Verwalten des Benutzerzugriffs

Active IQ Unified Manager 9.10

NetApp
October 16, 2025

This PDF was generated from https://docs.netapp.com/de-de/active-iq-unified-manager-910/config/task_create_database_user.html on October 16, 2025. Always check docs.netapp.com for the latest.

Inhalt

Verwalten des Benutzerzugriffs . . . 1
- Benutzer hinzufügen . . . 1
  - Erstellen eines Datenbankbenutzers . . . 1
- Bearbeiten der Benutzereinstellungen . . . 2
- Anzeigen von Benutzern . . . 3
- Benutzer oder Gruppen werden gelöscht . . . 3
- Was RBAC ist . . . 3
- Was ist die rollenbasierte Zugriffssteuerung . . . 4
- Definitionen der Benutzertypen . . . 4
- Definitionen von Benutzerrollen . . . 5
- Unified Manager Benutzer-Rollen und -Funktionen . . . 6

Verwalten des Benutzerzugriffs

Sie können Rollen erstellen und Funktionen zuweisen, um den Benutzerzugriff auf ausgewählte Cluster-Objekte zu steuern. Sie können Benutzer identifizieren, die über die erforderlichen Funktionen für den Zugriff auf ausgewählte Objekte in einem Cluster verfügen. Nur diese Benutzer haben Zugriff, um Cluster-Objekte zu managen.

Benutzer hinzufügen

Sie können lokale Benutzer oder Datenbankbenutzer über die Seite Benutzer hinzufügen. Sie können auch Remote-Benutzer oder -Gruppen hinzufügen, die zu einem Authentifizierungsserver gehören. Sie können diesen Benutzern Rollen zuweisen. Anhand der Berechtigungen der Rollen können Benutzer Storage-Objekte und -Daten mit Unified Manager managen oder die Daten in einer Datenbank anzeigen.

Was Sie brauchen

- Sie müssen über die Anwendungsadministratorrolle verfügen.
- Um einen Remote-Benutzer oder eine Remotegruppe hinzuzufügen, müssen Sie die Remote-Authentifizierung aktiviert und Ihren Authentifizierungsserver konfiguriert haben.
- Wenn Sie die SAML-Authentifizierung so konfigurieren möchten, dass ein Identitäts-Provider (IdP) Benutzer authentifiziert, die auf die grafische Schnittstelle zugreifen, stellen Sie sicher, dass diese Benutzer als „`remote`“-Benutzer definiert sind.

  Der Zugriff auf die Benutzeroberfläche ist Benutzern vom Typ „`local`“ oder „`maintBuße`“ nicht erlaubt, wenn die SAML-Authentifizierung aktiviert ist.

Wenn Sie eine Gruppe aus Windows Active Directory hinzufügen, können sich alle direkten Mitglieder und geschachtelten Untergruppen bei Unified Manager authentifizieren, es sei denn, geschachtelte Untergruppen sind deaktiviert. Wenn Sie eine Gruppe von OpenLDAP oder anderen Authentifizierungsdiensten hinzufügen, können sich nur die direkten Mitglieder dieser Gruppe bei Unified Manager authentifizieren.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Allgemein** > **Benutzer**.
2. Klicken Sie auf der Seite Benutzer auf **Hinzufügen**.
3. Wählen Sie im Dialogfeld Benutzer hinzufügen den Benutzertyp aus, den Sie hinzufügen möchten, und geben Sie die erforderlichen Informationen ein.

   Wenn Sie die erforderlichen Benutzerinformationen eingeben, müssen Sie eine E-Mail-Adresse angeben, die für diesen Benutzer eindeutig ist. Sie müssen vermeiden, E-Mail-Adressen anzugeben, die von mehreren Benutzern gemeinsam verwendet werden.

4. Klicken Sie Auf **Hinzufügen**.

Erstellen eines Datenbankbenutzers

Um eine Verbindung zwischen Workflow Automation und Unified Manager zu unterstützen oder auf Datenbankansichten zuzugreifen, müssen Sie in der

Weboberfläche von Unified Manager zunächst einen Datenbankbenutzer mit dem Integrations-Schema oder dem Berichtschema erstellen.

Was Sie brauchen

Sie müssen über die Anwendungsadministratorrolle verfügen.

Datenbankbenutzer ermöglichen die Integration in Workflow Automation und den Zugriff auf Berichtsspezifische Datenbankansichten. Datenbankbenutzer haben keinen Zugriff auf die Unified Manager Web-UI oder die Wartungskonsole und können keine API-Aufrufe ausführen.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Allgemein** > **Benutzer**.
2. Klicken Sie auf der Seite Benutzer auf **Hinzufügen**.
3. Wählen Sie im Dialogfeld Benutzer hinzufügen in der Dropdown-Liste **Typ** die Option **Datenbankbenutzer** aus.
4. Geben Sie einen Namen und ein Kennwort für den Datenbankbenutzer ein.
5. Wählen Sie in der Dropdown-Liste **Rolle** die entsprechende Rolle aus.

Ihr Unternehmen	Wählen Sie diese Rolle aus
Verbindung von Unified Manager mit Workflow Automation	Integrationsschema
Zugriff auf Berichtsdaten und andere Datenbankansichten	Berichtschema

6. Klicken Sie Auf **Hinzufügen**.

Bearbeiten der Benutzereinstellungen

Sie können Benutzereinstellungen bearbeiten, z. B. die E-Mail-Adresse und die Rolle, die jeder Benutzer angegeben hat. Beispielsweise können Sie die Rolle eines Benutzers, der ein Speicheroperator ist, ändern und dem Benutzer Berechtigungen für Speicheradministratoren zuweisen.

Was Sie brauchen

Sie müssen über die Anwendungsadministratorrolle verfügen.

Wenn Sie die Rolle ändern, die einem Benutzer zugewiesen ist, werden die Änderungen angewendet, wenn eine der folgenden Aktionen ausgeführt wird:

- Der Benutzer meldet sich bei Unified Manager ab und meldet sich zurück.
- Das Sitzungszeitlimit von 24 Stunden wird erreicht.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Allgemein** > **Benutzer**.

2. Wählen Sie auf der Benutzerseite den Benutzer aus, für den Sie die Einstellungen bearbeiten möchten, und klicken Sie auf **Bearbeiten**.
3. Bearbeiten Sie im Dialogfeld Benutzer bearbeiten die entsprechenden Einstellungen, die für den Benutzer angegeben sind.
4. Klicken Sie Auf **Speichern**.

Anzeigen von Benutzern

Sie können die Seite Benutzer verwenden, um eine Liste der Benutzer anzuzeigen, die Storage-Objekte und Daten mit Unified Manager managen. Sie können Details zu den Benutzern anzeigen, z. B. den Benutzernamen, den Benutzertyp, die E-Mail-Adresse und die Rolle, die den Benutzern zugewiesen ist.

Was Sie brauchen

Sie müssen über die Anwendungsadministratorrolle verfügen.

Schritt

1. Klicken Sie im linken Navigationsbereich auf **Allgemein** > **Benutzer**.

Benutzer oder Gruppen werden gelöscht

Sie können einen oder mehrere Benutzer aus der Management-Server-Datenbank löschen, um den Zugriff bestimmter Benutzer auf Unified Manager zu verhindern. Sie können auch Gruppen löschen, sodass alle Benutzer der Gruppe nicht mehr auf den Verwaltungsserver zugreifen können.

Was Sie brauchen

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

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

- Sie müssen über die Anwendungsadministratorrolle verfügen.

Schritte

1. Klicken Sie im linken Navigationsbereich auf **Allgemein** > **Benutzer**.
2. Wählen Sie auf der Seite Benutzer die Benutzer oder Gruppen aus, die Sie löschen möchten, und klicken Sie dann auf **Löschen**.
3. Klicken Sie auf **Ja**, um den Löschvorgang zu bestätigen.

Was RBAC ist

RBAC (rollenbasierte Zugriffssteuerung) bietet die Möglichkeit, zu steuern, wer Zugriff auf verschiedene Funktionen und Ressourcen im Active IQ Unified Manager Server hat.

Was ist die rollenbasierte Zugriffssteuerung

Die rollenbasierte Zugriffssteuerung (Role Based Access Control, RBAC) ermöglicht Administratoren das Management von Benutzergruppen, indem sie Rollen definieren. Wenn Sie den Zugriff auf bestimmte Funktionen auf ausgewählte Administratoren beschränken müssen, müssen Sie Administratorkonten für diese einrichten. Wenn Sie die Informationen beschränken möchten, die Administratoren anzeigen können, und die Vorgänge, die sie ausführen können, müssen Sie Rollen auf die von Ihnen erstellten Administratorkonten anwenden.

Der Verwaltungsserver verwendet RBAC für Benutzeranmeldung und Rollenberechtigungen. Wenn Sie die Standardeinstellungen des Managementservers für den Administratorbenutzerzugriff nicht geändert haben, müssen Sie sich nicht anmelden, um sie anzuzeigen.

Wenn Sie einen Vorgang initiieren, der bestimmte Berechtigungen benötigt, fordert der Verwaltungsserver Sie zur Anmeldung auf. Zum Erstellen von Administratorkonten müssen Sie sich beispielsweise mit dem Zugriff auf das Anwendungsadministrator-Konto anmelden.

Definitionen der Benutzertypen

Ein Benutzertyp gibt die Art des Kontos an, das der Benutzer besitzt und umfasst Remote-Benutzer, Remote-Gruppen, lokale Benutzer, Datenbankbenutzer und Wartungbenutzer. Jeder dieser Typen hat seine eigene Rolle, die von einem Benutzer mit der Rolle „Administrator“ zugewiesen wird.

Unified Manager-Benutzertypen sind wie folgt:

- **Benutzer der Wartung**

  Erstellt während der Erstkonfiguration von Unified Manager. Der Wartungsbenutzer erstellt dann weitere Benutzer und weist Rollen zu. Der Benutzer der Wartung ist außerdem der einzige Benutzer, der Zugriff auf die Wartungskonsole hat. Wenn Unified Manager auf einem Red hat Enterprise Linux- oder CentOS-System installiert ist, erhält der Wartungbenutzer den Benutzernamen „`umadmin`.“.

- **Lokaler Benutzer**

  Greift auf die Unified Manager-Benutzeroberfläche zu und führt Funktionen basierend auf der Rolle durch, die der Wartungsbenutzer oder ein Benutzer mit der Anwendungsadministratorrolle angegeben hat.

- **Remote-Gruppe**

  Eine Gruppe von Benutzern, die mit den auf dem Authentifizierungsserver gespeicherten Anmeldeinformationen auf die Benutzeroberfläche von Unified Manager zugreifen. Der Name dieses Kontos muss mit dem Namen einer auf dem Authentifizierungsserver gespeicherten Gruppe übereinstimmen. Allen Benutzern innerhalb der Remote-Gruppe wird über ihre individuellen Benutzeranmeldeinformationen der Zugriff auf die Unified Manager-Benutzeroberfläche gewährt. Remote-Gruppen können Funktionen entsprechend ihren zugewiesenen Rollen ausführen.

- **Remote-Benutzer**

  Greift über die auf den Authentifizierungsserver gespeicherten Anmeldeinformationen auf die Unified

Manager-UI zu. Ein Remote-Benutzer führt Funktionen basierend auf der Rolle aus, die der Wartungsbenutzer oder ein Benutzer mit der Anwendungsadministratorrolle angegeben hat.

- **Datenbankbenutzer**

  Hat schreibgeschützten Zugriff auf Daten in der Unified Manager-Datenbank, hat keinen Zugriff auf die Unified Manager-Webschnittstelle oder die Wartungskonsole und kann keine API-Aufrufe ausführen.

Definitionen von Benutzerrollen

Der Wartungsbenutzer oder der Anwendungsadministrator weist jedem Benutzer eine Rolle zu. Jede Rolle enthält bestimmte Berechtigungen. Der Umfang der Aktivitäten, die Sie in Unified Manager ausführen können, hängt von der Ihnen zugewiesenen Rolle ab und welchen Berechtigungen die Rolle enthält.

Unified Manager enthält die folgenden vordefinierten Benutzerrollen:

- **Betreiber**

  Anzeige von Storage-Systeminformationen und anderen von Unified Manager erfassten Daten, einschließlich Verläufe und Kapazitätstrends Mit dieser Rolle kann der Speicherbetreiber Notizen zu den Ereignissen anzeigen, zuweisen, bestätigen, auflösen und hinzufügen.

- * Storage Administrator*

  Konfiguration von Storage-Managementvorgängen in Unified Manager Diese Rolle ermöglicht es dem Storage-Administrator, Schwellenwerte zu konfigurieren und Alarme sowie andere für das Storage-Management spezifische Optionen und Richtlinien zu erstellen.

- **Anwendungsadministrator**

  Konfiguriert Einstellungen, die in keinem Zusammenhang mit dem Storage-Management stehen. Diese Rolle ermöglicht das Management von Benutzern, Sicherheitszertifikaten, Datenbankzugriff und Verwaltungsoptionen, einschließlich Authentifizierung, SMTP, Networking und AutoSupport.

  Wenn Unified Manager auf Linux-Systemen installiert wird, heißt der erste Benutzer mit der Anwendungsadministratorrolle automatisch „`umadmin`“.

- **Integrationsschema**

  Diese Rolle bietet schreibgeschützten Zugriff auf Unified Manager Datenbankansichten für die Integration von Unified Manager mit OnCommand Workflow Automation (WFA).

- **Schema Melden**

  Diese Rolle ermöglicht einen schreibgeschützten Zugriff auf Reporting und andere Datenbankansichten direkt aus der Unified Manager Datenbank. Folgende Datenbanken stehen zur Verfügung:

  - netapp_Modell_Ansicht
  - netapp_Performance
  - Okum

- Ocum_Report
- Ocum_Report_birt
- opm
- Skalemonitor

Unified Manager Benutzer-Rollen und -Funktionen

Anhand der Ihnen zugewiesenen Benutzerrolle können Sie festlegen, welche Vorgänge Sie in Unified Manager ausführen können.

In der folgenden Tabelle sind die Funktionen aufgeführt, die die einzelnen Benutzerrollen ausführen können:

Funktion	Operator	Storage-Administrator	Applikationsadministrator	Integrationsschema	Berichtschema
Anzeigen von Speichersysteminformationen	•	•	•	•	•
Andere Daten wie Verläufe und Kapazitätstrends anzeigen	•	•	•	•	•
Ereignisse anzeigen, zuweisen und lösen	•	•	•		
Anzeigen von Storage-Serviceobjekten, z. B. SVM-Zuordnungen und Ressourcenpools	•	•	•		
Anzeigen von Schwellenwertrichtlinien	•	•	•		

Funktion	Operator	Storage-Administrator	Applikationsadministrator	Integrationsschema	Berichtschema
Management von Storage-Serviceobjekten wie SVM-Zuordnungen und Ressourcenpools		•	•		
Definieren von Warnmeldungen		•	•		
Optionen für das Storage Management managen		•	•		
Storage Management-Richtlinien managen		•	•		
Benutzer managen			•		
Management von Verwaltungsoptionen			•		
Definieren Sie Schwellenwertrichtlinien			•		
Datenbankzugriff managen			•		
Managen Sie die Integration in WFA und erhalten Sie Zugriff auf die Datenbankansichten				•	

Funktion	Operator	Storage-Administrator	Applikationsadministrator	Integrationsschema	Berichtschema
Planen und Speichern von Berichten		•	•		
Führen Sie „`Fix IT`“-Vorgänge aus Management Actions aus		•	•		
Schreibgeschützter Zugriff auf Datenbankansichten					•

Copyright-Informationen

Copyright © 2025 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.