Configurazione di Active IQ Unified Manager

Active IQ Unified Manager 9.11

NetApp
December 18, 2023

Sommario

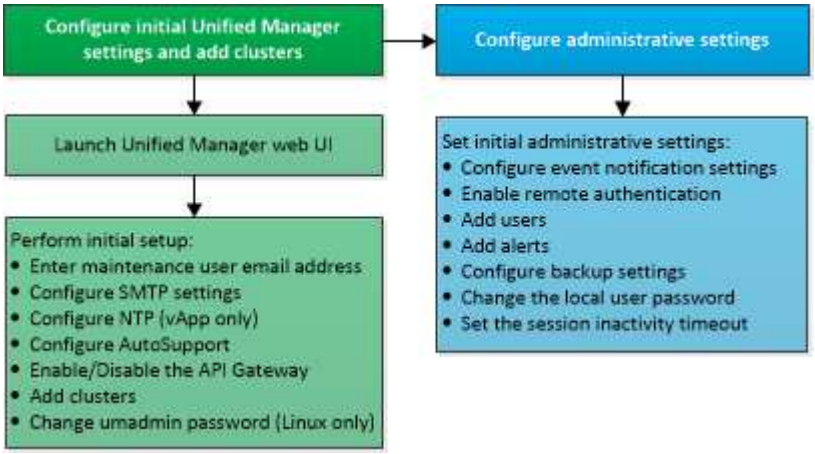
Configurazione di Active IQ Unified Manager

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

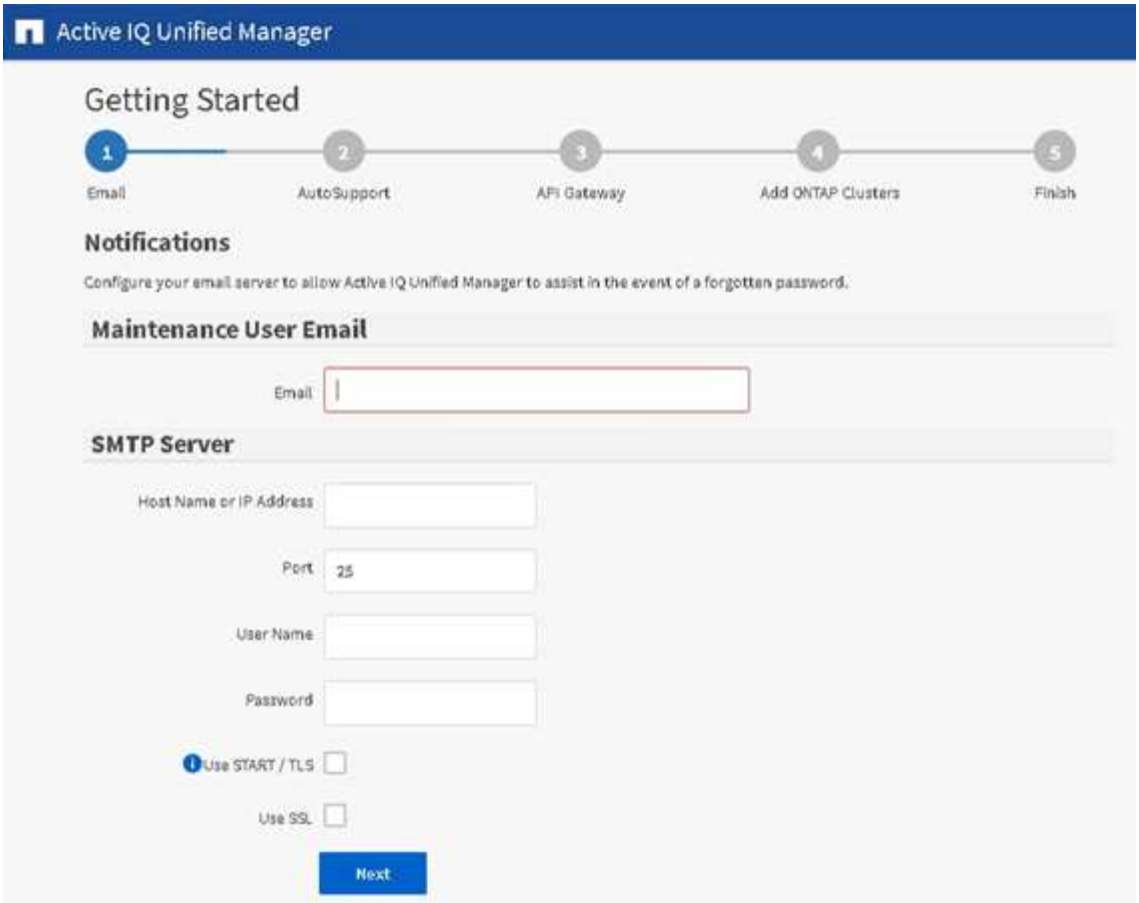
Per utilizzare Unified Manager, è necessario prima configurare le opzioni di configurazione iniziale, tra cui il server NTP, l'indirizzo e-mail dell'utente di manutenzione, l'host del server SMTP e l'aggiunta di cluster ONTAP.

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**.
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. Sui sistemi Red Hat e CentOS puoi 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. Sono necessari due tipi di certificati:

    Certificati server: Utilizzati per la registrazione. Per aggiungere un cluster è necessario un certificato valido. Se il certificato del server scade, è necessario rigenerarlo e riavviare Unified Manager affinché i servizi vengano nuovamente registrati automaticamente. Per informazioni sulla generazione dei certificati, consultare l'articolo della Knowledge base (KB): "Come rinnovare un certificato SSL in ONTAP 9"

    Certificati client: Utilizzati per l'autenticazione. Per aggiungere un cluster è necessario un certificato

valido. 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. Non è necessario rigenerare il certificato client.

> È possibile aggiungere cluster protetti da NAT/firewall utilizzando l'indirizzo IP NAT di Unified Manager. Tutti i sistemi di automazione del flusso di lavoro o SnapProtect collegati devono essere protetti da NAT/firewall e le chiamate API SnapProtect devono utilizzare l'indirizzo IP NAT per identificare il cluster.

- 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.

È possibile monitorare un singolo cluster mediante due istanze di Unified Manager, a condizione che sia stata configurata una seconda LIF di gestione del cluster sul cluster in modo che ogni istanza di Unified Manager si connetta attraverso una LIF diversa.

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**.

   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.

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 e fare clic su **Salva**.

   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.

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**.

Se si seleziona…	Quindi…
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**.
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.

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.