Esegui attività di configurazione e amministrative

Active IQ Unified Manager

NetApp
November 13, 2026

This PDF was generated from https://docs.netapp.com/it-it/active-iq-unified-manager-918/config/concept_configure_unified_manager.html on November 13, 2026. Always check docs.netapp.com for the latest.

Sommario

Esegui attività di configurazione e amministrative . . . 1
Configura Active IQ Unified Manager . . . 1
Scopri come configurare Active IQ Unified Manager . . . 1
Scopri la sequenza di configurazione in Active IQ Unified Manager . . . 1
Accedi all'interfaccia utente web in Active IQ Unified Manager . . . 1
Esegui la configurazione iniziale dell'interfaccia utente web di Active IQ Unified Manager . . . 2
Aggiungi cluster ad Active IQ Unified Manager . . . 4
Configura le notifiche . . . 6
Cambia la password dell'utente locale in Active IQ Unified Manager . . . 15
Imposta il timeout di inattività della sessione in Active IQ Unified Manager . . . 15
Imposta il timeout della sessione tramite la CLI in Active IQ Unified Manager . . . 16
Modifica l'host name di Unified Manager . . . 16
Abilita e disabilita la gestione dello storage basata su policy in Active IQ Unified Manager . . . 20
Configura il backup di Active IQ Unified Manager . . . 21
Gestisci le impostazioni delle funzionalità . . . 21
Scopri le impostazioni delle funzionalità in Active IQ Unified Manager . . . 21
Abilita la gestione dello storage basata su policy in Active IQ Unified Manager . . . 22
Scopri la funzionalità API Gateway in Active IQ Unified Manager . . . 22
Specifica il timeout di inattività in Active IQ Unified Manager . . . 23
Abilita gli eventi del portale Active IQ in Active IQ Unified Manager . . . 23
Attiva e disattiva le impostazioni di sicurezza per la conformità in Active IQ Unified Manager . . . 23
Abilita e disabilita il caricamento degli script in Active IQ Unified Manager . . . 24
Aggiungi un banner di accesso in Active IQ Unified Manager . . . 25
Usa la console di manutenzione . . . 25
Scopri la console di manutenzione in Active IQ Unified Manager . . . 25
Scopri l'utente di manutenzione in Active IQ Unified Manager . . . 26
Funzionalità utente di diagnostica in Active IQ Unified Manager . . . 26
Accedi alla console di manutenzione in Active IQ Unified Manager . . . 26
Accedi alla console di manutenzione usando la console VM vSphere in Active IQ Unified Manager . . . 27
Menu della console di manutenzione . . . 27
Cambia la password dell'utente di manutenzione su Windows in Active IQ Unified Manager . . . 33
Cambia la password umadmin di Active IQ Unified Manager sui sistemi Linux . . . 33
Modifica le porte che Active IQ Unified Manager usa per i protocolli HTTP e HTTPS . . . 33
Aggiungi interfacce di rete ad Active IQ Unified Manager . . . 34
Rigenera il certificato client in Active IQ Unified Manager . . . 35
Aggiungi spazio su disco . . . 35
Gestisci l'accesso degli utenti . . . 39
Aggiungi utenti . . . 39
Modifica le impostazioni utente in Active IQ Unified Manager . . . 40
Visualizza gli utenti in Active IQ Unified Manager . . . 40
Elimina utenti o gruppi in Active IQ Unified Manager . . . 41
Scopri il controllo degli accessi in base al ruolo in Active IQ Unified Manager . . . 41
Scopri le tipologie di utente in Active IQ Unified Manager . . . 41

Scopri i ruoli utente in Active IQ Unified Manager . . . 42
Scopri i ruoli e le funzionalità degli utenti in Active IQ Unified Manager . . . 43
Gestisci le impostazioni di autenticazione SAML . . . 45
Abilita l'autenticazione SAML in Active IQ Unified Manager . . . 45
Usa un provider di identità in Active IQ Unified Manager . . . 45
Abilita l'autenticazione SAML in Active IQ Unified Manager . . . 46
Cambia il provider di identità per l'autenticazione SAML in Active IQ Unified Manager . . . 47
Aggiorna le impostazioni di autenticazione SAML dopo una modifica del certificato di sicurezza di Active IQ Unified Manager . . . 48
Disabilita l'autenticazione SAML in Active IQ Unified Manager . . . 49
Disabilita l'autenticazione SAML dalla console di manutenzione di Active IQ Unified Manager . . . 50
Usa la pagina di autenticazione SAML in Active IQ Unified Manager . . . 50
Gestisci l'autenticazione . . . 51
Modifica i server di autenticazione in Active IQ Unified Manager . . . 51
Elimina i server di autenticazione in Active IQ Unified Manager . . . 52
Autenticati con Active Directory o OpenLDAP in Active IQ Unified Manager . . . 52
Registrazione di audit . . . 52
Usa la pagina di autenticazione remota in Active IQ Unified Manager . . . 55
Gestisci i certificati di sicurezza . . . 58
Visualizza il certificato di sicurezza HTTPS in Active IQ Unified Manager . . . 58
Scarica una richiesta di firma del certificato HTTPS in Active IQ Unified Manager . . . 59
Installa un certificato HTTPS firmato da una CA in Active IQ Unified Manager . . . 59
Scopri i certificati HTTPS generati utilizzando strumenti esterni in Active IQ Unified Manager Unified Manager . . . 60
Descrizioni delle pagine per la gestione dei certificati . . . 62

Esegui attività di configurazione e amministrative

Configura Active IQ Unified Manager

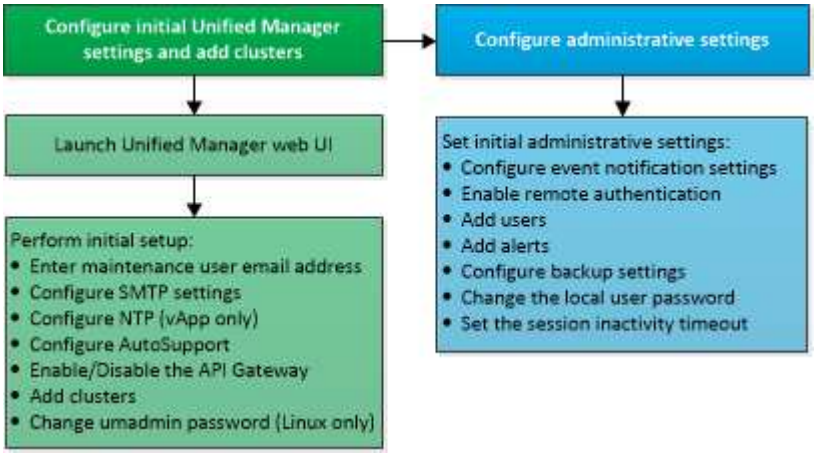
Scopri come configurare Active IQ Unified Manager

Dopo aver installato Active IQ Unified Manager (precedentemente OnCommand Unified Manager) devi completare la configurazione iniziale (chiamata anche procedura guidata della prima esperienza) per accedere all'interfaccia utente web. Quindi puoi eseguire ulteriori attività di configurazione, come aggiungere cluster, configurare l'autenticazione remota, aggiungere utenti e aggiungere avvisi.

Alcune delle procedure descritte in questo manuale sono necessarie per completare la configurazione iniziale della tua istanza di Unified Manager. Altre procedure sono impostazioni di configurazione consigliate, utili da impostare sulla tua nuova istanza o da conoscere prima di iniziare il monitoraggio regolare dei tuoi sistemi ONTAP.

Scopri la sequenza di configurazione in Active IQ Unified Manager

Il flusso di configurazione descrive le attività che devi eseguire prima di poter utilizzare Unified Manager.



Accedi all'interfaccia utente web in Active IQ Unified Manager

Dopo aver installato Unified Manager, puoi accedere all'interfaccia web per configurare Unified Manager e iniziare a monitorare i tuoi sistemi ONTAP.

Prima di iniziare

- Se è la prima volta che accedi all'interfaccia utente web, devi accedere come utente di manutenzione (o come utente umadmin per le installazioni Linux).
- Se intendi consentire agli utenti di accedere a Unified Manager utilizzando il nome breve anziché il fully qualified domain name (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. Puoi accettare il rischio per continuare l'accesso oppure installare un certificato digitale firmato da un'Autorità di Certificazione (CA) per l'autenticazione del server.

Passaggi

1. Avvia l'interfaccia utente web di Unified Manager dal browser utilizzando l'URL visualizzato al termine dell'installazione. L'URL corrisponde all'indirizzo IP o al fully qualified domain name (FQDN) del server Unified Manager.

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

2. Accedi all'interfaccia utente web di Unified Manager utilizzando le credenziali del tuo utente di manutenzione.

> Se effettui tre tentativi consecutivi di accesso all'interfaccia web senza successo entro un'ora, verrai bloccato fuori dal sistema e dovrai contattare il tuo system administrator. Questa procedura si applica solo agli utenti locali.

Esegui la configurazione iniziale dell'interfaccia utente web di Active IQ Unified Manager

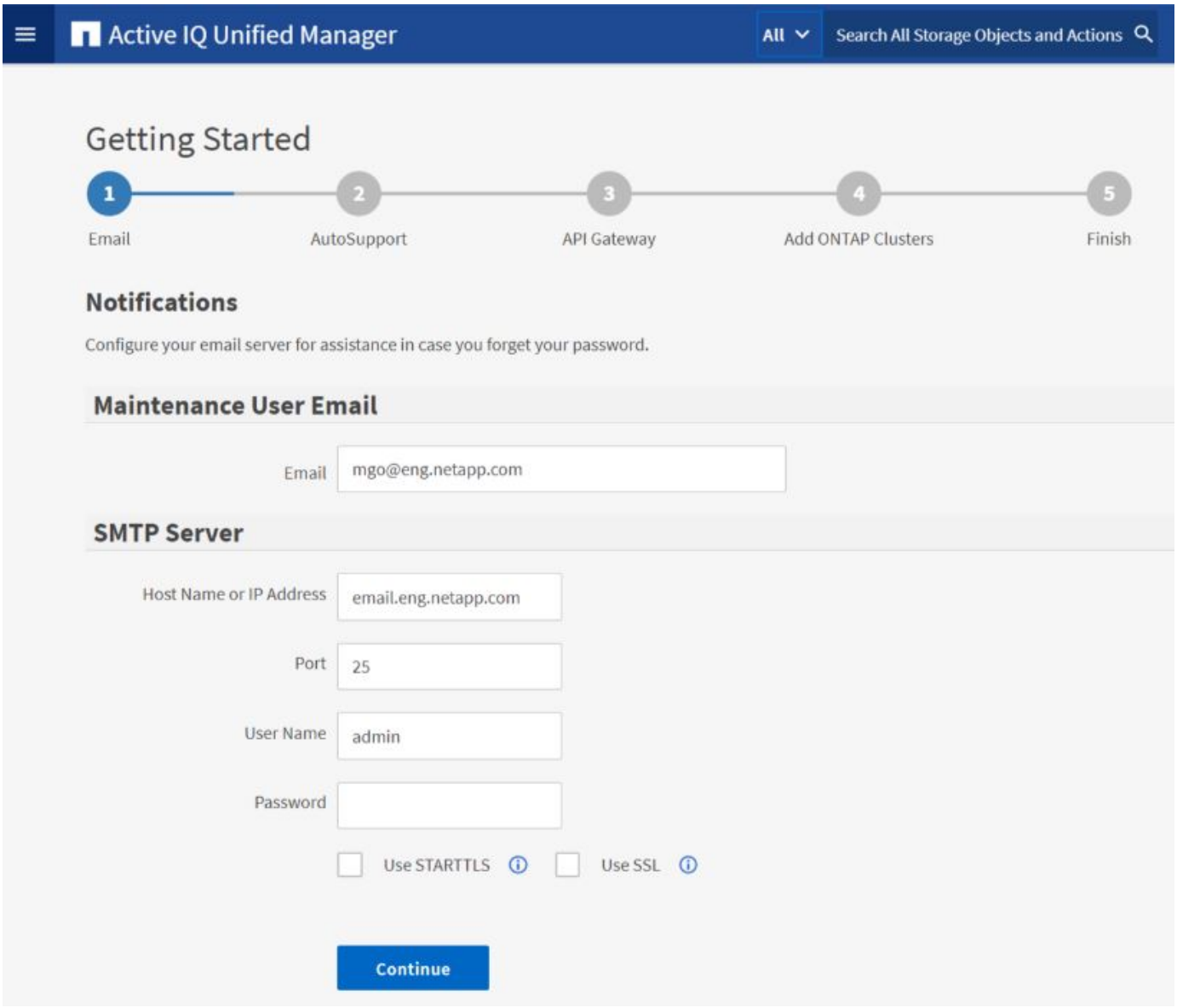
Per utilizzare Unified Manager, devi prima configurare le opzioni di configurazione iniziale, tra cui il server NTP, l'indirizzo email dell'utente di manutenzione, l'host del server SMTP e l'aggiunta dei cluster ONTAP.

Prima di iniziare

Devi aver eseguito le seguenti operazioni:

- Avviata l'interfaccia utente web di Unified Manager utilizzando l'URL fornito dopo l'installazione
- Hai effettuato l'accesso utilizzando il nome utente e la password di manutenzione (utente umadmin per le installazioni Linux) creati durante l'installazione

La pagina Getting Started di Active IQ Unified ManagerGetting viene visualizzata solo quando accedi per la prima volta all'interfaccia utente web. La pagina seguente proviene da un'installazione su VMware.



Se vuoi modificare una di queste opzioni in seguito, puoi selezionare la tua scelta dalle opzioni generali nel riquadro di navigazione sinistro di Unified Manager. Tieni presente che l'impostazione NTP è valida solo per le installazioni VMware e può essere modificata in seguito tramite la console di manutenzione di Unified Manager.

Passaggi

1. Nella pagina Initial Setup di Active IQ Unified Manager, inserisci l'indirizzo email dell'utente di manutenzione, l'host name del server SMTP ed eventuali opzioni SMTP aggiuntive, nonché il server NTP (solo per le installazioni VMware). Quindi fai clic su **Continue**.

   Se hai selezionato l'opzione **Usa STARTTLS** o **Usa SSL**, dopo aver cliccato sul pulsante **Continua** verrà visualizzata una pagina relativa al certificato. Verifica i dettagli del certificato e accettalo per proseguire con le impostazioni di configurazione iniziali dell'interfaccia web.

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

   Se devi designare un proxy per fornire l'accesso a Internet e inviare contenuti di AutoSupport, oppure se vuoi disabilitare AutoSupport, usa l'opzione **General** > **AutoSupport** dall'interfaccia web.

3. Sui sistemi Red Hat, modifica la password dell'utente umadmin dalla stringa predefinita "admin" a una stringa personalizzata.
4. Nella pagina Configura API Gateway, seleziona se vuoi utilizzare la funzionalità API Gateway che consente a Unified Manager di gestire i cluster ONTAP che intendi monitorare tramite le API REST di ONTAP. Quindi fai clic su **Continua**.

   In seguito puoi abilitare o disabilitare questa impostazione nell'interfaccia utente web da **Generale** > **Impostazioni funzionalità** > **API Gateway**. Per ulteriori informazioni sulle API, consulta "Guida introduttiva alle API REST di Active IQ Unified Manager".

5. Aggiungi i cluster che vuoi far gestire a Unified Manager, quindi fai clic su **Avanti**. Per ogni cluster che prevedi di gestire, devi disporre dell'host name o dell'indirizzo IP di gestione del cluster (IPv4 o IPv6), oltre alle credenziali di nome utente e password; l'utente deve avere il ruolo "admin".

   Questo passaggio è facoltativo. Puoi aggiungere i cluster in un secondo momento nell'interfaccia web da **Storage Management** > **Cluster Setup**.

6. Nella pagina Riepilogo, verifica che tutte le impostazioni siano corrette e fai clic su **Finish**.

La pagina "Per iniziare" si chiude e viene visualizzata la pagina "Dashboard di Unified Manager".

Aggiungi cluster ad Active IQ Unified Manager

Puoi aggiungere un cluster ad Active IQ Unified Manager per monitorare il cluster. Ciò include la possibilità di ottenere informazioni sul cluster, come lo stato di salute, la capacità, le prestazioni e la configurazione del cluster, in modo da poter individuare e risolvere eventuali problemi.

Prima di iniziare

- Devi disporre del ruolo di Amministratore dell'applicazione o di Amministratore dello storage.
- Devi avere le seguenti informazioni:
  - Unified Manager supporta cluster ONTAP on-premises, ONTAP Select, Cloud Volumes ONTAP.
  - host name o indirizzo IP di gestione del cluster

    L'host name è il nome di dominio completo (FQDN) o il nome breve che Unified Manager utilizza per connettersi al cluster. L'host name deve risolversi nell'indirizzo IP di gestione del cluster.

    L'indirizzo IP di gestione del cluster deve corrispondere alla LIF di gestione del cluster della storage virtual machine (SVM) amministrativa. Se usi una LIF di gestione dei nodi, l'operazione non riesce.

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

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

  - Il numero di porta per connetterti al cluster utilizzando il protocollo HTTPS (in genere la porta 443)
  - Possiedi i certificati richiesti:

    Certificato SSL (HTTPS): questo certificato appartiene a Unified Manager. Un certificato SSL (HTTPS) autofirmato predefinito viene generato con una nuova installazione di Unified Manager. NetApp

consiglia di aggiornarlo a un certificato firmato da una CA per una maggiore sicurezza. Se il certificato del server scade, devi rigenerarlo e riavviare Unified Manager perché i servizi incorporino il nuovo certificato. Per ulteriori informazioni sulla rigenerazione del certificato SSL, vedi "Generazione di un certificato di sicurezza HTTPS".

Certificato EMS: Questo certificato appartiene a Unified Manager. Lo usi durante l'autenticazione per le notifiche EMS ricevute da ONTAP.

Certificati per la comunicazione TLS reciproca: Utilizzati durante la comunicazione TLS reciproca tra Unified Manager e ONTAP. L'autenticazione basata su certificati 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 certificati non è abilitata.

L'autenticazione basata su certificato non viene abilitata automaticamente per un cluster se stai aggiornando una versione precedente di Unified Manager. Tuttavia, puoi abilitarla modificando e salvando i dettagli del cluster. Se il certificato scade, devi rigenerarlo per incorporare il nuovo certificato. Per ulteriori informazioni su come visualizzare e rigenerare il certificato, consulta "Modifica dei cluster".



- Puoi aggiungere un cluster dall'interfaccia utente web e l'autenticazione basata su certificati viene abilitata automaticamente.
- Puoi aggiungere un cluster tramite la CLI di Unified Manager; l'autenticazione basata su certificati non è abilitata per impostazione predefinita. Se aggiungi un cluster utilizzando la CLI di Unified Manager, devi modificare il cluster utilizzando l'interfaccia utente di Unified Manager. Puoi consultare "Comandi CLI di Unified Manager supportati" per aggiungere un cluster utilizzando la CLI di Unified Manager.
- Se per un cluster è abilitata l'autenticazione basata su certificato e esegui il backup di Unified Manager da un server e lo ripristini su un altro server Unified Manager in cui il nome host o l'indirizzo IP sono cambiati, il monitoraggio del cluster potrebbe non riuscire. Per evitare il problema, modifica e salva i dettagli del cluster. Per ulteriori informazioni su come modificare i dettagli del cluster, consulta "Modifica dei cluster".

+ **Certificati del cluster**: Questo certificato è di proprietà di ONTAP. Non puoi aggiungere un cluster a Unified Manager con un certificato scaduto e, se il certificato è già scaduto, devi rigenerarlo prima di aggiungere il cluster. Per informazioni sulla generazione dei certificati, consulta l'articolo della knowledge base (KB) "Come rinnovare un certificato autofirmato di ONTAP nell'interfaccia utente di System Manager".

- Devi disporre di spazio sufficiente sul server Unified Manager. Non puoi aggiungere un cluster al server se oltre il 90% dello spazio nella directory del database è già occupato.

Per una configurazione MetroCluster, devi aggiungere sia il cluster locale che quello remoto e i cluster devono essere configurati correttamente.

Passaggi

1. Nel riquadro di navigazione a sinistra, fai clic su **Gestione dello storage** > **Configurazione del cluster**.
2. Nella pagina Configurazione cluster, fai clic su **Aggiungi**.
3. Nella finestra di dialogo Aggiungi cluster, specifica i valori richiesti, come l'host name o l'indirizzo IP del cluster, il nome utente, la password e il numero di porta.

   Puoi 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. Fai clic su **Submit**.
5. Nella finestra di dialogo Authorize Host, fai clic su **View Certificate** per visualizzare le informazioni sul certificato del cluster.
6. Fai clic su **Yes**.

   Dopo aver salvato i dettagli del cluster, puoi visualizzare il certificato per la comunicazione TLS reciproca di un cluster.

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

Una volta individuati tutti gli oggetti per un nuovo cluster, Unified Manager inizia a raccogliere i dati storici sulle prestazioni relativi ai 15 giorni precedenti. Queste statistiche vengono raccolte utilizzando la funzionalità di raccolta della continuità dei dati. Questa funzionalità ti fornisce oltre due settimane di informazioni sulle prestazioni di un cluster immediatamente dopo che è stato aggiunto. Al termine del ciclo di raccolta della continuità dei dati, i dati real-time sulle prestazioni del cluster vengono raccolti, per impostazione predefinita, ogni cinque minuti.



Poiché la raccolta di 15 giorni di dati sulle prestazioni richiede un elevato utilizzo della CPU, ti consigliamo di scaglionare l'aggiunta di nuovi cluster in modo che i processi di raccolta della continuità dei dati non vengano eseguiti contemporaneamente su troppi cluster. Inoltre, se riavvii Unified Manager durante il periodo di raccolta della continuità dei dati, la raccolta verrà interrotta e vedrai delle lacune nei grafici delle prestazioni per l'intervallo di tempo mancante.



Se ricevi un messaggio di errore che indica che non puoi aggiungere il cluster, verifica se gli orologi dei due sistemi non sono sincronizzati e se la data di inizio del certificato HTTPS di Unified Manager è successiva alla data del cluster. Devi assicurarti che gli orologi siano sincronizzati tramite NTP o un servizio simile.

Informazioni correlate

"Installazione di un certificato HTTPS firmato e restituito da una CA"

Configura le notifiche

Configura Active IQ Unified Manager per inviare notifiche di avviso

Puoi configurare Unified Manager per inviare notifiche che ti avvisano degli eventi nel tuo ambiente. Prima di poter inviare le notifiche, devi configurare diverse altre opzioni di Unified Manager.

Prima di iniziare

Devi avere il ruolo di Amministratore dell'applicazione.

Dopo aver distribuito Unified Manager e completato la configurazione iniziale, dovresti prendere in considerazione la configurazione del tuo ambiente per attivare avvisi e generare notifiche via email o trap SNMP in base alla ricezione di eventi.

Passaggi

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

Se desideri ricevere notifiche di avviso quando si verificano determinati eventi nel tuo ambiente, devi configurare un server SMTP e fornire un indirizzo e-mail da cui inviare le notifiche di avviso. Se preferisci utilizzare le trap SNMP, puoi selezionare questa opzione e fornire le informazioni necessarie.

2. "Abilita l'autenticazione remota".

   Se vuoi che gli utenti remoti di LDAP o Active Directory accedano all'istanza di Unified Manager e ricevano notifiche di avviso, devi abilitare l'autenticazione remota.

3. "Aggiungi server di autenticazione".

   Puoi aggiungere server di autenticazione in modo che gli utenti remoti nel server di autenticazione possano accedere a Unified Manager.

4. "Aggiungi utenti".

   Puoi aggiungere diversi tipi di utenti locali o remoti e assegnare ruoli specifici. Quando crei un avviso, assegni un utente per ricevere le notifiche dell'avviso.

5. "Aggiungi avvisi".

   Dopo aver aggiunto l'indirizzo email per l'invio delle notifiche, aver aggiunto gli utenti che le riceveranno, aver configurato le impostazioni di rete e le opzioni SMTP e SNMP necessarie per il tuo ambiente, puoi assegnare gli avvisi.

Configura le impostazioni di notifica degli eventi in Active IQ Unified Manager

Puoi configurare Unified Manager per inviare notifiche di avviso quando viene generato un evento o quando un evento viene assegnato a un utente. Puoi configurare il server SMTP utilizzato per inviare l'avviso e impostare diversi meccanismi di notifica; ad esempio, le notifiche di avviso possono essere inviate come email o trap SNMP.

Prima di iniziare

Devi avere le seguenti informazioni:

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

  L'indirizzo email compare nel campo "From" nelle notifiche di avviso inviate. Se l'email non può essere recapitata per qualsiasi motivo, questo indirizzo email viene utilizzato anche come destinatario della posta non recapitabile.

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

  Per specificare più destinazioni trap, separa ciascun host con una virgola. In questo caso, tutte le altre impostazioni SNMP, come la versione e la porta trap outbound, devono essere uguali per tutti gli host nell'elenco.

Devi disporre del ruolo di Amministratore dell'applicazione o di Amministratore dello storage.

Passaggi

1. Nel riquadro di navigazione a sinistra, fai clic su **Generale** > **Notifiche**.

2. Nella pagina Notifiche, configura le impostazioni appropriate.

   Note:

   - Se il campo "Da" è precompilato con l'indirizzo "ActiveIQUnifiedManager@localhost.com", devi modificarlo con un indirizzo email reale e funzionante per assicurarti che tutte le notifiche email vengano recapitate correttamente.
   - Se non è possibile risolvere l'host name del server SMTP, puoi specificare l'indirizzo IP (IPv4 o IPv6) del server SMTP al posto dell'host name.

3. Fare clic su **Save**.
4. Se hai selezionato l'opzione **Usa STARTTLS** o **Usa SSL**, dopo aver cliccato sul pulsante **Salva** verrà visualizzata una pagina relativa al certificato. Verifica i dettagli del certificato e accettalo per salvare le impostazioni di notifica.

   Puoi fare clic sul pulsante **Visualizza dettagli certificato** per visualizzare i dettagli del certificato. Se il certificato esistente è scaduto, deseleziona la casella **Usa STARTTLS** o **Usa SSL**, salva le impostazioni di notifica e seleziona nuovamente la casella **Usa STARTTLS** o **Usa SSL** per visualizzare un nuovo certificato.

Abilita l'autenticazione remota in Active IQ Unified Manager

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

Prima di iniziare

Devi avere il ruolo di Amministratore dell'applicazione.

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

Puoi abilitare l'autenticazione remota usando Open LDAP o Active Directory. Se l'autenticazione remota è disabilitata, gli utenti remoti non possono accedere a Unified Manager.

L'autenticazione remota è supportata tramite LDAP e LDAPS (LDAP sicuro). Unified Manager utilizza la porta 389 come porta predefinita per le comunicazioni non sicure e la porta 636 come porta predefinita per le comunicazioni sicure.

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

Passaggi

1. Nel riquadro di navigazione a sinistra, fai clic su **Generale** > **Autenticazione remota**.
2. Seleziona la casella **Abilita l'autenticazione remota…**.
3. Nel campo Servizio di autenticazione, seleziona il tipo di servizio e configura il servizio di autenticazione.

Per il tipo di autenticazione…	Inserisci 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 di amministratore • Nome distinto di base (utilizzando la notazione LDAP appropriata)
Open LDAP	• Nome distinto di bind (nella notazione LDAP appropriata) • Password di bind • Nome distinto di base

Se l'autenticazione di un utente di Active Directory richiede molto tempo o va in timeout, è probabile che il server di autenticazione impieghi molto tempo a rispondere. Disabilitare il supporto per i gruppi nidificati in Unified Manager potrebbe ridurre il tempo di autenticazione.

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

4. **Facoltativo:** Aggiungi server di autenticazione e verifica l'autenticazione.
5. Fare clic su **Save**.

Disabilita i gruppi nidificati dall'autenticazione remota in Active IQ Unified Manager

Se hai abilitato l'autenticazione remota, puoi disabilitare l'autenticazione dei gruppi nidificati in modo che solo i singoli utenti, e non i membri dei gruppi, possano autenticarsi in remoto a Unified Manager. Puoi disabilitare i gruppi nidificati quando vuoi migliorare i tempi di risposta dell'autenticazione di Active Directory.

Prima di iniziare

- Devi avere il ruolo di Amministratore dell'applicazione.
- La disabilitazione dei gruppi nidificati si applica solo quando utilizzi Active Directory.

Disabilitare il supporto per i gruppi nidificati in Unified Manager potrebbe ridurre il tempo di autenticazione. Se il supporto per i gruppi nidificati è disabilitato e aggiungi un gruppo remoto a Unified Manager, i singoli utenti devono essere membri del gruppo remoto per autenticarsi in Unified Manager.

Passaggi

1. Nel riquadro di navigazione a sinistra, fai clic su **Generale** > **Autenticazione remota**.
2. Seleziona la casella **Disabilita la ricerca di gruppi nidificati**.
3. Fare clic su **Save**.

Configura i servizi di autenticazione in Active IQ Unified Manager

I servizi di autenticazione consentono di autenticare utenti o gruppi remoti in un server di autenticazione prima di concedere loro l'accesso a Unified Manager. Puoi autenticare gli utenti utilizzando servizi di autenticazione predefiniti (come Active Directory o OpenLDAP) oppure configurando un meccanismo di autenticazione personalizzato.

Prima di iniziare

- Devi aver abilitato l'autenticazione remota.
- Devi avere il ruolo di Amministratore dell'applicazione.

Passaggi

1. Nel riquadro di navigazione a sinistra, fai clic su **Generale** > **Autenticazione remota**.
2. Seleziona uno dei seguenti servizi di autenticazione:

Se selezioni…	Poi fai così…
Active Directory	a. Inserisci il nome e la password dell'amministratore. b. Specifica il nome distinto di base del server di autenticazione. Ad esempio, se il domain name del server di autenticazione è ou@domain.com, il nome distinto di base è **cn=ou,dc=domain,dc=com**.
OpenLDAP	a. Inserisci il nome distinto di bind e la password di bind. b. Specifica il nome distinto di base del server di autenticazione. Ad esempio, se il domain name del server di autenticazione è ou@domain.com, il nome distinto di base è **cn=ou,dc=domain,dc=com**.
Altri	a. Inserisci il nome distinto di bind e la password di bind. b. Specifica il nome distinto di base del server di autenticazione. Ad esempio, se il domain name del server di autenticazione è ou@domain.com, il nome distinto di base è **cn=ou,dc=domain,dc=com**. c. Specifica la versione del protocollo LDAP supportata dal server di autenticazione. d. Inserisci il nome utente, l'appartenenza al gruppo, il gruppo utente e gli attributi del membro.

Se vuoi modificare il servizio di autenticazione, devi eliminare tutti i server di autenticazione

esistenti e quindi aggiungere nuovi server di autenticazione.

3. Fare clic su **Save**.

Aggiungi i server di autenticazione ad Active IQ Unified Manager

Puoi 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.

Prima di iniziare

- Devono essere disponibili le seguenti informazioni:
  - host name o indirizzo IP del server di autenticazione
  - Numero di porta del server di autenticazione
- Devi aver abilitato 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.
- Devi avere il ruolo di Amministratore dell'applicazione.

Se il server di autenticazione che stai aggiungendo fa parte di una coppia ad alta disponibilità (HA) (che utilizza lo stesso database), puoi 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.

Passaggi

1. Nel riquadro di navigazione a sinistra, fai clic su **Generale** > **Autenticazione remota**.
2. Attiva o disattiva l'opzione **Utilizza connessione sicura**:

Se vuoi…	Poi fai così…
Abilitalo	a. Seleziona l'opzione **Usa connessione sicura**. b. Nell'area Server di autenticazione, fai clic su **Aggiungi**. c. Nella finestra di dialogo Aggiungi server di autenticazione, immetti il nome di autenticazione o l'indirizzo IP (IPv4 o IPv6) del server. d. Nella finestra di dialogo Autorizza host, fai clic su Visualizza certificato. e. Nella finestra di dialogo Visualizza certificato, verifica le informazioni del certificato e poi fai clic su **Chiudi**. f. Nella finestra di dialogo Autorizza host, fai clic su **Sì**. Quando abiliti l'opzione **Utilizza l'autenticazione tramite connessione sicura**, Unified Manager comunica con il server di autenticazione e visualizza il certificato. Unified Manager utilizza la porta 636 come porta predefinita per la comunicazione sicura e la porta 389 per la comunicazione non sicura.
Disabilitalo	a. Deseleziona l'opzione **Use Secure Connection**. b. Nell'area Server di autenticazione, fai clic su **Aggiungi**. c. Nella finestra di dialogo Aggiungi server di autenticazione, specifica l'host name o l'indirizzo IP (IPv4 o IPv6) del server e i dettagli della porta. d. Fai clic su **Add**.

Il server di autenticazione che hai aggiunto viene visualizzato nell'area Servers.

3. Esegui un'autenticazione di prova per verificare di poter autenticare gli utenti nel server di autenticazione che hai aggiunto.

Verifica la configurazione dei server di autenticazione in Active IQ Unified Manager

Puoi convalidare la configurazione dei server di autenticazione per assicurarti che il server di gestione sia in grado di comunicare con essi. Puoi convalidare la configurazione cercando un utente o un gruppo remoto nei tuoi server di autenticazione e autenticandoli utilizzando le impostazioni configurate.

Prima di iniziare

- Devi aver abilitato 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.
- Devi aver aggiunto i server di autenticazione affinché il server di gestione possa cercare l'utente remoto o il gruppo remoto su questi server e autenticarli.
- Devi avere il ruolo di Amministratore dell'applicazione.

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

Passaggi

1. Nel riquadro di navigazione a sinistra, fai clic su **Generale** > **Autenticazione remota**.
2. Fai clic su **Test Authentication**.
3. Nella finestra di dialogo Test User, specifica il nome utente e la password dell'utente remoto o il nome utente del gruppo remoto, quindi fai clic su **Test**.

   Se stai autenticando un gruppo remoto, non devi inserire la password.

Aggiungi avvisi in Active IQ Unified Manager

Puoi configurare gli avvisi per ricevere una notifica quando viene generato un evento specifico. Puoi configurare gli avvisi per una singola risorsa, per un gruppo di risorse o per eventi di un particolare tipo di severità. Puoi specificare la frequenza con cui vuoi ricevere le notifiche e associare uno script all'avviso.

Prima di iniziare

- Devi aver configurato le impostazioni di notifica, come l'indirizzo email dell'utente, il server SMTP e l'host delle trap SNMP, affinché il server Active IQ Unified Manager possa utilizzare tali impostazioni per inviare notifiche agli utenti quando viene generato un evento.
- Devi conoscere le risorse e gli eventi per i quali vuoi attivare l'avviso, nonché i nomi utente o gli indirizzi e-mail degli utenti che vuoi avvisare.
- Se vuoi che uno script venga eseguito in base all'evento, devi aver aggiunto lo script a Unified Manager usando la pagina Script.
- Devi disporre del ruolo di Amministratore dell'applicazione o di Amministratore dello storage.

Puoi creare un avviso direttamente dalla pagina Dettagli evento dopo aver ricevuto un evento, oltre a crearlo dalla pagina Configurazione avvisi, come descritto qui.

Passaggi

1. Nel riquadro di navigazione a sinistra, fai clic su **Storage Management** > **Alert Setup**.
2. Nella pagina Configurazione avvisi, fai clic su **Aggiungi**.
3. Nella finestra di dialogo Aggiungi avviso, fai clic su **Nome** e inserisci un nome e una descrizione per l'avviso.
4. Fai clic su **Risorse** e seleziona le risorse da includere o da escludere dall'avviso.

   Puoi impostare un filtro specificando una stringa di testo nel campo **Il nome contiene** per selezionare un gruppo di risorse. In base alla stringa di testo che specifichi, l'elenco delle risorse disponibili mostra solo

quelle che corrispondono alla regola di filtro. La stringa di testo che specifichi fa distinzione tra maiuscole e minuscole.

Se una risorsa soddisfa sia le regole di inclusione sia quelle di esclusione che hai specificato, la regola di esclusione ha la precedenza su quella di inclusione e non viene generato alcun avviso per gli eventi correlati alla risorsa esclusa.

5. Fai clic su **Eventi** e seleziona gli eventi in base al nome dell'evento o al tipo di severità per i quali vuoi attivare un avviso.



Per selezionare più di un evento, tieni premuto il tasto Ctrl mentre fai le tue selezioni.

6. Fai clic su **Azioni**, seleziona gli utenti che vuoi notificare, scegli la frequenza di notifica, scegli se inviare una trap SNMP al ricevitore trap e assegna uno script da eseguire quando si genera un avviso.



Se modifichi l'indirizzo email specificato per l'utente e riapri l'avviso per modificarlo, il campo Nome appare vuoto perché l'indirizzo email modificato non è più associato all'utente selezionato in precedenza. Inoltre, se modifichi l'indirizzo email dell'utente selezionato dalla pagina Users, l'indirizzo email modificato non viene aggiornato per l'utente selezionato.

Puoi anche scegliere di notificare gli utenti tramite trap SNMP.

7. Fare clic su **Save**.

Esempio di aggiunta di un avviso

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

- Nome dell'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 critici relativi all'integrità
- Azioni: include "sample@domain.com", uno script "Test" e l'utente deve essere avvisato ogni 15 minuti

Esegui i seguenti passaggi nella finestra di dialogo Aggiungi avviso:

Passaggi

1. Fai clic su **Nome** e inserisci **HealthTest** nel campo **Nome avviso**.
2. Fai clic su **Risorse**, e nella scheda Includi seleziona **Volumi** dall'elenco a discesa.
   a. Inserisci **abc** nel campo **Il nome contiene** per visualizzare i volumi il cui nome contiene "abc".
   b. Seleziona **<<All Volumes whose name contains 'abc'>>** dall'area Risorse disponibili e spostalo nell'area Risorse selezionate.
   c. Fai clic su **Escludi**, inserisci **xyz** nel campo **Il nome contiene** e poi fai clic su **Aggiungi**.
3. Fai clic su **Eventi** e seleziona **Critico** dal campo **Gravità evento**.
4. Seleziona **Tutti gli eventi critici** dall'area Eventi corrispondenti e spostalo nell'area Eventi selezionati.
5. Fai clic su **Azioni** e inserisci **sample@domain.com** nel campo Avvisa questi utenti.
6. Seleziona **Ricorda ogni 15 minuti** per inviare una notifica all'utente ogni 15 minuti.

   Puoi configurare un avviso in modo che invii ripetutamente notifiche ai destinatari per un periodo di tempo specificato. Devi determinare l'ora a partire dalla quale la notifica dell'evento è attiva per l'avviso.

7. Nel menu Seleziona script da eseguire, seleziona lo script **Test**.
8. Fare clic su **Save**.

Cambia la password dell'utente locale in Active IQ Unified Manager

Puoi modificare la password di accesso dell'utente locale per prevenire potenziali rischi per la sicurezza.

Prima di iniziare

Devi aver effettuato l'accesso come utente locale.

Le password dell'utente di manutenzione e degli utenti remoti non possono essere modificate seguendo questi passaggi. Per modificare la password di un utente remoto, contatta l'amministratore delle password. Per modificare la password dell'utente di manutenzione, consulta "Utilizzo della console di manutenzione".

Passaggi

1. Accedi a Unified Manager.
2. Dalla barra dei menu in alto, fai clic sull'icona dell'utente e poi su **Cambia password**.

   L'opzione **Cambia password** non compare se sei un utente remoto.

3. Nella finestra di dialogo Cambia password, immetti la password corrente e la nuova password.
4. Fare clic su **Save**.

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

Imposta il timeout di inattività della sessione in Active IQ Unified Manager

Puoi specificare il valore del timeout di inattività per Unified Manager in modo che la sessione termini automaticamente dopo un determinato periodo di inattività. Per impostazione predefinita, il timeout è impostato su 4.320 minuti (72 ore).

Prima di iniziare

Devi avere il ruolo di Amministratore dell'applicazione.

Questa impostazione influisce su tutte le sessioni utente attualmente connesse.

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

Passaggi

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

Se vuoi…	Poi fai così…
Non impostare alcun timeout in modo che la sessione non si chiuda mai automaticamente	Nel pannello **Timeout di inattività**, sposta il cursore verso sinistra (disattivato) e fai clic su **Applica**.

Se vuoi…	Poi fai così…
Imposta un numero specifico di minuti come valore di timeout	Nel pannello **Timeout di inattività**, sposta il cursore verso destra (attivo), specifica il valore del timeout di inattività in minuti e fai clic su **Applica**.

Imposta il timeout della sessione tramite la CLI in Active IQ Unified Manager

Puoi impostare un valore massimo di timeout della sessione per Unified Manager utilizzando la CLI, in modo che la sessione termini automaticamente dopo un determinato periodo di tempo. Per impostazione predefinita, il timeout della sessione è impostato sul valore massimo, ovvero 4,320 minuti (72 ore). Ciò significa che la sessione termina automaticamente dopo 72 ore, anche se hai effettuato l'accesso e stai utilizzando attivamente Unified Manager.

Informazioni su questa attività

Devi avere il ruolo di Amministratore dell'applicazione.

L'impostazione del timeout di sessione influisce su tutte le sessioni degli utenti che hanno effettuato l'accesso.

Passaggi

1. Accedi alla CLI di Unified Manager inserendo il comando `um cli login`. Usa un nome utente e una password validi per l'autenticazione.
2. Inserisci il `um option set max.session.timeout.value=<in mins>` comando per modificare il valore di timeout della sessione.

Modifica l'host name di Unified Manager

Cambia l'host name della virtual appliance Active IQ Unified Manager

All'host di rete viene assegnato un nome quando l'appliance virtuale Unified Manager viene distribuita per la prima volta. Puoi modificare l'host name dopo la distribuzione. Se modifichi l'host name, devi anche rigenerare il certificato HTTPS.

Prima di iniziare

Per eseguire queste attività, devi aver effettuato l'accesso a Unified Manager come utente di manutenzione oppure disporre del ruolo Application Administrator.

Puoi utilizzare l'host name (o l'indirizzo IP dell'host) per accedere all'interfaccia utente web di Unified Manager. Se durante la distribuzione hai configurato un indirizzo IP statico per la rete, allora hai assegnato un nome all'host di rete. Se hai configurato la rete tramite DHCP, l'host name dovrebbe essere ricavato dal DNS. Se DHCP o DNS non sono configurati correttamente, l'host name "Unified Manager" viene assegnato automaticamente e associato al certificato di sicurezza.

Indipendentemente da come è stato assegnato l'host name, se cambi l'host name e intendi utilizzare il nuovo host name per accedere all'interfaccia utente web di Unified Manager, devi generare un nuovo certificato di sicurezza.

Se accedi all'interfaccia utente web utilizzando l'indirizzo IP del server anziché l'host name, non è necessario generare un nuovo certificato se modifichi l'host name. Tuttavia, è best practice aggiornare il certificato in modo che l'host name nel certificato corrisponda all'host name effettivo.

Se cambi l'host name in Unified Manager, devi aggiornare manualmente l'host name in OnCommand Workflow Automation (WFA). L'host name non viene aggiornato automaticamente in WFA.

Il nuovo certificato non entra in vigore finché la macchina virtuale Unified Manager non viene riavviata.

Passaggi

1. Genera un certificato di sicurezza HTTPS

   Se vuoi utilizzare il nuovo host name per accedere all'interfaccia utente web di Unified Manager, devi rigenerare il certificato HTTPS per associarlo al nuovo host name.

2. Riavvia la macchina virtuale di Unified Manager

   Dopo aver rigenerato il certificato HTTPS, devi riavviare la macchina virtuale Unified Manager.

Genera un certificato di sicurezza HTTPS in Active IQ Unified Manager

Quando installi Active IQ Unified Manager per la prima volta, viene installato un certificato HTTPS predefinito. Puoi generare un nuovo certificato di sicurezza HTTPS che sostituisce quello esistente.

Prima di iniziare

Devi avere il ruolo di Amministratore dell'applicazione.

Esistono diversi motivi per rigenerare il certificato, ad esempio per ottenere valori migliori per il Distinguished Name (DN), per avere una chiave di dimensioni maggiori, un periodo di scadenza più lungo o se il certificato corrente è scaduto.

Se non hai accesso all'interfaccia utente web di Unified Manager, puoi rigenerare il certificato HTTPS con gli stessi valori utilizzando la console di manutenzione. Durante la rigenerazione dei certificati, puoi definire la dimensione della chiave e la durata di validità della chiave. Se usi l' `Reset Server Certificate` opzione dalla console di manutenzione, viene creato un nuovo certificato HTTPS valido per 397 giorni. Questo certificato avrà una chiave RSA di 2048 bit.

Passaggi

1. Nel riquadro di navigazione a sinistra, fai clic su **Generale** > **Certificato HTTPS**.
2. Fai clic su **Rigenera certificato HTTPS**.

   Viene visualizzata la finestra di dialogo Rigenera certificato HTTPS.

3. Seleziona una delle seguenti opzioni a seconda di come vuoi generare il certificato:

Se vuoi…	Fai così…
Rigenera il certificato con i valori correnti	Fai clic sull'opzione **Rigenera utilizzando gli attributi del certificato corrente**.

Se vuoi…	Fai così…
Genera il certificato utilizzando valori diversi	Fai clic sull'opzione **Aggiorna gli attributi del certificato corrente**. I campi Common Name e Alternative Names useranno i valori del certificato esistente se non inserisci nuovi valori. Il campo "Common Name" deve essere impostato sul FQDN dell'host. Gli altri campi non richiedono valori, ma puoi inserirli, ad esempio, per EMAIL, COMPANY, DEPARTMENT, Città, Stato e Paese, se vuoi che questi valori vengano popolati nel certificato. Puoi anche selezionare tra i valori disponibili di KEY SIZE (l'algoritmo della chiave è "RSA".) e VALIDITY PERIOD. • 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. Sebbene sia consentito un periodo di validità di 36500 giorni, ti consigliamo di usare un periodo di validità non superiore a 397 giorni o 13 mesi. Questo perché, se selezioni un periodo di validità superiore a 397 giorni e prevedi di esportare un CSR per questo certificato e di farlo firmare da una CA nota, la validità del certificato firmato che la CA ti restituisce verrà ridotta a 397 giorni. • Puoi selezionare la casella di controllo "Escludi informazioni di identificazione locali (ad es. localhost)" se vuoi rimuovere le informazioni di identificazione locali dal campo Nomi alternativi del certificato. Quando questa casella di controllo è selezionata, nel campo Nomi alternativi viene usato solo ciò che inserisci nel campo. Se lasciato vuoto, il certificato risultante non avrà alcun campo Nomi alternativi.

4. Fai clic su **Sì** per rigenerare il certificato.

5. Riavvia il server Unified Manager affinché il nuovo certificato diventi effettivo.
6. Verifica le informazioni del nuovo certificato visualizzando il certificato HTTPS.

Riavvia la macchina virtuale Active IQ Unified Manager

Puoi riavviare la macchina virtuale dalla console di manutenzione di Unified Manager. Devi riavviare dopo aver generato un nuovo certificato di sicurezza o se si verifica un problema con la macchina virtuale.

Prima di iniziare

L'appliance virtuale è accesa.

Hai effettuato l'accesso alla console di manutenzione come utente di manutenzione.

Puoi anche riavviare la macchina virtuale da vSphere utilizzando l'opzione **Restart Guest**. Per ulteriori informazioni, consulta la documentazione VMware.

Passaggi

1. Accedi alla console di manutenzione.
2. Seleziona **Configurazione di sistema** > **Riavvia macchina virtuale**.

Cambia l'host name di Active IQ Unified Manager sui sistemi Linux

A un certo punto, potresti voler modificare l'host name della macchina Red Hat Enterprise Linux su cui hai installato Unified Manager. Ad esempio, potresti voler 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 elenchi le tue macchine Linux.

Prima di iniziare

Devi avere accesso come utente root al sistema Linux su cui è installato Unified Manager.

Puoi utilizzare l'host name (o l'indirizzo IP dell'host) per accedere all'interfaccia utente web di Unified Manager. Se durante la distribuzione hai configurato un indirizzo IP statico per la tua rete, avrai assegnato un nome all'host di rete. Se hai configurato la rete tramite DHCP, l'host name dovrebbe essere ricavato dal DNS server.

Indipendentemente da come è stato assegnato l'host name, se cambi l'host name e intendi utilizzare il nuovo host name per accedere all'interfaccia utente web di Unified Manager, devi generare un nuovo certificato di sicurezza.

Se accedi all'interfaccia web utilizzando l'indirizzo IP del server anziché l'host name, non devi generare un nuovo certificato se modifichi l'host name. Tuttavia, è best practice aggiornare il certificato, in modo che l'host name nel certificato corrisponda all'host name effettivo. Il nuovo certificato non ha effetto finché non riavvii la macchina Linux.

Se cambi l'host name in Unified Manager, devi aggiornare manualmente l'host name in OnCommand Workflow Automation (WFA). L'host name non viene aggiornato automaticamente in WFA.

Passaggi

1. Accedi come utente root al sistema Unified Manager che desideri modificare.
2. Arresta il software Unified Manager e il relativo software MySQL immettendo il seguente comando:

```
systemctl stop ocieau ocie mysqld
```

3. Modifica l'host name usando il comando Linux `hostnamectl`:

```
hostnamectl set-hostname new_FQDN
```

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

4. Rigenera il certificato HTTPS per il server:

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

5. Riavvia il servizio di rete:

```
systemctl restart NetworkManager.service
```

6. Dopo il riavvio del servizio, verifica se il nuovo host name riesce a eseguire un ping verso se stesso:

```
ping new_hostname
```

```
ping nuhost
```

Questo comando dovrebbe restituire lo stesso indirizzo IP impostato in precedenza per l'host name originale.

7. Dopo aver completato e verificato la modifica dell'host name, riavvia Unified Manager immettendo il seguente comando:

```
systemctl start mysqld ocie ocieau
```

Abilita e disabilita la gestione dello storage basata su policy in Active IQ Unified Manager

A partire da Unified Manager 9.7, puoi eseguire il provisioning dei carichi di lavoro dello storage (volumi e LUN) sui cluster ONTAP e gestire questi carichi di lavoro in base ai livelli di servizio delle prestazioni assegnati. Questa funzionalità è simile alla creazione di carichi di lavoro in ONTAP System Manager e all'associazione di policy QoS, ma se la applichi tramite Unified Manager puoi eseguire il provisioning e gestire i carichi di lavoro in tutti i cluster monitorati dalla tua istanza di Unified Manager.

Devi avere il ruolo di Amministratore dell'applicazione.

Questa opzione è abilitata per impostazione predefinita, ma puoi disabilitarla se non vuoi eseguire il provisioning e gestire i carichi di lavoro tramite Unified Manager.

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

Nuovi contenuti	Posizione
Una pagina per il provisioning di nuovi carichi di lavoro	Disponibile da **Attività comuni** > **Provisioning**

Nuovi contenuti	Posizione
Una pagina per creare policy dei livelli di servizio delle prestazioni	Disponibile in **Impostazioni** > **Policy** > **Livelli di servizio delle prestazioni**
Una pagina per creare criteri di efficienza dello storage per le prestazioni	Disponibile in **Impostazioni** > **Criteri** > **Efficienza di archiviazione**
Pannelli che descrivono le prestazioni correnti del workload e gli IOPS del workload	Disponibile dalla Dashboard

Per ulteriori informazioni su queste pagine e su questa funzionalità, consulta la guida online nel prodotto.

Passaggi

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

Se vuoi…	Poi fai così…
Disabilita la gestione dello storage basata su policy	Nel pannello **Gestione dello storage basata su policy**, sposta il cursore verso sinistra.
Abilita la gestione dello storage basata su policy	Nel pannello **Gestione dello storage basata su policy**, sposta il cursore verso destra.

Configura il backup di Active IQ Unified Manager

Puoi configurare la funzionalità di backup su Unified Manager attraverso una serie di passaggi di configurazione da eseguire sui sistemi host e tramite la console di manutenzione.

Per informazioni sulle fasi di configurazione, consulta "Gestione delle operazioni di backup e ripristino".

Gestisci le impostazioni delle funzionalità

Scopri le impostazioni delle funzionalità in Active IQ Unified Manager

La pagina Impostazioni delle funzionalità ti consente di abilitare e disabilitare funzionalità specifiche in Active IQ Unified Manager. Ciò include la creazione e la gestione di oggetti di storage in base a policy, l'abilitazione di API Gateway e Login Banner, il caricamento di script per la gestione degli avvisi, la chiusura di una sessione della Web UI in base al tempo di inattività e la disabilitazione della ricezione degli eventi della piattaforma Active IQ.

La pagina Impostazioni funzionalità è disponibile solo per gli utenti con il ruolo di Amministratore dell'applicazione.

Per informazioni su Scripts Upload, consulta "Abilitazione e disabilitazione del caricamento degli script".

Abilita la gestione dello storage basata su policy in Active IQ Unified Manager

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

Attivando questa funzionalità, puoi eseguire il provisioning dei carichi di lavoro di storage sui cluster ONTAP aggiunti alla tua istanza di Active IQ Unified Manager e gestire questi carichi di lavoro in base ai Performance Service Levels e alle Storage Efficiency Policies assegnati.

Puoi scegliere di attivare o disattivare questa funzione da **General** > **Feature Settings** > **Policy-based storage management**. Quando attivi questa funzione, le seguenti pagine sono disponibili per il funzionamento e il monitoraggio:

- Provisioning (provisioning dei carichi di lavoro di storage)
- **Politiche** > **Livelli di servizio delle prestazioni**
- **Politiche** > **Efficienza dello storage**
- Colonna Carichi di lavoro gestiti da Performance Service Level nella pagina Configurazione cluster
- Pannello Prestazioni del carico di lavoro nella **Dashboard**

Puoi utilizzare le schermate per creare livelli di servizio delle prestazioni e policy di efficienza dello storage, nonché per eseguire il provisioning dei carichi di lavoro di storage. Puoi anche monitorare i carichi di lavoro di storage conformi ai livelli di servizio delle prestazioni assegnati, oltre a quelli non conformi. Il pannello Prestazioni del carico di lavoro e IOPS del carico di lavoro ti consente anche di valutare la capacità e le prestazioni (IOPS) totali, disponibili e utilizzate dei cluster nel data center in base ai carichi di lavoro di storage di cui è stato eseguito il provisioning.

Dopo aver attivato questa funzionalità, puoi eseguire le API REST di Unified Manager per svolgere alcune di queste funzioni da **Menu Bar** > **Help button** > **API Documentation** > categoria **storage-provider**. In alternativa, puoi immettere l'host name o l'indirizzo IP e l'URL per accedere alla pagina dell'API REST nel formato https://<hostname>/docs/api/

Per ulteriori informazioni sulle API, vedi "Guida introduttiva alle API REST di Active IQ Unified Manager".

Scopri la funzionalità API Gateway in Active IQ Unified Manager

La funzionalità API Gateway consente ad Active IQ Unified Manager di fungere da unico pannello di controllo da cui puoi gestire più cluster ONTAP, senza dover accedere singolarmente a ciascuno di essi.

Puoi abilitare questa funzione dalle pagine di configurazione visualizzate quando accedi per la prima volta a Unified Manager. In alternativa, puoi abilitare o disabilitare questa funzione da **Generale** > **Impostazioni funzionalità** > **API Gateway**.

Le API REST di Unified Manager sono diverse dalle API REST di ONTAP e non tutte le funzionalità delle API REST di ONTAP sono disponibili usando le API REST di Unified Manager. Tuttavia, se hai un requisito di business specifico che richiede l'accesso alle API di ONTAP per gestire funzionalità specifiche non esposte in Unified Manager, puoi abilitare la funzionalità API Gateway ed eseguire le API di ONTAP. Il gateway funge da proxy per inoltrare tramite tunnel le richieste API mantenendo le richieste di intestazione e corpo nello stesso formato delle API di ONTAP. Puoi usare le credenziali di Unified Manager ed eseguire le API specifiche per accedere ai cluster ONTAP e gestirli senza dover fornire le credenziali dei singoli cluster. Unified Manager

funge da punto di gestione centralizzato per eseguire le API nei cluster ONTAP gestiti dalla tua istanza di Unified Manager. La risposta restituita dalle API è la stessa restituita dalle rispettive API REST di ONTAP eseguite direttamente da ONTAP.

Dopo aver abilitato questa funzionalità, puoi eseguire le API REST di Unified Manager da **Menu Bar** > **Help button** > **API Documentation** > categoria **gateway**. In alternativa, puoi immettere host name o indirizzo IP e l'URL per accedere alla pagina della REST API nel formato `https://<hostname>/docs/api/`

Per ulteriori informazioni sulle API, vedi "Guida introduttiva alle API REST di Active IQ Unified Manager".

Specifica il timeout di inattività in Active IQ Unified Manager

Puoi specificare il valore del timeout di inattività per Active IQ Unified Manager. Dopo il periodo di inattività specificato, l'applicazione esegue automaticamente il logout. Questa opzione è abilitata per impostazione predefinita.

Puoi disattivare questa funzione o modificarne il tempo da **Generale** > **Impostazioni funzione** > **Timeout di inattività**. Una volta attivata questa funzione, devi specificare il limite di tempo di inattività (in minuti) nel campo **DISCONNETTI DOPO**, trascorso il quale il sistema esegue automaticamente il logout. Il valore predefinito è 4320 minuti (72 ore).

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

Abilita gli eventi del portale Active IQ in Active IQ Unified Manager

Puoi specificare se vuoi abilitare o disabilitare gli eventi del portale Active IQ. Questa impostazione consente al portale Active IQ di rilevare e visualizzare eventi aggiuntivi sulla configurazione del sistema, il cablaggio e così via. Questa opzione è abilitata per impostazione predefinita.

Attivando questa funzionalità, Active IQ Unified Manager visualizza gli eventi rilevati dal portale Active IQ. Questi eventi vengono creati eseguendo una serie di regole sui 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 relativi alla configurazione del sistema, al cablaggio, alle best practice e ai problemi di disponibilità.

Puoi scegliere di attivare o disattivare questa funzionalità da **General** > **Feature Settings** > **Active IQ Portal Events**. Nei siti senza accesso alla rete esterna, devi caricare manualmente le regole da **Storage Management** > **Event Setup** > **Upload Rules**.

Questa funzione è abilitata per impostazione predefinita. Se disabiliti questa funzione, Active IQ non rileva né visualizza più gli eventi in Unified Manager. Quando è disabilitata, attivando questa funzione consenti a Unified Manager di ricevere gli eventi Active IQ su un cluster all'ora predefinita di 00:15 per il fuso orario di quel cluster.

Attiva e disattiva le impostazioni di sicurezza per la conformità in Active IQ Unified Manager

Utilizzando il pulsante **Customize** nel pannello **Security Dashboard** della pagina **Features Settings**, puoi abilitare o disabilitare i parametri di sicurezza per il monitoraggio

della conformità su Unified Manager.

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

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

I criteri di sicurezza per i tuoi cluster ONTAP, le VM di storage e i volumi vengono valutati in base alle raccomandazioni definite nel "Guida al rafforzamento della sicurezza per NetApp ONTAP 9". Il pannello Security nella dashboard e la pagina Security mostrano lo stato predefinito di conformità della sicurezza dei tuoi cluster, delle VM di storage e dei volumi. Il sistema genera inoltre eventi di sicurezza e abilita azioni di gestione per i cluster e le VM di storage che presentano violazioni della sicurezza.

Personalizza le impostazioni di sicurezza

Per personalizzare le impostazioni di monitoraggio della conformità in base al tuo ambiente ONTAP, segui questi passaggi:

Passaggi

1. Fai clic su **Generale > Impostazioni funzionalità > Dashboard di sicurezza > Personalizza**. Compare la finestra a comparsa **Personalizza le impostazioni del dashboard di sicurezza**.

   I parametri di conformità della sicurezza che abiliti o disabiliti possono influire direttamente sulle visualizzazioni di sicurezza predefinite, sui report e sui report pianificati nelle schermate Clusters e Storage VMs. Se avevi caricato un report excel da queste schermate prima di modificare i parametri di sicurezza, i report excel scaricati potrebbero essere errati.

2. Per abilitare o disabilitare le impostazioni personalizzate per i tuoi cluster ONTAP, seleziona l'impostazione generale desiderata in **Cluster**. Per informazioni sulle opzioni per personalizzare la conformità del cluster, consulta "Categorie di conformità del cluster".
3. Per abilitare o disabilitare le impostazioni personalizzate per le VM di storage, seleziona l'impostazione generale richiesta in **Storage VM**. Per informazioni sulle opzioni per personalizzare la conformità delle VM di storage, consulta "Categorie di conformità delle Storage VM".

Personalizza AutoSupport e le impostazioni di autenticazione

Nella sezione **AutoSupport Impostazioni**, puoi specificare se usare il trasporto HTTPS per inviare messaggi AutoSupport da ONTAP.

Dalla sezione **Impostazioni di autenticazione**, puoi abilitare la generazione di avvisi di Unified Manager per l'utente amministratore ONTAP predefinito.

Abilita e disabilita il caricamento degli script in Active IQ Unified Manager

La possibilità di caricare script su Unified Manager ed eseguirli è abilitata per impostazione predefinita. Se la tua organizzazione non desidera consentire questa attività per motivi di sicurezza, puoi disabilitare questa funzionalità.

Prima di iniziare

Devi avere il ruolo di Amministratore dell'applicazione.

Passaggi

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

Se vuoi…	Poi fai così…
Disabilita gli script	Nel pannello **Caricamento script**, sposta il cursore verso sinistra.
Abilita gli script	Nel pannello **Caricamento script**, sposta il cursore verso destra.

Aggiungi un banner di accesso in Active IQ Unified Manager

Aggiungendo un banner di accesso, la tua organizzazione può visualizzare informazioni come chi è autorizzato ad accedere al sistema e i termini e le condizioni d'uso durante l'accesso e il logout.

Qualsiasi utente, come gli operatori dello storage o gli amministratori, può visualizzare questo banner popup di accesso durante il login, il logout e il timeout della sessione.

Usa la console di manutenzione

Scopri la console di manutenzione in Active IQ Unified Manager

La console di manutenzione di Unified Manager ti consente di gestire le impostazioni del tuo sistema Unified Manager e di apportare le modifiche necessarie per evitare eventuali problemi.

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

- Risolvi eventuali problemi con la tua appliance virtuale, soprattutto se l'interfaccia web di Unified Manager non è disponibile
- Esegui l'aggiornamento a versioni più recenti di Unified Manager
- Genera pacchetti di supporto da inviare al supporto tecnico
- Configura le impostazioni di rete
- Cambia la password dell'utente di manutenzione
- Connettiti a un provider di dati esterno per inviare statistiche sulle performance
- Modifica l'impostazione interna della raccolta dei dati sulle prestazioni
- Ripristina il database e le impostazioni di configurazione di Unified Manager da una versione di backup salvata in precedenza.

Scopri l'utente di manutenzione in Active IQ Unified Manager

L'utente di manutenzione viene creato durante l'installazione di Unified Manager su un sistema Red Hat Enterprise Linux. Il nome dell'utente di manutenzione è "umadmin". L'utente di manutenzione ha il ruolo di Application Administrator nell'interfaccia utente web e può creare altri utenti e assegnare loro ruoli.

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

Funzionalità utente di diagnostica in Active IQ Unified Manager

Lo scopo dell'accesso diagnostico è consentire al supporto tecnico di assisterti nella risoluzione dei problemi e dovresti usarlo solo quando te lo indica il supporto tecnico.

L'utente con privilegi di diagnostica può eseguire comandi a livello di sistema operativo su indicazione del supporto tecnico, per la risoluzione dei problemi.

Accedi alla console di manutenzione in Active IQ Unified Manager

Se l'interfaccia utente di Unified Manager non è operativa, o se devi eseguire funzioni non disponibili nell'interfaccia utente, puoi accedere alla console di manutenzione per gestire il tuo sistema Unified Manager.

Prima di iniziare

Devi aver installato e configurato Unified Manager.

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

Se è installato su VMware, se hai già effettuato l'accesso come utente di manutenzione tramite la console VMware, non puoi accedere contemporaneamente usando Secure Shell.

Passaggio

1. Segui questi passaggi per accedere alla console di manutenzione:

Su questo sistema operativo…	Segui questi passaggi…
VMware	a. Usando Secure Shell, connettiti all'indirizzo IP o al fully qualified domain name dell'appliance virtuale di Unified Manager. b. Accedi alla console di manutenzione utilizzando il tuo nome utente e la password di manutenzione.

Su questo sistema operativo…	Segui questi passaggi…
Linux	a. Usando Secure Shell, connettiti all'indirizzo IP o al fully qualified domain del sistema Unified Manager. b. Accedi al sistema con il nome utente e la password dell'utente di manutenzione (umadmin). c. Inserisci il comando `maintenance_console` e premi Invio.
Windows	a. Accedi al sistema Unified Manager con le credenziali di amministratore. b. Avvia PowerShell come amministratore di Windows. c. Inserisci il comando `maintenance_console` e premi Invio.

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

Accedi alla console di manutenzione usando la console VM vSphere in Active IQ Unified Manager

Se l'interfaccia utente di Unified Manager non è operativa, oppure se devi eseguire funzioni non disponibili nell'interfaccia utente, puoi accedere alla console di manutenzione per riconfigurare la tua appliance virtuale.

Prima di iniziare

- Devi essere l'utente di manutenzione.
- L'appliance virtuale deve essere accesa per accedere alla console di manutenzione.

Passaggi

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

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

Menu della console di manutenzione

Scopri i menu della console di manutenzione in Active IQ Unified Manager

La console di manutenzione è composta da diversi menu che ti consentono di eseguire la manutenzione e gestire le funzionalità speciali e le impostazioni di configurazione del server Unified Manager.

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

- Aggiorna Unified Manager (solo per VMware)
- Configurazione di rete (solo VMware)
- Configurazione del sistema (solo VMware)
  a. Supporto/Diagnostica
  b. Reimposta il certificato del server
  c. Rigenera il certificato client
  d. Backup e ripristino
  e. Fornitore di dati esterno
  f. Configurazione dell'intervallo di polling delle prestazioni
  g. Disabilita l'autenticazione SAML
  h. Visualizza/Modifica le porte dell'applicazione
  i. Configurazione del log di debug
  j. Controlla l'accesso alla porta MySQL 3306
  k. Esci

Selezioni il numero dall'elenco per accedere alla specifica opzione di menu. Ad esempio, per backup e ripristino, selezioni *4*.

Menu Configurazione rete in Active IQ Unified Manager

Il menu Configurazione di rete ti consente di gestire le impostazioni di rete. Dovresti usare 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 o su Microsoft Windows.

Sono disponibili le seguenti opzioni di menu.

- **Visualizza le impostazioni dell'indirizzo IP**

  Visualizza le impostazioni di rete correnti per l'appliance virtuale, inclusi l'indirizzo IP, la rete, l'indirizzo di broadcast, la netmask, il gateway e i server DNS.

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

  Ti consente di modificare qualsiasi impostazione di rete dell'appliance virtuale, inclusi l'indirizzo IP, la subnet mask, il gateway o i server DNS. Se passi dalle impostazioni di rete DHCP alla rete statica usando la console di manutenzione, non puoi modificare il host name. Devi selezionare **Applica modifiche** perché le modifiche abbiano effetto.

- **Visualizza le impostazioni di ricerca del domain name**

  Visualizza l'elenco di ricerca del domain name utilizzato per la risoluzione degli host name.

- **Modifica le impostazioni di ricerca del domain name**

  Ti consente di modificare i domain name in cui vuoi cercare durante la risoluzione dei host name. Devi selezionare **Commit Changes** perché le modifiche abbiano effetto.

- **Visualizza route statiche**

  Visualizza i percorsi di rete statici correnti.

- **Modifica route statiche**

  Ti consente di aggiungere o eliminare percorsi di rete statici. Devi selezionare **Commit Changes** affinché le modifiche abbiano effetto.

  - **Aggiungi route**

    Ti consente di aggiungere una route statica.

  - **Elimina route**

    Ti consente di eliminare una rotta statica.

  - **Indietro**

    Ti riporta al **menu principale**.

  - **Uscita**

    Esci dalla console di manutenzione.

- **Disabilita l'interfaccia di rete**

  Disabilita tutte le interfacce di rete disponibili. Se è disponibile una sola interfaccia di rete, non puoi disabilitarla. Devi selezionare **Applica modifiche** perché le modifiche abbiano effetto.

- **Abilita l'interfaccia di rete**

  Abilita le interfacce di rete disponibili. Devi selezionare **Applica modifiche** affinché le modifiche abbiano effetto.

- **Conferma le modifiche**

  Applica tutte le modifiche apportate alle impostazioni di rete per l'appliance virtuale. Devi selezionare questa opzione affinché le modifiche abbiano effetto, altrimenti non verranno applicate.

- **Esegui il ping di un host**

  Esegue un ping verso un host di destinazione per confermare le modifiche all'indirizzo IP o alle configurazioni DNS.

- **Ripristina le impostazioni predefinite**

  Ripristina tutte le impostazioni ai valori predefiniti di fabbrica. Devi selezionare **Applica modifiche** affinché le modifiche abbiano effetto.

- **Indietro**

  Ti riporta al **menu principale**.

- **Uscita**

Esci dalla console di manutenzione.

Usa il menu Configurazione di sistema in Active IQ Unified Manager

Il menu System Configuration ti consente di gestire l'appliance virtuale offrendo diverse opzioni, come visualizzare lo stato del server, riavviare e spegnere la 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".

Sono disponibili le seguenti opzioni di menu:

- **Visualizza lo stato del server**

  Visualizza lo stato attuale del server. Le opzioni di stato includono In esecuzione e Non in esecuzione.

  Se il server non è in esecuzione, potresti dover contattare il supporto tecnico.

- **Riavvia la macchina virtuale**

  Riavvia la macchina virtuale, arrestando tutti i servizi. Dopo il riavvio, la macchina virtuale e i servizi si riavviano.

- **Arresta la macchina virtuale**

  Arresta la macchina virtuale, interrompendo tutti i servizi.

  Puoi selezionare questa opzione solo dalla console della macchina virtuale.

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

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

- **Aumenta le dimensioni del disco dati**

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

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

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

- **Cambia fuso orario**

  Modifica il fuso orario in base alla tua posizione.

- **Modifica il server NTP**

  Modifica le impostazioni del server NTP, come l'indirizzo IP o il fully qualified domain name (FQDN).

- **Modifica servizio NTP**

  Passa tra i servizi `ntp` e `systemd-timesyncd`.

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

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

- **Ripristina il certificato del server**

  Reimposta il certificato di sicurezza del server.

- **Modifica l'host name**

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

- **Indietro**

  Esce dal menu Configurazione di sistema e torna al menu principale.

- **Uscita**

  Esce dal menu della console di manutenzione.

Usa il menu Supporto e diagnostica in Active IQ Unified Manager

Il menu Supporto e diagnostica ti consente di generare un pacchetto di supporto che puoi inviare al supporto tecnico per ottenere aiuto nella risoluzione dei problemi.

Sono disponibili le seguenti opzioni di menu:

- **Genera il Light Support Bundle**

  Ti consente di creare un pacchetto di supporto leggero che contiene solo 30 giorni di log e record del database di configurazione — esclude i dati sulle prestazioni, i file di registrazione dell'acquisizione e il dump dell'heap del server.

- **Genera bundle di supporto**

  Ti consente di creare un pacchetto di supporto completo (file 7-Zip) contenente informazioni diagnostiche nella home directory dell'utente diagnostico. Se il tuo sistema è connesso a Internet, puoi anche caricare il pacchetto di supporto su NetApp.

  Il file include informazioni generate da un messaggio AutoSupport, il contenuto del database di Unified Manager, dati dettagliati sugli elementi interni del server di Unified Manager e log di livello verboso che normalmente non sono inclusi nei messaggi AutoSupport o nel pacchetto di supporto semplificato.

Scopri le opzioni aggiuntive del menu della console di manutenzione in Active IQ Unified Manager

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

Sono disponibili le seguenti opzioni di menu:

- **Ripristina il certificato del server**

  Rigenera il certificato del server HTTPS.

  Puoi rigenerare il certificato del server nella GUI di Unified Manager facendo clic su **General** > **HTTPS Certificates** > **Regenerate HTTPS Certificate**.

- **Disabilita l'autenticazione SAML**

  Disabilita 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 in genere utilizzata quando un problema con il server IdP o con la configurazione SAML impedisce agli utenti di accedere alla GUI di Unified Manager.

- **Fornitore di dati esterno**

  Offre opzioni per connettere Unified Manager a un provider di dati esterno. Dopo aver stabilito la connessione, i dati sulle prestazioni vengono inviati a un server esterno in modo che gli esperti di performance dello storage possano creare grafici delle metriche utilizzando software di terze parti. Vengono visualizzate le seguenti opzioni:

  - **Visualizza configurazione server**--Visualizza le impostazioni di connessione e configurazione correnti per un provider di dati esterno.
  - **Aggiungi / Modifica connessione al server**--Consente di inserire nuove impostazioni di connessione per un provider di dati esterno o modificare le impostazioni esistenti.
  - **Modifica configurazione server**--Consente di immettere nuove impostazioni di configurazione per un provider di dati esterno o di modificare le impostazioni esistenti.
  - **Elimina connessione al server**--Elimina la connessione a un provider di dati esterno.

    Dopo l'eliminazione della connessione, Unified Manager perde la connessione al server esterno.

- **Ripristino del backup**

  Per ulteriori informazioni, consulta gli argomenti in "Gestione delle operazioni di backup e ripristino".

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

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

  Se riscontri che la raccolta di dati da cluster di grandi dimensioni non si completa in tempo, puoi modificare questo intervallo impostandolo su 10 o 15 minuti.

- **Visualizza/Modifica le porte dell'applicazione**

  Consente di 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 3306 di MySQL**

  Controlla l'accesso host alla porta MySQL predefinita 3306. Per motivi di sicurezza, l'accesso tramite questa porta è limitato al solo localhost durante una nuova installazione di Unified Manager su sistemi Linux, Windows e VMware vSphere. Questa opzione ti consente di modificare la visibilità di questa porta tra localhost e host remoti, cioè, se nel tuo ambiente è abilitata solo per localhost, puoi rendere questa porta disponibile anche per gli host remoti. In alternativa, quando è abilitata per tutti gli host, puoi limitare l'accesso a questa porta al solo localhost. Se in precedenza l'accesso era abilitato sugli host remoti, la configurazione viene mantenuta in uno scenario di aggiornamento. Dopo aver modificato la visibilità della porta, dovresti controllare le impostazioni del firewall sui sistemi Windows e disabilitarle se sono configurate per limitare l'accesso alla porta MySQL 3306.

- **Uscita**

Esce dal menu della console di manutenzione.

Cambia la password dell'utente di manutenzione su Windows in Active IQ Unified Manager

Puoi modificare la password dell'utente di manutenzione di Unified Manager quando necessario.

Passaggi

1. Dalla pagina di accesso dell'interfaccia utente web di Unified Manager, fai clic su **Forgot Password**.

   Viene visualizzata una pagina che ti chiede di inserire il nome dell'utente di cui vuoi reimpostare la password.

2. Inserisci il nome utente e fai clic su **Invia**.

   Un'email con un link per reimpostare la password viene inviata all'indirizzo email definito per quel nome utente.

3. Fai clic sul link **per reimpostare la password** nell'email e definisci la nuova password.
4. Torna all'interfaccia web e accedi a Unified Manager usando la nuova password.

Cambia la password umadmin di Active IQ Unified Manager sui sistemi Linux

Per motivi di sicurezza, devi modificare la password predefinita dell'utente umadmin di Unified Manager immediatamente dopo aver completato il processo di installazione. Se necessario, puoi modificare nuovamente la password in qualsiasi momento.

Prima di iniziare

- Unified Manager deve essere installato su un sistema Red Hat Enterprise Linux Linux.
- Devi disporre delle credenziali dell'utente root per il sistema Linux su cui è installato Unified Manager.

Passaggi

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

   ```
   passwd umadmin
   ```

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

Modifica le porte che Active IQ Unified Manager usa 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.

Prima di iniziare

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

Alcune porte sono considerate non sicure quando utilizzi i browser Mozilla Firefox o Google Chrome. Verifica con il tuo 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 l'assistenza clienti per risolvere il problema.

L'istanza di Unified Manager si riavvia automaticamente dopo aver modificato la porta, quindi assicurati che sia il momento opportuno per arrestare il sistema per un breve periodo di tempo.

1. Accedi all'host di Unified Manager tramite SSH utilizzando l'utente di manutenzione.

   Vedi i prompt della console di manutenzione di Unified Manager.

2. Digita il numero dell'opzione del menu denominata **Visualizza/Modifica porte dell'applicazione**, quindi premi Invio.
3. Se richiesto, inserisci di nuovo la password dell'utente di manutenzione.
4. Digita i nuovi numeri di porta per le porte HTTP e HTTPS, quindi premi Invio.

   Se lasci vuoto il numero di porta, viene assegnata la porta predefinita per il protocollo.

   Ti viene chiesto se vuoi modificare le porte e riavviare Unified Manager ora.

5. Digita **y** per cambiare le porte e riavviare Unified Manager.
6. Esci 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.

Aggiungi interfacce di rete ad Active IQ Unified Manager

Puoi aggiungere nuove interfacce di rete se devi separare il traffico di rete.

Prima di iniziare

Devi aver aggiunto l'interfaccia di rete all'appliance virtuale usando vSphere.

L'appliance virtuale deve essere accesa.

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

Passaggi

1. Nel menu principale della console vSphere, seleziona **Configurazione di sistema** > **Riavvia il sistema operativo**.

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

2. Accedi alla console di manutenzione.
3. Seleziona **Configurazione di rete** > **Abilita interfaccia di rete**.
4. Seleziona la nuova interfaccia di rete e premi **Invio**.

   Seleziona **eth1** e premi **Invio**.

5. Digita **y** per abilitare l'interfaccia di rete.
6. Inserisci le impostazioni di rete.

   Ti viene richiesto di inserire le impostazioni di rete se utilizzi un'interfaccia statica o se il DHCP non viene rilevato.

   Dopo aver inserito le impostazioni di rete, torni automaticamente al menu **Configurazione di rete**.

7. Seleziona **Commit Changes**.

   Devi eseguire il commit delle modifiche per aggiungere l'interfaccia di rete.

Rigenera il certificato client in Active IQ Unified Manager

Puoi usare la console di manutenzione per rigenerare il certificato client di Unified Manager. Il tuo certificato ha un periodo di validità esteso di cinque anni.

Passaggi

1. Accedi come utente di manutenzione.
2. Seleziona **Rigenera certificato client** e premi **Invio**.
3. Se il sistema richiede l'autenticazione, inserisci le credenziali richieste.
4. Seleziona **Confirm Regeneration** e premi **Enter**.
5. Dopo aver rigenerato il certificato, riavvia il servizio Unified Manager per applicare le modifiche.
6. Per verificare il certificato aggiornato accedi a ONTAP. Visualizza lo stato del certificato client e il suo stato di validità.

Informazioni correlate "Gestisci i certificati ONTAP con System Manager"

Aggiungi spazio su disco

Aggiungi spazio su disco alla directory del database di Active IQ Unified Manager

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

Ad esempio, la directory del database potrebbe riempirsi se Unified Manager sta raccogliendo dati da un numero elevato di cluster, ciascuno con molti nodi. Riceverai un evento di avviso quando la directory del database è piena al 90% e un evento critico quando la directory è piena al 95%.

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

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

Aggiungi spazio alla directory dei dati su un host Linux in Active IQ Unified Manager

Se inizialmente hai assegnato uno spazio su disco insufficiente alla `/opt/netapp/data` directory per supportare Unified Manager quando hai configurato l'host Linux e poi

installato Unified Manager, puoi aggiungere spazio su disco dopo l'installazione aumentandolo nella `/opt/netapp/data` directory.

Prima di iniziare

Devi avere accesso come utente root alla macchina Red Hat Enterprise Linux su cui è installato Unified Manager.

Ti consigliamo di eseguire un backup del database di Unified Manager prima di aumentare le dimensioni della directory dei dati.

Passaggi

1. Accedi come utente root alla macchina Linux sulla quale vuoi aggiungere spazio su disco.
2. Arresta il servizio Unified Manager e il software MySQL associato nell'ordine indicato:

   ```
   systemctl stop ocieau ocie mysqld
   ```

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

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

5. Se SE Linux è abilitato:

   a. Ottieni il tipo SE Linux per le cartelle sulla cartella `/opt/netapp/data` esistente:

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

      Il sistema restituisce una conferma simile alla seguente:

   ```
   echo $se_type
   mysqld_db_t
   ```

   a. Esegui il comando chcon per impostare il tipo SE Linux per la directory di backup:

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

6. Elimina il contenuto della `/opt/netapp/data` directory:

   a. `cd /opt/netapp/data`

   b. `rm -rf *`

7. Espandi le dimensioni della `/opt/netapp/data` directory fino a un minimo di 150 GB tramite i comandi LVM o aggiungendo dischi aggiuntivi.

   Se hai creato `/opt/netapp/data` da un disco, non dovresti provare a montarlo `/opt/netapp/data` come NFS o CIFS share. Questo perché, in questo caso, se provi a espandere lo spazio su disco, alcuni comandi LVM, come `resize` e `extend`, potrebbero

non funzionare come previsto.

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

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

   Il sistema restituisce una conferma simile alla seguente:

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

9. Se SE Linux è abilitato, verifica che il contesto della directory `/opt/netapp/data`sia ancora impostato su mysqld_db_t:

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

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

      Il sistema restituisce una conferma simile alla seguente:

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

10. Elimina il file abc in modo che questo file superfluo non causi un errore del database in futuro.
11. Copia il contenuto da backup-data nella directory `/opt/netapp/data` espansa:

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

12. Se SE Linux è abilitato, esegui il seguente comando:

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

13. Avvia il servizio MySQL:

    ```
    systemctl start mysqld
    ```

14. Dopo l'avvio del servizio MySQL, avvia i servizi ocie e ocieau nell'ordine indicato:

    ```
    systemctl start ocie ocieau
    ```

15. Dopo aver avviato tutti i servizi, elimina la cartella di backup `/backup-data`:

    ```
    rm -rf /backup-data
    ```

Aggiungi spazio al disco dati di una macchina virtuale VMware in Active IQ Unified Manager

Se devi aumentare la quantità di spazio sul disco dati per il database di Unified Manager, puoi aggiungere capacità dopo l'installazione aumentando lo spazio su disco tramite la console di manutenzione di Unified Manager.

Prima di iniziare

- Devi avere accesso al vSphere Client.
- La macchina virtuale non deve avere snapshot memorizzati localmente.
- Devi disporre delle credenziali dell'utente di manutenzione.

Ti consigliamo di eseguire un backup della macchina virtuale prima di aumentare le dimensioni dei dischi virtuali.

Passaggi

1. Nel client vSphere, seleziona la macchina virtuale Unified Manager, quindi aggiungi ulteriore capacità del disco ai dati `disk 3`. Per i dettagli, consulta la documentazione VMware.

   In alcuni rari casi, la distribuzione di Unified Manager utilizza "Hard Disk 2" per il disco dati invece di "Hard Disk 3". Se questo si è verificato nella tua distribuzione, aumenta lo spazio del disco più grande. Il disco dati avrà sempre più spazio dell'altro disco.

2. Nel client vSphere, seleziona la macchina virtuale Unified Manager, quindi seleziona la scheda **Console**.
3. Fai clic nella finestra della console, quindi accedi alla console di manutenzione utilizzando il tuo nome utente e la password.
4. Nel menu principale, immetti il numero corrispondente all'opzione **Configurazione di sistema**.
5. Nel menu Configurazione di sistema, inserisci il numero dell'opzione **Aumenta dimensione disco dati**.

Aggiungi spazio all'unità logica su un server Windows in Active IQ Unified Manager

Se devi aumentare lo spazio su disco per il database di Unified Manager, puoi aggiungere capacità all'unità logica su cui è installato Unified Manager.

Prima di iniziare

Devi disporre dei privilegi di amministratore di Windows.

Ti consigliamo di eseguire un backup del database di Unified Manager prima di aggiungere spazio su disco.

Passaggi

1. Accedi come amministratore al server Windows sul quale desideri aggiungere spazio su disco.
2. Segui il passaggio corrispondente al metodo che vuoi utilizzare per aggiungere ulteriore spazio:

Opzione	Descrizione
Su un server fisico, aggiungi capacità all'unità logica su cui è installato il server Unified Manager.	Segui i passaggi descritti nell'argomento Microsoft: "Estendere un volume di base"
Su un server fisico, aggiungi un disco rigido.	Segui i passaggi descritti nell'argomento Microsoft: "Aggiunta di dischi rigidi"
Su una macchina virtuale, aumenta le dimensioni di una partizione del disco.	Segui i passaggi descritti nell'argomento relativo a VMware: "Aumentare le dimensioni di una partizione del disco"

Gestisci l’accesso degli utenti

Aggiungi utenti

Aggiungi utenti in Active IQ Unified Manager

Puoi aggiungere utenti locali o utenti del database utilizzando la pagina Utenti. Puoi anche aggiungere utenti remoti o gruppi che appartengono a un server di autenticazione. Puoi assegnare ruoli a questi utenti e, in base ai privilegi dei ruoli, gli utenti possono gestire gli oggetti di storage e i dati con Unified Manager oppure visualizzare i dati in un database.

Prima di iniziare

- Devi avere il ruolo di Amministratore dell’applicazione.
- Per aggiungere un utente o un gruppo remoto, devi aver abilitato l’autenticazione remota e configurato il server di autenticazione.
- Se intendi configurare l’autenticazione SAML in modo che un provider di identità (IdP) autentichi gli utenti che accedono all’interfaccia grafica, assicurati che questi utenti siano definiti come utenti “remote”.

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

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

Passaggi

1. Nel riquadro di navigazione a sinistra, fai clic su **Generale** > **Utenti**.
2. Nella pagina Utenti, fai clic su **Aggiungi**.
3. Nella finestra di dialogo Aggiungi utente, seleziona il tipo di utente che desideri aggiungere e inserisci le informazioni richieste.

   Quando inserisci le informazioni utente richieste, devi specificare un indirizzo email univoco per quell’utente. Devi evitare di specificare indirizzi email condivisi da più utenti.

4. Fai clic su **Add**.

Crea un utente database in Active IQ Unified Manager

Per supportare una connessione tra Workflow Automation e Unified Manager, o per accedere alle viste del database, devi prima creare un utente del database con il ruolo Integration Schema o Report Schema nell’interfaccia web di Unified Manager.

Prima di iniziare

Devi avere il ruolo di Amministratore dell’applicazione.

Gli utenti del database consentono l’integrazione con Workflow Automation e l’accesso alle viste del database specifiche per i report. Gli utenti del database non hanno accesso all’interfaccia utente web di Unified Manager né alla console di manutenzione e non possono eseguire chiamate API.

Passaggi

1. Nel riquadro di navigazione a sinistra, fai clic su **Generale** > **Utenti**.
2. Nella pagina Utenti, fai clic su **Aggiungi**.
3. Nella finestra di dialogo Aggiungi utente, seleziona **Utente database** nell'elenco a discesa **Tipo**.
4. Inserisci un nome e una password per l'utente del database.
5. Nel menu a discesa **Ruolo**, seleziona il ruolo appropriato.

Se sei…	Scegli questo ruolo
Collegamento di Unified Manager con Workflow Automation	Schema di integrazione
Accesso ai report e ad altre viste del database	Schema di report

6. Fai clic su **Add**.

Modifica le impostazioni utente in Active IQ Unified Manager

Puoi modificare le impostazioni utente, come l'indirizzo e-mail e il ruolo, specificate per ciascun utente. Ad esempio, potresti voler modificare il ruolo di un utente che è un operatore dello storage e assegnargli i privilegi di amministratore dello storage.

Prima di iniziare

Devi avere il ruolo di Amministratore dell'applicazione.

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

- Esci e accedi nuovamente a Unified Manager.
- Hai raggiunto il timeout della sessione di 24 ore.

Passaggi

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

Visualizza gli utenti in Active IQ Unified Manager

Puoi usare la pagina Utenti per visualizzare l'elenco degli utenti che gestiscono oggetti di storage e dati usando Unified Manager. Puoi visualizzare i dettagli degli utenti, come il nome utente, il tipo di utente, l'indirizzo e-mail e il ruolo assegnato agli utenti.

Prima di iniziare

Devi avere il ruolo di Amministratore dell'applicazione.

Passaggio

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

Elimina utenti o gruppi in Active IQ Unified Manager

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

Prima di iniziare

- Quando elimini i gruppi remoti, devi aver riassegnato gli eventi assegnati agli utenti di tali gruppi.

  Se elimini utenti locali o utenti remoti, gli eventi assegnati a questi utenti vengono automaticamente disassegnati.

- Devi avere il ruolo di Amministratore dell'applicazione.

Passaggi

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

Scopri il controllo degli accessi in base al ruolo in Active IQ Unified Manager

RBAC (in base al ruolo, role-based access control) offre la possibilità di controllare chi ha accesso a varie funzionalità e risorse nel server Active IQ Unified Manager. RBAC permette agli amministratori di gestire gruppi di utenti definendo i ruoli. Se hai bisogno di limitare l'accesso a specifiche funzionalità per determinati amministratori, devi creare account amministratore per loro. Se vuoi limitare le informazioni che gli amministratori possono visualizzare e le operazioni che possono eseguire, devi applicare ruoli agli account amministratore che crei.

Il server di gestione utilizza il controllo degli accessi basato sui ruoli (RBAC) per l'accesso utente e le autorizzazioni del ruolo. Se non hai modificato le impostazioni predefinite del server di gestione per l'accesso dell'utente amministrativo, non devi accedere per visualizzarle.

Quando avvii un'operazione che richiede privilegi specifici, il server di gestione ti chiede di accedere. Ad esempio, per creare account amministratore, devi accedere con un account con accesso Application Administrator.

Scopri le tipologie di utente in Active IQ Unified Manager

Un tipo di utente specifica il tipo di account dell'utente e include utenti remoti, gruppi remoti, utenti locali, utenti del database e utenti della manutenzione. Ognuno di questi tipi ha un proprio ruolo, che viene assegnato da un utente con il ruolo di Administrator.

Le tipologie di utente di Unified Manager sono le seguenti:

- **Utente di manutenzione**

  Creato durante la configurazione iniziale di Unified Manager. L'utente addetto alla manutenzione crea quindi altri utenti e assegna loro i ruoli. L'utente addetto alla manutenzione è anche l'unico utente con accesso alla console di manutenzione. Quando Unified Manager viene installato su un sistema Red Hat

Enterprise Linux, all'utente addetto alla manutenzione viene assegnato il nome utente "umadmin."

- **Utente locale**

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

- **Gruppo remoto**

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

- **Utente remoto**

  Accede all'interfaccia utente di Unified Manager utilizzando le credenziali memorizzate sul 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 Application Administrator.

- **Utente del database**

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

Scopri i ruoli utente in Active IQ Unified Manager

L'utente di manutenzione o l'Application Administrator assegna un ruolo a ogni utente. Ogni ruolo contiene determinati privilegi. L'ambito delle attività che puoi svolgere in Unified Manager dipende dal ruolo che ti è stato assegnato e dai privilegi che tale ruolo contiene.

Unified Manager include i seguenti ruoli utente predefiniti:

- **Operatore**

  Visualizza le informazioni del sistema storage e altri dati raccolti da Unified Manager, inclusi lo storico e l'andamento della capacità. Questo ruolo consente all'operatore storage di visualizzare, assegnare, confermare, risolvere e aggiungere note agli eventi.

- **Amministratore dello storage**

  Configura le operazioni di gestione dello storage all'interno di 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, rete e AutoSupport.

  Quando Unified Manager viene installato su sistemi Linux, all'utente iniziale con il ruolo di

Amministratore dell'applicazione viene assegnato automaticamente il nome "umadmin".

- **Schema di integrazione**

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

- **Schema del report**

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

  - netapp_model_view
  - netapp_performance
  - ocum
  - ocum_report
  - ocum_report_birt
  - opm
  - scalemonitor

Scopri i ruoli e le funzionalità degli utenti in Active IQ Unified Manager

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

La tabella seguente mostra le funzioni che ciascun ruolo utente può svolgere:

Funzione	Operatore	Amministratore dello storage	Amministratore dell'applicazione	Schema di integrazione	Schema di report
Visualizza le informazioni del sistema storage	•	•	•	•	•
Visualizza altri dati, come cronologie e andamenti della capacità	•	•	•	•	•
Visualizza, assegna e risolvi gli eventi	•	•	•		
Visualizza gli oggetti del servizio storage, come le associazioni SVM e i pool di risorse	•	•	•		

Funzione	Operatore	Amministratore dello storage	Amministratore dell'applicazione	Schema di integrazione	Schema di report
Visualizza le politiche relative alle soglie	•	•	•		
Gestisci gli oggetti del servizio storage, come le associazioni SVM e i pool di risorse		•	•		
Definisci gli avvisi		•	•		
Gestisci le opzioni di gestione dello storage		•	•		
Gestisci le policy di gestione dello storage		•	•		
Gestisci utenti			•		
Gestisci le opzioni amministrative			•		
Definire le politiche di soglia			•		
Gestisci l'accesso al database			•		
Gestisci l'integrazione con WFA e fornisci l'accesso alle viste del database				•	
Pianifica e salva i report		•	•		
Esegui le operazioni "Fix It" da Management Actions		•	•		
Fornisci accesso in sola lettura alle viste del database					•

Gestisci le impostazioni di autenticazione SAML

Abilita l'autenticazione SAML in Active IQ Unified Manager

Dopo aver configurato le impostazioni di autenticazione remota, puoi abilitare l'autenticazione SAML (Security Assertion Markup Language) in modo che gli utenti remoti siano autenticati da un provider di identità (IdP) sicuro prima di poter accedere all'interfaccia utente web di Unified Manager.

Tieni presente che, dopo aver abilitato l'autenticazione SAML, solo gli utenti remoti avranno accesso all'interfaccia utente grafica di Unified Manager. Gli utenti locali e gli utenti Maintenance non potranno accedere alla UI. Questa configurazione non ha alcun impatto sugli utenti che accedono alla console di manutenzione.

Usa un provider di identità in Active IQ Unified Manager

Quando configuri Unified Manager per utilizzare un provider di identità (IdP) per eseguire l'autenticazione SAML per tutti gli utenti remoti, devi tenere presenti alcune impostazioni di configurazione obbligatorie affinché la connessione a Unified Manager abbia esito positivo.

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

Standard di crittografia supportati

- Advanced Encryption Standard (AES): AES-128 e AES-256
- Algoritmo di hash sicuro (SHA): SHA-1 e SHA-256

Fornitori di identità validati

- Shibboleth
- Active Directory Federation Services (ADFS)

Requisiti di configurazione di ADFS

- Devi definire tre regole di attestazione nel seguente ordine, necessarie affinché Unified Manager possa analizzare le risposte SAML di ADFS per questa voce di trust della relying party.

Regola attestazioni	Valore
SAM-account-name	ID nome
SAM-account-name	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

- Devi impostare il metodo di autenticazione su "Forms Authentication", altrimenti gli utenti potrebbero ricevere un errore quando escono da Unified Manager. Segui questi passaggi:
  a. Apri la console di gestione ADFS.

b. Fai clic sulla cartella Criteri di autenticazione nella visualizzazione ad albero a sinistra.

c. In Azioni sulla destra, fai clic su Modifica criterio di autenticazione primaria globale.

d. Imposta il metodo di autenticazione Intranet su “Forms Authentication” invece dell’impostazione predefinita “Windows Authentication”.

- In alcuni casi l’accesso tramite l’IdP viene rifiutato quando il certificato di sicurezza di Unified Manager è firmato da una CA. Esistono due soluzioni alternative per risolvere questo problema:
  - Segui le istruzioni indicate nel link per disabilitare il controllo di revoca sul server ADFS per la relying party associata al certificato CA nella catena:

    "Disabilita il controllo della revoca per Relying Party Trust"

  - Assicurati che il server CA risieda all’interno del server ADFS per firmare la richiesta di certificato del server Unified Manager.

Altri requisiti di configurazione

- Lo scostamento dell’orologio di Unified Manager è impostato su 5 minuti, quindi la differenza di orario tra il server IdP e il server Unified Manager non può essere superiore a 5 minuti, altrimenti l’autenticazione non riuscirà.

Abilita l’autenticazione SAML in Active IQ Unified Manager

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

Prima di iniziare

- Devi aver configurato l’autenticazione remota e aver verificato che sia andata a buon fine.
- Devi aver creato almeno un Remote User o un Remote Group con il ruolo di Application Administrator.
- Il provider di identità (IdP) deve essere supportato da Unified Manager e deve essere configurato.
- Devi disporre dell’URL dell’IdP e dei metadati.
- Devi avere accesso al server IdP.

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

Solo gli utenti remoti avranno accesso all’interfaccia utente grafica di Unified Manager dopo che avrai abilitato l’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 si riavvia automaticamente al termine della configurazione SAML su questa pagina.

Passaggi

1. Nel riquadro di navigazione a sinistra, fai clic su **Generale** > **Autenticazione SAML**.

2. Seleziona la casella di controllo **Abilita autenticazione SAML**.

   Vedi i campi necessari per configurare la connessione IdP.

3. Inserisci l'URI dell'IdP e i metadati dell'IdP necessari per connettere il server Unified Manager al server IdP.

   Se il server IdP è accessibile direttamente dal server Unified Manager, dopo aver inserito l'URI dell'IdP, puoi fare clic sul pulsante **Recupera metadati IdP** per compilare automaticamente il campo Metadati IdP.

4. Copia l'URI dei metadati dell'host di Unified Manager oppure salva i metadati dell'host in un file di testo XML.

   Puoi configurare il server IdP con queste informazioni in questo momento.

5. Fare clic su **Save**.

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

6. Fai clic su **Confirm and Logout** e Unified Manager si riavvia.

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

Se non l'hai già fatto, accedi al tuo IdP e inserisci l'URI del server Unified Manager e i metadati per completare la configurazione.

> Quando usi ADFS come provider di identità, la GUI di Unified Manager non rispetta il timeout di ADFS e continua a funzionare finché non viene raggiunto il timeout della sessione di Unified Manager. Puoi modificare il timeout della sessione della GUI facendo clic su **Generale** > **Impostazioni funzionalità** > **Timeout di inattività**.

Cambia il provider di identità per l'autenticazione SAML in Active IQ Unified Manager

Puoi modificare il provider di identità (IdP) che Unified Manager utilizza per autenticare gli utenti remoti.

Prima di iniziare

- Devi disporre dell'URL dell'IdP e dei metadati.
- Devi avere accesso all'IdP.

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

Passaggi

1. Nel riquadro di navigazione a sinistra, fai clic su **Generale** > **Autenticazione SAML**.
2. Inserisci il nuovo URI dell'IdP e i metadati dell'IdP necessari per connettere il server Unified Manager all'IdP.

   Se l'IdP è accessibile direttamente dal server Unified Manager, dopo aver inserito l'URL dell'IdP, puoi fare clic sul pulsante **Recupera metadati IdP** per compilare automaticamente il campo Metadati IdP.

3. Copia l'URI dei metadati di Unified Manager oppure salva i metadati in un file di testo XML.
4. Fai clic su **Salva configurazione**.

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

5. Fare clic su **OK**.

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

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

Aggiorna le impostazioni di autenticazione SAML dopo una modifica del certificato di sicurezza di Active IQ Unified Manager

Qualsiasi modifica al certificato di sicurezza HTTPS installato sul server Unified Manager richiede che tu aggiorni le impostazioni di configurazione dell'autenticazione SAML. Il certificato viene aggiornato se rinomini il sistema host, assegni un nuovo indirizzo IP al sistema host o modifichi manualmente il certificato di sicurezza del sistema.

Dopo la modifica del certificato di sicurezza e il riavvio del server Unified Manager, l'autenticazione SAML non funzionerà e gli utenti non potranno accedere all'interfaccia grafica di Unified Manager. Devi aggiornare le impostazioni di autenticazione SAML sia sul server IdP sia sul server Unified Manager per riattivare l'accesso all'interfaccia utente.

Passaggi

1. Accedi alla console di manutenzione.
2. Nel **Menu principale**, inserisci il numero corrispondente all'opzione **Disabilita autenticazione SAML**.

   Viene visualizzato un messaggio per confermare che vuoi disabilitare l'autenticazione SAML e riavviare Unified Manager.

3. Avvia l'interfaccia utente di Unified Manager utilizzando il FQDN o l'indirizzo IP aggiornato, accetta il certificato del server aggiornato nel browser ed effettua l'accesso utilizzando le credenziali dell'utente di manutenzione.
4. Nella pagina **Configurazione/Autenticazione**, seleziona la scheda **Autenticazione SAML** e configura la connessione IdP.
5. Copia l'URI dei metadati dell'host di Unified Manager oppure salva i metadati dell'host in un file di testo XML.
6. Fare clic su **Save**.

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

7. Fai clic su **Confirm and Logout** e Unified Manager si riavvia.
8. Accedi al tuo server IdP e inserisci l'URI del server Unified Manager e i metadati per completare la configurazione.

Fornitore di identità	Passaggi di configurazione
ADFS	a. Elimina la voce esistente di relying party trust nella GUI di gestione di ADFS. b. Aggiungi una nuova voce di attendibilità della relying party utilizzando il `saml_sp_metadata.xml` dal server Unified Manager aggiornato. c. Definisci le tre regole di attestazione necessarie affinché Unified Manager possa analizzare le risposte SAML di ADFS per questa voce di trust della relying party. d. Riavvia il servizio Windows ADFS.
Shibboleth	a. Aggiorna il nuovo FQDN del server Unified Manager nei file `attribute-filter.xml` e `relying-party.xml`. b. Riavvia il server web Apache Tomcat e attendi che la porta 8005 torni online.

9. Accedi a Unified Manager e verifica che l'autenticazione SAML funzioni correttamente tramite il tuo IdP.

Disabilita l'autenticazione SAML in Active IQ Unified Manager

Puoi disabilitare l'autenticazione SAML quando vuoi 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 disabilitata, i provider di servizi directory configurati, come Active Directory o LDAP, eseguono l'autenticazione di accesso.

Dopo aver disabilitato l'autenticazione SAML, oltre agli utenti remoti configurati, anche gli utenti locali e gli utenti di manutenzione potranno accedere all'interfaccia utente grafica.

Puoi anche disabilitare l'autenticazione SAML usando la console di manutenzione di Unified Manager se non hai accesso all'interfaccia utente grafica.

Unified Manager si riavvia automaticamente dopo la disattivazione dell'autenticazione SAML.

Passaggi

1. Nel riquadro di navigazione a sinistra, fai clic su **Generale** > **Autenticazione SAML**.
2. Deseleziona la casella di controllo **Abilita l'autenticazione SAML**.
3. Fare clic su **Save**.

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

4. Fai clic su **Confirm and Logout** e Unified Manager si riavvia.

La prossima volta che gli utenti remoti tenteranno di accedere all'interfaccia grafica di Unified Manager, dovranno inserire le proprie credenziali nella pagina di accesso di Unified Manager anziché nella pagina di

accesso dell'IdP.

Accedi al tuo IdP ed elimina l'URI del server Unified Manager e i metadati.

Disabilita l'autenticazione SAML dalla console di manutenzione di Active IQ Unified Manager

Potresti dover disabilitare l'autenticazione SAML dalla console di manutenzione quando non hai accesso alla GUI di Unified Manager. Ciò potrebbe verificarsi in caso di configurazione errata o se l'IdP non è accessibile.

Prima di iniziare

Devi avere accesso alla console di manutenzione come utente di manutenzione.

Quando l'autenticazione SAML è disabilitata, i provider di servizi di directory configurati, come Active Directory o LDAP, eseguono l'autenticazione di accesso. Oltre agli utenti remoti configurati, anche gli utenti locali e gli utenti di manutenzione potranno accedere all'interfaccia utente grafica.

Puoi anche disabilitare l'autenticazione SAML dalla pagina Setup/Authentication nella UI.

Unified Manager si riavvia automaticamente dopo la disattivazione dell'autenticazione SAML.

Passaggi

1. Accedi alla console di manutenzione.
2. Nel **Menu principale**, inserisci il numero corrispondente all'opzione **Disabilita autenticazione SAML**.

   Viene visualizzato un messaggio per confermare che vuoi disabilitare l'autenticazione SAML e riavviare Unified Manager.

3. Digita **y**, quindi premi Invio e Unified Manager si riavvia.

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

Se necessario, accedi al tuo IdP ed elimina l'URL del server Unified Manager e i metadati.

Usa la pagina di autenticazione SAML in Active IQ Unified Manager

Puoi usare la pagina Autenticazione SAML per configurare Unified Manager in modo che autentichi gli utenti remoti tramite SAML attraverso un provider di identità (IdP) sicuro prima che possano accedere all'interfaccia utente web di Unified Manager.

- Per creare o modificare la configurazione SAML, devi disporre del ruolo Application Administrator.
- Devi aver configurato l'autenticazione remota.
- Devi aver configurato almeno un utente remoto o un gruppo remoto.

Dopo aver configurato l'autenticazione remota e gli utenti remoti, puoi selezionare la casella di controllo Abilita autenticazione SAML per abilitare l'autenticazione tramite un provider di identità sicuro.

- **URI IdP**

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

  Esempio di URI ADFS:

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

  Esempio di URI Shibboleth:

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

- **Metadati dell'IdP**

  I metadati IdP in formato XML.

  Se l'URL dell'IdP è accessibile dal server Unified Manager, puoi fare clic sul pulsante **Recupera metadati IdP** per compilare questo campo.

- **Sistema host (FQDN)**

  Il FQDN del sistema host Unified Manager come definito durante l'installazione. Puoi modificare questo valore se necessario.

- **URI dell'host**

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

- **Metadati dell'host**

  I metadati del sistema host in formato XML.

Gestisci l'autenticazione

Modifica i server di autenticazione in Active IQ Unified Manager

Puoi cambiare la porta che il server Unified Manager usa per comunicare con il tuo server di autenticazione.

Prima di iniziare

Devi avere il ruolo di Amministratore dell'applicazione.

Passaggi

1. Nel riquadro di navigazione a sinistra, fai clic su **Generale** > **Autenticazione remota**.
2. Seleziona la casella **Disable Nested Group Lookup**.
3. Nell'area **Server di autenticazione**, seleziona il server di autenticazione che vuoi modificare, quindi fai clic su **Modifica**.
4. Nella finestra di dialogo **Modifica server di autenticazione**, modifica i dettagli della porta.
5. Fare clic su **Save**.

Elimina i server di autenticazione in Active IQ Unified Manager

Puoi eliminare un server di autenticazione se vuoi impedire al server Unified Manager di comunicare con il server di autenticazione. Ad esempio, se vuoi cambiare un server di autenticazione con cui comunica il server di gestione, puoi eliminare il server di autenticazione e aggiungerne uno nuovo.

Prima di iniziare

Devi avere il ruolo di Amministratore dell'applicazione.

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

Passaggi

1. Nel riquadro di navigazione a sinistra, fai clic su **Generale** > **Autenticazione remota**.
2. Seleziona uno o più server di autenticazione che desideri eliminare, quindi fai clic su **Elimina**.
3. Fai clic su **Sì** per confermare la richiesta di eliminazione.

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

Autenticati con Active Directory o OpenLDAP in Active IQ Unified Manager

Puoi abilitare l'autenticazione remota sul server di gestione e configurarlo in modo che comunichi con i server di autenticazione, così gli utenti presenti in tali server possono accedere a Unified Manager.

Puoi utilizzare uno dei seguenti servizi di autenticazione predefiniti oppure specificare un servizio di autenticazione personalizzato:

- Microsoft Active Directory

  Non puoi utilizzare Microsoft Lightweight Directory Services.

- OpenLDAP

Puoi selezionare il servizio di autenticazione richiesto e aggiungere i server di autenticazione appropriati per consentire agli utenti remoti presenti nel server di autenticazione di accedere a Unified Manager. Le credenziali per gli utenti o i 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 mantiene un 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 di audit

Scopri i registri di controllo in Active IQ Unified Manager

Puoi rilevare se i log di audit sono stati compromessi utilizzando Audit Logs. Tutte le attività eseguite da un utente vengono monitorate e registrate in Audit Logs. Gli audit vengono eseguiti per tutte le funzionalità dell'interfaccia utente e delle API esposte pubblicamente di Active IQ Unified Manager.

Puoi usare **Audit Log: File View** per visualizzare e accedere a tutti i file di audit log disponibili in Active IQ Unified Manager. I file in Audit Log: File View sono elencati in base alla data di creazione. Questa vista mostra le informazioni di tutti gli audit log acquisiti dall'installazione o dall'aggiornamento fino al presente nel sistema. Ogni volta che esegui un'azione in Unified Manager, le informazioni vengono aggiornate e sono disponibili nei log. Lo stato di ciascun file di log viene acquisito usando l'attributo "File Integrity Status", che viene monitorato attivamente per rilevare manomissioni o eliminazioni del file di log. Gli audit log possono avere uno dei seguenti stati quando sono disponibili nel sistema:

Stato	Descrizione
ATTIVO	File in cui sono attualmente registrati i log.
NORMALE	File inattivo, compresso e memorizzato nel sistema.
MANOMESSO	File compromesso da un utente che lo ha modificato manualmente.
MANUAL_DELETE	File eliminato da un utente autorizzato.
ROLLOVER_DELETE	File eliminato a causa della rimozione in base al criterio di configurazione Rolling.
UNEXPECTED_DELETE	File eliminato per motivi sconosciuti.

La pagina Audit Log include i seguenti pulsanti di comando:

- Configurare
- Elimina
- Scarica

Il pulsante **DELETE** ti consente di eliminare uno qualsiasi dei log di controllo elencati nella vista Audit Logs. Puoi eliminare un log di controllo e, facoltativamente, specificare un motivo per eliminare il file, il che ti aiuterà in futuro a determinare se l'eliminazione è valida. La colonna REASON elenca il motivo insieme al nome dell'utente che ha eseguito l'operazione di eliminazione.

Se elimini un file di log, il file verrà rimosso dal sistema, ma la relativa voce nella tabella DB non verrà eliminata.

Puoi scaricare i log di audit da Active IQ Unified Manager utilizzando il pulsante **DOWNLOAD** nella sezione Log di audit ed esportare i file di log di audit. I file contrassegnati come "NORMAL" o "TAMPERED" vengono scaricati in formato `.gzip` compresso.

I file di log di audit vengono archiviati periodicamente e salvati nel database per consultazione. Prima dell'archiviazione, i file di log di audit vengono firmati digitalmente per garantirne la sicurezza e l'integrità.

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

Configura i registri di controllo di Active IQ Unified Manager

Puoi usare il pulsante **Configure** nella sezione Audit Logs per configurare i criteri di rotazione per i file Audit Log e anche per abilitare la registrazione remota per gli Audit Logs.

Puoi impostare i valori di **MAX FILE SIZE** e **AUDIT LOG RETENTION DAYS** in base alla quantità e alla frequenza dei dati che vuoi archiviare nel sistema. Il valore nel campo **TOTAL AUDIT LOG SIZE** rappresenta la dimensione totale dei dati dell'audit log presenti nel sistema. La policy di rollover è determinata dai valori nei campi **AUDIT LOG RETENTION DAYS**, **MAX FILE SIZE** e **TOTAL AUDIT LOG SIZE**. Quando la dimensione del backup dell'audit log raggiunge il valore configurato in **TOTAL AUDIT LOG SIZE**, il file archiviato per primo viene eliminato. Questo significa che il file meno recente viene eliminato. Tuttavia, la voce del file continua a essere disponibile nel database ed è contrassegnata come "Rollover Delete". Il valore di **AUDIT LOG RETENTION DAYS** indica il numero di giorni per cui i file dell'audit log vengono conservati. Qualsiasi file più vecchio del valore impostato in questo campo viene sottoposto a rollover.

Passaggi

1. Fai clic su **Registri di controllo** > > **Configura**.
2. Inserisci i valori in **DIMENSIONE MASSIMA DEL FILE**, **DIMENSIONE TOTALE DEL LOG DI AUDIT** e **GIORNI DI CONSERVAZIONE DEL LOG DI AUDIT**.

   Per abilitare la registrazione remota, seleziona **Abilita registrazione remota**.

Abilita la registrazione remota dei log di controllo in Active IQ Unified Manager

Puoi selezionare la casella di controllo **Enable Remote Logging** nella finestra di dialogo Configure Audit Logs per abilitare la registrazione remota dei log di controllo. Puoi usare questa funzionalità per trasferire i log di controllo a un server Syslog remoto. In questo modo puoi gestire i log di controllo quando lo spazio è limitato.

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

Passaggi

1. Nella finestra di dialogo **Configura log di audit**, seleziona la casella di controllo **Abilita registrazione remota**.

   Vengono visualizzati campi aggiuntivi per configurare la registrazione remota.

2. Inserisci il **HOSTNAME** e **PORT** del server remoto a cui vuoi connetterti.
3. Nel campo **CERTIFICATO CA DEL SERVER**, fai 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 "hostname" selezionato come parte dell'attributo `SubjectAltName` (SAN).

4. Inserisci i valori per i seguenti campi: **CHARSET**, **CONNECTION TIMEOUT**, **RECONNECTION DELAY**.

   I valori per questi campi devono essere espressi in millisecondi.

5. Seleziona il formato Syslog e la versione del protocollo richiesti nei campi **FORMATO** e **PROTOCOLLO**.

6. Seleziona la casella di controllo **Abilita autenticazione del client** se il server Syslog di destinazione richiede l'autenticazione basata su certificati.

   Dovrai scaricare il certificato di autenticazione del client e caricarlo sul server Syslog prima di salvare la configurazione di Audit Log, altrimenti la connessione non riuscirà. A seconda del tipo di server Syslog, potresti dover creare un hash del certificato di autenticazione del client.

   Esempio: syslog-ng richiede che venga creato <hash> del certificato utilizzando il comando `openssl x509 -noout -hash -in cert.pem`, quindi dovresti creare un collegamento simbolico dal certificato di autenticazione del client a un file denominato in base a <hash> .0.

7. Fai clic su **Salva** per configurare la connessione con il tuo server e abilitare la registrazione remota.

   Sarai reindirizzato alla pagina dei log di audit.

> Il valore di **Timeout di connessione** può influire sulla configurazione. Se la configurazione impiega più tempo a rispondere rispetto al valore definito, può causare un errore della configurazione dovuto a un errore di connessione. Per stabilire una connessione corretta, aumenta il valore di **Timeout di connessione** e riprova la configurazione.

Usa la pagina di autenticazione remota in Active IQ Unified Manager

Puoi usare la pagina Autenticazione remota per configurare Unified Manager in modo che comunichi con il server di autenticazione per autenticare gli utenti remoti che tentano di accedere alla web UI di Unified Manager.

Devi disporre del ruolo di Amministratore dell'applicazione o di Amministratore dello storage.

Dopo aver selezionato la casella di controllo "Enable remote authentication", puoi abilitare l'autenticazione remota usando un server di autenticazione.

- **Servizio di autenticazione**

  Ti consente di configurare il server di gestione per autenticare gli utenti nei provider di servizi directory, come Active Directory e OpenLDAP, oppure di specificare un tuo meccanismo di autenticazione. Puoi specificare un servizio di autenticazione solo se hai abilitato l'autenticazione remota.

  - **Active Directory**
    - Nome dell'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 domain name del server di autenticazione è ou@domain.com, il nome distinto di base è **cn=ou,dc=domain,dc=com**.

    - Disabilita la ricerca di gruppi nidificati

Specifica se abilitare o disabilitare l'opzione di ricerca dei gruppi nidificati. Per impostazione predefinita, questa opzione è disabilitata. Se usi Active Directory, puoi velocizzare l'autenticazione disabilitando il supporto per i gruppi nidificati.

- Usa una connessione sicura

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

- **OpenLDAP**
  - Distinguished Name di bind

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

  - Password di 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 domain name del server di autenticazione è ou@domain.com, il nome distinto di base è **cn=ou,dc=domain,dc=com**.

  - Usa una connessione sicura

    Specifica che Secure LDAP viene usato per comunicare con i server di autenticazione LDAP.

- **Altri**
  - Distinguished Name di bind

    Specifica il nome distinto di bind utilizzato insieme al nome distinto di base per trovare gli utenti remoti nel server di autenticazione che hai configurato.

  - Password di 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 domain name 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 del protocollo LDAP (Lightweight Directory Access Protocol) supportata dal tuo server di autenticazione. Puoi specificare se la versione del protocollo deve essere rilevata automaticamente oppure impostarla su 2 o 3.

  - Attributo nome utente

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

- Attributo di appartenenza al gruppo

  Specifica un valore che assegna l'appartenenza al gruppo del 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 ti consente di assegnare l'appartenenza al gruppo del server di gestione agli utenti remoti in base a un attributo specificato in tale oggetto GroupOfUniqueNames.

- Disabilita la ricerca di gruppi nidificati

  Specifica se abilitare o disabilitare l'opzione di ricerca dei gruppi nidificati. Per impostazione predefinita, questa opzione è disabilitata. Se usi Active Directory, puoi velocizzare l'autenticazione disabilitando il supporto per i gruppi nidificati.

- Membro

  Specifica il nome dell'attributo che il server di autenticazione utilizza per memorizzare le informazioni sui singoli membri di un gruppo.

- Classe oggetto utente

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

- Classe oggetto di gruppo

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

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

- Usa una connessione sicura

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

  Se vuoi modificare il servizio di autenticazione, assicurati di eliminare tutti i server di autenticazione esistenti e di aggiungerne di nuovi.

Area dei server di autenticazione

L'area 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 gli utenti o i gruppi remoti vengono gestite dal server di autenticazione.

- **Pulsanti di comando**

  Ti consente di aggiungere, modificare o eliminare i server di autenticazione.

  - Aggiungi

    Consente di aggiungere un server di autenticazione.

  Se il server di autenticazione che stai aggiungendo fa parte di una coppia ad alta disponibilità (che utilizza

lo stesso database), puoi aggiungere anche il server di autenticazione partner. Questo consente al server di gestione di comunicare con il partner quando uno dei server di autenticazione non è raggiungibile.

  - Modifica

    Ti consente di modificare le impostazioni di un server di autenticazione selezionato.

  - Elimina

    Elimina i server di autenticazione selezionati.

- **Nome o indirizzo IP**

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

- **Porta**

  Visualizza il numero della porta del server di autenticazione.

- **Test di autenticazione**

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

  Durante la fase di test, se specifichi solo il nome utente, il server di gestione cerca l'utente remoto nel server di autenticazione, ma non lo autentica. Se specifichi sia il nome utente che la password, il server di gestione cerca e autentica l'utente remoto.

  Non puoi testare l'autenticazione se l'autenticazione remota è disabilitata.

Gestisci i certificati di sicurezza

Visualizza il certificato di sicurezza HTTPS in Active IQ Unified Manager

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

Prima di iniziare

Devi disporre del ruolo di Operatore, Amministratore di applicazioni o Amministratore di archiviazione.

Visualizzando il certificato, puoi verificare il contenuto di un certificato rigenerato oppure visualizzare i nomi alternativi del soggetto (SAN) tramite i quali puoi accedere a Unified Manager.

Passaggio

1. Nel riquadro di navigazione a sinistra, fai clic su **Generale** > **Certificato HTTPS**.

   Il certificato HTTPS viene visualizzato in alto nella pagina

Se hai bisogno di visualizzare informazioni più dettagliate sul certificato di sicurezza rispetto a quelle mostrate nella pagina HTTPS Certificate, puoi visualizzare il certificato di connessione nel tuo browser.

Scarica una richiesta di firma del certificato HTTPS in Active IQ Unified Manager

Puoi scaricare una richiesta di firma del certificato per il certificato di sicurezza HTTPS corrente, così da poter fornire il file a una Certificate Authority (CA) per la firma. Un certificato firmato da una CA contribuisce a prevenire gli attacchi man-in-the-middle e offre una protezione di sicurezza migliore rispetto a un certificato autofirmato.

Prima di iniziare

Devi avere il ruolo di Amministratore dell'applicazione.

Passaggi

1. Nel riquadro di navigazione a sinistra, fai clic su **Generale** > **Certificato HTTPS**.
2. Fai clic su **Scarica la richiesta di firma del certificato HTTPS**.
3. Salva il `<hostname>.csr` file.

Puoi fornire il file a un'autorità di certificazione per la firma e quindi installare il certificato firmato.

Installa un certificato HTTPS firmato da una CA in Active IQ Unified Manager

Puoi caricare e installare un certificato di sicurezza dopo che un'Autorità di certificazione lo ha firmato e restituito. Il file che carichi e installi deve essere una versione firmata del certificato autofirmato esistente. Un certificato firmato da un'Autorità di certificazione contribuisce a prevenire gli attacchi man-in-the-middle e offre una protezione di sicurezza migliore rispetto a un certificato autofirmato.

*Cosa fare prima di iniziare

Devi aver completato le seguenti azioni:

- Hai scaricato il file di richiesta di firma del certificato e lo hai fatto firmare da un'autorità di certificazione
- Catena di certificati salvata in formato PEM
- Sono inclusi tutti i certificati nella catena, dal certificato del server Unified Manager al certificato di firma radice, compresi eventuali certificati intermedi presenti

Devi avere il ruolo di Amministratore dell'applicazione.



Se la validità del certificato per il quale è stato creato un CSR è superiore a 397 giorni, l'autorità di certificazione (CA) la ridurrà a 397 giorni prima di firmare e restituire il certificato

Passaggi

1. Nel riquadro di navigazione a sinistra, fai clic su **Generale** > **Certificato HTTPS**.
2. Fai clic su **Installa certificato HTTPS**.
3. Nella finestra di dialogo visualizzata, fai clic su **Scegli file…** per individuare il file da caricare.
4. Seleziona il file, quindi fai clic su **Installa** per installarlo.

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

Esempio di catena di certificati

L'esempio seguente mostra come potrebbe apparire il file della catena di certificati:

```
-----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-----
```

Scopri i certificati HTTPS generati utilizzando strumenti esterni in Active IQ Unified Manager Unified Manager

Puoi installare certificati autofirmati o firmati da una CA e generati utilizzando uno strumento esterno come OpenSSL, BoringSSL, LetsEncrypt.

Devi caricare la chiave privata insieme alla catena di certificati, perché questi certificati sono coppie di chiavi pubblica-privata generate esternamente. Gli algoritmi consentiti per la coppia di chiavi sono "RSA" ed "EC". L'opzione **Install HTTPS Certificate** è disponibile nella pagina HTTPS Certificates, nella sezione General. Il file che carichi deve essere nel seguente formato di input.

1. Chiave privata del server che appartiene all'host Active IQ Unified Manager
2. Certificato del server corrispondente alla chiave privata
3. Certificato delle CA in ordine inverso fino alla radice, utilizzate per firmare il certificato precedente

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 caricare un certificato con una coppia di chiavi RSA

Le dimensioni 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-----
```

Dopo aver caricato il certificato, dovresti riavviare l'istanza di Active IQ Unified Manager affinché le modifiche abbiano effetto.

Verifiche durante il caricamento di certificati generati esternamente

Il sistema esegue controlli durante il caricamento di un certificato generato utilizzando strumenti esterni. Se uno qualsiasi dei controlli fallisce, il certificato viene rifiutato. Sono inoltre incluse convalide per i certificati generati dal CSR (Certificate Signing Request) all'interno del prodotto e per i certificati generati utilizzando strumenti esterni.

- La chiave privata nell'input viene convalidata rispetto al certificato host nell'input.
- Il nome comune (CN) nel certificato dell'host viene confrontato con il FQDN dell'host.
- Il nome comune (CN) del certificato dell'host non deve essere vuoto o composto solo da spazi e non deve essere impostato su localhost.
- La data di inizio validità non deve essere futura e la data di scadenza della validità del certificato non deve essere passata.

- Se esiste un Intermediate CA o un CA, la data di inizio della validità del certificato non deve essere nel futuro e la data di scadenza della validità non deve essere nel passato.

La chiave privata inserita non deve essere crittografata. Se sono presenti chiavi private crittografate, il sistema le rifiuta.

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-----
```

Se l'installazione del certificato non riesce, consulta l'articolo della knowledge base (KB): "ActiveIQ Unified Manager non riesce a installare un certificato generato esternamente"

Descrizioni delle pagine per la gestione dei certificati

Scopri la pagina relativa al certificato HTTPS in Active IQ Unified Manager

La pagina Certificato HTTPS consente di visualizzare il certificato di sicurezza corrente, scaricare una richiesta di firma del certificato, generare un nuovo certificato HTTPS autofirmato o installare un nuovo certificato HTTPS.

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

Pulsanti di comando

I pulsanti di comando consentono di eseguire le seguenti operazioni:

- **Scarica la richiesta di firma del certificato HTTPS**

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

- **Installa il certificato HTTPS**

  Ti consente di caricare e installare un certificato di sicurezza dopo che un'Autorità di Certificazione lo ha firmato e restituito. Il nuovo certificato entra in vigore dopo che riavvii il server di gestione.

- **Rigenera il certificato HTTPS**

  Ti consente di generare un nuovo certificato HTTPS autofirmato che sostituisce il certificato di sicurezza corrente. Il nuovo certificato sarà attivo dopo aver riavviato Unified Manager.

Finestra di dialogo Rigenera certificato HTTPS in Active IQ Unified Manager

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

Le informazioni correnti sul certificato sono visualizzate in questa pagina.

Le opzioni "Regenerate Using Current Certificate Attributes" e "Update the Current Certificate Attributes" ti consentono di rigenerare il certificato con le informazioni correnti oppure di generarne uno con nuove informazioni.

- **Nome comune**

  Obbligatorio. Il fully qualified domain name (FQDN) che desideri proteggere.

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

- **E-mail**

  Facoltativo. Un indirizzo e-mail per contattare la tua organizzazione; in genere l'indirizzo e-mail dell'amministratore dei certificati o del reparto IT.

- **Azienda**

  Facoltativo. In genere corrisponde alla ragione sociale della tua azienda.

- **Dipartimento**

  Facoltativo. Il nome del reparto nella tua azienda.

- **Città**

  Facoltativo. La città in cui si trova la tua azienda.

- **Stato**

  Facoltativo. Lo stato o la provincia in cui si trova la tua azienda, senza abbreviazioni.

- **Paese**

  Facoltativo. Il paese in cui ha sede la tua azienda. In genere si tratta di un codice ISO di due lettere che

identifica il paese.

- **Nomi alternativi**

  Obbligatorio. domain name aggiuntivi, non primari, che puoi usare per accedere a questo server oltre a localhost o ad altri indirizzi di rete esistenti. Separa ciascun nome alternativo con una virgola.

  Seleziona la casella di controllo “Escludi informazioni di identificazione locali (ad es. localhost)” se vuoi rimuovere le informazioni di identificazione locali dal campo Nomi alternativi del certificato. Quando selezioni questa casella di controllo, nel campo Nomi alternativi viene usato solo quello che inserisci nel campo. Se lo lasci vuoto, il certificato risultante non avrà alcun campo Nomi alternativi.

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

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

- **PERIODO DI VALIDITÀ**

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

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

Informazioni sul copyright

Copyright © 2026 NetApp, Inc. Tutti i diritti riservati. Stampato negli Stati Uniti d'America. Nessuna porzione di questo documento soggetta a copyright può essere riprodotta in qualsiasi formato o mezzo (grafico, elettronico o meccanico, inclusi fotocopie, registrazione, nastri o storage in un sistema elettronico) senza previo consenso scritto da parte del detentore del copyright.

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

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

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

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

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

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

Informazioni sul marchio commerciale

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