Gestione dell'accesso degli utenti

Active IQ Unified Manager 9.10

NetApp
December 18, 2023

This PDF was generated from https://docs.netapp.com/it-it/active-iq-unified-manager-910/config/task_create_database_user.html on December 18, 2023. Always check docs.netapp.com for the latest.

Sommario

Gestione dell’accesso degli utenti

È possibile creare ruoli e assegnare funzionalità per controllare l’accesso degli utenti agli oggetti del cluster selezionati. È possibile identificare gli utenti che dispongono delle funzionalità necessarie per accedere agli oggetti selezionati all’interno di un cluster. Solo a questi utenti viene fornito l’accesso per gestire gli oggetti del cluster.

Aggiunta di utenti

È possibile aggiungere utenti locali o utenti di database utilizzando la pagina utenti. È inoltre possibile aggiungere utenti o gruppi remoti appartenenti a un server di autenticazione. È possibile assegnare ruoli a questi utenti e, in base ai privilegi dei ruoli, gli utenti possono gestire gli oggetti e i dati di storage con Unified Manager o visualizzare i dati in un database.

Cosa ti serve

- È necessario disporre del ruolo di amministratore dell’applicazione.
- Per aggiungere un utente o un gruppo remoto, è necessario aver attivato l’autenticazione remota e configurato il server di autenticazione.
- Se si prevede di configurare l’autenticazione SAML in modo che un provider di identità (IdP) autentichi gli utenti che accedono all’interfaccia grafica, assicurarsi che questi utenti siano definiti come utenti “remote”.

  L’accesso all’interfaccia utente non è consentito per gli utenti di tipo “local” o “maintenance” quando l’autenticazione SAML è attivata.

Se si aggiunge un gruppo da Windows Active Directory, tutti i membri diretti e i sottogruppi nidificati possono autenticarsi in Unified Manager, a meno che i sottogruppi nidificati non siano disattivati. Se si aggiunge un gruppo da OpenLDAP o altri servizi di autenticazione, solo i membri diretti di tale gruppo possono autenticarsi in Unified Manager.

Fasi

1. Nel riquadro di navigazione a sinistra, fare clic su **Generale** > **utenti**.
2. Nella pagina utenti, fare clic su **Aggiungi**.
3. Nella finestra di dialogo Aggiungi utente, selezionare il tipo di utente che si desidera aggiungere e immettere le informazioni richieste.

   Quando si immettono le informazioni utente richieste, è necessario specificare un indirizzo e-mail univoco per l’utente. Evitare di specificare indirizzi e-mail condivisi da più utenti.

4. Fare clic su **Aggiungi**.

Creazione di un utente di database

Per supportare una connessione tra Workflow Automation e Unified Manager, o per accedere alle viste del database, è necessario innanzitutto creare un utente del database con il ruolo Schema di integrazione o Schema report nell’interfaccia utente Web di Unified Manager.

Cosa ti serve

È necessario disporre del ruolo di amministratore dell'applicazione.

Gli utenti dei database forniscono integrazione con Workflow Automation e accesso a viste di database specifiche per i report. Gli utenti del database non hanno accesso all'interfaccia utente Web di Unified Manager o alla console di manutenzione e non possono eseguire chiamate API.

Fasi

1. Nel riquadro di navigazione a sinistra, fare clic su **Generale** > **utenti**.
2. Nella pagina utenti, fare clic su **Aggiungi**.
3. Nella finestra di dialogo Add User (Aggiungi utente), selezionare **Database User** (utente database) nell'elenco a discesa **Type** (tipo).
4. Digitare un nome e una password per l'utente del database.
5. Nell'elenco a discesa **ruolo**, selezionare il ruolo appropriato.

Se sei…	Scegliere questo ruolo
Connessione di Unified Manager con Workflow Automation	Schema di integrazione
Accesso a report e altre viste del database	Schema del report

6. Fare clic su **Aggiungi**.

Modifica delle impostazioni utente

È possibile modificare le impostazioni utente, ad esempio l'indirizzo e-mail e il ruolo, specificate da ciascun utente. Ad esempio, è possibile modificare il ruolo di un utente che è un operatore di storage e assegnare all'utente i privilegi di amministratore dello storage.

Cosa ti serve

È necessario disporre del ruolo di amministratore dell'applicazione.

Quando si modifica il ruolo assegnato a un utente, le modifiche vengono applicate quando si verifica una delle seguenti azioni:

- L'utente si disconnette e si connette nuovamente a Unified Manager.
- È stato raggiunto il timeout della sessione di 24 ore.

Fasi

1. Nel riquadro di navigazione a sinistra, fare clic su **Generale** > **utenti**.
2. Nella pagina utenti, selezionare l'utente per cui si desidera modificare le impostazioni e fare clic su **Modifica**.
3. Nella finestra di dialogo Edit User (Modifica utente), modificare le impostazioni appropriate specificate per l'utente.
4. Fare clic su **Save** (Salva).

Visualizzazione degli utenti

È possibile utilizzare la pagina utenti per visualizzare l'elenco degli utenti che gestiscono gli oggetti e i dati di storage utilizzando Unified Manager. È possibile visualizzare i dettagli relativi agli utenti, ad esempio il nome utente, il tipo di utente, l'indirizzo e-mail e il ruolo assegnato agli utenti.

Cosa ti serve

È necessario disporre del ruolo di amministratore dell'applicazione.

Fase

1. Nel riquadro di navigazione a sinistra, fare clic su **Generale** > **utenti**.

Eliminazione di utenti o gruppi

È possibile eliminare uno o più utenti dal database del server di gestione per impedire a utenti specifici di accedere a Unified Manager. È inoltre possibile eliminare i gruppi in modo che tutti gli utenti del gruppo non possano più accedere al server di gestione.

Cosa ti serve

- Quando si eliminano gruppi remoti, è necessario riassegnare gli eventi assegnati agli utenti dei gruppi remoti.

  Se si eliminano utenti locali o remoti, gli eventi assegnati a tali utenti vengono automaticamente disassegnati.

- È necessario disporre del ruolo di amministratore dell'applicazione.

Fasi

1. Nel riquadro di navigazione a sinistra, fare clic su **Generale** > **utenti**.
2. Nella pagina utenti, selezionare gli utenti o i gruppi che si desidera eliminare, quindi fare clic su **Elimina**.
3. Fare clic su **Sì** per confermare l'eliminazione.

Cos'è RBAC

RBAC (role-based access control) consente di controllare chi ha accesso a varie funzionalità e risorse nel server Active IQ Unified Manager.

Che cosa fa il controllo degli accessi basato sui ruoli

RBAC (role-based access control) consente agli amministratori di gestire gruppi di utenti definendo i ruoli. Se è necessario limitare l'accesso per funzionalità specifiche agli amministratori selezionati, è necessario impostare account amministratore per tali amministratori. Se si desidera limitare le informazioni che gli amministratori possono visualizzare e le operazioni che possono eseguire, è necessario applicare i ruoli agli account amministratore creati.

Il server di gestione utilizza RBAC per le autorizzazioni di accesso utente e ruolo. Se non sono state modificate le impostazioni predefinite del server di gestione per l'accesso dell'utente amministrativo, non è necessario effettuare l'accesso per visualizzarle.

Quando si avvia un'operazione che richiede privilegi specifici, il server di gestione richiede di effettuare l'accesso. Ad esempio, per creare account amministratore, è necessario effettuare l'accesso con l'account amministratore dell'applicazione.

Definizioni dei tipi di utente

Un tipo di utente specifica il tipo di account che l'utente possiede e include utenti remoti, gruppi remoti, utenti locali, utenti di database e utenti di manutenzione. Ciascuno di questi tipi ha un proprio ruolo, assegnato da un utente con il ruolo di Amministratore.

I tipi di utenti di Unified Manager sono i seguenti:

- **Utente manutenzione**

  Creato durante la configurazione iniziale di Unified Manager. L'utente di manutenzione crea quindi utenti aggiuntivi e assegna ruoli. L'utente che esegue la manutenzione è anche l'unico utente ad avere accesso alla console di manutenzione. Quando Unified Manager viene installato su un sistema Red Hat Enterprise Linux o CentOS, all'utente che esegue la manutenzione viene assegnato il nome utente "umadmin".

- **Utente locale**

  Accede all'interfaccia utente di Unified Manager ed esegue le funzioni in base al ruolo assegnato dall'utente di manutenzione o da un utente con il ruolo di amministratore dell'applicazione.

- **Gruppo remoto**

  Gruppo di utenti che accedono all'interfaccia utente di Unified Manager utilizzando le credenziali memorizzate sul server di autenticazione. Il nome di questo account deve corrispondere al nome di un gruppo memorizzato nel server di autenticazione. A tutti gli utenti del gruppo remoto viene concesso l'accesso all'interfaccia utente di Unified Manager utilizzando le proprie credenziali utente individuali. I gruppi remoti possono eseguire le funzioni in base ai ruoli assegnati.

- **Utente remoto**

  Consente di accedere all'interfaccia utente di Unified Manager utilizzando le credenziali memorizzate nel server di autenticazione. Un utente remoto esegue le funzioni in base al ruolo assegnato dall'utente di manutenzione o da un utente con il ruolo di amministratore dell'applicazione.

- **Utente database**

  Dispone di accesso in sola lettura ai dati nel database di Unified Manager, non ha accesso all'interfaccia Web di Unified Manager o alla console di manutenzione e non può eseguire chiamate API.

Definizioni dei ruoli utente

L'utente addetto alla manutenzione o l'amministratore dell'applicazione assegna un ruolo a ogni utente. Ogni ruolo contiene alcuni privilegi. L'ambito delle attività che è possibile eseguire in Unified Manager dipende dal ruolo assegnato e dai privilegi contenuti nel

ruolo.

Unified Manager include i seguenti ruoli utente predefiniti:

- **Operatore**

  Visualizza le informazioni sul sistema storage e altri dati raccolti da Unified Manager, incluse cronologie e tendenze della capacità. Questo ruolo consente all'operatore di storage di visualizzare, assegnare, riconoscere, risolvere e aggiungere note per gli eventi.

- **Storage Administrator**

  Configura le operazioni di gestione dello storage in Unified Manager. Questo ruolo consente all'amministratore dello storage di configurare le soglie e di creare avvisi e altre opzioni e policy specifiche per la gestione dello storage.

- **Amministratore dell'applicazione**

  Configura impostazioni non correlate alla gestione dello storage. Questo ruolo consente la gestione di utenti, certificati di sicurezza, accesso al database e opzioni amministrative, tra cui autenticazione, SMTP, networking e AutoSupport.

  > Quando Unified Manager viene installato sui sistemi Linux, l'utente iniziale con il ruolo di amministratore dell'applicazione viene automaticamente chiamato "umadmin".

- **Schema di integrazione**

  Questo ruolo consente l'accesso in sola lettura alle viste del database di Unified Manager per l'integrazione di Unified Manager con OnCommand Workflow Automation (Wfa).

- **Schema report**

  Questo ruolo consente l'accesso in sola lettura ai report e ad altre viste del database direttamente dal database di Unified Manager. I database visualizzabili includono:

  - vista_modello_netapp
  - netapp_performance
  - ocum
  - ocum_report
  - ocum_report_birt
  - opm
  - scalemonitor

Ruoli e funzionalità degli utenti di Unified Manager

In base al ruolo utente assegnato, è possibile determinare le operazioni che è possibile eseguire in Unified Manager.

Nella tabella seguente sono riportate le funzioni che ciascun ruolo utente può eseguire:

Funzione	Operatore	Amministratore dello storage	Amministratore dell'applicazione	Schema di integrazione	Schema del report
Visualizzare le informazioni sul sistema di storage	•	•	•	•	•
Visualizzare altri dati, ad esempio cronologie e trend di capacità	•	•	•	•	•
Visualizzare, assegnare e risolvere gli eventi	•	•	•		
Visualizzare gli oggetti del servizio di storage, ad esempio le associazioni SVM e i pool di risorse	•	•	•		
Visualizzare i criteri di soglia	•	•	•		
Gestire gli oggetti del servizio di storage, come associazioni SVM e pool di risorse		•	•		
Definire gli avvisi		•	•		
Gestire le opzioni di gestione dello storage		•	•		
Gestire le policy di gestione dello storage		•	•		

Funzione	Operatore	Amministratore dello storage	Amministratore dell'applicazione	Schema di integrazione	Schema del report
Gestire gli utenti			•		
Gestire le opzioni amministrative			•		
Definire i criteri di soglia			•		
Gestire l'accesso al database			•		
Gestire l'integrazione con WFA e fornire l'accesso alle viste del database				•	
Pianificare e salvare i report		•	•		
Eseguire le operazioni "Fix it" dalle azioni di gestione		•	•		
Fornire l'accesso in sola lettura alle viste del database					•

Informazioni sul copyright

Copyright © 2023 NetApp, Inc. Tutti i diritti riservati. Stampato negli Stati Uniti d'America. Nessuna porzione di questo documento soggetta a copyright può essere riprodotta in qualsiasi formato o mezzo (grafico, elettronico o meccanico, inclusi fotocopie, registrazione, nastri o storage in un sistema elettronico) senza previo consenso scritto da parte del detentore del copyright.

Il software derivato dal materiale sottoposto a copyright di NetApp è soggetto alla seguente licenza e dichiarazione di non responsabilità:

IL PRESENTE SOFTWARE VIENE FORNITO DA NETAPP "COSÌ COM'È" E SENZA QUALSIVOGLIA TIPO DI GARANZIA IMPLICITA O ESPRESSA FRA CUI, A TITOLO ESEMPLIFICATIVO E NON ESAUSTIVO, GARANZIE IMPLICITE DI COMMERCIABILITÀ E IDONEITÀ PER UNO SCOPO SPECIFICO, CHE VENGONO DECLINATE DAL PRESENTE DOCUMENTO. NETAPP NON VERRÀ CONSIDERATA RESPONSABILE IN ALCUN CASO PER QUALSIVOGLIA DANNO DIRETTO, INDIRETTO, ACCIDENTALE, SPECIALE, ESEMPLARE E CONSEQUENZIALE (COMPRESI, A TITOLO ESEMPLIFICATIVO E NON ESAUSTIVO, PROCUREMENT O SOSTITUZIONE DI MERCI O SERVIZI, IMPOSSIBILITÀ DI UTILIZZO O PERDITA DI DATI O PROFITTI OPPURE INTERRUZIONE DELL'ATTIVITÀ AZIENDALE) CAUSATO IN QUALSIVOGLIA MODO O IN RELAZIONE A QUALUNQUE TEORIA DI RESPONSABILITÀ, SIA ESSA CONTRATTUALE, RIGOROSA O DOVUTA A INSOLVENZA (COMPRESA LA NEGLIGENZA O ALTRO) INSORTA IN QUALSIASI MODO ATTRAVERSO L'UTILIZZO DEL PRESENTE SOFTWARE ANCHE IN PRESENZA DI UN PREAVVISO CIRCA L'EVENTUALITÀ DI QUESTO TIPO DI DANNI.

NetApp si riserva il diritto di modificare in qualsiasi momento qualunque prodotto descritto nel presente documento senza fornire alcun preavviso. NetApp non si assume alcuna responsabilità circa l'utilizzo dei prodotti o materiali descritti nel presente documento, con l'eccezione di quanto concordato espressamente e per iscritto da NetApp. L'utilizzo o l'acquisto del presente prodotto non comporta il rilascio di una licenza nell'ambito di un qualche diritto di brevetto, marchio commerciale o altro diritto di proprietà intellettuale di NetApp.

Il prodotto descritto in questa guida può essere protetto da uno o più brevetti degli Stati Uniti, esteri o in attesa di approvazione.

LEGENDA PER I DIRITTI SOTTOPOSTI A LIMITAZIONE: l'utilizzo, la duplicazione o la divulgazione da parte degli enti governativi sono soggetti alle limitazioni indicate nel sottoparagrafo (b)(3) della clausola Rights in Technical Data and Computer Software del DFARS 252.227-7013 (FEB 2014) e FAR 52.227-19 (DIC 2007).

I dati contenuti nel presente documento riguardano un articolo commerciale (secondo la definizione data in FAR 2.101) e sono di proprietà di NetApp, Inc. Tutti i dati tecnici e il software NetApp forniti secondo i termini del presente Contratto sono articoli aventi natura commerciale, sviluppati con finanziamenti esclusivamente privati. Il governo statunitense ha una licenza irrevocabile limitata, non esclusiva, non trasferibile, non cedibile, mondiale, per l'utilizzo dei Dati esclusivamente in connessione con e a supporto di un contratto governativo statunitense in base al quale i Dati sono distribuiti. Con la sola esclusione di quanto indicato nel presente documento, i Dati non possono essere utilizzati, divulgati, riprodotti, modificati, visualizzati o mostrati senza la previa approvazione scritta di NetApp, Inc. I diritti di licenza del governo degli Stati Uniti per il Dipartimento della Difesa sono limitati ai diritti identificati nella clausola DFARS 252.227-7015(b) (FEB 2014).

Informazioni sul marchio commerciale

NETAPP, il logo NETAPP e i marchi elencati alla pagina http://www.netapp.com/TM sono marchi di NetApp, Inc. Gli altri nomi di aziende e prodotti potrebbero essere marchi dei rispettivi proprietari.