Gestisci l'accesso degli utenti

Active IQ Unified Manager

NetApp
October 15, 2025

Sommario

Gestisci l’accesso degli utenti

È possibile creare ruoli e assegnare capacità per controllare l’accesso degli utenti ad Active IQ Unified Manager. È possibile identificare gli utenti che dispongono delle capacità richieste per accedere agli oggetti selezionati all’interno di Unified Manager. Solo gli utenti che dispongono di questi ruoli e capacità possono gestire gli oggetti in Unified Manager.

Aggiungi utenti

È possibile aggiungere utenti locali o utenti del database utilizzando la pagina Utenti. È anche possibile aggiungere utenti o gruppi remoti che appartengono 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 di archiviazione e i dati con Unified Manager oppure visualizzare i dati in un database.

Prima di iniziare

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

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

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 disabilitati. Se si aggiunge un gruppo da OpenLDAP o da altri servizi di autenticazione, solo i membri diretti di quel gruppo potranno autenticarsi in Unified Manager.

Passi

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, seleziona il tipo di utente che desideri aggiungere e inserisci le informazioni richieste.

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

4. Fare clic su **Aggiungi**.

Creare un utente del database

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

Manager.

Prima di iniziare

È necessario disporre del ruolo di amministratore dell'applicazione.

Gli utenti del database forniscono l'integrazione con Workflow Automation e l'accesso a viste del database specifiche per 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.

Passi

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, seleziona **Utente database** nell'elenco a discesa **Tipo**.
4. Digitare un nome e una password per l'utente del database.
5. Nell'elenco a discesa **Ruolo**, seleziona il ruolo appropriato.

Se sei…	Scegli questo ruolo
Collegamento di Unified Manager con l'automazione del flusso di lavoro	Schema di integrazione
Accesso ai report e ad altre viste del database	Schema del report

6. Fare clic su **Aggiungi**.

Modifica le impostazioni utente

È possibile modificare le impostazioni utente, come l'indirizzo email e il ruolo, specificate per ciascun utente. Ad esempio, potresti voler modificare il ruolo di un utente che è un operatore di archiviazione e assegnare all'utente privilegi di amministratore di archiviazione.

Prima di iniziare

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 accede nuovamente a Unified Manager.
- È stato raggiunto il timeout di 24 ore della sessione.

Passi

1. Nel riquadro di navigazione a sinistra, fare clic su **Generale** > **Utenti**.
2. Nella pagina Utenti, seleziona l'utente per il quale desideri modificare le impostazioni e fai clic su **Modifica**.
3. Nella finestra di dialogo Modifica utente, modificare le impostazioni appropriate specificate per l'utente.
4. Fare clic su **Salva**.

Visualizza utenti

È possibile utilizzare la pagina Utenti per visualizzare l'elenco degli utenti che gestiscono oggetti di archiviazione e dati tramite Unified Manager. È possibile visualizzare i dettagli sugli utenti, come il nome utente, il tipo di utente, l'indirizzo e-mail e il ruolo assegnato agli utenti.

Prima di iniziare

È necessario disporre del ruolo di amministratore dell'applicazione.

Fare un passo

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

Elimina 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 anche possibile eliminare gruppi in modo che tutti gli utenti del gruppo non possano più accedere al server di gestione.

Prima di iniziare

- 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 rimossi.

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

Passi

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

Che cosa è RBAC

RBAC (controllo degli accessi basato sui ruoli) offre la possibilità di controllare chi ha accesso a varie funzionalità e risorse nel server Active IQ Unified Manager .

Cosa fa il controllo degli accessi basato sui ruoli

Il controllo degli accessi basato sui ruoli (RBAC) consente agli amministratori di gestire gruppi di utenti definendo i ruoli. Se è necessario limitare l'accesso a funzionalità specifiche ad amministratori selezionati, è necessario configurare per loro degli account amministratore. Se si desidera limitare le informazioni che gli amministratori possono visualizzare e le operazioni che possono eseguire, è necessario applicare ruoli agli account amministratore creati.

Il server di gestione utilizza RBAC per l'accesso degli utenti e le autorizzazioni dei ruoli. Se non hai modificato

le impostazioni predefinite del server di gestione per l'accesso degli utenti amministrativi, 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 accedere con l'account di amministratore dell'applicazione.

Definizioni dei tipi di utente

Un tipo di utente specifica il tipo di account di cui l'utente è titolare 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 addetto alla manutenzione**

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

- **Utente locale**

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

- **Gruppo remoto**

  Un 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 sul 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 svolgere funzioni in base ai ruoli assegnati.

- **Utente remoto**

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

- **Utente del database**

  Ha 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 determinati privilegi. L'ambito delle attività che puoi svolgere in Unified Manager dipende dal ruolo che ti è stato assegnato e dai privilegi che il ruolo contiene.

Unified Manager include i seguenti ruoli utente predefiniti:

- **Operatore**

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

- **Amministratore di archiviazione**

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

- **Amministratore dell'applicazione**

  Configura le impostazioni non correlate alla gestione dell'archiviazione. Questo ruolo consente la gestione degli utenti, dei certificati di sicurezza, dell'accesso al database e delle 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 denominato "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 del report**

  Questo ruolo consente l'accesso in sola lettura ai report e ad altre visualizzazioni del database direttamente dal database Unified Manager. I database che possono essere consultati includono:

  - netapp_model_view
  - prestazioni netapp
  - ocum
  - ocum_report
  - ocum_report_birt
  - opm
  - monitor di scala

Ruoli e capacità degli utenti di Unified Manager

In base al ruolo utente assegnato, puoi determinare quali operazioni puoi eseguire in Unified Manager.

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

Funzione	Operatore	Amministratore di archiviazione	Amministratore dell'applicazione	Schema di integrazione	Schema del report
Visualizza le informazioni sul sistema di archiviazione	•	•	•	•	•
Visualizza altri dati, come cronologie e tendenze della capacità	•	•	•	•	•
Visualizza, assegna e risolvi gli eventi	•	•	•		
Visualizza gli oggetti del servizio di archiviazione, come le associazioni SVM e i pool di risorse	•	•	•		
Visualizza le policy di soglia	•	•	•		
Gestire gli oggetti del servizio di archiviazione, come le associazioni SVM e i pool di risorse		•	•		
Definisci avvisi		•	•		
Gestisci le opzioni di gestione dell'archiviazione		•	•		

Funzione	Operatore	Amministratore di archiviazione	Amministratore dell'applicazione	Schema di integrazione	Schema del report
Gestire le policy di gestione dell'archiviazione		•	•		
Gestisci utenti			•		
Gestisci le opzioni amministrative			•		
Definire le politiche di soglia			•		
Gestire l'accesso al database			•		
Gestire l'integrazione con WFA e fornire l'accesso alle viste del database				•	
Pianifica e salva i report		•	•		
Eseguire le operazioni "Fix It" dalle azioni di gestione		•	•		
Fornire accesso in sola lettura alle viste del database					•

Informazioni sul copyright

Informazioni sul marchio commerciale