berechtigungen für die Ressourcen in der von Ihnen ausgewählten Organisation, dem Ordner oder dem Projekt erteilt.

   "Informationen zu Zugriffsrollen" .

9. Um Zugriff auf weitere Ordner, Projekte oder Rollen zu gewähren, wählen Sie **Rolle hinzufügen**, wählen Sie die Ordner-, Projekt- oder Rollenkategorie und anschließend eine Rolle aus.
10. Wenn Sie sich nicht für die Verwendung der JWT-Authentifizierung entschieden haben, laden Sie die Client-ID und das Client-Geheimnis herunter oder kopieren Sie sie.

    Die Konsole zeigt das Client-Geheimnis nur einmal an. Sicher kopieren; falls Sie es verlieren, können Sie es später wiederherstellen.

11. Wenn Sie die JWT-Authentifizierung gewählt haben, laden Sie die Client-ID und die JWT-Zielgruppe herunter oder kopieren Sie sie. Die Konsole zeigt diese Informationen nur einmal an und erlaubt es Ihnen nicht, sie später abzurufen.
12. Wählen Sie **Schließen**.

Fügen Sie Ihrer Organisation eine föderierte Gruppe hinzu.

Sie können eine föderierte Gruppe von Ihrem Identitätsanbieter (IdP) zu Ihrer Organisation hinzufügen und ihr eine oder mehrere Rollen zuweisen. Die Mitglieder der föderierten Gruppe erben die Rollen, die Sie der Gruppe in der Konsole zuweisen.

Bevor Sie einer föderierten Gruppe eine Rolle zuweisen können, stellen Sie Folgendes sicher:

- Richten Sie eine Föderation zwischen Ihrem IdP und der Konsole ein. "Erfahren Sie, wie Sie eine Föderation einrichten."
- Die Gruppe muss bereits in Ihrem Identitätsanbieter existieren und über App-Zugriff auf die Konsole verfügen.
- Benutzer, die dieser Gruppe angehören, müssen sich bereits für die NetApp Console registriert haben und ihnen muss explizit eine Rolle in der Console zugewiesen worden sein. NetApp empfiehlt, eine minimale Zugriffsrolle wie z. B. „Organisationsbetrachter“ zuzuweisen.

Schritte

1. Wählen Sie **Verwaltung > Identität und Zugriff**.
2. Wählen Sie **Mitglieder** aus.
3. Wählen Sie **Mitglied hinzufügen**.
4. Wählen Sie unter **Mitgliedstyp** die Option **Verbundgruppe**.
5. Wählen Sie den Verband aus, dem die Gruppe angehört.
6. Geben Sie unter **Gruppenname** den genauen Namen der Gruppe in Ihrem IdP ein.
7. Verwenden Sie den Abschnitt **Wählen Sie eine Organisation, einen Ordner oder ein Projekt aus**, um die Ebene Ihrer Ressourcenhierarchie auszuwählen, für die das Mitglied Berechtigungen haben soll.

   Beachten Sie Folgendes:

   - Sie können nur aus den Ordnern und Projekten auswählen, für die Sie Berechtigungen haben.
   - Durch die Auswahl einer Organisation oder eines Ordners erhält das Mitglied Zugriff auf alle Inhalte.
   - Sie können die Rolle **Organisationsadministrator** nur auf Organisationsebene zuweisen.

8. Wählen Sie eine **Kategorie** und anschließend eine **Rolle** aus, die dem Mitglied Berechtigungen für die Ressourcen in der von Ihnen ausgewählten Organisation, dem Ordner oder dem Projekt erteilt.

   "Informationen zu Zugriffsrollen" .

9. Um Zugriff auf weitere Ordner, Projekte oder Rollen zu gewähren, wählen Sie **Rolle hinzufügen**, wählen Sie die Ordner-, Projekt- oder Rollenkategorie und anschließend eine Rolle aus.

Ähnliche Informationen

- "Erfahren Sie mehr über Identitäts- und Zugriffsmanagement in der NetApp Console"
- "Erste Schritte mit Identität und Zugriff"
- "NetApp Console"
- "Erfahren Sie mehr über die API für Identität und Zugriff"

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." .

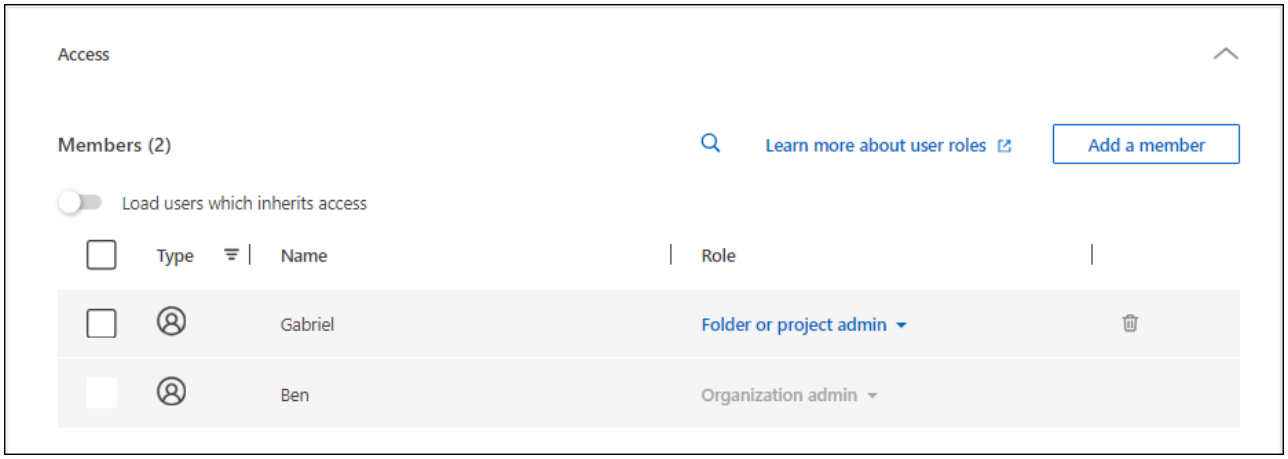
1. Navigieren Sie auf der Seite **Mitglieder** zu einem Mitglied in der Tabelle und wählen Sie es aus. ••• und wählen Sie dann **Details anzeigen**.
2. Erweitern Sie in der Tabelle die jeweilige Zeile für die Organisation, den Ordner oder das Projekt, in dem Sie die zugewiesene Rolle des Mitglieds anzeigen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

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.
"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.

Anwendungsrolle	Aufgaben
"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.

Datendienstrolle	Aufgaben
"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
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

Aufgabe	Organisationsadministrator	Ordner- oder Projektadministrator
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*:		
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

Funktion und Aktion	Keystone -Administrator	Keystone -Viewer
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
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			

Funktion und Aktion	Speicheradministrator	Systemintegritätsspezialist	Speicheranzeige
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			
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

Funktion und Aktion	Speicheradministrator	Systemintegritätsspezialist	Speicheranzeige
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
Erstellen, Teilen oder Löschen von Klonen	Ja	Nein	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 Wiederherstellungsklon-Administrator	Backup- und Wiederherstellungs-Viewer
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

Identitäts- und Zugriffs-API

Organisations- und Projekt-IDs

Ihre NetApp Console Konsolenorganisation hat einen Namen und eine ID. Sie können einen Namen für Ihre Organisation auswählen, um sie leichter zu identifizieren.

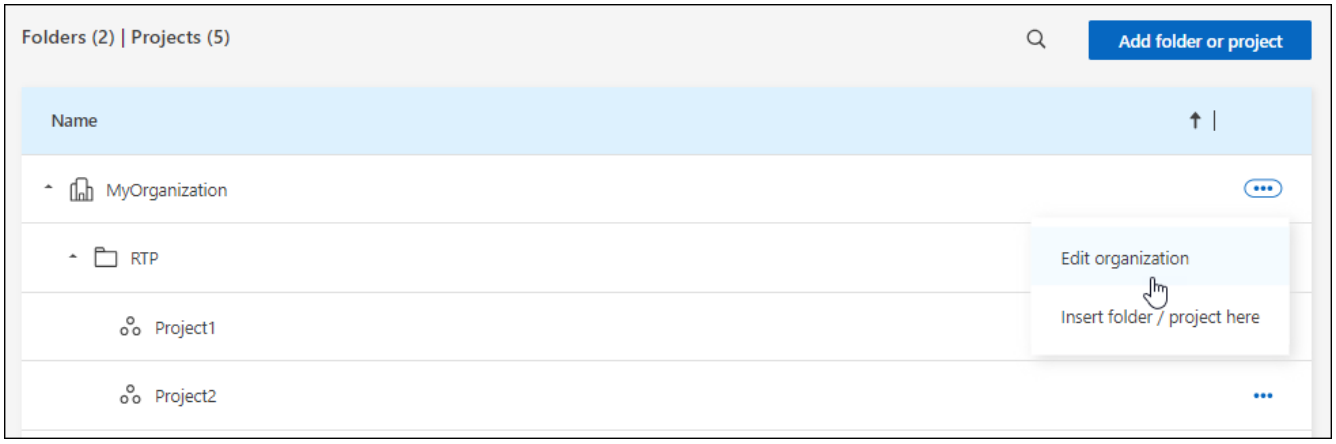
Möglicherweise müssen Sie für bestimmte Integrationen auch die Organisations-ID abrufen.

Benennen Sie Ihre Organisation um

Sie können Ihre Organisation umbenennen. Dies ist hilfreich, wenn Sie mehr als nur die Organisation unterstützen.

Schritte

1. Wählen Sie **Verwaltung > Identität und Zugriff**.
2. Wählen Sie **Organisation** aus.
3. Navigieren Sie auf der Seite **Organisation** zur ersten Zeile in der Tabelle und wählen Sie ••• und wählen Sie dann **Organisation bearbeiten**.



4. Geben Sie einen neuen Organisationsnamen ein und wählen Sie **Übernehmen**.

Abrufen der Organisations-ID

Die Organisations-ID wird für bestimmte Integrationen mit der Konsole verwendet.

Sie können die Organisations-ID auf der Seite „Organisationen“ anzeigen und sie für Ihren Bedarf in die Zwischenablage kopieren.

Schritte

1. Wählen Sie **Verwaltung > Identität und Zugriff** > **Organisation**.
2. Suchen Sie auf der Seite **Organisation** in der Übersichtsleiste nach Ihrer Organisations-ID und kopieren Sie sie in die Zwischenablage. Sie können dies zur späteren Verwendung speichern oder direkt dorthin kopieren, wo Sie es benötigen.

Abrufen der ID für ein Projekt

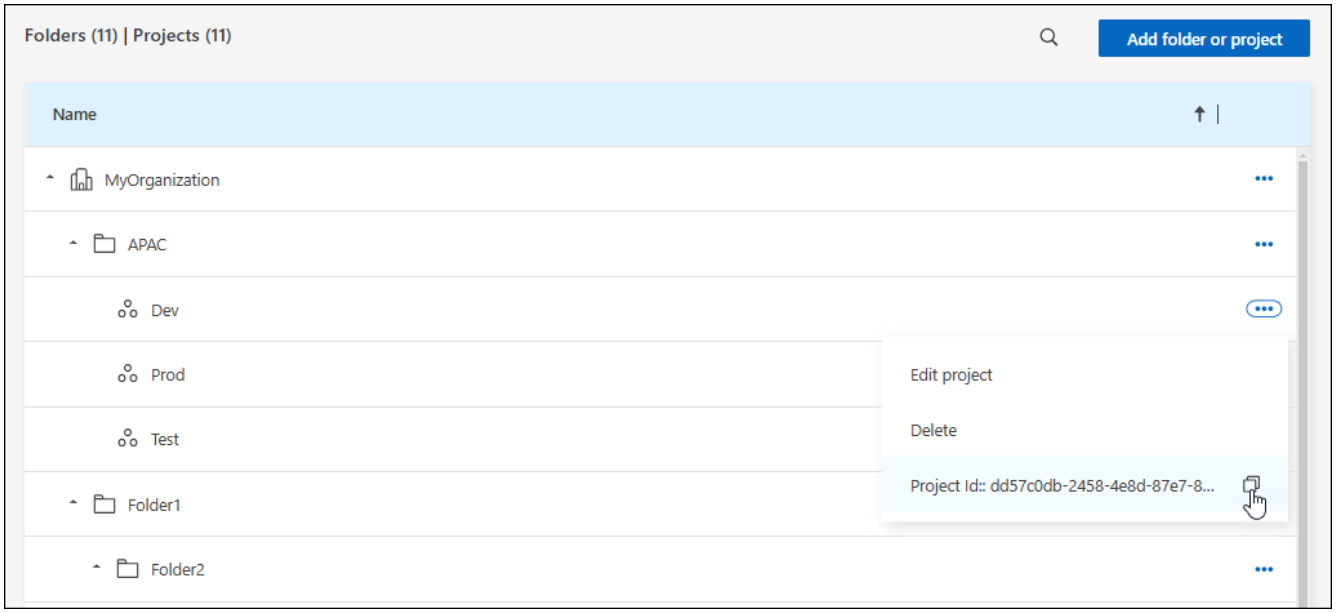
Sie müssen die ID für ein Projekt abrufen, wenn Sie die API verwenden. Beispielsweise beim Erstellen eines Cloud Volumes ONTAP -Systems.

Schritte

1. Navigieren Sie auf der Seite **Organisation** zu einem Projekt in der Tabelle und wählen Sie •••

   Die Projekt-ID wird angezeigt.

2. Um die ID zu kopieren, wählen Sie die Schaltfläche „Kopieren“.



Ähnliche Informationen

- "Erfahren Sie mehr über Identitäts- und Zugriffsverwaltung"
- "Erste Schritte mit Identität und Zugriff"
- "Erfahren Sie mehr über die API für Identität und Zugriff"