Eseguire attività amministrative e di configurazione

Active IQ Unified Manager 9.12

NetApp
December 18, 2023

Sommario

Eseguire attività amministrative e di configurazione

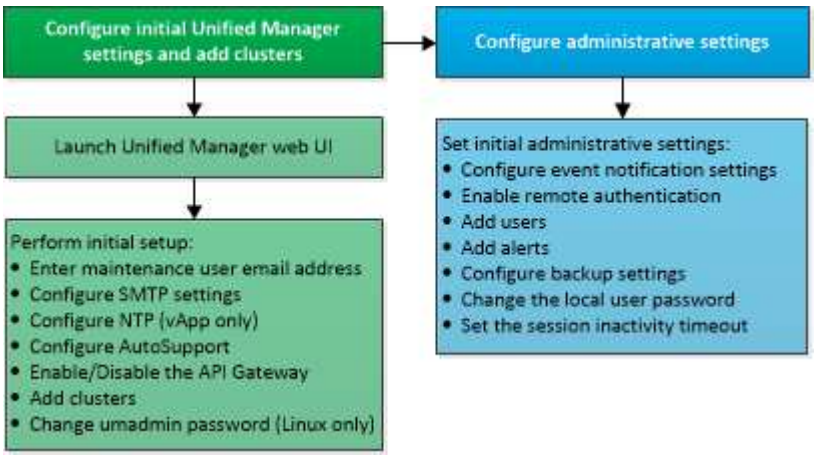
Configurazione di Active IQ Unified Manager

Dopo aver installato Active IQ Unified Manager (precedentemente noto come Gestore unificato di OnCommand), è necessario completare la configurazione iniziale (chiamata anche procedura guidata per la prima esperienza) per accedere all'interfaccia utente Web. È quindi possibile eseguire ulteriori attività di configurazione, ad esempio l'aggiunta di cluster, la configurazione dell'autenticazione remota, l'aggiunta di utenti e l'aggiunta di avvisi.

Alcune delle procedure descritte in questo manuale sono necessarie per completare la configurazione iniziale dell'istanza di Unified Manager. Altre procedure sono le impostazioni di configurazione consigliate che sono utili per la configurazione sulla nuova istanza o che sono utili prima di iniziare il monitoraggio regolare dei sistemi ONTAP.

Panoramica della sequenza di configurazione

Il flusso di lavoro di configurazione descrive le attività da eseguire prima di poter utilizzare Unified Manager.



Accesso all'interfaccia utente Web di Unified Manager

Dopo aver installato Unified Manager, è possibile accedere all'interfaccia utente Web per configurare Unified Manager in modo da poter iniziare il monitoraggio dei sistemi ONTAP.

Cosa ti serve

- Se si accede per la prima volta all'interfaccia utente Web, è necessario effettuare l'accesso come utente di manutenzione (o come utente umadmin per le installazioni Linux).
- Se si prevede di consentire agli utenti di accedere a Unified Manager utilizzando il nome breve invece di utilizzare il nome di dominio completo (FQDN) o l'indirizzo IP, la configurazione di rete deve risolvere questo nome breve in un FQDN valido.

- Se il server utilizza un certificato digitale autofirmato, il browser potrebbe visualizzare un avviso che indica che il certificato non è attendibile. È possibile riconoscere il rischio di continuare l'accesso o installare un certificato digitale firmato dall'autorità di certificazione (CA) per l'autenticazione del server.

Fasi

1. Avviare l'interfaccia utente Web di Unified Manager dal browser utilizzando l'URL visualizzato al termine dell'installazione. L'URL è l'indirizzo IP o FQDN (Fully Qualified Domain Name) del server Unified Manager.

   Il link è nel seguente formato: `https://URL`.

2. Accedere all'interfaccia utente Web di Unified Manager utilizzando le credenziali utente di manutenzione.

> Se si effettuano tre tentativi consecutivi di accesso all'interfaccia utente Web senza esito positivo entro un'ora, l'utente viene bloccato dal sistema e deve contattare l'amministratore di sistema. Questo è valido solo per gli utenti locali.

Esecuzione della configurazione iniziale dell'interfaccia utente Web di Unified Manager

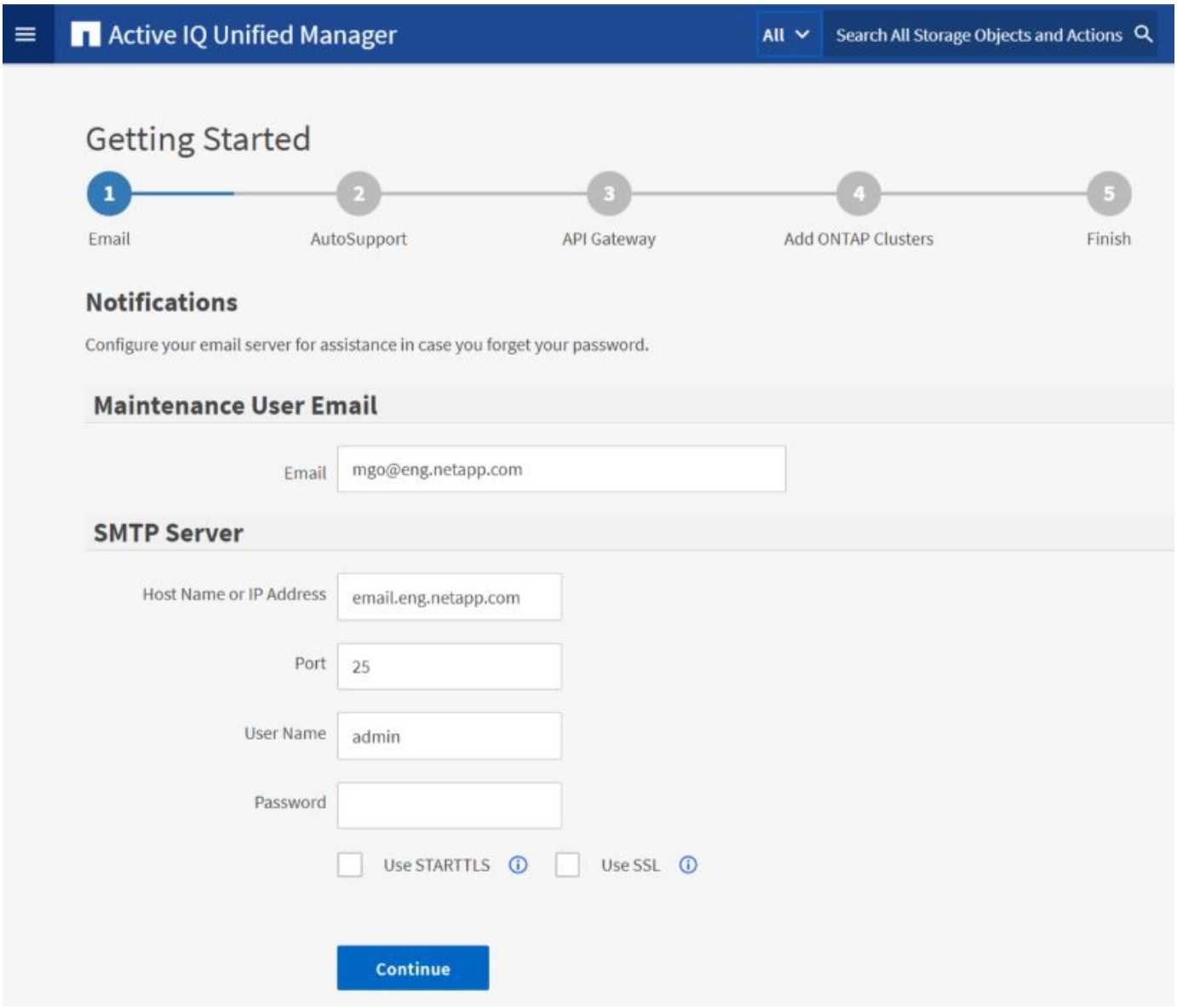
Per utilizzare Unified Manager, è necessario prima configurare le opzioni di configurazione iniziale, tra cui il server NTP, l'indirizzo e-mail dell'utente di manutenzione, l'host del server SMTP e l'aggiunta di cluster ONTAP.

Cosa ti serve

È necessario aver eseguito le seguenti operazioni:

- Ha avviato l'interfaccia utente Web di Unified Manager utilizzando l'URL fornito dopo l'installazione
- Accesso effettuato utilizzando il nome utente e la password di manutenzione (utente umadmin per installazioni Linux) creati durante l'installazione

La pagina Guida introduttiva di Active IQ Unified Managerviene visualizzata solo quando si accede per la prima volta all'interfaccia utente Web. La pagina riportata di seguito è tratta da un'installazione su VMware.



Se si desidera modificare una di queste opzioni in un secondo momento, è possibile selezionare una delle opzioni generali nel riquadro di navigazione sinistro di Unified Manager. Tenere presente che l'impostazione NTP è valida solo per le installazioni VMware e può essere modificata in un secondo momento utilizzando la console di manutenzione di Unified Manager.

Fasi

1. Nella pagina Configurazione iniziale di Active IQ Unified Manager, immettere l'indirizzo e-mail dell'utente di manutenzione, il nome host del server SMTP e le eventuali opzioni SMTP aggiuntive e il server NTP (solo installazioni VMware). Quindi fare clic su **continua**.

   Se è stata selezionata l'opzione **Use STARTTLS** or **Use SSL** (Usa STARTTLS* o **Use SSL**), dopo aver fatto clic sul pulsante **Continue** viene visualizzata una pagina di certificato. Verificare i dettagli del certificato e accettare il certificato per continuare con le impostazioni di configurazione iniziali dell'interfaccia utente Web.

2. Nella pagina AutoSupport, fare clic su **Accetto e continua** per abilitare l'invio di messaggi AutoSupport da Unified Manager a NetAppActive IQ.

   Se è necessario designare un proxy per fornire l'accesso a Internet per inviare contenuti AutoSupport o se

si desidera disattivare AutoSupport, utilizzare l'opzione **Generale** > **AutoSupport** dall'interfaccia utente Web.

3. Nei sistemi Red Hat e CentOS, modificare la password utente di umadmin dalla stringa predefinita "admin" a una stringa personalizzata.
4. Nella pagina Set up API Gateway (Configura gateway API), selezionare se si desidera utilizzare la funzione API Gateway che consente a Unified Manager di gestire i cluster ONTAP che si intende monitorare utilizzando le API REST di ONTAP. Quindi fare clic su **continua**.

   È possibile attivare o disattivare questa impostazione in un secondo momento nell'interfaccia utente Web da **Generale** > **Impostazioni delle funzioni** > **Gateway API**. Per ulteriori informazioni sulle API, vedere "Introduzione alle API REST di Active IQ Unified Manager".

5. Aggiungere i cluster che si desidera gestire con Unified Manager, quindi fare clic su **Avanti**. Per ogni cluster che si intende gestire, è necessario disporre del nome host o dell'indirizzo IP di gestione del cluster (IPv4 o IPv6) insieme alle credenziali del nome utente e della password. L'utente deve avere il ruolo "admin".

   Questo passaggio è facoltativo. È possibile aggiungere cluster in un secondo momento nell'interfaccia utente Web da **Storage Management** > **Cluster Setup**.

6. Nella pagina Summary (Riepilogo), verificare che tutte le impostazioni siano corrette e fare clic su **Finish** (fine).

La pagina Getting Started (Guida introduttiva) si chiude e viene visualizzata la pagina Unified Manager Dashboard.

Aggiunta di cluster

È possibile aggiungere un cluster a Active IQ Unified Manager in modo da poter monitorare il cluster. Ciò include la possibilità di ottenere informazioni sul cluster, come lo stato di salute, la capacità, le performance e la configurazione del cluster, in modo da individuare e risolvere eventuali problemi che potrebbero verificarsi.

Cosa ti serve

- È necessario disporre del ruolo di amministratore dell'applicazione o di amministratore dello storage.
- È necessario disporre delle seguenti informazioni:
  - Nome host o indirizzo IP di gestione del cluster

    Il nome host è l'FQDN o il nome breve utilizzato da Unified Manager per connettersi al cluster. Il nome host deve essere risolto nell'indirizzo IP di gestione del cluster.

    L'indirizzo IP di gestione del cluster deve essere la LIF di gestione del cluster della SVM (Administrative Storage Virtual Machine). Se si utilizza una LIF di gestione dei nodi, l'operazione non riesce.

  - Il cluster deve eseguire il software ONTAP versione 9.1 o superiore.
  - Nome utente e password dell'amministratore di ONTAP

    Questo account deve avere il ruolo *admin* con accesso applicazione impostato su *ontapi*, *console* e *http*.

- Il numero di porta per la connessione al cluster utilizzando il protocollo HTTPS (generalmente la porta 443).
- Si dispone dei certificati richiesti. Unified Manager installa i certificati di sicurezza quando si aggiunge un cluster:

  Certificati server: Questo certificato è di proprietà di Unified Manager. Un certificato SSL (HTTPS) autofirmato predefinito viene generato con una nuova installazione di Unified Manager. NetApp consiglia di eseguire l'upgrade al certificato firmato CA per una maggiore sicurezza. Se il certificato del server scade, è necessario rigenerarlo e riavviare Unified Manager affinché i servizi incorporino il nuovo certificato. Per ulteriori informazioni sulla rigenerazione del certificato SSL, vedere "Generazione di un certificato di protezione HTTPS".

  Certificati per la comunicazione TLS reciproca: Utilizzati durante la comunicazione TLS reciproca tra Unified Manager e ONTAP. L'autenticazione basata su certificato è abilitata per un cluster, in base alla versione di ONTAP. Se il cluster che esegue la versione di ONTAP è inferiore alla 9.5, l'autenticazione basata su certificato non viene attivata.

  L'autenticazione basata su certificato non viene attivata automaticamente per un cluster, se si aggiorna una versione precedente di Unified Manager a Unified Manager 9.12. Tuttavia, è possibile abilitarla modificando e salvando i dettagli del cluster. Se il certificato scade, è necessario rigenerarlo per incorporare il nuovo certificato. Per ulteriori informazioni sulla visualizzazione e la rigenerazione del certificato, vedere "Modifica dei cluster".

  - L'autenticazione basata su certificato viene attivata automaticamente se si aggiunge un cluster dall'interfaccia utente Web. Se si aggiunge un cluster dalla console di manutenzione, l'autenticazione basata su certificato non viene attivata.
  - Se l'autenticazione basata su certificato è abilitata per un cluster e si esegue il backup di Unified Manager da un server e si esegue il ripristino su un altro server Unified Manager in cui viene modificato il nome host o l'indirizzo IP, il monitoraggio del cluster potrebbe non riuscire. Per evitare il guasto, modificare e salvare i dettagli del cluster. Per ulteriori informazioni sulla modifica dei dettagli del cluster, vedere "Modifica dei cluster".

  + **Certificati client**: Utilizzati durante l'autenticazione per i messaggi EMS ricevuti da ONTAP. Questo certificato è di proprietà di ONTAP e viene richiesto quando si aggiunge un cluster ONTAP a Unified Manager. Non è possibile aggiungere un cluster a Unified Manager con un certificato scaduto e, se il certificato client è già scaduto, è necessario rigenerarlo prima di aggiungere il cluster. Tuttavia, se il certificato scade per un cluster già aggiunto e viene utilizzato da Unified Manager, la messaggistica EMS continua a funzionare con il certificato scaduto. Per informazioni sulla generazione dei certificati, consultare l'articolo della Knowledge base (KB) "Come rinnovare un certificato autofirmato ONTAP nell'interfaccia utente di System Manager".

- È necessario disporre di spazio sufficiente sul server Unified Manager. Non è possibile aggiungere un cluster al server quando più del 90% dello spazio nella directory del database è già occupato.

Per una configurazione MetroCluster, è necessario aggiungere i cluster locali e remoti e i cluster devono essere configurati correttamente.

Fasi

1. Nel riquadro di navigazione a sinistra, fare clic su **Storage Management** > **Cluster Setup**.
2. Nella pagina Cluster Setup, fare clic su **Add** (Aggiungi).
3. Nella finestra di dialogo Add Cluster (Aggiungi cluster), specificare i valori richiesti, ad esempio il nome host o l'indirizzo IP del cluster, il nome utente, la password e il numero di porta.

È possibile modificare l'indirizzo IP di gestione del cluster da IPv6 a IPv4 o da IPv4 a IPv6. Il nuovo indirizzo IP viene visualizzato nella griglia del cluster e nella pagina di configurazione del cluster al termine del successivo ciclo di monitoraggio.

4. Fare clic su **Invia**.
5. Nella finestra di dialogo Authorize host (autorizza host), fare clic su **View Certificate** (Visualizza certificato) per visualizzare le informazioni sul certificato del cluster.
6. Fare clic su **Sì**.

   In Unified Manager 9.12, dopo aver salvato i dettagli del cluster, è possibile visualizzare il certificato per la comunicazione TLS reciproca per un cluster.

   Se l'autenticazione basata su certificato non è abilitata, Unified Manager controlla il certificato solo quando il cluster viene aggiunto inizialmente. Unified Manager non controlla il certificato per ogni chiamata API a ONTAP.

Una volta individuati tutti gli oggetti di un nuovo cluster, Unified Manager inizia a raccogliere dati storici sulle performance per i 15 giorni precedenti. Queste statistiche vengono raccolte utilizzando la funzionalità di raccolta della continuità dei dati. Questa funzionalità fornisce oltre due settimane di informazioni sulle performance per un cluster subito dopo l'aggiunta. Una volta completato il ciclo di raccolta della continuità dei dati, i dati delle performance del cluster in tempo reale vengono raccolti, per impostazione predefinita, ogni cinque minuti.

Dato che la raccolta di 15 giorni di dati sulle performance richiede un uso intensivo della CPU, si consiglia di eseguire l'aggiunta di nuovi cluster in modo che i sondaggi per la raccolta della continuità dei dati non vengano eseguiti su troppi cluster contemporaneamente. Inoltre, se si riavvia Unified Manager durante il periodo di raccolta della continuità dei dati, la raccolta viene interrotta e vengono visualizzate lacune nei grafici delle performance per il periodo di tempo mancante.

Se viene visualizzato un messaggio di errore che indica che non è possibile aggiungere il cluster, controllare se gli orologi sui due sistemi non sono sincronizzati e se la data di inizio del certificato HTTPS di Unified Manager è successiva alla data sul cluster. È necessario assicurarsi che gli orologi siano sincronizzati utilizzando NTP o un servizio simile.

Informazioni correlate

"Installazione di un certificato HTTPS firmato e restituito dalla CA"

Configurazione di Unified Manager per l'invio di notifiche di avviso

È possibile configurare Unified Manager in modo che invii notifiche che avvisano l'utente in merito a eventi nel proprio ambiente. Prima di poter inviare le notifiche, è necessario configurare diverse altre opzioni di Unified Manager.

Cosa ti serve

È necessario disporre del ruolo di amministratore dell'applicazione.

Dopo aver implementato Unified Manager e aver completato la configurazione iniziale, è necessario configurare l'ambiente in modo da attivare avvisi e generare messaggi e-mail di notifica o trap SNMP in base alla ricezione degli eventi.

Fasi

1. "Configurare le impostazioni di notifica degli eventi".

   Se si desidera inviare notifiche di avviso quando si verificano determinati eventi nell'ambiente, è necessario configurare un server SMTP e fornire un indirizzo e-mail da cui inviare la notifica di avviso. Se si desidera utilizzare i trap SNMP, è possibile selezionare tale opzione e fornire le informazioni necessarie.

2. "Abilitare l'autenticazione remota".

   Se si desidera che gli utenti LDAP o Active Directory remoti accedano all'istanza di Unified Manager e ricevano notifiche di avviso, è necessario attivare l'autenticazione remota.

3. "Aggiungere server di autenticazione".

   È possibile aggiungere server di autenticazione in modo che gli utenti remoti all'interno del server di autenticazione possano accedere a Unified Manager.

4. "Aggiungere utenti".

   È possibile aggiungere diversi tipi di utenti locali o remoti e assegnare ruoli specifici. Quando si crea un avviso, si assegna a un utente la ricezione delle notifiche.

5. "Aggiungere avvisi".

   Dopo aver aggiunto l'indirizzo e-mail per l'invio delle notifiche, aver aggiunto gli utenti per la ricezione delle notifiche, aver configurato le impostazioni di rete e configurato le opzioni SMTP e SNMP necessarie per l'ambiente, è possibile assegnare gli avvisi.

Configurazione delle impostazioni di notifica degli eventi

È possibile configurare Unified Manager in modo che invii notifiche di avviso quando viene generato un evento o quando viene assegnato un evento a un utente. È possibile configurare il server SMTP utilizzato per inviare l'avviso e impostare vari meccanismi di notifica, ad esempio le notifiche di avviso possono essere inviate come e-mail o trap SNMP.

Cosa ti serve

È necessario disporre delle seguenti informazioni:

- Indirizzo e-mail da cui viene inviata la notifica di avviso

  L'indirizzo e-mail viene visualizzato nel campo "da" nelle notifiche di avviso inviate. Se non è possibile recapitarlo per qualsiasi motivo, questo indirizzo e-mail viene utilizzato anche come destinatario per la posta non recapitabile.

- Nome host del server SMTP, nome utente e password per accedere al server
- Nome host o indirizzo IP dell'host di destinazione trap che riceverà il trap SNMP, oltre alla versione SNMP, alla porta trap in uscita, alla community e ad altri valori di configurazione SNMP richiesti

  Per specificare più destinazioni di trap, separare ciascun host con una virgola. In questo caso, tutte le altre impostazioni SNMP, ad esempio versione e porta trap in uscita, devono essere le stesse per tutti gli host dell'elenco.

È necessario disporre del ruolo di amministratore dell'applicazione o di amministratore dello storage.

Fasi

1. Nel riquadro di navigazione a sinistra, fare clic su **Generale** > **Notifiche**.
2. Nella pagina Notifiche, configurare le impostazioni appropriate.

   Note:

   - Se l'indirizzo da è pre-compilato con l'indirizzo "ActiveIQUnifiedManager@localhost.com", devi cambiarlo in un indirizzo e-mail reale e funzionante per assicurarti che tutte le notifiche e-mail siano inviate correttamente.
   - Se il nome host del server SMTP non può essere risolto, è possibile specificare l'indirizzo IP (IPv4 o IPv6) del server SMTP invece del nome host.
3. Fare clic su **Save** (Salva).
4. Se è stata selezionata l'opzione **Use STARTTLS** or **Use SSL** (Usa STARTTLS* o **Use SSL**), dopo aver fatto clic sul pulsante **Save** (Salva) viene visualizzata una pagina del certificato. Verificare i dettagli del certificato e accettare il certificato per salvare le impostazioni di notifica.

   Per visualizzare i dettagli del certificato, fare clic sul pulsante **View Certificate Details** (Visualizza dettagli certificato). Se il certificato esistente è scaduto, deselezionare la casella **Usa STARTTLS** o **Usa SSL**, salvare le impostazioni di notifica e selezionare nuovamente la casella **Usa STARTTLS** o **Usa SSL** per visualizzare un nuovo certificato.

Attivazione dell'autenticazione remota

È possibile attivare l'autenticazione remota in modo che il server Unified Manager possa comunicare con i server di autenticazione. Gli utenti del server di autenticazione possono accedere all'interfaccia grafica di Unified Manager per gestire i dati e gli oggetti di storage.

Cosa ti serve

È necessario disporre del ruolo di amministratore dell'applicazione.

> Il server Unified Manager deve essere connesso direttamente al server di autenticazione. È necessario disattivare tutti i client LDAP locali come SSSD (System Security Services Daemon) o NSLCD (Name Service LDAP Caching Daemon).

È possibile attivare l'autenticazione remota utilizzando Open LDAP o Active Directory. Se l'autenticazione remota è disattivata, gli utenti remoti non possono accedere a Unified Manager.

L'autenticazione remota è supportata su LDAP e LDAPS (Secure LDAP). Unified Manager utilizza 389 come porta predefinita per le comunicazioni non protette e 636 come porta predefinita per le comunicazioni protette.

> Il certificato utilizzato per autenticare gli utenti deve essere conforme al formato X.509.

Fasi

1. Nel riquadro di spostamento di sinistra, fare clic su **Generale** > **autenticazione remota**.
2. Selezionare la casella **Enable remote Authentication…** (attiva autenticazione remota…).

3. Nel campo Servizio di autenticazione, selezionare il tipo di servizio e configurare il servizio di autenticazione.

Per tipo di autenticazione…	Inserire le seguenti informazioni…
Active Directory	• Nome dell'amministratore del server di autenticazione in uno dei seguenti formati: ◦ `domainname\username` ◦ `username@domainname` ◦ `Bind Distinguished Name` (Utilizzando la notazione LDAP appropriata) • Password dell'amministratore • Nome distinto di base (utilizzando la notazione LDAP appropriata)
Aprire LDAP	• Nome distinto di binding (nella notazione LDAP appropriata) • Associare la password • Nome distinto di base

Se l'autenticazione di un utente di Active Directory richiede molto tempo o si verifica un timeout, il server di autenticazione probabilmente impiega molto tempo per rispondere. La disattivazione del supporto per i gruppi nidificati in Unified Manager potrebbe ridurre il tempo di autenticazione.

Se si seleziona l'opzione Usa connessione protetta per il server di autenticazione, Unified Manager comunica con il server di autenticazione utilizzando il protocollo SSL (Secure Sockets Layer).

4. **Opzionale:** aggiungere server di autenticazione e verificare l'autenticazione.
5. Fare clic su **Save** (Salva).

Disattivazione dei gruppi nidificati dall'autenticazione remota

Se l'autenticazione remota è attivata, è possibile disattivare l'autenticazione dei gruppi nidificati in modo che solo i singoli utenti e non i membri del gruppo possano autenticarsi in remoto in Unified Manager. È possibile disattivare i gruppi nidificati quando si desidera migliorare i tempi di risposta per l'autenticazione di Active Directory.

Cosa ti serve

- È necessario disporre del ruolo di amministratore dell'applicazione.
- La disattivazione dei gruppi nidificati è applicabile solo quando si utilizza Active Directory.

La disattivazione del supporto per i gruppi nidificati in Unified Manager potrebbe ridurre il tempo di autenticazione. Se il supporto di gruppi nidificati è disattivato e se un gruppo remoto viene aggiunto a Unified Manager, i singoli utenti devono essere membri del gruppo remoto per autenticarsi in Unified Manager.

Fasi

1. Nel riquadro di spostamento di sinistra, fare clic su **Generale** > **autenticazione remota**.
2. Selezionare la casella **Disable Nested Group Lookup** (Disattiva ricerca gruppi nidificati).
3. Fare clic su **Save** (Salva).

Impostazione dei servizi di autenticazione

I servizi di autenticazione consentono l'autenticazione di utenti remoti o gruppi remoti in un server di autenticazione prima di fornire loro l'accesso a Unified Manager. È possibile autenticare gli utenti utilizzando servizi di autenticazione predefiniti (ad esempio Active Directory o OpenLDAP) o configurando il proprio meccanismo di autenticazione.

Cosa ti serve

- È necessario aver attivato l'autenticazione remota.
- È necessario disporre del ruolo di amministratore dell'applicazione.

Fasi

1. Nel riquadro di spostamento di sinistra, fare clic su **Generale** > **autenticazione remota**.
2. Selezionare uno dei seguenti servizi di autenticazione:

Se si seleziona…	Quindi…
Active Directory	a. Immettere il nome e la password dell'amministratore. b. Specificare il nome distinto di base del server di autenticazione. Ad esempio, se il nome di dominio del server di autenticazione è ou@domain.com, il nome distinto di base è **cn=ou,DC=domain,DC=com**.
OpenLDAP	a. Immettere il nome distinto e la password di bind. b. Specificare il nome distinto di base del server di autenticazione. Ad esempio, se il nome di dominio del server di autenticazione è ou@domain.com, il nome distinto di base è **cn=ou,DC=domain,DC=com**.

Se si seleziona…	Quindi…
Altri	a. Immettere il nome distinto e la password di bind. b. Specificare il nome distinto di base del server di autenticazione. Ad esempio, se il nome di dominio del server di autenticazione è ou@domain.com, il nome distinto di base è **cn=ou,DC=domain,DC=com**. c. Specificare la versione del protocollo LDAP supportata dal server di autenticazione. d. Immettere il nome utente, l'appartenenza al gruppo, il gruppo di utenti e gli attributi del membro.

Se si desidera modificare il servizio di autenticazione, è necessario eliminare tutti i server di autenticazione esistenti e aggiungere nuovi server di autenticazione.

3. Fare clic su **Save** (Salva).

Aggiunta di server di autenticazione

È possibile aggiungere server di autenticazione e abilitare l'autenticazione remota sul server di gestione in modo che gli utenti remoti all'interno del server di autenticazione possano accedere a Unified Manager.

Cosa ti serve

- Devono essere disponibili le seguenti informazioni:
  - Nome host o indirizzo IP del server di autenticazione
  - Numero di porta del server di autenticazione
- È necessario aver attivato l'autenticazione remota e configurato il servizio di autenticazione in modo che il server di gestione possa autenticare utenti o gruppi remoti nel server di autenticazione.
- È necessario disporre del ruolo di amministratore dell'applicazione.

Se il server di autenticazione che si sta aggiungendo fa parte di una coppia ad alta disponibilità (ha) (utilizzando lo stesso database), è possibile aggiungere anche il server di autenticazione partner. Ciò consente al server di gestione di comunicare con il partner quando uno dei server di autenticazione non è raggiungibile.

Fasi

1. Nel riquadro di spostamento di sinistra, fare clic su **Generale** > **autenticazione remota**.
2. Attivare o disattivare l'opzione **Usa connessione protetta**:

Se si desidera…	Quindi…
Abilitarlo	a. Selezionare l'opzione **Usa connessione protetta**. b. Nella sezione Authentication Servers (Server di autenticazione), fare clic su **Add** (Aggiungi) c. Nella finestra di dialogo Add Authentication Server (Aggiungi server di autenticazione), immettere il nome di autenticazione o l'indirizzo IP (IPv4 o IPv6) del server. d. Nella finestra di dialogo autorizza host, fare clic su Visualizza certificato. e. Nella finestra di dialogo Visualizza certificato, verificare le informazioni del certificato, quindi fare clic su **Chiudi**. f. Nella finestra di dialogo autorizza host, fare clic su **Sì**. Quando si attiva l'opzione **Usa autenticazione connessione sicura**, Unified Manager comunica con il server di autenticazione e visualizza il certificato. Unified Manager utilizza 636 come porta predefinita per comunicazioni sicure e il numero di porta 389 per comunicazioni non sicure.
Disattivarlo	a. Deselezionare l'opzione **Usa connessione protetta**. b. Nella sezione Authentication Servers (Server di autenticazione), fare clic su **Add** (Aggiungi) c. Nella finestra di dialogo Add Authentication Server (Aggiungi server di autenticazione), specificare il nome host o l'indirizzo IP (IPv4 o IPv6) del server e i dettagli della porta. d. Fare clic su **Aggiungi**.

Il server di autenticazione aggiunto viene visualizzato nell'area Server.

3. Eseguire un'autenticazione di prova per confermare che è possibile autenticare gli utenti nel server di autenticazione aggiunto.

Verifica della configurazione dei server di autenticazione

È possibile convalidare la configurazione dei server di autenticazione per garantire che il server di gestione sia in grado di comunicare con essi. È possibile convalidare la

configurazione ricercando un utente remoto o un gruppo remoto dai server di autenticazione e autenticandoli utilizzando le impostazioni configurate.

Cosa ti serve

- È necessario aver attivato l'autenticazione remota e configurato il servizio di autenticazione in modo che il server Unified Manager possa autenticare l'utente remoto o il gruppo remoto.
- È necessario aggiungere i server di autenticazione in modo che il server di gestione possa cercare l'utente remoto o il gruppo remoto da questi server e autenticarli.
- È necessario disporre del ruolo di amministratore dell'applicazione.

Se il servizio di autenticazione è impostato su Active Directory e si sta convalidando l'autenticazione degli utenti remoti che appartengono al gruppo primario del server di autenticazione, le informazioni sul gruppo primario non vengono visualizzate nei risultati dell'autenticazione.

Fasi

1. Nel riquadro di spostamento di sinistra, fare clic su **Generale** > **autenticazione remota**.
2. Fare clic su **Test Authentication**.
3. Nella finestra di dialogo Test User, specificare il nome utente e la password dell'utente remoto o il nome utente del gruppo remoto, quindi fare clic su **Test**.

   Se si sta autenticando un gruppo remoto, non è necessario immettere la password.

Aggiunta di avvisi

È possibile configurare gli avvisi in modo che notifichino quando viene generato un determinato evento. È possibile configurare gli avvisi per una singola risorsa, per un gruppo di risorse o per eventi di un particolare tipo di severità. È possibile specificare la frequenza con cui si desidera ricevere una notifica e associare uno script all'avviso.

Cosa ti serve

- Per consentire al server Active IQ Unified Manager di utilizzare queste impostazioni per inviare notifiche agli utenti quando viene generato un evento, è necessario aver configurato le impostazioni di notifica, ad esempio l'indirizzo e-mail dell'utente, il server SMTP e l'host trap SNMP.
- È necessario conoscere le risorse e gli eventi per i quali si desidera attivare l'avviso, nonché i nomi utente o gli indirizzi e-mail degli utenti che si desidera notificare.
- Se si desidera eseguire uno script in base all'evento, è necessario aggiungere lo script a Unified Manager utilizzando la pagina script.
- È necessario disporre del ruolo di amministratore dell'applicazione o di amministratore dello storage.

È possibile creare un avviso direttamente dalla pagina Dettagli evento dopo aver ricevuto un evento, oltre a creare un avviso dalla pagina Configurazione avviso, come descritto di seguito.

Fasi

1. Nel riquadro di navigazione a sinistra, fare clic su **Storage Management** > **Alert Setup**.
2. Nella pagina Alert Setup, fare clic su **Add** (Aggiungi).
3. Nella finestra di dialogo Aggiungi avviso, fare clic su **Nome** e immettere un nome e una descrizione per l'avviso.

4. Fare clic su **risorse** e selezionare le risorse da includere o escludere dall'avviso.

   È possibile impostare un filtro specificando una stringa di testo nel campo **Nome contiene** per selezionare un gruppo di risorse. In base alla stringa di testo specificata, l'elenco delle risorse disponibili visualizza solo le risorse corrispondenti alla regola di filtro. La stringa di testo specificata fa distinzione tra maiuscole e minuscole.

   Se una risorsa è conforme alle regole di inclusione ed esclusione specificate, la regola di esclusione ha la precedenza sulla regola di inclusione e l'avviso non viene generato per gli eventi correlati alla risorsa esclusa.

5. Fare clic su **Eventi** e selezionare gli eventi in base al nome dell'evento o al tipo di severità per cui si desidera attivare un avviso.

   Per selezionare più eventi, premere il tasto Ctrl mentre si effettuano le selezioni.

6. Fare clic su **azioni**, selezionare gli utenti che si desidera notificare, scegliere la frequenza di notifica, scegliere se inviare una trap SNMP al ricevitore della trap e assegnare uno script da eseguire quando viene generato un avviso.

   Se si modifica l'indirizzo di posta elettronica specificato per l'utente e si riapre l'avviso per la modifica, il campo Nome appare vuoto perché l'indirizzo di posta elettronica modificato non è più associato all'utente precedentemente selezionato. Inoltre, se l'indirizzo e-mail dell'utente selezionato è stato modificato dalla pagina utenti, l'indirizzo e-mail modificato non viene aggiornato per l'utente selezionato.

   È inoltre possibile scegliere di inviare una notifica agli utenti tramite trap SNMP.

7. Fare clic su **Save** (Salva).

Esempio di aggiunta di un avviso

Questo esempio mostra come creare un avviso che soddisfi i seguenti requisiti:

- Nome avviso: HealthTest
- Risorse: Include tutti i volumi il cui nome contiene "abc" ed esclude tutti i volumi il cui nome contiene "xyz"
- Eventi: Include tutti gli eventi sanitari critici
- Azioni: Include "sample@domain.com", uno script "Test" e l'utente deve ricevere una notifica ogni 15 minuti

Nella finestra di dialogo Aggiungi avviso, attenersi alla seguente procedura:

Fasi

1. Fare clic su **Nome** e immettere **HealthTest** nel campo **Nome avviso**.
2. Fare clic su **Resources** (risorse) e nella scheda include (Includi) selezionare **Volumes** (volumi) dall'elenco a discesa.
   a. Immettere **abc** nel campo **Nome contiene** per visualizzare i volumi il cui nome contiene "abc".
   b. Selezionare **<<All Volumes whose name contains 'abc'>>** dall'area risorse disponibili e spostarla nell'area risorse selezionate.
   c. Fare clic su **Escludi**, immettere **xyz** nel campo **Nome contiene**, quindi fare clic su **Aggiungi**.
3. Fare clic su **Eventi** e selezionare **critico** dal campo gravità evento.

4. Selezionare **All Critical Events** (tutti gli eventi critici) dall'area Matching Events (Eventi corrispondenti) e spostarla nell'area Selected Events (Eventi selezionati).
5. Fare clic su **azioni** e digitare **sample@domain.com** nel campo Avvisa questi utenti.
6. Selezionare **promemoria ogni 15 minuti** per avvisare l'utente ogni 15 minuti.

   È possibile configurare un avviso per inviare ripetutamente notifiche ai destinatari per un periodo di tempo specificato. È necessario determinare l'ora in cui la notifica dell'evento è attiva per l'avviso.

7. Nel menu Select script to Execute (Seleziona script da eseguire), selezionare **Test** script.
8. Fare clic su **Save** (Salva).

Modifica della password utente locale

È possibile modificare la password di accesso utente locale per evitare potenziali rischi per la sicurezza.

Cosa ti serve

Devi essere connesso come utente locale.

Le password per l'utente di manutenzione e per gli utenti remoti non possono essere modificate seguendo questa procedura. Per modificare la password di un utente remoto, contattare l'amministratore della password. Per modificare la password utente per la manutenzione, vedere "Utilizzando la console di manutenzione".

Fasi

1. Accedere a Unified Manager.
2. Dalla barra dei menu superiore, fare clic sull'icona dell'utente, quindi fare clic su **Change Password** (Modifica password).

   L'opzione **Change Password** (Modifica password) non viene visualizzata se si è utenti remoti.

3. Nella finestra di dialogo Change Password (Modifica password), immettere la password corrente e la nuova password.
4. Fare clic su **Save** (Salva).

Se Unified Manager è configurato in una configurazione ad alta disponibilità, è necessario modificare la password sul secondo nodo dell'installazione. Entrambe le istanze devono avere la stessa password.

Impostazione del timeout di inattività della sessione

È possibile specificare il valore di timeout di inattività per Unified Manager in modo che la sessione venga terminata automaticamente dopo un determinato periodo di tempo. Per impostazione predefinita, il timeout è impostato su 4,320 minuti (72 ore).

Cosa ti serve

È necessario disporre del ruolo di amministratore dell'applicazione.

Questa impostazione ha effetto su tutte le sessioni utente registrate.

Questa opzione non è disponibile se è stata attivata l'autenticazione SAML (Security Assertion Markup Language).

Fasi

1. Nel riquadro di navigazione a sinistra, fare clic su **Generale** > **Impostazioni funzionalità**.
2. Nella pagina **Feature Settings**, specificare il timeout di inattività scegliendo una delle seguenti opzioni:

Se si desidera…	Quindi…
Non impostare alcun timeout in modo che la sessione non venga mai chiusa automaticamente	Nel pannello **Timeout inattività**, spostare il dispositivo di scorrimento verso sinistra (Off) e fare clic su **Apply** (Applica).
Impostare un numero specifico di minuti come valore di timeout	Nel pannello **Timeout inattività**, spostare il cursore a destra (on), specificare il valore del timeout di inattività in minuti e fare clic su **Applica**.

Modifica del nome host di Unified Manager

A un certo punto, potrebbe essere necessario modificare il nome host del sistema su cui è stato installato Unified Manager. Ad esempio, è possibile rinominare l'host per identificare più facilmente i server Unified Manager in base al tipo, al gruppo di lavoro o al gruppo di cluster monitorato.

I passaggi necessari per modificare il nome host variano a seconda che Unified Manager sia in esecuzione su un server VMware ESXi, Red Hat o CentOS Linux o Microsoft Windows.

Modifica del nome host dell'appliance virtuale Unified Manager

All'host di rete viene assegnato un nome quando l'appliance virtuale di Unified Manager viene implementata per la prima volta. È possibile modificare il nome host dopo l'implementazione. Se si modifica il nome host, è necessario rigenerare anche il certificato HTTPS.

Cosa ti serve

Per eseguire queste attività, è necessario essere connessi a Unified Manager come utente di manutenzione o avere il ruolo di amministratore dell'applicazione assegnato.

È possibile utilizzare il nome host (o l'indirizzo IP host) per accedere all'interfaccia utente Web di Unified Manager. Se durante l'implementazione è stato configurato un indirizzo IP statico per la rete, sarebbe stato designato un nome per l'host di rete. Se la rete è stata configurata utilizzando DHCP, il nome host deve essere preso dal DNS. Se DHCP o DNS non sono configurati correttamente, il nome host "Unified Manager" viene assegnato automaticamente e associato al certificato di protezione.

Indipendentemente dalla modalità di assegnazione del nome host, se si modifica il nome host e si intende utilizzare il nuovo nome host per accedere all'interfaccia utente Web di Unified Manager, è necessario generare un nuovo certificato di protezione.

Se si accede all'interfaccia utente Web utilizzando l'indirizzo IP del server invece del nome host, non è

necessario generare un nuovo certificato se si modifica il nome host. Tuttavia, è consigliabile aggiornare il certificato in modo che il nome host del certificato corrisponda al nome host effettivo.

Se si modifica il nome host in Unified Manager, è necessario aggiornare manualmente il nome host in OnCommand Workflow Automation (Wfa). Il nome host non viene aggiornato automaticamente in WFA.

Il nuovo certificato non ha effetto fino al riavvio della macchina virtuale di Unified Manager.

Fasi

1. Generare un certificato di protezione HTTPS

   Se si desidera utilizzare il nuovo nome host per accedere all'interfaccia utente Web di Unified Manager, è necessario rigenerare il certificato HTTPS per associarlo al nuovo nome host.

2. Riavviare la macchina virtuale di Unified Manager

   Dopo aver rigenerato il certificato HTTPS, è necessario riavviare la macchina virtuale di Unified Manager.

Generazione di un certificato di protezione HTTPS

Quando Active IQ Unified Manager viene installato per la prima volta, viene installato un certificato HTTPS predefinito. È possibile generare un nuovo certificato di protezione HTTPS che sostituisce il certificato esistente.

Cosa ti serve

È necessario disporre del ruolo di amministratore dell'applicazione.

Possono esserci diversi motivi per rigenerare il certificato, ad esempio se si desidera ottenere valori migliori per Nome distinto (DN) o se si desidera una dimensione della chiave più elevata o un periodo di scadenza più lungo o se il certificato corrente è scaduto.

Se non si dispone dell'accesso all'interfaccia utente Web di Unified Manager, è possibile rigenerare il certificato HTTPS con gli stessi valori utilizzando la console di manutenzione. Durante la rigenerazione dei certificati, è possibile definire la dimensione della chiave e la durata della validità della chiave. Se si utilizza `Reset Server Certificate` Dalla console di manutenzione, viene creato un nuovo certificato HTTPS valido per 397 giorni. Questo certificato avrà una chiave RSA di 2048 bit.

Fasi

1. Nel riquadro di spostamento a sinistra, fare clic su **Generale** > **certificato HTTPS**.
2. Fare clic su **Rigenera certificato HTTPS**.

   Viene visualizzata la finestra di dialogo Rigenera certificato HTTPS.

3. Selezionare una delle seguenti opzioni a seconda della modalità di generazione del certificato:

Se si desidera…	Eseguire questa operazione…
Rigenera il certificato con i valori correnti	Fare clic sull'opzione **Rigenera using Current Certificate Attributes**.

Se si desidera…	Eseguire questa operazione…
Generare il certificato utilizzando valori diversi	Fare clic sull'opzione **Update the Current Certificate Attributes** (Aggiorna attributi del certificato corrente). I campi Nome comune e nomi alternativi utilizzano i valori del certificato esistente se non vengono immessi nuovi valori. Il campo "Common Name" deve essere impostato sull'FQDN dell'host. Gli altri campi non richiedono valori, ma è possibile inserire valori, ad esempio, per L'EMAIL, LA SOCIETÀ, IL REPARTO, Città, Stato e Paese se si desidera inserire tali valori nel certificato. È inoltre possibile selezionare una DELLE DIMENSIONI DELLA CHIAVE disponibili (l'algoritmo della chiave è "RSA"). E PERIODO di validità. • I valori consentiti per la dimensione della chiave sono `2048`, `3072` e. `4096`. • I periodi di validità vanno da un minimo di 1 giorno a un massimo di 36500 giorni. Anche se è consentito un periodo di validità di 36500 giorni, si consiglia di utilizzare un periodo di validità non superiore a 397 giorni o 13 mesi. Poiché se si seleziona un periodo di validità superiore a 397 giorni e si prevede di esportare una CSR per questo certificato e di ottenerla firmata da una CA nota, la validità del certificato firmato restituito dalla CA sarà ridotta a 397 giorni. • Selezionare la casella di controllo "Escludi informazioni di identificazione locali (ad es. Host locale)" se si desidera rimuovere le informazioni di identificazione locali dal campo dei nomi alternativi del certificato. Quando questa casella di controllo è selezionata, nel campo nomi alternativi viene utilizzato solo il valore immesso nel campo. Se lasciato vuoto, il certificato risultante non avrà alcun campo di nomi alternativi.

4. Fare clic su **Sì** per rigenerare il certificato.
5. Riavviare il server Unified Manager in modo che il nuovo certificato abbia effetto.
6. Verificare le informazioni sul nuovo certificato visualizzando il certificato HTTPS.

Riavvio della macchina virtuale di Unified Manager

È possibile riavviare la macchina virtuale dalla console di manutenzione di Unified Manager. Riavviare dopo aver generato un nuovo certificato di protezione o in caso di problemi con la macchina virtuale.

Cosa ti serve

L'appliance virtuale è accesa.

Si è connessi alla console di manutenzione come utente di manutenzione.

È inoltre possibile riavviare la macchina virtuale da vSphere utilizzando l'opzione **Restart Guest**. Per ulteriori informazioni, consultare la documentazione di VMware.

Fasi

1. Accedere alla console di manutenzione.
2. Selezionare **Configurazione del sistema** > **riavvio della macchina virtuale**.

Modifica del nome host di Unified Manager sui sistemi Linux

A un certo punto, potrebbe essere necessario modificare il nome host della macchina Red Hat Enterprise Linux o CentOS su cui è stato installato Unified Manager. Ad esempio, è possibile rinominare l'host per identificare più facilmente i server Unified Manager in base al tipo, al gruppo di lavoro o al gruppo di cluster monitorato quando si elencano i computer Linux.

Cosa ti serve

È necessario disporre dell'accesso utente root al sistema Linux su cui è installato Unified Manager.

È possibile utilizzare il nome host (o l'indirizzo IP host) per accedere all'interfaccia utente Web di Unified Manager. Se durante l'implementazione è stato configurato un indirizzo IP statico per la rete, sarebbe stato designato un nome per l'host di rete. Se la rete è stata configurata utilizzando DHCP, il nome host deve essere preso dal server DNS.

Indipendentemente dalla modalità di assegnazione del nome host, se si modifica il nome host e si intende utilizzare il nuovo nome host per accedere all'interfaccia utente Web di Unified Manager, è necessario generare un nuovo certificato di protezione.

Se si accede all'interfaccia utente Web utilizzando l'indirizzo IP del server invece del nome host, non è necessario generare un nuovo certificato se si modifica il nome host. Tuttavia, è consigliabile aggiornare il certificato in modo che il nome host del certificato corrisponda al nome host effettivo. Il nuovo certificato non ha effetto fino al riavvio della macchina Linux.

Se si modifica il nome host in Unified Manager, è necessario aggiornare manualmente il nome host in OnCommand Workflow Automation (Wfa). Il nome host non viene aggiornato automaticamente in WFA.

Fasi

1. Accedere come utente root al sistema Unified Manager che si desidera modificare.
2. Arrestare il software Unified Manager e il software MySQL associato immettendo il seguente comando:

   ```
   systemctl stop ocieau ocie mysqld
   ```

3. Modificare il nome host utilizzando Linux `hostnamectl` comando:

   ```
   hostnamectl set-hostname new_FQDN
   ```

   ```
   hostnamectl set-hostname nuhost.corp.widget.com
   ```

4. Rigenerare il certificato HTTPS per il server:

   ```
   /opt/netapp/essentials/bin/cert.sh create
   ```

5. Riavviare il servizio di rete:

   ```
   service network restart
   ```

6. Una volta riavviato il servizio, verificare se il nuovo nome host è in grado di eseguire il ping:

   ```
   ping new_hostname
   ```

   ```
   ping nuhost
   ```

   Questo comando dovrebbe restituire lo stesso indirizzo IP precedentemente impostato per il nome host originale.

7. Dopo aver completato e verificato la modifica del nome host, riavviare Unified Manager immettendo il seguente comando:

   ```
   systemctl start mysqld ocie ocieau
   ```

Attivazione e disattivazione della gestione dello storage basata su policy

A partire da Unified Manager 9.7, è possibile eseguire il provisioning dei carichi di lavoro dello storage (volumi e LUN) sui cluster ONTAP e gestire tali carichi di lavoro in base ai livelli di servizio delle performance assegnati. Questa funzionalità è simile alla creazione di carichi di lavoro in Gestione di sistema ONTAP e al collegamento di policy di qualità del servizio, ma se applicata con Gestione unificata è possibile eseguire il provisioning e la gestione dei carichi di lavoro in tutti i cluster monitorati dall'istanza di Gestione unificata.

È necessario disporre del ruolo di amministratore dell'applicazione.

Questa opzione è attivata per impostazione predefinita, ma è possibile disattivarla se non si desidera eseguire il provisioning e la gestione dei carichi di lavoro utilizzando Unified Manager.

Se attivata, questa opzione fornisce molti nuovi elementi nell'interfaccia utente:

Nuovi contenuti	Posizione
Una pagina per il provisioning di nuovi workload	Disponibile da **attività comuni** > **Provisioning**
Una pagina per creare policy sui livelli di servizio per le performance	Disponibile in **Impostazioni** > **politiche** > **livelli di servizio delle performance**
Una pagina per creare policy di efficienza dello storage per le performance	Disponibile in **Impostazioni** > **politiche** > **efficienza dello storage**
Pannelli che descrivono gli IOPS correnti relativi a workload Performance e workload	Disponibile nella dashboard

Per ulteriori informazioni su queste pagine e su questa funzionalità, consultare la guida in linea del prodotto.

Fasi

1. Nel riquadro di navigazione a sinistra, fare clic su **Generale** > **Impostazioni funzionalità**.
2. Nella pagina **Feature Settings**, disattivare o attivare la gestione dello storage basata su policy scegliendo una delle seguenti opzioni:

Se si desidera…	Quindi…
Disattiva la gestione dello storage basata su policy	Nel pannello **Policy-based storage management** (Gestione dello storage basata su policy), spostare il pulsante di scorrimento verso sinistra.
Gestione dello storage basata su policy	Nel pannello **Policy-based storage management** (Gestione dello storage basata su policy), spostare il pulsante di scorrimento verso destra.

Configurazione del backup di Unified Manager

È possibile configurare la funzionalità di backup su Unified Manager attraverso una serie di procedure di configurazione da eseguire sui sistemi host e sulla console di manutenzione.

Per informazioni sulla procedura di configurazione, vedere "Gestione delle operazioni di backup e ripristino".

Gestione delle impostazioni delle funzioni

La pagina Impostazioni funzionalità consente di attivare e disattivare funzioni specifiche in Active IQ Unified Manager. Ciò include la creazione e la gestione di oggetti di storage in base a policy, l'abilitazione del gateway API e del banner di accesso, il caricamento di script per la gestione degli avvisi, il timeout di una sessione dell'interfaccia utente Web in base al tempo di inattività e la disattivazione della ricezione degli eventi della piattaforma Active IQ.

La pagina Feature Settings (Impostazioni funzionalità) è disponibile solo per gli utenti con ruolo di amministratore dell'applicazione.

Per informazioni sul caricamento degli script, vedere "Attivazione e disattivazione del caricamento degli script".

Gestione dello storage basata su policy

L'opzione **Gestione dello storage basata su policy** consente la gestione dello storage in base agli obiettivi del livello di servizio (SLO). Questa opzione è attivata per impostazione predefinita.

Attivando questa funzionalità, è possibile eseguire il provisioning dei carichi di lavoro dello storage sui cluster ONTAP aggiunti alla propria istanza di Active IQ Unified Manager e gestire questi carichi di lavoro in base ai livelli di servizio delle performance assegnati e alle policy di efficienza dello storage.

Puoi scegliere di attivare o disattivare questa funzione da **Generale** > **Impostazioni funzionalità** > **Gestione dello storage basata su policy**. All'attivazione di questa funzione, sono disponibili le seguenti pagine per il funzionamento e il monitoraggio:

- Provisioning (provisioning del carico di lavoro dello storage)
- **Policy** > **Performance Service level**
- **Criteri** > **efficienza dello storage**
- Workload gestiti da Performance Service Level nella pagina Clusters Setup
- Pannello delle performance del carico di lavoro sul pannello **Dashboard**

È possibile utilizzare le schermate per creare livelli di servizio delle performance e policy di efficienza dello storage e per eseguire il provisioning dei carichi di lavoro dello storage. È inoltre possibile monitorare i carichi di lavoro dello storage conformi ai livelli di Performance Service assegnati, nonché quelli non conformi. Il pannello Workload Performance and workload IOPS (IOPS workload Performance e workload IOPS) consente inoltre di valutare la capacità e le performance totali, disponibili e utilizzate dei cluster nel data center in base ai carichi di lavoro storage su di essi forniti.

Dopo aver attivato questa funzione, è possibile eseguire le API REST di Unified Manager per eseguire alcune di queste funzioni dalla **barra dei menu** > **pulsante della Guida** > **documentazione API** > **categoria storage-provider**. In alternativa, è possibile inserire il nome host o l'indirizzo IP e l'URL per accedere alla pagina API REST nel formato https://<hostname>/docs/api/

Per ulteriori informazioni sulle API, vedere "Introduzione alle API REST di Active IQ Unified Manager".

Abilitazione di API Gateway

La funzione gateway API consente a Active IQ Unified Manager di essere un singolo piano di controllo da cui è possibile gestire più cluster ONTAP, senza dover effettuare l'accesso singolarmente.

È possibile attivare questa funzione dalle pagine di configurazione visualizzate quando si accede per la prima volta a Unified Manager. In alternativa, è possibile attivare o disattivare questa funzione da **Generale** > **Impostazioni funzionalità** > **Gateway API**.

Le API REST di Unified Manager sono diverse dalle API REST di ONTAP e non tutte le funzionalità delle API REST di ONTAP possono essere utilizzate utilizzando le API REST di Unified Manager. Tuttavia, se si dispone

di un requisito di business specifico per l'accesso alle API di ONTAP per la gestione di funzionalità specifiche non esposte a Unified Manager, è possibile attivare la funzione di gateway API ed eseguire le API di ONTAP. Il gateway funge da proxy per il tunneling delle richieste API mantenendo le richieste di intestazione e corpo nello stesso formato delle API ONTAP. È possibile utilizzare le credenziali di Unified Manager ed eseguire le API specifiche per accedere e gestire i cluster ONTAP senza passare le credenziali dei singoli cluster. Unified Manager funziona come un singolo punto di gestione per l'esecuzione delle API nei cluster ONTAP gestiti dall'istanza di Unified Manager. La risposta restituita dalle API è la stessa della risposta restituita dalle rispettive API REST ONTAP eseguite direttamente da ONTAP.

Dopo aver attivato questa funzione, è possibile eseguire le API REST di Unified Manager da **barra dei menu** > **pulsante della Guida** > **documentazione API** > **gateway** categoria. In alternativa, è possibile inserire il nome host o l'indirizzo IP e l'URL per accedere alla pagina API REST nel formato `https://<hostname>/docs/api/`

Per ulteriori informazioni sulle API, vedere "Introduzione alle API REST di Active IQ Unified Manager".

Specifica del timeout di inattività

È possibile specificare il valore di timeout di inattività per Active IQ Unified Manager. Dopo un periodo di inattività pari al tempo specificato, l'applicazione viene disconnessa automaticamente. Questa opzione è attivata per impostazione predefinita.

È possibile disattivare questa funzione o modificare l'ora da **Generale** > **Impostazioni funzionalità** > **Timeout inattività**. Una volta attivata questa funzione, specificare il limite di tempo di inattività (in minuti) nel campo **DISCONNETTI DOPO**, dopodiché il sistema si disconnette automaticamente. Il valore predefinito è 4320 minuti (72 ore).

Questa opzione non è disponibile se è stata attivata l'autenticazione SAML (Security Assertion Markup Language).

Attivazione degli eventi del portale Active IQ

È possibile specificare se si desidera attivare o disattivare gli eventi del portale Active IQ. Questa impostazione consente al portale Active IQ di rilevare e visualizzare eventi aggiuntivi relativi alla configurazione del sistema, al cablaggio e così via. Questa opzione è attivata per impostazione predefinita.

Attivando questa funzione, Active IQ Unified Manager visualizza gli eventi rilevati dal portale Active IQ. Questi eventi vengono creati eseguendo una serie di regole per i messaggi AutoSupport generati da tutti i sistemi di storage monitorati. Questi eventi sono diversi dagli altri eventi di Unified Manager e identificano incidenti o rischi correlati a problemi di configurazione del sistema, cablaggio, Best practice e disponibilità.

Puoi scegliere di attivare o disattivare questa funzione da **Generale** > **Impostazioni funzionalità** > **Eventi portale Active IQ**. Nei siti senza accesso alla rete esterna, è necessario caricare manualmente le regole da **Storage Management** > **Event Setup** > **Upload Rules**.

Questa funzione è attivata per impostazione predefinita. La disattivazione di questa funzione impedisce il rilevamento o la visualizzazione degli eventi Active IQ in Unified Manager. Se disattivata, questa funzione consente a Unified Manager di ricevere gli eventi Active IQ su un cluster a un'ora predefinita di 00:15 per quel fuso orario del cluster.

Attivazione e disattivazione delle impostazioni di sicurezza per la conformità

Utilizzando il pulsante **Customize** (Personalizza) nel pannello **Security Dashboard** della pagina Features Settings (Impostazioni funzionalità), è possibile attivare o disattivare i parametri di sicurezza per il monitoraggio della conformità in Unified Manager.

Le impostazioni attivate o disattivate in questa pagina regolano lo stato di conformità generale dei cluster e delle VM di storage su Unified Manager. In base alle selezioni, le colonne corrispondenti sono visibili nella vista **sicurezza: Tutti i cluster** della pagina di inventario dei cluster e nella vista **sicurezza: Tutte le macchine virtuali di storage** della pagina di inventario delle macchine virtuali di storage.

Solo gli utenti con ruolo di amministratore possono modificare queste impostazioni.

I criteri di sicurezza per i cluster ONTAP, le VM di storage e i volumi vengono valutati in base alle raccomandazioni definite nella "Guida al rafforzamento della sicurezza per NetApp ONTAP 9". Il pannello Security (sicurezza) della dashboard e la pagina Security (sicurezza) visualizzano lo stato di conformità di sicurezza predefinito di cluster, storage VM e volumi. Vengono inoltre generati eventi di sicurezza e attivate azioni di gestione per i cluster e le VM di storage che presentano violazioni della sicurezza.

Personalizzazione delle impostazioni di sicurezza

Per personalizzare le impostazioni per il monitoraggio della conformità in base all'ambiente ONTAP in uso, attenersi alla seguente procedura:

Fasi

1. Fare clic su **General > Feature Settings > Security Dashboard > Customize** (Generale > Impostazioni funzionalità > pannello di protezione > Personalizza) Viene visualizzata la finestra a comparsa **Customize Security Dashboard Settings** (Personalizza impostazioni dashboard di protezione).

   I parametri di conformità della sicurezza che si abilitano o disabilitano possono influire direttamente sulle viste di sicurezza predefinite, sui report e sui report pianificati nelle schermate Clusters e Storage VM. Se è stato caricato un report excel da queste schermate prima di modificare i parametri di sicurezza, i report excel scaricati potrebbero essere errati.

2. Per attivare o disattivare le impostazioni personalizzate per i cluster ONTAP, selezionare l'impostazione generale richiesta in **cluster**. Per informazioni sulle opzioni di personalizzazione della conformità del cluster, vedere "Categorie di compliance del cluster".
3. Per attivare o disattivare le impostazioni personalizzate per le VM di storage, selezionare l'impostazione generale richiesta in **Storage VM**. Per informazioni sulle opzioni di personalizzazione della conformità delle macchine virtuali dello storage, vedere "Categorie di conformità delle VM di storage".

Personalizzazione delle impostazioni di autenticazione e AutoSupport

Nella sezione **Impostazioni AutoSupport**, è possibile specificare se utilizzare il trasporto HTTPS per l'invio di messaggi AutoSupport da ONTAP.

Dalla sezione **Impostazioni di autenticazione**, è possibile attivare gli avvisi di Unified Manager per l'utente amministratore ONTAP predefinito.

Attivazione e disattivazione del caricamento degli script

Per impostazione predefinita, è attivata la possibilità di caricare gli script in Unified Manager ed eseguirli. Se l'organizzazione non desidera consentire questa attività per motivi di sicurezza, è possibile disattivare questa funzionalità.

Cosa ti serve

È necessario disporre del ruolo di amministratore dell'applicazione.

Fasi

1. Nel riquadro di navigazione a sinistra, fare clic su **Generale** > **Impostazioni funzionalità**.
2. Nella pagina **Impostazioni funzionalità**, disattivare o attivare lo scripting scegliendo una delle seguenti opzioni:

Se si desidera…	Quindi…
Disattivare gli script	Nel pannello **script Upload**, spostare il cursore verso sinistra.
Abilitare gli script	Nel pannello **script Upload**, spostare il cursore verso destra.

Aggiunta banner di accesso

L'aggiunta di un banner di accesso consente all'organizzazione di visualizzare qualsiasi informazione, ad esempio chi ha accesso al sistema e i termini e le condizioni di utilizzo durante l'accesso e la disconnessione.

Qualsiasi utente, ad esempio gli operatori di storage o gli amministratori, può visualizzare questa finestra a comparsa del banner di accesso durante l'accesso, la disconnessione e il timeout della sessione.

Utilizzando la console di manutenzione

È possibile utilizzare la console di manutenzione per configurare le impostazioni di rete, configurare e gestire il sistema su cui è installato Unified Manager ed eseguire altre attività di manutenzione che consentono di prevenire e risolvere eventuali problemi.

Quali funzionalità offre la console di manutenzione

La console di manutenzione di Unified Manager consente di mantenere le impostazioni del sistema Unified Manager e di apportare le modifiche necessarie per evitare che si verifichino problemi.

A seconda del sistema operativo su cui è stato installato Unified Manager, la console di manutenzione offre le seguenti funzioni:

- Risolvere eventuali problemi relativi all'appliance virtuale, in particolare se l'interfaccia Web di Unified

Manager non è disponibile

- Eseguire l'aggiornamento alle versioni più recenti di Unified Manager
- Generare pacchetti di supporto da inviare al supporto tecnico
- Configurare le impostazioni di rete
- Modificare la password utente per la manutenzione
- Connettersi a un provider di dati esterno per inviare statistiche sulle prestazioni
- Modificare la raccolta di dati sulle performance interna
- Ripristinare il database e le impostazioni di configurazione di Unified Manager da una versione precedentemente sottoposta a backup.

Cosa fa l'utente che effettua la manutenzione

L'utente di manutenzione viene creato durante l'installazione di Unified Manager su un sistema Red Hat Enterprise Linux o CentOS. Il nome utente per la manutenzione è l'utente "umadmin". L'utente di manutenzione ha il ruolo di amministratore dell'applicazione nell'interfaccia utente Web e può creare utenti successivi e assegnarli ruoli.

L'utente di manutenzione, o umadmin, può anche accedere alla console di manutenzione di Unified Manager.

Funzionalità diagnostiche per l'utente

Lo scopo dell'accesso diagnostico è quello di consentire al supporto tecnico di fornire assistenza nella risoluzione dei problemi e utilizzarlo solo quando richiesto dal supporto tecnico.

L'utente della diagnostica può eseguire comandi a livello di sistema operativo quando richiesto dal supporto tecnico, a scopo di risoluzione dei problemi.

Accesso alla console di manutenzione

Se l'interfaccia utente di Unified Manager non è in funzione o se è necessario eseguire funzioni non disponibili nell'interfaccia utente, è possibile accedere alla console di manutenzione per gestire il sistema Unified Manager.

Cosa ti serve

Unified Manager deve essere installato e configurato.

Dopo 15 minuti di inattività, la console di manutenzione si disconnette.

> Una volta installato su VMware, se si è già effettuato l'accesso come utente di manutenzione tramite la console VMware, non è possibile effettuare l'accesso simultaneo utilizzando Secure Shell.

Fase

1. Per accedere alla console di manutenzione, procedere come segue:

Su questo sistema operativo…	Attenersi alla procedura descritta di seguito…
VMware	a. Utilizzando Secure Shell, connettersi all'indirizzo IP o al nome di dominio completo dell'appliance virtuale Unified Manager. b. Accedere alla console di manutenzione utilizzando il nome utente e la password di manutenzione.
Linux	a. Utilizzando Secure Shell, connettersi all'indirizzo IP o al nome di dominio completo del sistema Unified Manager. b. Accedere al sistema con il nome utente di manutenzione (umadmin) e la password. c. Immettere il comando `maintenance_console` E premere Invio.
Windows	a. Accedere al sistema Unified Manager con le credenziali di amministratore. b. Avviare PowerShell come amministratore di Windows. c. Immettere il comando `maintenance_console` E premere Invio.

Viene visualizzato il menu della console di manutenzione di Unified Manager.

Accesso alla console di manutenzione mediante la console vSphere VM

Se l'interfaccia utente di Unified Manager non è in funzione o se è necessario eseguire funzioni non disponibili nell'interfaccia utente, è possibile accedere alla console di manutenzione per riconfigurare l'appliance virtuale.

Cosa ti serve

- È necessario essere l'utente che esegue la manutenzione.
- L'appliance virtuale deve essere accesa per accedere alla console di manutenzione.

Fasi

1. In vSphere Client, individuare l'appliance virtuale Unified Manager.
2. Fare clic sulla scheda **Console**.
3. Fare clic all'interno della finestra della console per accedere.
4. Accedere alla console di manutenzione utilizzando il nome utente e la password.

   Dopo 15 minuti di inattività, la console di manutenzione si disconnette.

Menu della console di manutenzione

La console di manutenzione è composta da diversi menu che consentono di gestire e gestire funzioni speciali e impostazioni di configurazione del server Unified Manager.

A seconda del sistema operativo su cui è stato installato Unified Manager, la console di manutenzione è composta dai seguenti menu:

- Upgrade di Unified Manager (solo VMware)
- Configurazione di rete (solo VMware)
- Configurazione del sistema (solo VMware)
  a. Supporto/Diagnostica
  b. Reimposta certificato server
  c. Provider di dati esterno
  d. Backup Restore (Ripristino backup
  e. Configurazione dell'intervallo di polling delle performance
  f. Disattiva l'autenticazione SAML
  g. Visualizzare/modificare le porte dell'applicazione
  h. Configurazione del registro di debug
  i. Controlla l'accesso alla porta MySQL 3306
  j. Esci

Selezionare il numero dall'elenco per accedere all'opzione di menu specifica. Ad esempio, per il backup e il ripristino, selezionare *4*.

Menu Network Configuration (Configurazione di rete)

Il menu Configurazione di rete consente di gestire le impostazioni di rete. Utilizzare questo menu quando l'interfaccia utente di Unified Manager non è disponibile.

Questo menu non è disponibile se Unified Manager è installato su Red Hat Enterprise Linux, CentOS o Microsoft Windows.

Sono disponibili le seguenti opzioni di menu.

- **Visualizza impostazioni indirizzo IP**

  Visualizza le impostazioni di rete correnti per l'appliance virtuale, inclusi indirizzo IP, rete, indirizzo di trasmissione, netmask, gateway, E server DNS.

- **Modifica delle impostazioni dell'indirizzo IP**

  Consente di modificare le impostazioni di rete dell'appliance virtuale, inclusi l'indirizzo IP, la netmask, il gateway o i server DNS. Se si passa dalle impostazioni di rete DHCP alle reti statiche utilizzando la console di manutenzione, non è possibile modificare il nome host. Per apportare le modifiche, selezionare **Conferma modifiche**.

- **Visualizza impostazioni di ricerca nome dominio**

Visualizza l’elenco di ricerca dei nomi di dominio utilizzato per risolvere i nomi host.

- **Modifica impostazioni di ricerca nome dominio**

  Consente di modificare i nomi di dominio di cui si desidera eseguire la ricerca durante la risoluzione dei nomi host. Per apportare le modifiche, selezionare **Conferma modifiche**.

- **Visualizza percorsi statici**

  Visualizza i percorsi di rete statici correnti.

- **Modifica percorsi statici**

  Consente di aggiungere o eliminare percorsi di rete statici. Per apportare le modifiche, selezionare **Conferma modifiche**.

  - **Aggiungi percorso**

    Consente di aggiungere un percorso statico.

  - **Elimina percorso**

    Consente di eliminare un percorso statico.

  - **Indietro**

    Consente di tornare al **Menu principale**.

  - **Esci**

    Consente di uscire dalla console di manutenzione.

- **Disattiva interfaccia di rete**

  Disattiva tutte le interfacce di rete disponibili. Se è disponibile una sola interfaccia di rete, non è possibile disattivarla. Per apportare le modifiche, selezionare **Conferma modifiche**.

- **Attiva interfaccia di rete**

  Abilita le interfacce di rete disponibili. Per apportare le modifiche, selezionare **Conferma modifiche**.

- **Conferma modifiche**

  Applica le modifiche apportate alle impostazioni di rete dell’appliance virtuale. È necessario selezionare questa opzione per applicare le modifiche apportate, altrimenti le modifiche non si verificano.

- **Ping di un host**

  Esegue il ping di un host di destinazione per confermare le modifiche dell’indirizzo IP o le configurazioni DNS.

- **Ripristina impostazioni predefinite**

  Ripristina tutte le impostazioni predefinite. Per apportare le modifiche, selezionare **Conferma modifiche**.

- **Indietro**

Consente di tornare al **Menu principale**.

- **Esci**

  Consente di uscire dalla console di manutenzione.

Menu Configurazione di sistema

Il menu System Configuration (Configurazione di sistema) consente di gestire l'appliance virtuale fornendo varie opzioni, ad esempio la visualizzazione dello stato del server, il riavvio e l'arresto della macchina virtuale.

> Quando Unified Manager è installato su un sistema Linux o Microsoft Windows, da questo menu è disponibile solo l'opzione "Restore from a Unified Manager Backup" (Ripristina da un backup di Unified Manager).

Sono disponibili le seguenti opzioni di menu:

- **Visualizza stato server**

  Visualizza lo stato corrente del server. Le opzioni di stato includono in esecuzione e non in esecuzione.

  Se il server non è in esecuzione, potrebbe essere necessario contattare il supporto tecnico.

- **Riavviare la macchina virtuale**

  Riavvia la macchina virtuale, interrompendo tutti i servizi. Dopo il riavvio, la macchina virtuale e i servizi vengono riavviati.

- **Spegnere la macchina virtuale**

  Arresta la macchina virtuale, interrompendo tutti i servizi.

  È possibile selezionare questa opzione solo dalla console della macchina virtuale.

- **Modifica password utente <logged in user>**

  Modifica la password dell'utente attualmente connesso, che può essere solo l'utente di manutenzione.

- **Aumentare le dimensioni del disco dati**

  Aumenta le dimensioni del disco dati (disco 3) nella macchina virtuale.

- **Aumentare le dimensioni del disco di swap**

  Aumenta le dimensioni del disco di swap (disco 2) nella macchina virtuale.

- **Modifica fuso orario**

  Consente di modificare il fuso orario in base alla posizione.

- **Cambia server NTP**

  Modifica le impostazioni del server NTP, ad esempio l'indirizzo IP o il nome di dominio completo (FQDN).

- **Cambia servizio NTP**

  Consente di passare da `ntp` e. `systemd-timesyncd` servizi.

- **Ripristino da un backup di Unified Manager**

  Ripristina il database e le impostazioni di configurazione di Unified Manager da una versione precedentemente sottoposta a backup.

- **Ripristina certificato server**

  Ripristina il certificato di sicurezza del server.

- **Modifica nome host**

  Modifica il nome dell'host su cui è installata l'appliance virtuale.

- **Indietro**

  Consente di uscire dal menu Configurazione di sistema e tornare al menu principale.

- **Esci**

  Consente di uscire dal menu della console di manutenzione.

Menu Support and Diagnostics (supporto e diagnostica)

Il menu Support and Diagnostics (supporto e diagnostica) consente di generare un pacchetto di supporto che è possibile inviare al supporto tecnico per ottenere assistenza per la risoluzione dei problemi.

Sono disponibili le seguenti opzioni di menu:

- **Genera bundle di supporto leggero**

  Consente di produrre un bundle di supporto leggero che contiene solo 30 giorni di registri e record del database di configurazione, escludendo i dati sulle performance, i file di registrazione dell'acquisizione e il dump dell'heap del server.

- **Genera bundle di supporto**

  Consente di creare un bundle di supporto completo (file 7-zip) contenente informazioni diagnostiche nella home directory dell'utente di diagnostica. Se il sistema è connesso a Internet, è anche possibile caricare il pacchetto di supporto su NetApp.

  Il file include le informazioni generate da un messaggio AutoSupport, il contenuto del database di Unified Manager, i dati dettagliati sugli interni del server di Unified Manager e i registri a livello dettagliato non normalmente inclusi nei messaggi AutoSupport o nel bundle di supporto leggero.

Opzioni di menu aggiuntive

Le seguenti opzioni di menu consentono di eseguire varie attività amministrative sul server Unified Manager.

Sono disponibili le seguenti opzioni di menu:

- **Ripristina certificato server**

  Rigenera il certificato del server HTTPS.

  È possibile rigenerare il certificato del server nella GUI di Unified Manager facendo clic su **Generale** > **certificati HTTPS** > **Rigenera certificato HTTPS**.

- **Disattiva autenticazione SAML**

  Disattiva l'autenticazione SAML in modo che il provider di identità (IdP) non fornisca più l'autenticazione di accesso per gli utenti che accedono alla GUI di Unified Manager. Questa opzione della console viene generalmente utilizzata quando un problema con il server IdP o la configurazione SAML impedisce agli utenti di accedere alla GUI di Unified Manager.

- **Fornitore di dati esterno**

  Fornisce opzioni per la connessione di Unified Manager a un provider di dati esterno. Una volta stabilita la connessione, i dati delle performance vengono inviati a un server esterno in modo che gli esperti delle performance dello storage possano tracciare le metriche delle performance utilizzando software di terze parti. Vengono visualizzate le seguenti opzioni:

  - **Display Server Configuration**-: Visualizza le impostazioni di connessione e configurazione correnti per un provider di dati esterno.
  - **Aggiungi / Modifica connessione server**--consente di inserire nuove impostazioni di connessione per un provider di dati esterno o di modificare le impostazioni esistenti.
  - **Modifica configurazione server**--consente di inserire nuove impostazioni di configurazione per un provider di dati esterno o di modificare le impostazioni esistenti.
  - **Delete Server Connection**--Elimina la connessione a un provider di dati esterno.

    Una volta eliminata la connessione, Unified Manager perde la connessione al server esterno.

- **Backup Restore**

  Per ulteriori informazioni, consultare gli argomenti della sezione "Gestione delle operazioni di backup e ripristino".

- **Configurazione dell'intervallo di polling delle prestazioni**

  Fornisce un'opzione per configurare la frequenza con cui Unified Manager raccoglie i dati statistici delle performance dai cluster. L'intervallo di raccolta predefinito è di 5 minuti.

  È possibile modificare questo intervallo in 10 o 15 minuti se si scopre che le raccolte di cluster di grandi dimensioni non vengono completate in tempo.

- **Visualizza/Modifica porte applicazione**

  Fornisce un'opzione per modificare le porte predefinite utilizzate da Unified Manager per i protocolli HTTP e HTTPS, se necessario per motivi di sicurezza. Le porte predefinite sono 80 per HTTP e 443 per HTTPS.

- **Controlla l'accesso alla porta MySQL 3306**

  Controlla l'accesso degli host alla porta MySQL predefinita 3306. Per motivi di sicurezza, l'accesso tramite

questa porta è limitato solo all'host locale durante una nuova installazione di Unified Manager su sistemi Linux, Windows e VMware vSphere. Questa opzione consente di alternare la visibilità di questa porta tra l'host locale e gli host remoti, vale a dire che se è abilitata per l'host locale solo nel proprio ambiente, è possibile rendere questa porta disponibile anche agli host remoti. In alternativa, se attivata per tutti gli host, è possibile limitare l'accesso a questa porta solo a localhost. Se l'accesso era stato precedentemente attivato sugli host remoti, la configurazione viene mantenuta in uno scenario di aggiornamento.

- **Esci**

  Consente di uscire dal menu della console di manutenzione.

Modifica della password utente per la manutenzione in Windows

Se necessario, è possibile modificare la password utente per la manutenzione di Unified Manager.

Fasi

1. Dalla pagina di accesso all'interfaccia utente Web di Unified Manager, fare clic su **Password dimenticata**.

   Viene visualizzata una pagina che richiede il nome dell'utente di cui si desidera reimpostare la password.

2. Inserire il nome utente e fare clic su **Submit** (Invia).

   Un'e-mail con un collegamento per reimpostare la password viene inviata all'indirizzo e-mail definito per tale nome utente.

3. Fare clic sul collegamento **reset password** nell'e-mail e definire la nuova password.
4. Tornare all'interfaccia utente Web e accedere a Unified Manager utilizzando la nuova password.

Modifica della password di umadmin sui sistemi Linux

Per motivi di sicurezza, è necessario modificare la password predefinita per l'utente di Unified Manager umadmin subito dopo aver completato il processo di installazione. Se necessario, è possibile modificare nuovamente la password in un secondo momento.

Cosa ti serve

- Unified Manager deve essere installato su un sistema Red Hat Enterprise Linux o CentOS Linux.
- È necessario disporre delle credenziali utente root per il sistema Linux su cui è installato Unified Manager.

Fasi

1. Accedere come utente root al sistema Linux su cui è in esecuzione Unified Manager.
2. Modificare la password di umadmin:

   ```
   passwd umadmin
   ```

   Il sistema richiede di inserire una nuova password per l'utente umadmin.

Modifica delle porte utilizzate da Unified Manager per i protocolli HTTP e HTTPS

Le porte predefinite utilizzate da Unified Manager per i protocolli HTTP e HTTPS possono essere modificate dopo l'installazione, se necessario per motivi di sicurezza. Le porte predefinite sono 80 per HTTP e 443 per HTTPS.

Cosa ti serve

Per accedere alla console di manutenzione del server Unified Manager, è necessario disporre di un ID utente e di una password autorizzati.

> Alcune porte sono considerate non sicure quando si utilizzano i browser Mozilla Firefox o Google Chrome. Verificare con il browser prima di assegnare un nuovo numero di porta per il traffico HTTP e HTTPS. La selezione di una porta non sicura potrebbe rendere il sistema inaccessibile, il che richiederebbe di contattare il supporto clienti per una risoluzione.

L'istanza di Unified Manager viene riavviata automaticamente dopo aver modificato la porta, quindi assicurarsi che questo sia il momento giusto per spegnere il sistema per un breve periodo di tempo.

1. Accedere utilizzando SSH come utente di manutenzione all'host di Unified Manager.

   Vengono visualizzati i prompt della console di Unified Managermaintenance.

2. Digitare il numero dell'opzione di menu **View/Change Application Ports** (Visualizza/Modifica porte applicazione), quindi premere Invio.
3. Se richiesto, inserire nuovamente la password utente per la manutenzione.
4. Digitare i nuovi numeri di porta per le porte HTTP e HTTPS, quindi premere Invio.

   Lasciando vuoto un numero di porta, viene assegnata la porta predefinita per il protocollo.

   Viene richiesto se si desidera modificare le porte e riavviare Unified Manager ora.

5. Digitare **y** per modificare le porte e riavviare Unified Manager.
6. Uscire dalla console di manutenzione.

Dopo questa modifica, gli utenti devono includere il nuovo numero di porta nell'URL per accedere all'interfaccia utente Web di Unified Manager, ad esempio https://host.company.com:1234, https://12.13.14.15:1122 o https://[2001:db8:0:1]:2123.

Aggiunta di interfacce di rete

È possibile aggiungere nuove interfacce di rete se è necessario separare il traffico di rete.

Cosa ti serve

È necessario aggiungere l'interfaccia di rete all'appliance virtuale utilizzando vSphere.

L'appliance virtuale deve essere accesa.

> Non è possibile eseguire questa operazione se Unified Manager è installato su Red Hat Enterprise Linux o su Microsoft Windows.

Fasi

1. Nel menu principale della console vSphere, selezionare **Configurazione di sistema** > **riavvio del sistema operativo**.

   Dopo il riavvio, la console di manutenzione è in grado di rilevare la nuova interfaccia di rete aggiunta.

2. Accedere alla console di manutenzione.
3. Selezionare **Network Configuration** (Configurazione di rete) > **Enable Network Interface** (attiva interfaccia di rete).
4. Selezionare la nuova interfaccia di rete e premere **Invio**.

   Selezionare **eth1** e premere **Invio**.

5. Digitare **y** per attivare l'interfaccia di rete.
6. Immettere le impostazioni di rete.

   Viene richiesto di inserire le impostazioni di rete se si utilizza un'interfaccia statica o se DHCP non viene rilevato.

   Una volta inserite le impostazioni di rete, si torna automaticamente al menu **Configurazione di rete**.

7. Selezionare **Conferma modifiche**.

   Per aggiungere l'interfaccia di rete, è necessario salvare le modifiche.

Aggiunta di spazio su disco alla directory del database di Unified Manager

La directory del database di Unified Manager contiene tutti i dati relativi allo stato e alle performance raccolti dai sistemi ONTAP. In alcuni casi, potrebbe essere necessario aumentare le dimensioni della directory del database.

Ad esempio, la directory del database potrebbe essere piena se Unified Manager sta raccogliendo dati da un gran numero di cluster in cui ciascun cluster ha molti nodi. Si riceverà un avviso quando la directory del database è piena al 90% e un evento critico quando la directory è piena al 95%.

Non vengono raccolti dati aggiuntivi dai cluster dopo che la directory raggiunge il 95% di riempimento.

I passaggi necessari per aggiungere capacità alla directory dei dati sono diversi a seconda che Unified Manager sia in esecuzione su un server VMware ESXi, Red Hat o CentOS Linux o su un server Microsoft Windows.

Aggiunta di spazio alla directory dei dati dell'host Linux

Se è stato assegnato spazio su disco insufficiente a `/opt/netapp/data` Directory per supportare Unified Manager quando si configura originariamente l'host Linux e si installa Unified Manager, è possibile aggiungere spazio su disco dopo l'installazione aumentando lo spazio su disco su `/opt/netapp/data` directory.

Cosa ti serve

È necessario disporre dell'accesso utente root alla macchina Red Hat Enterprise Linux o CentOS Linux su cui è installato Unified Manager.

Si consiglia di eseguire il backup del database di Unified Manager prima di aumentare le dimensioni della directory dei dati.

Fasi

1. Accedere come utente root alla macchina Linux su cui si desidera aggiungere spazio su disco.
2. Arrestare il servizio Unified Manager e il software MySQL associato nell'ordine indicato:

   ```
   systemctl stop ocieau ocie mysqld
   ```

3. Creare una cartella di backup temporanea (ad esempio, `/backup-data`) con spazio su disco sufficiente per contenere i dati nella corrente `/opt/netapp/data` directory.
4. Copiare il contenuto e la configurazione dei privilegi dell'esistente `/opt/netapp/data` directory nella directory dei dati di backup:

   ```
   cp -arp /opt/netapp/data/* /backup-data
   ```

5. Se Linux è attivato:

   a. Ottenere il tipo di se Linux per le cartelle esistenti `/opt/netapp/data` cartella:

      ```
      se_type= ls -Z /opt/netapp/data | awk '{print $4}' | awk -F: '{print $3}' |
      head -1
      ```

      Il sistema restituisce una conferma simile a quanto segue:

   ```
   echo $se_type
   mysqld_db_t
   ```

   a. Eseguire il comando chcon per impostare il tipo di se Linux per la directory di backup:

      ```
      chcon -R --type=mysqld_db_t /backup-data
      ```

6. Rimuovere il contenuto di `/opt/netapp/data` directory:

   a. `cd /opt/netapp/data`

   b. `rm -rf *`

7. Espandere le dimensioni di `/opt/netapp/data` Directory fino a un minimo di 150 GB tramite comandi LVM o aggiungendo dischi aggiuntivi.

   > Se hai creato `/opt/netapp/data` da un disco, quindi non si dovrebbe provare a montare `/opt/netapp/data` Come condivisione NFS o CIFS. Perché, in questo caso, se si tenta di espandere lo spazio su disco, alcuni comandi LVM, ad esempio `resize` e. `extend` potrebbe non funzionare come previsto.

8. Verificare che il `/opt/netapp/data` il proprietario della directory (mysql) e il gruppo (root) rimangono invariati:

`ls -ltr /opt/netapp/ | grep data`

Il sistema restituisce una conferma simile a quanto segue:

```
drwxr-xr-x.  17 mysql root  4096 Aug 28 13:08 data
```

9. Se Linux è attivato, verificare che il contesto per `/opt/netapp/data` la directory è ancora impostata su mysqld_db_t:

   a. `touch /opt/netapp/data/abc`

   b. `ls -Z /opt/netapp/data/abc`

      Il sistema restituisce una conferma simile a quanto segue:

```
-rw-r--r--. root root unconfined_u:object_r:mysqld_db_t:s0
/opt/netapp/data/abc
```

10. Eliminare il file abc in modo che questo file estraneo non causi un errore di database in futuro.
11. Copiare di nuovo i contenuti dai dati di backup all'espansione `/opt/netapp/data` directory:

    `cp -arp /backup-data/* /opt/netapp/data/`

12. Se Linux è attivato, eseguire il seguente comando:

    `chcon -R --type=mysqld_db_t /opt/netapp/data`

13. Avviare il servizio MySQL:

    `systemctl start mysqld`

14. Una volta avviato il servizio MySQL, avviare i servizi ocie e ocieau nell'ordine indicato:

    `systemctl start ocie ocieau`

15. Una volta avviati tutti i servizi, eliminare la cartella di backup `/backup-data`:

    `rm -rf /backup-data`

Aggiunta di spazio al disco dati della macchina virtuale VMware

Se è necessario aumentare la quantità di spazio sul disco dati per il database di Unified Manager, è possibile aggiungere capacità dopo l'installazione aumentando lo spazio su disco utilizzando la console di manutenzione di Unified Manager.

Cosa ti serve

- È necessario disporre dell'accesso al client vSphere.

- La macchina virtuale non deve contenere snapshot memorizzate localmente.
- È necessario disporre delle credenziali utente di manutenzione.

Si consiglia di eseguire il backup della macchina virtuale prima di aumentare le dimensioni dei dischi virtuali.

Fasi

1. Nel client vSphere, selezionare la macchina virtuale Unified Manager, quindi aggiungere ulteriore capacità del disco ai dati `disk 3`. Per ulteriori informazioni, consultare la documentazione di VMware.

   In alcuni rari casi, l'implementazione di Unified Manager utilizza "Hard Disk 2" per il disco dati invece di "Hard Disk 3". Se questo si è verificato durante l'implementazione, aumentare lo spazio di qualsiasi disco più grande. Il disco dati avrà sempre più spazio rispetto all'altro disco.

2. Nel client vSphere, selezionare la macchina virtuale Unified Manager, quindi selezionare la scheda **Console**.
3. Fare clic su nella finestra della console, quindi accedere alla console di manutenzione utilizzando il nome utente e la password.
4. Nel menu principale, inserire il numero dell'opzione **Configurazione di sistema**.
5. Nel menu System Configuration (Configurazione di sistema), inserire il numero dell'opzione **aumenta dimensioni disco dati**.

Aggiunta di spazio all'unità logica del server Microsoft Windows

Se è necessario aumentare la quantità di spazio su disco per il database di Unified Manager, è possibile aggiungere capacità all'unità logica su cui è installato Unified Manager.

Cosa ti serve

È necessario disporre dei privilegi di amministratore di Windows.

Si consiglia di eseguire il backup del database di Unified Manager prima di aggiungere spazio su disco.

Fasi

1. Accedere come amministratore al server Windows su cui si desidera aggiungere spazio su disco.
2. Seguire la procedura corrispondente al metodo che si desidera utilizzare per aggiungere ulteriore spazio:

Opzione	Descrizione
Su un server fisico, aggiungere capacità all'unità logica su cui è installato il server Unified Manager.	Seguire la procedura descritta nell'argomento Microsoft: "Estensione di un volume di base"
Su un server fisico, aggiungere un disco rigido.	Seguire la procedura descritta nell'argomento Microsoft: "Aggiunta di dischi rigidi"

Opzione	Descrizione
Su una macchina virtuale, aumentare le dimensioni di una partizione del disco.	Seguire la procedura descritta nell'argomento VMware: "Aumento delle dimensioni di una partizione del disco"

Gestione dell'accesso degli utenti

È possibile creare ruoli e assegnare funzionalità per controllare l'accesso degli utenti a Active IQ Unified Manager. È possibile identificare gli utenti che dispongono delle funzionalità necessarie per accedere agli oggetti selezionati in Unified Manager. Solo gli utenti che dispongono di questi ruoli e funzionalità possono gestire gli oggetti in Unified Manager.

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		•	•		

Funzione	Operatore	Amministratore dello storage	Amministratore dell'applicazione	Schema di integrazione	Schema del report
Gestire le opzioni di gestione dello storage		•	•		
Gestire le policy di gestione dello storage		•	•		
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					•

Gestione delle impostazioni di autenticazione SAML

Dopo aver configurato le impostazioni di autenticazione remota, è possibile attivare l'autenticazione SAML (Security Assertion Markup Language) in modo che gli utenti

remoti vengano autenticati da un provider di identità sicuro (IdP) prima di poter accedere all'interfaccia utente Web di Unified Manager.

Tenere presente che solo gli utenti remoti avranno accesso all'interfaccia utente grafica di Unified Manager dopo l'attivazione dell'autenticazione SAML. Gli utenti locali e gli utenti di manutenzione non potranno accedere all'interfaccia utente. Questa configurazione non influisce sugli utenti che accedono alla console di manutenzione.

Requisiti del provider di identità

Quando si configura Unified Manager per utilizzare un provider di identità (IdP) per eseguire l'autenticazione SAML per tutti gli utenti remoti, è necessario conoscere alcune impostazioni di configurazione necessarie per consentire la connessione a Unified Manager.

È necessario immettere l'URI e i metadati di Unified Manager nel server IdP. È possibile copiare queste informazioni dalla pagina autenticazione SAML di Unified Manager. Unified Manager è considerato il service provider (SP) nello standard SAML (Security Assertion Markup Language).

Standard di crittografia supportati

- AES (Advanced Encryption Standard): AES-128 e AES-256
- Secure Hash Algorithm (SHA): SHA-1 e SHA-256

Provider di identità validati

- Shibboleth
- Active Directory Federation Services (ADFS)

Requisiti di configurazione di ADFS

- È necessario definire tre regole per le attestazioni nell'ordine seguente, necessarie affinché Unified Manager analizzi le risposte SAML di ADFS per questa voce di trust della parte che si basa.

Regola della richiesta di rimborso	Valore
Nome-account-SAM	ID nome
Nome-account-SAM	urn:oid:0.9.2342.19200300.100.1.1
Gruppi di token — Nome non qualificato	urn:oid:1.3.6.1.4.1.5923.1.5.1.1

- È necessario impostare il metodo di autenticazione su "Forms Authentication" (autenticazione moduli), altrimenti gli utenti potrebbero ricevere un errore durante la disconnessione da Unified Manager . Attenersi alla seguente procedura:
  a. Aprire la console di gestione ADFS.
  b. Fare clic sulla cartella Authentication Policies (Criteri di autenticazione) nella vista ad albero a sinistra.
  c. Nella sezione azioni a destra, fare clic su Modifica policy di autenticazione primaria globale.

d. Impostare il metodo di autenticazione Intranet su “Forms Authentication” invece di “Windows Authentication” predefinito.

- In alcuni casi, l’accesso tramite IdP viene rifiutato quando il certificato di sicurezza di Unified Manager è firmato dalla CA. Esistono due soluzioni alternative per risolvere questo problema:
  - Seguire le istruzioni indicate nel collegamento per disattivare il controllo di revoca sul server ADFS per la parte di base associata al certificato CA concatenato:

    "Disattiva il controllo di revoca per fiducia della parte che si basa"

  - Fare in modo che il server CA si trovi all’interno del server ADFS per firmare la richiesta di certificazione del server Unified Manager.

Altri requisiti di configurazione

- L’inclinazione dell’orologio di Unified Manager è impostata su 5 minuti, quindi la differenza di tempo tra il server IdP e il server Unified Manager non può superare i 5 minuti o l’autenticazione non riesce.

Attivazione dell’autenticazione SAML

È possibile attivare l’autenticazione SAML (Security Assertion Markup Language) in modo che gli utenti remoti vengano autenticati da un provider di identità sicuro (IdP) prima di poter accedere all’interfaccia utente Web di Unified Manager.

Cosa ti serve

- È necessario aver configurato l’autenticazione remota e verificato che sia stata eseguita correttamente.
- È necessario aver creato almeno un utente remoto o un gruppo remoto con il ruolo di amministratore dell’applicazione.
- Il provider di identità (IdP) deve essere supportato da Unified Manager e deve essere configurato.
- È necessario disporre dell’URL IdP e dei metadati.
- È necessario disporre dell’accesso al server IdP.

Dopo aver abilitato l’autenticazione SAML da Unified Manager, gli utenti non possono accedere all’interfaccia utente grafica fino a quando IdP non è stato configurato con le informazioni sull’host del server Unified Manager. Pertanto, è necessario essere pronti a completare entrambe le parti della connessione prima di avviare il processo di configurazione. L’IdP può essere configurato prima o dopo la configurazione di Unified Manager.

Solo gli utenti remoti avranno accesso all’interfaccia utente grafica di Unified Manager dopo l’attivazione dell’autenticazione SAML. Gli utenti locali e gli utenti di manutenzione non potranno accedere all’interfaccia utente. Questa configurazione non influisce sugli utenti che accedono alla console di manutenzione, ai comandi di Unified Manager o alle ZAPI.

Unified Manager viene riavviato automaticamente dopo aver completato la configurazione SAML in questa pagina.

Fasi

1. Nel riquadro di spostamento a sinistra, fare clic su **General** > **SAML Authentication**.
2. Selezionare la casella di controllo **Enable SAML Authentication** (attiva autenticazione SAML).

Vengono visualizzati i campi necessari per configurare la connessione IdP.

3. Immettere l'URI IdP e i metadati IdP richiesti per connettere il server Unified Manager al server IdP.

   Se il server IdP è accessibile direttamente dal server Unified Manager, è possibile fare clic sul pulsante **Fetch IdP Metadata** (Scarica metadati IdP) dopo aver immesso l'URI IdP per popolare automaticamente il campo IdP Metadata (metadati IdP).

4. Copiare l'URI dei metadati host di Unified Manager o salvare i metadati host in un file di testo XML.

   In questo momento è possibile configurare il server IdP con queste informazioni.

5. Fare clic su **Save** (Salva).

   Viene visualizzata una finestra di messaggio per confermare che si desidera completare la configurazione e riavviare Unified Manager.

6. Fare clic su **Confirm and Logout** (Conferma e Disconnetti) per riavviare Unified Manager.

La volta successiva che gli utenti remoti autorizzati tenteranno di accedere all'interfaccia grafica di Unified Manager, inseriranno le proprie credenziali nella pagina di accesso di IdP anziché nella pagina di accesso di Unified Manager.

Se non è già stato completato, accedere all'IdP e immettere l'URI e i metadati del server Unified Manager per completare la configurazione.

> Quando si utilizza ADFS come provider di identità, la GUI di Unified Manager non rispetta il timeout ADFS e continuerà a funzionare fino al raggiungimento del timeout della sessione di Unified Manager. È possibile modificare il timeout della sessione GUI facendo clic su **General** > **Feature Settings** > **Inactivity Timeout**.

Modifica del provider di identità utilizzato per l'autenticazione SAML

È possibile modificare il provider di identità (IdP) utilizzato da Unified Manager per autenticare gli utenti remoti.

Cosa ti serve

- È necessario disporre dell'URL IdP e dei metadati.
- È necessario disporre dell'accesso all'IdP.

Il nuovo IdP può essere configurato prima o dopo la configurazione di Unified Manager.

Fasi

1. Nel riquadro di spostamento a sinistra, fare clic su **General** > **SAML Authentication**.
2. Inserire il nuovo URI IdP e i metadati IdP richiesti per connettere il server Unified Manager all'IdP.

   Se l'IdP è accessibile direttamente dal server di Unified Manager, è possibile fare clic sul pulsante **Fetch IdP Metadata** (Scarica metadati IdP) dopo aver immesso l'URL IdP per compilare automaticamente il campo IdP Metadata (metadati IdP).

3. Copiare l'URI dei metadati di Unified Manager o salvare i metadati in un file di testo XML.

4. Fare clic su **Save Configuration** (Salva configurazione).

   Viene visualizzata una finestra di messaggio per confermare che si desidera modificare la configurazione.

5. Fare clic su **OK**.

Accedere al nuovo IdP e immettere l'URI e i metadati del server Unified Manager per completare la configurazione.

La volta successiva che gli utenti remoti autorizzati tenteranno di accedere all'interfaccia grafica di Unified Manager, inseriranno le proprie credenziali nella nuova pagina di accesso IdP anziché nella vecchia pagina di accesso IdP.

Aggiornamento delle impostazioni di autenticazione SAML dopo la modifica del certificato di protezione di Unified Manager

Qualsiasi modifica al certificato di protezione HTTPS installato sul server Unified Manager richiede l'aggiornamento delle impostazioni di configurazione per l'autenticazione SAML. Il certificato viene aggiornato se si rinomina il sistema host, si assegna un nuovo indirizzo IP al sistema host o si modifica manualmente il certificato di protezione del sistema.

Una volta modificato il certificato di protezione e riavviato il server Unified Manager, l'autenticazione SAML non funzionerà e gli utenti non potranno accedere all'interfaccia grafica di Unified Manager. Per riattivare l'accesso all'interfaccia utente, è necessario aggiornare le impostazioni di autenticazione SAML sul server IdP e sul server Unified Manager.

Fasi

1. Accedere alla console di manutenzione.
2. Nel **Menu principale**, inserire il numero dell'opzione **Disattiva autenticazione SAML**.

   Viene visualizzato un messaggio per confermare che si desidera disattivare l'autenticazione SAML e riavviare Unified Manager.

3. Avviare l'interfaccia utente di Unified Manager utilizzando l'FQDN o l'indirizzo IP aggiornato, accettare il certificato del server aggiornato nel browser e accedere utilizzando le credenziali utente di manutenzione.
4. Nella pagina **Setup/Authentication**, selezionare la scheda **SAML Authentication** e configurare la connessione IdP.
5. Copiare l'URI dei metadati host di Unified Manager o salvare i metadati host in un file di testo XML.
6. Fare clic su **Save** (Salva).

   Viene visualizzata una finestra di messaggio per confermare che si desidera completare la configurazione e riavviare Unified Manager.

7. Fare clic su **Confirm and Logout** (Conferma e Disconnetti) per riavviare Unified Manager.
8. Accedere al server IdP e immettere l'URI e i metadati del server Unified Manager per completare la configurazione.

Provider di identità	Fasi di configurazione
ADFS	a. Eliminare la voce di trust esistente della parte che si basa nella GUI di gestione di ADFS. b. Aggiungere una nuova voce di attendibilità della parte che si basa utilizzando `saml_sp_metadata.xml` Dal server Unified Manager aggiornato. c. Definire le tre regole di attestazione richieste da Unified Manager per analizzare le risposte SAML di ADFS per questa voce di attendibilità della parte che si basa. d. Riavviare il servizio Windows di ADFS.
Shibboleth	a. Aggiornare il nuovo FQDN del server Unified Manager in `attribute-filter.xml` e. `relying-party.xml` file. b. Riavviare il server Web Apache Tomcat e attendere che la porta 8005 sia online.

9. Accedere a Unified Manager e verificare che l'autenticazione SAML funzioni come previsto attraverso l'IdP.

Disattivazione dell'autenticazione SAML

È possibile disattivare l'autenticazione SAML quando si desidera interrompere l'autenticazione degli utenti remoti tramite un provider di identità sicuro (IdP) prima che possano accedere all'interfaccia utente Web di Unified Manager. Quando l'autenticazione SAML è disattivata, i provider di servizi di directory configurati, ad esempio Active Directory o LDAP, eseguono l'autenticazione di accesso.

Una volta disattivata l'autenticazione SAML, gli utenti locali e gli utenti di manutenzione potranno accedere all'interfaccia grafica utente oltre agli utenti remoti configurati.

Se non si dispone dell'accesso all'interfaccia utente grafica, è possibile disattivare l'autenticazione SAML anche utilizzando la console di manutenzione di Unified Manager.

Unified Manager viene riavviato automaticamente dopo la disattivazione dell'autenticazione SAML.

Fasi

1. Nel riquadro di spostamento a sinistra, fare clic su **General** > **SAML Authentication**.
2. Deselezionare la casella di controllo **Enable SAML Authentication** (attiva autenticazione SAML).
3. Fare clic su **Save** (Salva).

   Viene visualizzata una finestra di messaggio per confermare che si desidera completare la configurazione e riavviare Unified Manager.

4. Fare clic su **Confirm and Logout** (Conferma e Disconnetti) per riavviare Unified Manager.

La volta successiva che gli utenti remoti tenteranno di accedere all'interfaccia grafica di Unified Manager, inseriranno le proprie credenziali nella pagina di accesso di Unified Manager anziché nella pagina di accesso di IdP.

Accedere all'ID ed eliminare l'URI e i metadati del server Unified Manager.

Disattivazione dell'autenticazione SAML dalla console di manutenzione

Potrebbe essere necessario disattivare l'autenticazione SAML dalla console di manutenzione quando non è possibile accedere alla GUI di Unified Manager. Ciò potrebbe verificarsi in caso di errata configurazione o se l'IdP non è accessibile.

Cosa ti serve

È necessario avere accesso alla console di manutenzione come utente di manutenzione.

Quando l'autenticazione SAML è disattivata, i provider di servizi di directory configurati, ad esempio Active Directory o LDAP, eseguono l'autenticazione di accesso. Gli utenti locali e gli utenti di manutenzione potranno accedere all'interfaccia utente grafica oltre agli utenti remoti configurati.

È inoltre possibile disattivare l'autenticazione SAML dalla pagina Setup/Authentication (Configurazione/autenticazione) dell'interfaccia utente.

Unified Manager viene riavviato automaticamente dopo la disattivazione dell'autenticazione SAML.

Fasi

1. Accedere alla console di manutenzione.
2. Nel **Menu principale**, inserire il numero dell'opzione **Disattiva autenticazione SAML**.

   Viene visualizzato un messaggio per confermare che si desidera disattivare l'autenticazione SAML e riavviare Unified Manager.

3. Digitare **y**, quindi premere Invio per riavviare Unified Manager.

La volta successiva che gli utenti remoti tenteranno di accedere all'interfaccia grafica di Unified Manager, inseriranno le proprie credenziali nella pagina di accesso di Unified Manager anziché nella pagina di accesso di IdP.

Se necessario, accedere all'IdP ed eliminare l'URL e i metadati del server Unified Manager.

Pagina SAML Authentication

È possibile utilizzare la pagina SAML Authentication per configurare Unified Manager in modo che autentichi gli utenti remoti utilizzando SAML tramite un provider di identità sicuro (IdP) prima che possano accedere all'interfaccia utente Web di Unified Manager.

- Per creare o modificare la configurazione SAML, è necessario disporre del ruolo di amministratore dell'applicazione.
- È necessario aver configurato l'autenticazione remota.
- È necessario aver configurato almeno un utente remoto o un gruppo remoto.

Dopo aver configurato l'autenticazione remota e gli utenti remoti, selezionare la casella di controllo Enable SAML Authentication (attiva autenticazione SAML) per abilitare l'autenticazione utilizzando un provider di identità sicuro.

- **IDP URI**

  L'URI per accedere all'IdP dal server Unified Manager. Di seguito sono elencati gli URI di esempio.

  URI di esempio ADFS:

  ```
  https://win2016-dc.ntap2016.local/federationmetadata/2007-
  06/federationmetadata.xml
  ```

  URI di esempio Shibboleth:

  ```
  https://centos7.ntap2016.local/idp/shibboleth
  ```

- **Metadati IdP**

  I metadati IdP in formato XML.

  Se l'URL IdP è accessibile dal server di Unified Manager, fare clic sul pulsante **Fetch IdP Metadata** (Scarica metadati IdP) per compilare questo campo.

- **Sistema host (FQDN)**

  L'FQDN del sistema host di Unified Manager come definito durante l'installazione. Se necessario, è possibile modificare questo valore.

- **URI host**

  L'URI per accedere al sistema host di Unified Manager da IdP.

- **Metadati host**

  I metadati del sistema host in formato XML.

Gestione dell'autenticazione

È possibile attivare l'autenticazione utilizzando LDAP o Active Directory sul server Unified Manager e configurarlo per l'utilizzo con i server per l'autenticazione degli utenti remoti.

Per abilitare l'autenticazione remota, impostare i servizi di autenticazione e aggiungere server di autenticazione, vedere la sezione precedente su **Configurazione di Unified Manager per l'invio di notifiche di avviso**.

Modifica dei server di autenticazione

È possibile modificare la porta utilizzata dal server Unified Manager per comunicare con il server di autenticazione.

Cosa ti serve

È necessario disporre del ruolo di amministratore dell'applicazione.

Fasi

1. Nel riquadro di spostamento di sinistra, fare clic su **Generale** > **autenticazione remota**.
2. Selezionare la casella **Disable Nested Group Lookup** (Disattiva ricerca gruppi nidificati).
3. Nell'area **Authentication Servers** (Server di autenticazione), selezionare il server di autenticazione che si desidera modificare, quindi fare clic su **Edit** (Modifica).
4. Nella finestra di dialogo **Edit Authentication Server** (Modifica server di autenticazione), modificare i dettagli della porta.
5. Fare clic su **Save** (Salva).

Eliminazione dei server di autenticazione

È possibile eliminare un server di autenticazione se si desidera impedire al server Unified Manager di comunicare con il server di autenticazione. Ad esempio, se si desidera modificare un server di autenticazione con cui il server di gestione sta comunicando, è possibile eliminare il server di autenticazione e aggiungere un nuovo server di autenticazione.

Cosa ti serve

È necessario disporre del ruolo di amministratore dell'applicazione.

Quando si elimina un server di autenticazione, gli utenti remoti o i gruppi del server di autenticazione non potranno più accedere a Unified Manager.

Fasi

1. Nel riquadro di spostamento di sinistra, fare clic su **Generale** > **autenticazione remota**.
2. Selezionare uno o più server di autenticazione che si desidera eliminare, quindi fare clic su **Delete** (Elimina).
3. Fare clic su **Sì** per confermare la richiesta di eliminazione.

   Se l'opzione **Usa connessione sicura** è attivata, i certificati associati al server di autenticazione vengono cancellati insieme al server di autenticazione.

Autenticazione con Active Directory o OpenLDAP

È possibile attivare l'autenticazione remota sul server di gestione e configurare il server di gestione per comunicare con i server di autenticazione in modo che gli utenti all'interno dei server di autenticazione possano accedere a Unified Manager.

È possibile utilizzare uno dei seguenti servizi di autenticazione predefiniti o specificare un servizio di autenticazione personalizzato:

- Microsoft Active Directory

  Non è possibile utilizzare Microsoft Lightweight Directory Services.

- OpenLDAP

È possibile selezionare il servizio di autenticazione richiesto e aggiungere i server di autenticazione appropriati per consentire agli utenti remoti nel server di autenticazione di accedere a Unified Manager. Le credenziali per utenti o gruppi remoti vengono gestite dal server di autenticazione. Il server di gestione utilizza il protocollo LDAP (Lightweight Directory Access Protocol) per autenticare gli utenti remoti all'interno del server di autenticazione configurato.

Per gli utenti locali creati in Unified Manager, il server di gestione gestisce il proprio database di nomi utente e password. Il server di gestione esegue l'autenticazione e non utilizza Active Directory o OpenLDAP per l'autenticazione.

Registrazione dell'audit

È possibile rilevare se i registri di controllo sono stati compromessi con l'utilizzo dei registri di controllo. Tutte le attività eseguite da un utente vengono monitorate e registrate nei registri di controllo. I controlli vengono eseguiti per tutte le funzionalità dell'interfaccia utente e delle API` esposte pubblicamente di Active IQ Unified Manager.

È possibile utilizzare il registro di controllo: Visualizzazione file* per visualizzare e accedere a tutti i file di registro di controllo disponibili in Active IQ Unified Manager. I file nella visualizzazione file del registro di controllo sono elencati in base alla data di creazione. Questa vista visualizza le informazioni di tutti i log di controllo acquisiti dall'installazione o dall'aggiornamento al presente nel sistema. Ogni volta che si esegue un'azione in Unified Manager, le informazioni vengono aggiornate e sono disponibili nei registri. Lo stato di ciascun file di log viene acquisito utilizzando l'attributo "file Integrity Status", che viene monitorato attivamente per rilevare la manomissione o l'eliminazione del file di log. I registri di controllo possono avere uno dei seguenti stati quando i registri di controllo sono disponibili nel sistema:

Stato	Descrizione
ATTIVO	File in cui vengono attualmente registrati i log.
NORMALE	File inattivo, compresso e memorizzato nel sistema.
MANOMESSO	File che è stato compromesso da un utente che ha modificato manualmente il file.
MANUAL_DELETE	File eliminato da un utente autorizzato.
ROLLOVER_DELETE	File che è stato eliminato a causa dell'annullamento in base a criteri di configurazione a rotazione.
UNEXPECTED_DELETE	File eliminato per motivi sconosciuti.

La pagina Registro di controllo include i seguenti pulsanti di comando:

- Configurare
- Eliminare
- Scarica

Il pulsante **DELETE** consente di eliminare qualsiasi registro di controllo elencato nella vista registri di controllo. È possibile eliminare un registro di controllo e, facoltativamente, fornire un motivo per eliminare il file, in modo da poter determinare un'eliminazione valida in futuro. La colonna REASON (MOTIVO) elenca il motivo insieme al nome dell'utente che ha eseguito l'operazione di eliminazione.

L'eliminazione di un file di log causerà l'eliminazione del file dal sistema, ma la voce nella tabella DB non verrà eliminata.

È possibile scaricare i registri di controllo da Active IQ Unified Manager utilizzando il pulsante **DOWNLOAD** nella sezione registri di controllo ed esportare i file di registro di controllo. I file contrassegnati con "NORMAL" o "MANOMESSI" vengono scaricati in un file compresso `.gzip` formato.

I file di log di audit vengono archiviati periodicamente e salvati nel database per riferimento. Prima dell'archiviazione, i registri di controllo sono dotati di firma digitale per garantire la sicurezza e l'integrità.

Quando viene generato un bundle AutoSupport completo, il bundle di supporto include file di log di audit sia archiviati che attivi. Tuttavia, quando viene generato un bundle di supporto leggero, include solo i registri di controllo attivi. I registri di controllo archiviati non sono inclusi.

Configurazione dei registri di audit

È possibile utilizzare il pulsante **Configura** nella sezione registri di controllo per configurare i criteri di rolling per i file di registro di controllo e per attivare la registrazione remota per i registri di controllo.

È possibile impostare i valori nei CAMPI **MAX FILE SIZE** e **AUDIT LOG RETENTION DAYS** in base alla quantità e alla frequenza desiderate dei dati che si desidera memorizzare nel sistema. Il valore nel campo **TOTAL AUDIT LOG SIZE** (DIMENSIONE TOTALE REGISTRO DI CONTROLLO) è la dimensione dei dati totali del registro di controllo presenti nel sistema. La policy di rollover è determinata dai valori nel campo **GIORNI DI CONSERVAZIONE DEL REGISTRO DI CONTROLLO**, **dimensione DEL FILE MAX** e **DIMENSIONE TOTALE DEL REGISTRO DI CONTROLLO**. Quando la dimensione del backup del registro di controllo raggiunge il valore configurato in **TOTAL AUDIT LOG SIZE**, il file archiviato per primo viene cancellato. Ciò significa che il file meno recente viene cancellato. Tuttavia, la voce del file continua a essere disponibile nel database ed è contrassegnata come "Elimina rollover". Il valore **GIORNI di CONSERVAZIONE del REGISTRO DI CONTROLLO** corrisponde al numero di giorni in cui i file di registro di controllo vengono conservati. Viene eseguito il rollover di qualsiasi file precedente al valore impostato in questo campo.

Fasi

1. Fare clic su **Audit Logs** > > **Configure**.
2. Inserire i valori nelle voci **MAX FILE SIZE**, **TOTAL AUDIT LOG SIZE** e **AUDIT LOG RETENTION DAYS**.

   Se si desidera attivare la registrazione remota, selezionare **Enable Remote Logging** (attiva registrazione remota).

Abilitazione della registrazione remota dei registri di controllo

È possibile selezionare la casella di controllo **Enable Remote Logging** (attiva registrazione remota) nella finestra di dialogo Configure Audit Logs (Configura registri di controllo) per attivare la registrazione remota dell'audit. È possibile utilizzare questa funzione per trasferire i registri di controllo a un server Syslog remoto. In questo modo, è possibile gestire i registri di controllo in caso di limiti di spazio.

La registrazione remota dei registri di controllo fornisce un backup a prova di manomissione nel caso in cui i file di registro di controllo sul server Active IQ Unified Manager vengano manomessi.

Fasi

1. Nella finestra di dialogo **Configura registri di controllo**, selezionare la casella di controllo **attiva registrazione remota**.

   Vengono visualizzati ulteriori campi per configurare la registrazione remota.

2. Immettere il **NOME HOST** e la **PORTA** del server remoto a cui si desidera connettersi.
3. Nel campo **CERTIFICATO CA DEL SERVER**, fare clic su **SFOGLIA** per selezionare un certificato pubblico del server di destinazione.

   Il certificato deve essere caricato in `.pem` formato. Questo certificato deve essere ottenuto dal server Syslog di destinazione e non deve essere scaduto. Il certificato deve contenere il "hostname" selezionato come parte di `SubjectAltName` (SAN).

4. Immettere i valori per i seguenti campi: **CHARSET**, **TIMEOUT CONNESSIONE**, **RITARDO DI RICONNESSIONE**.

   I valori devono essere espressi in millisecondi per questi campi.

5. Selezionare il formato Syslog e la versione del protocollo TLS richiesti nei campi **FORMAT** e **PROTOCOL**.
6. Selezionare la casella di controllo **Enable Client Authentication** (attiva autenticazione client) se il server Syslog di destinazione richiede l'autenticazione basata su certificato.

   Prima di salvare la configurazione del registro di controllo, sarà necessario scaricare il certificato di autenticazione del client e caricarlo sul server Syslog, altrimenti la connessione non avrà esito positivo. A seconda del tipo di server Syslog, potrebbe essere necessario creare un hash del certificato di autenticazione del client.

   Esempio: Syslog-ng richiede la creazione di un <hash> del certificato utilizzando il comando `openssl x509 -noout -hash -in cert.pem`, quindi collegare simbolicamente il certificato di autenticazione del client a un file denominato dopo <hash> .0.

7. Fare clic su **Save** (Salva) per configurare la connessione con il server e attivare la registrazione remota.

   Verrà reindirizzato alla pagina Audit Logs (registri di controllo).

Pagina Remote Authentication (autenticazione remota

È possibile utilizzare la pagina Remote Authentication (autenticazione remota) per configurare Unified Manager in modo che comunichi con il server di autenticazione per autenticare gli utenti remoti che tentano di accedere all'interfaccia utente Web di Unified Manager.

È necessario disporre del ruolo di amministratore dell'applicazione o di amministratore dello storage.

Dopo aver selezionato la casella di controllo Enable remote Authentication (attiva autenticazione remota), è possibile attivare l'autenticazione remota utilizzando un server di autenticazione.

- **Servizio di autenticazione**

Consente di configurare il server di gestione per autenticare gli utenti nei provider di servizi di directory, ad esempio Active Directory, OpenLDAP o specificare il proprio meccanismo di autenticazione. È possibile specificare un servizio di autenticazione solo se è stata attivata l'autenticazione remota.

- **Active Directory**
  - Nome amministratore

    Specifica il nome dell'amministratore del server di autenticazione.

  - Password

    Specifica la password per accedere al server di autenticazione.

  - Nome distinto di base

    Specifica la posizione degli utenti remoti nel server di autenticazione. Ad esempio, se il nome di dominio del server di autenticazione è ou@domain.com, il nome distinto di base è **cn=ou,DC=domain,DC=com**.

  - Disattiva ricerca gruppi nidificati

    Specifica se attivare o disattivare l'opzione di ricerca di gruppi nidificati. Per impostazione predefinita, questa opzione è disattivata. Se si utilizza Active Directory, è possibile accelerare l'autenticazione disattivando il supporto per i gruppi nidificati.

  - USA connessione sicura

    Specifica il servizio di autenticazione utilizzato per comunicare con i server di autenticazione.

- **OpenLDAP**
  - Associa nome distinto

    Specifica il nome distinto di binding utilizzato insieme al nome distinto di base per trovare gli utenti remoti nel server di autenticazione.

  - Password bind

    Specifica la password per accedere al server di autenticazione.

  - Nome distinto di base

    Specifica la posizione degli utenti remoti nel server di autenticazione. Ad esempio, se il nome di dominio del server di autenticazione è ou@domain.com, il nome distinto di base è **cn=ou,DC=domain,DC=com**.

  - USA connessione sicura

    Specifica che il protocollo LDAP protetto viene utilizzato per comunicare con i server di autenticazione LDAP.

- **Altri**
  - Associa nome distinto

    Specifica il nome distinto di binding utilizzato insieme al nome distinto di base per trovare gli utenti

remoti nel server di autenticazione configurato.

- Password bind

  Specifica la password per accedere al server di autenticazione.

- Nome distinto di base

  Specifica la posizione degli utenti remoti nel server di autenticazione. Ad esempio, se il nome di dominio del server di autenticazione è ou@domain.com, il nome distinto di base è **cn=ou,DC=domain,DC=com**.

- Versione del protocollo

  Specifica la versione LDAP (Lightweight Directory Access Protocol) supportata dal server di autenticazione. È possibile specificare se la versione del protocollo deve essere rilevata automaticamente o impostata su 2 o 3.

- Attributo User Name

  Specifica il nome dell'attributo nel server di autenticazione che contiene i nomi di accesso dell'utente da autenticare dal server di gestione.

- Attributo Group Membership

  Specifica un valore che assegna l'appartenenza al gruppo di server di gestione agli utenti remoti in base a un attributo e a un valore specificati nel server di autenticazione dell'utente.

- UGID

  Se gli utenti remoti sono inclusi come membri di un oggetto GroupOfUniqueNames nel server di autenticazione, questa opzione consente di assegnare l'appartenenza al gruppo di server di gestione agli utenti remoti in base a un attributo specificato nell'oggetto GroupOfUniqueNames.

- Disattiva ricerca gruppi nidificati

  Specifica se attivare o disattivare l'opzione di ricerca di gruppi nidificati. Per impostazione predefinita, questa opzione è disattivata. Se si utilizza Active Directory, è possibile accelerare l'autenticazione disattivando il supporto per i gruppi nidificati.

- Membro

  Specifica il nome dell'attributo utilizzato dal server di autenticazione per memorizzare informazioni sui singoli membri di un gruppo.

- User Object Class (Classe oggetto utente)

  Specifica la classe di oggetti di un utente nel server di autenticazione remoto.

- Group Object Class (Classe oggetti gruppo)

  Specifica la classe di oggetti di tutti i gruppi nel server di autenticazione remoto.

I valori immessi per gli attributi *Member*, *User Object Class* e *Group Object Class* devono coincidere con quelli aggiunti nelle configurazioni Active Directory, OpenLDAP e LDAP. In caso contrario, l'autenticazione potrebbe non riuscire.

- USA connessione sicura

  Specifica il servizio di autenticazione utilizzato per comunicare con i server di autenticazione.

Se si desidera modificare il servizio di autenticazione, assicurarsi di eliminare tutti i server di autenticazione esistenti e aggiungere nuovi server di autenticazione.

Area Authentication Servers

L'area Authentication Servers (Server di autenticazione) visualizza i server di autenticazione con cui il server di gestione comunica per individuare e autenticare gli utenti remoti. Le credenziali per utenti o gruppi remoti vengono gestite dal server di autenticazione.

- **Pulsanti di comando**

  Consente di aggiungere, modificare o eliminare i server di autenticazione.

  - Aggiungi

    Consente di aggiungere un server di autenticazione.

  Se il server di autenticazione che si sta aggiungendo fa parte di una coppia ad alta disponibilità (utilizzando lo stesso database), è possibile aggiungere anche il server di autenticazione partner. Ciò consente al server di gestione di comunicare con il partner quando uno dei server di autenticazione non è raggiungibile.

  - Modifica

    Consente di modificare le impostazioni di un server di autenticazione selezionato.

  - Eliminare

    Elimina i server di autenticazione selezionati.

- **Nome o indirizzo IP**

  Visualizza il nome host o l'indirizzo IP del server di autenticazione utilizzato per autenticare l'utente sul server di gestione.

- **Porta**

  Visualizza il numero di porta del server di autenticazione.

- **Verifica dell'autenticazione**

  Questo pulsante convalida la configurazione del server di autenticazione autenticando un utente o un gruppo remoto.

  Durante il test, se si specifica solo il nome utente, il server di gestione ricerca l'utente remoto nel server di autenticazione, ma non autenticare l'utente. Se si specificano sia il nome utente che la password, il server

di gestione ricerca e autentica l'utente remoto.

Non è possibile verificare l'autenticazione se l'autenticazione remota è disattivata.

Gestione dei certificati di sicurezza

È possibile configurare HTTPS nel server Unified Manager per monitorare e gestire i cluster su una connessione sicura.

Visualizzazione del certificato di protezione HTTPS

È possibile confrontare i dettagli del certificato HTTPS con il certificato recuperato nel browser per garantire che la connessione crittografata del browser a Unified Manager non venga intercettata.

Cosa ti serve

È necessario disporre del ruolo di operatore, amministratore dell'applicazione o amministratore dello storage.

La visualizzazione del certificato consente di verificare il contenuto di un certificato rigenerato o di visualizzare i nomi Alt (SAN) del soggetto da cui è possibile accedere a Unified Manager.

Fase

1. Nel riquadro di spostamento a sinistra, fare clic su **Generale** > **certificato HTTPS**.

   Il certificato HTTPS viene visualizzato nella parte superiore della pagina

Per visualizzare informazioni più dettagliate sul certificato di protezione rispetto a quelle visualizzate nella pagina del certificato HTTPS, è possibile visualizzare il certificato di connessione nel browser.

Download di una richiesta di firma del certificato HTTPS

È possibile scaricare una richiesta di firma della certificazione per il certificato di protezione HTTPS corrente in modo da fornire il file a un'autorità di certificazione da firmare. Un certificato con firma CA aiuta a prevenire gli attacchi man-in-the-middle e offre una protezione migliore rispetto a un certificato autofirmato.

Cosa ti serve

È necessario disporre del ruolo di amministratore dell'applicazione.

Fasi

1. Nel riquadro di spostamento a sinistra, fare clic su **Generale** > **certificato HTTPS**.
2. Fare clic su **Scarica richiesta firma certificato HTTPS**.
3. Salvare `<hostname>.csr` file.

È possibile fornire il file a un'autorità di certificazione per firmare e installare il certificato firmato.

Installazione di un certificato HTTPS firmato e restituito dalla CA

È possibile caricare e installare un certificato di sicurezza dopo che un'autorità di certificazione ha firmato e restituito il certificato. Il file caricato e installato deve essere una versione firmata del certificato autofirmato esistente. Un certificato con firma CA aiuta a prevenire gli attacchi man-in-the-middle e offre una protezione migliore rispetto a un certificato autofirmato.

Cosa ti serve

È necessario aver completato le seguenti operazioni:

- Il file Certificate Signing Request è stato scaricato e firmato da un'autorità di certificazione
- La catena di certificati è stata salvata in formato PEM
- Inclusi tutti i certificati nella catena, dal certificato del server Unified Manager al certificato di firma root, inclusi eventuali certificati intermedi presenti

È necessario disporre del ruolo di amministratore dell'applicazione.

Se la validità del certificato per il quale è stata creata una CSR è superiore a 397 giorni, la validità verrà ridotta a 397 giorni dalla CA prima della firma e della restituzione del certificato

Fasi

1. Nel riquadro di spostamento a sinistra, fare clic su **Generale** > **certificato HTTPS**.
2. Fare clic su **Installa certificato HTTPS**.
3. Nella finestra di dialogo visualizzata, fare clic su **Scegli file…** per individuare il file da caricare.
4. Selezionare il file, quindi fare clic su **Installa** per installarlo.

   Per ulteriori informazioni, vedere "Installazione di un certificato HTTPS generato utilizzando strumenti esterni".

Esempio di catena di certificati

Nell'esempio seguente viene illustrato come potrebbe essere visualizzato il file di catena del certificato:

```
-----BEGIN CERTIFICATE-----
<*Server certificate*>
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
<*Intermediate certificate \#1 (if present)*>
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
<*Intermediate certificate \#2 (if present)*>
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
<*Root signing certificate*>
-----END CERTIFICATE-----
```

Installazione di un certificato HTTPS generato utilizzando strumenti esterni

È possibile installare i certificati autofirmati o con firma CA e generati utilizzando uno strumento esterno come OpenSSL, BoringSSL, LetsEncrypt.

È necessario caricare la chiave privata insieme alla catena di certificati, poiché questi certificati sono coppia di chiavi pubbliche e private generate esternamente. Gli algoritmi di coppia di chiavi consentiti sono “RSA” e “EC”. L’opzione **Installa certificato HTTPS** è disponibile nella pagina certificati HTTPS nella sezione Generale. Il file caricato deve essere nel seguente formato di input.

1. Chiave privata del server che appartiene all’host Active IQ Unified Manager
2. Certificato del server che corrisponde alla chiave privata
3. Certificato delle CA invertito fino alla root, che vengono utilizzate per firmare il certificato di cui sopra

Formato per il caricamento di un certificato con una coppia di chiavi EC

Le curve consentite sono “prime256v1” e “secp384r1”. Esempio di certificato con una coppia EC generata esternamente:

```
 -----BEGIN EC PRIVATE KEY-----
<EC private key of Server>
-----END EC PRIVATE KEY-----
```

```
-----BEGIN CERTIFICATE-----
<Server certificate>
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
<Intermediate certificate #1 (if present)>
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
<Intermediate certificate #2 (if present)>
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
<Root signing certificate>
-----END CERTIFICATE-----
```

Formato per il caricamento di un certificato con una coppia di chiavi RSA

Le dimensioni delle chiavi consentite per la coppia di chiavi RSA appartenente al certificato host sono 2048, 3072 e 4096. Certificato con una coppia di chiavi * RSA generata esternamente*:

```
-----BEGIN RSA PRIVATE KEY-----
<RSA private key of Server>
-----END RSA PRIVATE KEY-----
-----BEGIN CERTIFICATE-----
<Server certificate>
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
<Intermediate certificate #1 (if present)>
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
<Intermediate certificate #2 (if present)>
-----END CERTIFICATE-----
-----BEGIN CERTIFICATE-----
<Root signing certificate>
-----END CERTIFICATE-----
```

Una volta caricato il certificato, riavviare l'istanza di Active IQ Unified Manager per rendere effettive le modifiche.

Verifica durante il caricamento dei certificati generati esternamente

Il sistema esegue controlli durante il caricamento di un certificato generato mediante strumenti esterni. Se uno dei controlli non riesce, il certificato viene rifiutato. Sono incluse anche le validazioni per i certificati generati dalla CSR all'interno del prodotto e per i certificati generati utilizzando strumenti esterni.

- La chiave privata nell'input viene convalidata in base al certificato host nell'input.
- Il nome comune (CN) nel certificato host viene verificato in base all'FQDN dell'host.

- Il nome comune (CN) del certificato host non deve essere vuoto o vuoto e non deve essere impostato su localhost.
- La data di inizio della validità non deve essere futura e la data di scadenza del certificato non deve essere passata.
- Se esiste una CA o una CA intermedia, la data di inizio della validità del certificato non deve essere futura e la data di scadenza della validità non deve essere passata.

La chiave privata nell'input non deve essere crittografata. Se sono presenti chiavi private crittografate, queste vengono rifiutate dal sistema.

Esempio 1

```
----BEGIN ENCRYPTED PRIVATE KEY-----
<Encrypted private key>
-----END ENCRYPTED PRIVATE KEY-----
```

Esempio 2

```
-----BEGIN RSA PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
<content here>
-----END RSA PRIVATE KEY-----
```

Esempio 3

```
-----BEGIN EC PRIVATE KEY-----
Proc-Type: 4,ENCRYPTED
<content here>
-----END EC PRIVATE KEY-----
```

Descrizioni delle pagine per la gestione dei certificati

È possibile utilizzare la pagina HTTPS Certificate (certificato HTTPS) per visualizzare i certificati di protezione correnti e generare nuovi certificati HTTPS.

Pagina del certificato HTTPS

La pagina HTTPS Certificate (certificato HTTPS) consente di visualizzare il certificato di protezione corrente, scaricare una richiesta di firma del certificato, generare un nuovo certificato HTTPS autofirmato o installare un nuovo certificato HTTPS.

Se non è stato generato un nuovo certificato HTTPS autofirmato, il certificato visualizzato in questa pagina corrisponde al certificato generato durante l'installazione.

Pulsanti di comando

I pulsanti di comando consentono di eseguire le seguenti operazioni:

- **Scarica richiesta firma certificato HTTPS**

  Scarica una richiesta di certificazione per il certificato HTTPS attualmente installato. Il browser richiede di salvare il file <hostname>.csr in modo da fornire il file a un'autorità di certificazione per la firma.

- **Installare il certificato HTTPS**

  Consente di caricare e installare un certificato di sicurezza dopo che un'autorità di certificazione ha firmato e restituito il certificato. Il nuovo certificato è in vigore dopo il riavvio del server di gestione.

- **Rigenera certificato HTTPS**

  Consente di generare un nuovo certificato HTTPS autofirmato, che sostituisce il certificato di protezione corrente. Il nuovo certificato è in vigore dopo il riavvio di Unified Manager.

Finestra di dialogo Rigenera certificato HTTPS

La finestra di dialogo Rigenera certificato HTTPS consente di personalizzare le informazioni di protezione e generare un nuovo certificato HTTPS con tali informazioni.

In questa pagina vengono visualizzate le informazioni sul certificato corrente.

La selezione "Regenerate using Current Certificate Attributes" e "Update the Current Certificate Attributes" consente di rigenerare il certificato con le informazioni correnti o di generare un certificato con nuove informazioni.

- **Nome comune**

  Obbligatorio. Il nome di dominio completo (FQDN) che si desidera proteggere.

  Nelle configurazioni ad alta disponibilità di Unified Manager, utilizzare l'indirizzo IP virtuale.

- **E-mail**

  Opzionale. Un indirizzo e-mail per contattare l'organizzazione, in genere l'indirizzo e-mail dell'amministratore dei certificati o del reparto IT.

- **Azienda**

  Opzionale. In genere, il nome della società.

- **Reparto**

  Opzionale. Il nome del reparto della società.

- **Città**

  Opzionale. La località della tua azienda.

- **Stato**

Opzionale. L’ubicazione dello stato o della provincia, non abbreviata, dell’azienda.

- **Paese**

  Opzionale. L’ubicazione del paese dell’azienda. Si tratta in genere di un codice ISO di due lettere del paese.

- **Nomi alternativi**

  Obbligatorio. Nomi di dominio aggiuntivi non primari che possono essere utilizzati per accedere a questo server oltre all’host locale o ad altri indirizzi di rete esistenti. Separare ciascun nome alternativo con una virgola.

  Selezionare la casella di controllo “Exclude local identifying information (e.g. localhost)” (Escludi informazioni di identificazione locale) se si desidera rimuovere le informazioni di identificazione locale dal campo dei nomi alternativi nel certificato. Quando questa casella di controllo è selezionata, solo i dati immessi nel campo vengono utilizzati nel campo nomi alternativi. Se lasciato vuoto, il certificato risultante non avrà alcun campo di nomi alternativi.

- **DIMENSIONE DELLA CHIAVE (ALGORITMO CHIAVE: RSA)**

  L’algoritmo delle chiavi è impostato su RSA. È possibile selezionare una delle dimensioni delle chiavi: 2048, 3072 o 4096 bit. La dimensione predefinita della chiave è impostata su 2048 bit.

- **PERIODO DI VALIDITÀ**

  Il periodo di validità predefinito è 397 giorni. Se è stato eseguito l’aggiornamento da una versione precedente, la validità del certificato precedente potrebbe essere invariata.

Per ulteriori informazioni, vedere "Generazione di certificati HTTPS".

Informazioni sul copyright

Informazioni sul marchio commerciale