Benutzerzugriff verwalten

Active IQ Unified Manager

NetApp
November 13, 2026

This PDF was generated from https://docs.netapp.com/de-de/active-iq-unified-manager-918/config/task_add_users.html on November 13, 2026. Always check docs.netapp.com for the latest.

Inhalt

Benutzerzugriff verwalten . . . 1
- Benutzer hinzufügen . . . 1
  - Hinzufügen von Benutzern in Active IQ Unified Manager . . . 1
  - Erstellen eines Datenbankbenutzers in Active IQ Unified Manager . . . 1
- Benutzereinstellungen in Active IQ Unified Manager bearbeiten . . . 2
- Benutzer in Active IQ Unified Manager anzeigen . . . 3
- Löschen von Benutzern oder Gruppen in Active IQ Unified Manager . . . 3
- Informationen zur rollenbasierten Zugriffssteuerung in Active IQ Unified Manager . . . 3
- Informationen zu Benutzertypen in Active IQ Unified Manager . . . 4
- Informationen zu Benutzerrollen in Active IQ Unified Manager . . . 5
- Informationen zu Benutzerrollen und Berechtigungen in Active IQ Unified Manager . . . 6

Benutzerzugriff verwalten

Benutzer hinzufügen

Hinzufügen von Benutzern in Active IQ Unified Manager

Sie können lokale Benutzer oder Datenbankbenutzer über die Seite „Benutzer“ hinzufügen. Außerdem können Sie Remote-Benutzer oder Gruppen hinzufügen, die zu einem Authentifizierungsserver gehören. Diesen Benutzern können Sie Rollen zuweisen, und auf Grundlage der Berechtigungen dieser Rollen können Benutzer mit Unified Manager die Storage Objekte und Daten managen oder die Daten in einer Datenbank anzeigen.

Bevor Sie beginnen

- Sie benötigen die Rolle des Anwendungsadministrators.
- Um einen Remote-Benutzer oder eine Remote-Gruppe hinzuzufügen, müssen Sie die Remote-Authentifizierung aktiviert und Ihren Authentifizierungsserver konfiguriert haben.
- Wenn Sie die SAML-Authentifizierung so konfigurieren möchten, dass ein Identitätsanbieter (IdP) die Benutzer authentifiziert, die auf die grafische Benutzeroberfläche zugreifen, sollten Sie darauf achten, dass diese Benutzer als “remote” Benutzer definiert sind.

  Der Zugriff auf die Benutzeroberfläche ist für Benutzer vom Typ “local” oder “maintenance” nicht gestattet, wenn die SAML-Authentifizierung aktiviert ist.

Wenn Sie eine Gruppe aus Windows Active Directory hinzufügen, können sich alle direkten Mitglieder und verschachtelten Untergruppen bei Unified Manager authentifizieren, sofern verschachtelte Untergruppen nicht deaktiviert sind. Wenn Sie eine Gruppe aus OpenLDAP oder anderen Authentifizierungs-Services hinzufügen, können sich nur die direkten Mitglieder dieser Gruppe bei Unified Manager authentifizieren.

Schritte

1. Im linken Navigationsbereich erfolgt die Auswahl von **Allgemein** > **Benutzer**.
2. Auf der Seite „Benutzer“ erfolgt ein Klick auf **Hinzufügen**.
3. Im Dialogfeld „Benutzer hinzufügen“ erfolgt die Auswahl des Benutzertyps, den Sie hinzufügen möchten, sowie die Eingabe der erforderlichen Informationen.

   Bei der Eingabe der erforderlichen Benutzerinformationen müssen Sie eine E-Mail-Adresse angeben, die für diesen Benutzer eindeutig ist. E-Mail-Adressen, die von mehreren Benutzern gemeinsam genutzt werden, dürfen nicht angegeben werden.

4. Klicken Sie auf **Add**.

Erstellen eines Datenbankbenutzers in Active IQ Unified Manager

Um eine Verbindung zwischen Workflow Automation und Unified Manager zu unterstützen oder auf Datenbankansichten zuzugreifen, müssen Sie zunächst in der Unified Manager web UI einen Datenbankbenutzer mit der Rolle Integration Schema oder Report Schema erstellen.

Bevor Sie beginnen

Sie benötigen die Rolle des Anwendungsadministrators.

Datenbankbenutzer ermöglichen die Integration mit Workflow Automation und den Zugriff auf berichtsspezifische Datenbankansichten. Datenbankbenutzer haben keinen Zugriff auf die Web-UI von Unified Manager oder die Wartungs-Managementplattform und können keine API-Aufrufe ausführen.

Schritte

1. Im linken Navigationsbereich erfolgt die Auswahl von **Allgemein** > **Benutzer**.
2. Auf der Seite „Benutzer“ wählen Sie **Hinzufügen** aus.
3. Im Dialogfeld „Benutzer hinzufügen“ ist in der Dropdown-Liste „Typ“ die Option „Datenbankbenutzer“ auszuwählen.
4. Für den Datenbankbenutzer werden ein Name und ein Passwort eingegeben.
5. In der Dropdown-Liste **Rolle** wird die passende Rolle gewählt.

Wenn Sie…	Diese Rolle auswählen
Verbinden von Unified Manager mit Workflow Automation	Integrationsschema
Zugriff auf Berichte und andere Datenbankansichten	Berichtsschema

6. Klicken Sie auf **Add**.

Benutzereinstellungen in Active IQ Unified Manager bearbeiten

Sie können die Benutzereinstellungen, wie E-Mail-Adresse und Rolle, bearbeiten, die für jeden Benutzer festgelegt sind. Beispielsweise können Sie die Rolle eines Benutzers ändern, der ein Storage-Operator ist, und dem Benutzer Storage-Administratorrechte zuweisen.

Bevor Sie beginnen

Sie benötigen die Rolle des Anwendungsadministrators.

Wenn Sie die einem Benutzer zugewiesene Rolle ändern, werden die Änderungen übernommen, sobald eine der folgenden Aktionen eintritt:

- Der Benutzer meldet sich ab und wieder bei Unified Manager an.
- Die Sitzungszeitüberschreitung von 24 Stunden ist erreicht.

Schritte

1. Im linken Navigationsbereich erfolgt die Auswahl von **Allgemein** > **Benutzer**.
2. Auf der Seite „Benutzer“ den Benutzer auswählen, dessen Einstellungen bearbeitet werden sollen, und auf **Edit** klicken.
3. Im Dialogfeld „Benutzer bearbeiten“ können Sie die für den Benutzer festgelegten Einstellungen bearbeiten.

4. Auf **Speichern** klicken.

Benutzer in Active IQ Unified Manager anzeigen

Auf der Seite „Benutzer“ kann die Liste der Benutzer angezeigt werden, die Storage Objekte und Daten mit Unified Manager managen. Dort können Details zu den Benutzern angezeigt werden, z. B. Benutzername, Benutzertyp, E-Mail-Adresse und die den Benutzern zugewiesene Rolle.

Bevor Sie beginnen

Sie benötigen die Rolle des Anwendungsadministrators.

Schritt

1. Im linken Navigationsbereich erfolgt die Auswahl von **Allgemein** > **Benutzer**.

Löschen von Benutzern oder Gruppen in Active IQ Unified Manager

Sie können einen oder mehrere Benutzer aus der Datenbank des Managementservers löschen, um bestimmten Benutzern den Zugriff auf Unified Manager zu verweigern. Sie können auch Gruppen löschen, sodass alle Benutzer dieser Gruppe keinen Zugriff mehr auf den Managementserver haben.

Bevor Sie beginnen

- Wenn Sie Remote-Gruppen löschen, müssen Sie die den Benutzern der Remote-Gruppen zugewiesenen Ereignisse zuvor neu zugewiesen haben.

  Wenn Sie lokale Benutzer oder Remote-Benutzer löschen, wird die Zuweisung der diesen Benutzern zugewiesenen Ereignisse automatisch aufgehoben.

- Sie benötigen die Rolle des Anwendungsadministrators.

Schritte

1. Im linken Navigationsbereich erfolgt die Auswahl von **Allgemein** > **Benutzer**.
2. Auf der Seite „Benutzer“ erfolgt die Auswahl der Benutzer oder Gruppen, die gelöscht werden sollen; anschließend erfolgt ein Klick auf **Löschen**.
3. Zum Bestätigen der Löschung auf **Ja** klicken.

Informationen zur rollenbasierten Zugriffssteuerung in Active IQ Unified Manager

RBAC (rollenbasierte Zugriffssteuerung) bietet die Möglichkeit, zu steuern, wer Zugriff auf verschiedene Funktionen und Ressourcen auf dem Active IQ Unified Manager Server hat. RBAC ermöglicht Administratoren die Verwaltung von Benutzergruppen durch die Definition von Rollen. Wenn der Zugriff auf bestimmte Funktionen auf ausgewählte Administratoren beschränkt werden muss, müssen für diese Administratorkonten eingerichtet werden. Wenn die Informationen, die Administratoren anzeigen können, und

die Vorgänge, die sie ausführen können, eingeschränkt werden sollen, müssen den erstellten Administratorkonten Rollen zugewiesen werden.

Der Verwaltungsserver verwendet rollenbasierte Zugriffskontrolle (RBAC) für die Benutzeranmeldung und Rollenberechtigungen. Wenn Sie die Standardeinstellungen des Verwaltungsservers für den administrativen Benutzerzugriff nicht geändert haben, müssen Sie sich nicht anmelden, um diese anzuzeigen.

Wenn Sie einen Vorgang initiieren, der bestimmte Berechtigungen erfordert, fordert der Managementserver Sie zur Anmeldung auf. Um beispielsweise Administratorkonten zu erstellen, müssen Sie sich mit einem Konto mit Zugriff als Application Administrator anmelden.

Informationen zu Benutzertypen in Active IQ Unified Manager

Ein Benutzertyp legt die Art des Benutzerkontos fest und umfasst Remote-Benutzer, Remote-Gruppen, lokale Benutzer, Datenbankbenutzer und Wartungsbenutzer. Jeder dieser Typen hat eine eigene Rolle, die ein Benutzer mit der Rolle „Administrator“ zuweist.

Die Unified Manager Benutzertypen sind wie folgt:

- **Wartungsbenutzer**

  Wird bei der Erstkonfiguration von Unified Manager erstellt. Der Wartungsbenutzer erstellt anschließend weitere Benutzer und weist ihnen Rollen zu. Der Wartungsbenutzer ist außerdem der einzige Benutzer mit Zugriff auf die Managementplattform. Wenn Unified Manager auf einem Red Hat Enterprise Linux-System installiert wird, erhält der Wartungsbenutzer den Benutzernamen “umadmin.”

- **Lokaler Benutzer**

  Greift auf die Unified Manager-Benutzeroberfläche zu und führt je nach der vom Wartungsbenutzer oder von einem Benutzer mit der Rolle "Application Administrator" zugewiesenen Rolle Funktionen aus.

- **Remote-Gruppe**

  Eine Gruppe von Benutzern, die mit den auf dem Authentifizierungsserver gespeicherten Anmeldedaten auf die Unified Manager UI zugreifen. Der Name dieses Kontos sollte mit dem Namen einer auf dem Authentifizierungsserver gespeicherten Gruppe übereinstimmen. Alle Benutzer innerhalb der Remote-Gruppe erhalten mit ihren individuellen Benutzeranmeldeinformationen Zugriff auf die Unified Manager UI. Remote-Gruppen können entsprechend ihren zugewiesenen Rollen Funktionen ausführen.

- **Remote-Benutzer**

  Der Zugriff auf die Unified Manager UI erfolgt mithilfe der Anmeldedaten, die auf dem Authentifizierungsserver gespeichert sind. Ein Remote-Benutzer führt Funktionen basierend auf der Rolle aus, die ihm vom Wartungsbenutzer oder von einem Benutzer mit der Rolle „Application Administrator“ zugewiesen wurde.

- **Datenbankbenutzer**

  Verfügt über Lesezugriff auf Daten in der Unified Manager Datenbank, hat keinen Zugriff auf die Unified Manager Weboberfläche oder die Wartungsmanagementplattform und kann keine API-Aufrufe ausführen.

Informationen zu Benutzerrollen in Active IQ Unified Manager

Der Wartungsbenutzer oder Anwendungsadministrator weist jedem Benutzer eine Rolle zu. Jede Rolle beinhaltet bestimmte Berechtigungen. Der Umfang der Aktivitäten, die Sie im Unified Manager ausführen können, hängt von Ihrer zugewiesenen Rolle und den damit verbundenen Berechtigungen ab.

Unified Manager umfasst die folgenden vordefinierten Benutzerrollen:

- **Operator**

  Zeigt Storage-Systeminformationen und andere von Unified Manager erfasste Daten an, einschließlich Verlaufsdaten und Kapazitätstrends. Diese Rolle ermöglicht dem Storage-Operator, Ereignisse anzuzeigen, zuzuweisen, zu bestätigen, zu beheben und mit Notizen zu versehen.

- **Storage-Administrator**

  Konfiguriert Storage-Managementvorgänge in Unified Manager. Diese Rolle ermöglicht dem Storage-Administrator die Konfiguration von Schwellenwerten sowie die Erstellung von Warnungen und anderen spezifischen Optionen und Richtlinien für das Storage-Management.

- **Anwendungsadministrator**

  Konfiguriert Einstellungen, die nicht mit dem Storage-Management zusammenhängen. Diese Rolle ermöglicht die Verwaltung von Benutzern, Sicherheitszertifikaten, Datenbankzugriff und administrativen Optionen, einschließlich Authentifizierung, SMTP, Netzwerk und AutoSupport.

  Bei der Installation von Unified Manager auf Linux-Systemen erhält der erste Benutzer mit der Rolle des Anwendungsadministrators automatisch den Namen “umadmin”.

- **Integrationsschema**

  Diese Rolle ermöglicht schreibgeschützten Zugriff auf Unified Manager Datenbankansichten zur Integration von Unified Manager mit OnCommand Workflow Automation (WFA).

- **Berichtsschema**

  Diese Rolle ermöglicht schreibgeschützten Zugriff auf Berichte und andere Datenbankansichten direkt aus der Unified Manager Datenbank. Zu den einsehbaren Datenbanken gehören:

  - netapp_model_view
  - netapp_performance
  - ocum
  - ocum_report
  - ocum_report_birt
  - opm
  - scalemonitor

Informationen zu Benutzerrollen und Berechtigungen in Active IQ Unified Manager

Anhand Ihrer zugewiesenen Benutzerrolle können Sie ermitteln, welche Operationen Sie im Unified Manager durchführen können.

Die folgende Tabelle zeigt die Funktionen, die jede Benutzerrolle ausführen kann:

Funktion	Operator	Storage-Administrator	Anwendungsadministrator	Integrationsschema	Berichtsschema
Anzeigen von Informationen zum Storage-System	•	•	•	•	•
Andere Daten wie z. B. Verläufe und Kapazitätstrends lassen sich anzeigen.	•	•	•	•	•
Ereignisse anzeigen, zuweisen und beheben	•	•	•		
Storage-Service-Objekte wie SVM-Zuordnungen und Ressourcenpools anzeigen	•	•	•		
Anzeige von Schwellenwertrichtlinien	•	•	•		
Management von Storage-Serviceobjekten wie SVM-Zuordnungen und Ressourcenpools		•	•		
Warnmeldungen definieren		•	•		
Storage-Managementoptionen managen		•	•		

Funktion	Operator	Storage-Administrator	Anwendungsadministrator	Integrationsschema	Berichtsschema
Storage-Managementrichtlinien managen		•	•		
Benutzer verwalten			•		
Administrative Optionen managen			•		
Definition von Schwellenwertrichtlinien			•		
Datenbankzugriff managen			•		
Integration mit WFA managen und Zugriff auf die Datenbankansichten gewähren				•	
Berichte planen und speichern		•	•		
Ausführung von “Fix It”-Vorgängen über Management Actions		•	•		
Bereitstellung von schreibgeschütztem Zugriff auf Datenbankansichten					•

Copyright-Informationen

Copyright © 2026 NetApp. Alle Rechte vorbehalten. Gedruckt in den USA. Dieses urheberrechtlich geschützte Dokument darf ohne die vorherige schriftliche Genehmigung des Urheberrechtsinhabers in keiner Form und durch keine Mittel – weder grafische noch elektronische oder mechanische, einschließlich Fotokopieren, Aufnehmen oder Speichern in einem elektronischen Abrufsystem – auch nicht in Teilen, vervielfältigt werden.

Software, die von urheberrechtlich geschütztem NetApp Material abgeleitet wird, unterliegt der folgenden Lizenz und dem folgenden Haftungsausschluss:

DIE VORLIEGENDE SOFTWARE WIRD IN DER VORLIEGENDEN FORM VON NETAPP ZUR VERFÜGUNG GESTELLT, D. H. OHNE JEGLICHE EXPLIZITE ODER IMPLIZITE GEWÄHRLEISTUNG, EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKT AUF DIE STILLSCHWEIGENDE GEWÄHRLEISTUNG DER MARKTGÄNGIGKEIT UND EIGNUNG FÜR EINEN BESTIMMTEN ZWECK, DIE HIERMIT AUSGESCHLOSSEN WERDEN. NETAPP ÜBERNIMMT KEINERLEI HAFTUNG FÜR DIREKTE, INDIREKTE, ZUFÄLLIGE, BESONDERE, BEISPIELHAFTE SCHÄDEN ODER FOLGESCHÄDEN (EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKT AUF DIE BESCHAFFUNG VON ERSATZWAREN ODER -DIENSTLEISTUNGEN, NUTZUNGS-, DATEN- ODER GEWINNVERLUSTE ODER UNTERBRECHUNG DES GESCHÄFTSBETRIEBS), UNABHÄNGIG DAVON, WIE SIE VERURSACHT WURDEN UND AUF WELCHER HAFTUNGSTHEORIE SIE BERUHEN, OB AUS VERTRAGLICH FESTGELEGTER HAFTUNG, VERSCHULDENSUNABHÄNGIGER HAFTUNG ODER DELIKTSHAFTUNG (EINSCHLIESSLICH FAHRLÄSSIGKEIT ODER AUF ANDEREM WEGE), DIE IN IRGENDEINER WEISE AUS DER NUTZUNG DIESER SOFTWARE RESULTIEREN, SELBST WENN AUF DIE MÖGLICHKEIT DERARTIGER SCHÄDEN HINGEWIESEN WURDE.

NetApp behält sich das Recht vor, die hierin beschriebenen Produkte jederzeit und ohne Vorankündigung zu ändern. NetApp übernimmt keine Verantwortung oder Haftung, die sich aus der Verwendung der hier beschriebenen Produkte ergibt, es sei denn, NetApp hat dem ausdrücklich in schriftlicher Form zugestimmt. Die Verwendung oder der Erwerb dieses Produkts stellt keine Lizenzierung im Rahmen eines Patentrechts, Markenrechts oder eines anderen Rechts an geistigem Eigentum von NetApp dar.

Das in diesem Dokument beschriebene Produkt kann durch ein oder mehrere US-amerikanische Patente, ausländische Patente oder anhängige Patentanmeldungen geschützt sein.

ERLÄUTERUNG ZU „RESTRICTED RIGHTS“: Nutzung, Vervielfältigung oder Offenlegung durch die US-Regierung unterliegt den Einschränkungen gemäß Unterabschnitt (b)(3) der Klausel „Rights in Technical Data – Noncommercial Items“ in DFARS 252.227-7013 (Februar 2014) und FAR 52.227-19 (Dezember 2007).

Die hierin enthaltenen Daten beziehen sich auf ein kommerzielles Produkt und/oder einen kommerziellen Service (wie in FAR 2.101 definiert) und sind Eigentum von NetApp, Inc. Alle technischen Daten und die Computersoftware von NetApp, die unter diesem Vertrag bereitgestellt werden, sind gewerblicher Natur und wurden ausschließlich unter Verwendung privater Mittel entwickelt. Die US-Regierung besitzt eine nicht ausschließliche, nicht übertragbare, nicht unterlizenzierbare, weltweite, limitierte unwiderrufliche Lizenz zur Nutzung der Daten nur in Verbindung mit und zur Unterstützung des Vertrags der US-Regierung, unter dem die Daten bereitgestellt wurden. Sofern in den vorliegenden Bedingungen nicht anders angegeben, dürfen die Daten ohne vorherige schriftliche Genehmigung von NetApp, Inc. nicht verwendet, offengelegt, vervielfältigt, geändert, aufgeführt oder angezeigt werden. Die Lizenzrechte der US-Regierung für das US-Verteidigungsministerium sind auf die in DFARS-Klausel 252.227-7015(b) (Februar 2014) genannten Rechte beschränkt.

Markeninformationen

NETAPP, das NETAPP Logo und die unter http://www.netapp.com/TM aufgeführten Marken sind Marken von NetApp, Inc. Andere Firmen und Produktnamen können Marken der jeweiligen Eigentümer sein.