Verwalten des Benutzerzugriffs

OnCommand Unified Manager 9.5

NetApp
October 23, 2024

Inhalt

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 Verwaltung/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.

Bevor Sie beginnen

- Sie müssen die OnCommand-Administratorrolle besitzen.
- 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.

Über diese Aufgabe

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 in der Symbolleiste auf  , und klicken Sie dann im linken Menü Verwaltung auf **Benutzer**.
2. Klicken Sie auf der Seite **Verwaltung/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**.

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.

Bevor Sie beginnen

Sie müssen die OnCommand-Administratorrolle besitzen.

Über diese Aufgabe

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 in der Symbolleiste auf , und klicken Sie dann im linken Menü Verwaltung auf **Benutzer**.
2. Wählen Sie auf der Seite **Verwaltung/Benutzer** 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**.

Testen eines Remote-Benutzers oder einer Remote-Gruppe

Sie können überprüfen, ob ein Remote-Benutzer oder eine Remote-Gruppe auf den Unified Manager-Server zugreifen kann, indem Sie die für Ihre Authentifizierungsserver festgelegten Authentifizierungseinstellungen verwenden.

Bevor Sie beginnen

- Sie müssen die Remote-Authentifizierung aktiviert und die Authentifizierungseinstellungen so konfiguriert haben, dass der Unified Manager-Server den Remote-Benutzer oder die Remote-Gruppe validieren kann.
- Sie müssen die OnCommand-Administratorrolle besitzen.

Schritte

1. Klicken Sie in der Symbolleiste auf , und klicken Sie dann im linken Menü Verwaltung auf **Benutzer**.
2. Wählen Sie auf der Seite * Management/Users* einen Remote-Benutzer oder eine Remote-Gruppe aus, die Sie validieren möchten, und klicken Sie dann auf **Test**.

Anzeigen von Benutzern

Sie können die Seite „Management/Benutzer“ verwenden, um die 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.

Bevor Sie beginnen

Sie müssen die OnCommand-Administratorrolle besitzen.

Schritte

1. Klicken Sie in der Symbolleiste auf , und klicken Sie dann im linken Menü Verwaltung auf **Benutzer**.

   Die Liste der Benutzer wird auf der Seite Verwaltung/Benutzer angezeigt.

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.

Bevor Sie beginnen

- 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 die OnCommand-Administratorrolle besitzen.

Schritte

1. Klicken Sie in der Symbolleiste auf , und klicken Sie dann im linken Menü Verwaltung auf **Benutzer**.
2. Wählen Sie auf der Seite **Verwaltung/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.

Ändern des lokalen Benutzerpassworts

Sie können Ihr lokales Benutzeranmeldeswort ändern, um potenzielle Sicherheitsrisiken zu vermeiden.

Bevor Sie beginnen

Sie müssen als lokaler Benutzer angemeldet sein.

Über diese Aufgabe

Die Passwörter für den Wartungsbenutzer und für Remote-Benutzer können mit diesen Schritten nicht geändert werden. Wenden Sie sich an Ihren Passwortadministrator, um ein Kennwort für Remote-Benutzer zu ändern. Informationen zum Ändern des Wartungs-Benutzerpassworts finden Sie unter "Verwenden der Wartungskonsole".

Schritte

1. Melden Sie sich bei Unified Manager an.
2. Klicken Sie in der oberen Menüleiste auf das Benutzersymbol und dann auf **Passwort ändern**.

   Die Option **Passwort ändern** wird nicht angezeigt, wenn Sie ein Remote-Benutzer sind.

3. Geben Sie im Dialogfeld **Passwort ändern** das aktuelle Passwort und das neue Passwort ein.
4. Klicken Sie Auf **Speichern**.

Nachdem Sie fertig sind

Wenn Unified Manager in einer Hochverfügbarkeitskonfiguration konfiguriert ist, müssen Sie das Passwort auf dem zweiten Node des Setup ändern. Beide Instanzen müssen dasselbe Passwort haben.

Was der Wartungsbenutzer tut

Der Wartungbenutzer wird während der Installation von Unified Manager auf einem Red hat Enterprise Linux oder CentOS System erstellt. Der Wartungs-Benutzername ist der Benutzer „`umadmin`“. Der Wartungsbenutzer hat die OnCommand-Administratorrolle in der Web-UI, und dieser Benutzer kann nachfolgende Benutzer erstellen und ihnen Rollen zuweisen.

Der Wartungsbenutzer oder umadmin-Benutzer kann auch auf die Unified Manager Wartungskonsole zugreifen.

Was RBAC ist

RBAC (rollenbasierte Zugriffssteuerung) bietet die Möglichkeit, zu steuern, wer Zugriff auf verschiedene Funktionen und Ressourcen im OnCommand 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 z. B. mit Administrator-Kontozugriff 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 „OnCommand 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 Benutzer mit der OnCommand-Administratorrolle 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 OnCommand-Administratorrolle zugewiesen 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 Wartungs-Benutzer oder der OnCommand-Administrator 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.

- **OnCommand-Administrator**

  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 ursprüngliche Benutzer mit der OnCommand-Administratorrolle 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	OnCommand Administrator	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	•	•	•		
Management von Storage-Serviceobjekten wie SVM-Zuordnungen und Ressourcenpools		•	•		
Definieren von Warnmeldungen		•	•		

Funktion	Operator	Storage-Administrator	OnCommand Administrator	Integrationsschema	Berichtschema
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				•	
Schreibgeschützter Zugriff auf Berichte und andere Datenbankansichten					•
Planen und Speichern von Berichten	•	•	•		

Funktion	Operator	Storage-Administrator	OnCommand Administrator	Integrationsschema	Berichtschema
Importierte Berichte importieren und löschen			•		

Beschreibung der Benutzerzugriffsfenster und Dialogfelder

Basierend auf den RBAC-Einstellungen können Sie Benutzer auf der Seite Management/Users hinzufügen und diesen Benutzern geeignete Rollen zuweisen, um die Cluster aufzurufen und zu überwachen.

Management-/Benutzerseite

Auf der Seite Verwaltung/Benutzer wird eine Liste Ihrer Benutzer und Gruppen angezeigt und enthält Informationen wie den Namen, den Benutzertyp und die E-Mail-Adresse. Auf dieser Seite können Sie auch Aufgaben wie das Hinzufügen, Bearbeiten, Löschen und Testen von Benutzern ausführen.

Befehlsschaltflächen

Mit den Befehlsschaltflächen können Sie für ausgewählte Benutzer die folgenden Aufgaben ausführen:

- **Hinzufügen**

  Zeigt das Dialogfeld Benutzer hinzufügen an, in dem Sie einen lokalen Benutzer, einen Remote-Benutzer, eine Remote-Gruppe oder einen Datenbankbenutzer hinzufügen können.

  Sie können Remote-Benutzer oder -Gruppen nur hinzufügen, wenn Ihr Authentifizierungsserver aktiviert und konfiguriert ist.

- **Bearbeiten**

  Zeigt das Dialogfeld Benutzer bearbeiten an, in dem Sie die Einstellungen für den ausgewählten Benutzer bearbeiten können.

- **Löschen**

  Löscht die ausgewählten Benutzer aus der Management-Server-Datenbank.

- **Test**

  Hiermit können Sie überprüfen, ob ein Remote-Benutzer oder eine Gruppe im Authentifizierungsserver vorhanden ist.

  Sie können diese Aufgabe nur ausführen, wenn Ihr Authentifizierungsserver aktiviert und konfiguriert ist.

Listenansicht

Die Listenansicht zeigt in tabellarischer Form Informationen zu den erstellten Benutzern an. Mit den Spaltenfiltern können Sie die angezeigten Daten anpassen.

- **Name**

  Zeigt den Namen des Benutzers oder der Gruppe an.

- **Typ**

  Zeigt den Benutzertyp an: Lokaler Benutzer, Remote-Benutzer, Remote-Gruppe, Datenbankbenutzer oder Wartungbenutzer.

- **E-Mail**

  Zeigt die E-Mail-Adresse des Benutzers an.

- * Rolle*

  Zeigt den Typ der Rolle an, die dem Benutzer zugewiesen ist: Operator, Storage Administrator, OnCommand Administrator, Integrations- Schema oder Berichtschema.

Dialogfeld Benutzer hinzufügen

Sie können lokale Benutzer oder Datenbankbenutzer erstellen, Remote-Benutzer oder Remote-Gruppen hinzufügen und Rollen zuweisen, sodass diese Benutzer Storage-Objekte und Daten mit Unified Manager managen können.

Sie können einen Benutzer hinzufügen, indem Sie die folgenden Felder ausfüllen:

- **Typ**

  Ermöglicht die Angabe des Benutzertyps, den Sie erstellen möchten.

- **Name**

  Ermöglicht Ihnen, einen Benutzernamen anzugeben, mit dem sich ein Benutzer bei Unified Manager anmelden kann.

- **Passwort**

  Ermöglicht Ihnen die Angabe eines Passworts für den angegebenen Benutzernamen. Dieses Feld wird nur angezeigt, wenn Sie einen lokalen Benutzer oder einen Datenbankbenutzer hinzufügen.

- **Passwort Bestätigen**

  Ermöglicht Ihnen die erneute Eingabe Ihres Kennworts, um die Genauigkeit der Angaben im Feld „Kennwort“ sicherzustellen. Dieses Feld wird nur angezeigt, wenn Sie einen lokalen Benutzer oder einen Datenbankbenutzer hinzufügen.

- **E-Mail**

  Ermöglicht Ihnen die Angabe einer E-Mail-Adresse für den Benutzer; die angegebene E-Mail-Adresse muss eindeutig dem Benutzernamen entsprechen. Dieses Feld wird nur angezeigt, wenn Sie einen

Remote-Benutzer oder einen lokalen Benutzer hinzufügen.

- * Rolle*

  Ermöglicht es Ihnen, dem Benutzer eine Rolle zuzuweisen und den Umfang der Aktivitäten festzulegen, die der Benutzer durchführen kann. Als Rolle können OnCommand-Administrator, Storage-Administrator, Operator, Integrations-Schema oder das Berichtschema verwendet werden.

Befehlsschaltflächen

Mit den Schaltflächen können Sie die folgenden Aufgaben ausführen:

- **Hinzufügen**

  Fügt den Benutzer hinzu und schließt das Dialogfeld Benutzer hinzufügen.

- **Abbrechen**

  Bricht die Änderungen ab und schließt das Dialogfeld Benutzer hinzufügen.

Dialogfeld „Benutzer bearbeiten“

Im Dialogfeld Benutzer bearbeiten können Sie je nach ausgewähltem Benutzer nur bestimmte Einstellungen bearbeiten.

Details

Im Bereich Details können Sie die folgenden Informationen über einen ausgewählten Benutzer bearbeiten:

- **Typ**

  Dieses Feld kann nicht bearbeitet werden.

- **Name**

  Dieses Feld kann nicht bearbeitet werden.

- **Passwort**

  Ermöglicht Ihnen das Bearbeiten des Kennworts, wenn der ausgewählte Benutzer ein Datenbankbenutzer ist.

- **Passwort Bestätigen**

  Hiermit können Sie das bestätigte Kennwort bearbeiten, wenn der ausgewählte Benutzer ein Datenbankbenutzer ist.

- **E-Mail**

  Ermöglicht Ihnen die Bearbeitung der E-Mail-Adresse des ausgewählten Benutzers. Dieses Feld kann bearbeitet werden, wenn der ausgewählte Benutzer ein lokaler Benutzer, ein LDAP-Benutzer oder ein Wartungbenutzer ist.

- * Rolle*

Ermöglicht Ihnen die Bearbeitung der Rolle, die dem Benutzer zugewiesen ist. Dieses Feld kann bearbeitet werden, wenn der ausgewählte Benutzer ein lokaler Benutzer, ein Remote-Benutzer oder eine Remote-Gruppe ist.

Befehlsschaltflächen

Mit den Schaltflächen können Sie die folgenden Aufgaben ausführen:

- **Speichern**

  Speichert die Änderungen und schließt das Dialogfeld Benutzer bearbeiten.

- **Abbrechen**

  Bricht die Änderungen ab und schließt das Dialogfeld Benutzer bearbeiten.