Eseguire attività di configurazione e amministrative

Active IQ Unified Manager

NetApp
October 15, 2025

Sommario

Eseguire attività di configurazione e amministrative

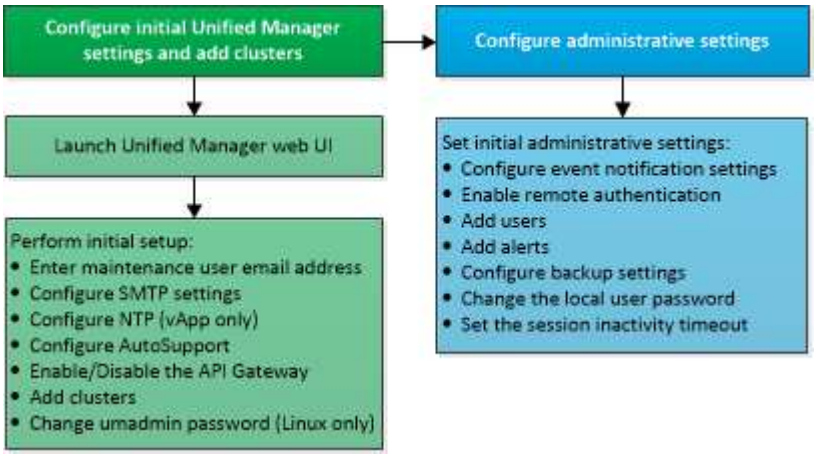
Configura Active IQ Unified Manager

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

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

Panoramica della sequenza di configurazione

Il flusso di lavoro di configurazione descrive le attività che è necessario eseguire prima di poter utilizzare Unified Manager.



Accedi all'interfaccia utente web di Unified Manager

Dopo aver installato Unified Manager, puoi accedere all'interfaccia utente 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 effettuare l'accesso come utente di manutenzione (o utente umadmin per le installazioni Linux).
- Se si prevede di consentire agli utenti di accedere a Unified Manager utilizzando il nome breve anziché il nome di dominio completo (FQDN) o l'indirizzo IP, la configurazione di rete deve risolvere questo nome breve in un FQDN valido.
- Se il server utilizza un certificato digitale autofirmato, il browser potrebbe visualizzare un avviso che indica che il certificato non è attendibile. È possibile accettare il rischio di continuare l'accesso oppure installare un certificato digitale firmato da un'autorità di certificazione (CA) per l'autenticazione del server.

Passi

1. Avviare l'interfaccia utente Web di Unified Manager dal browser utilizzando l'URL visualizzato al termine dell'installazione. L'URL è l'indirizzo IP o il nome di dominio completo (FQDN) del server Unified Manager.

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

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

> Se effettui tre tentativi consecutivi di accesso all'interfaccia utente web senza successo nell'arco di un'ora, verrai bloccato fuori dal sistema e dovrai contattare l'amministratore di sistema. Questa opzione è valida solo per gli utenti locali.

Eseguire la configurazione iniziale dell'interfaccia utente Web di Unified Manager

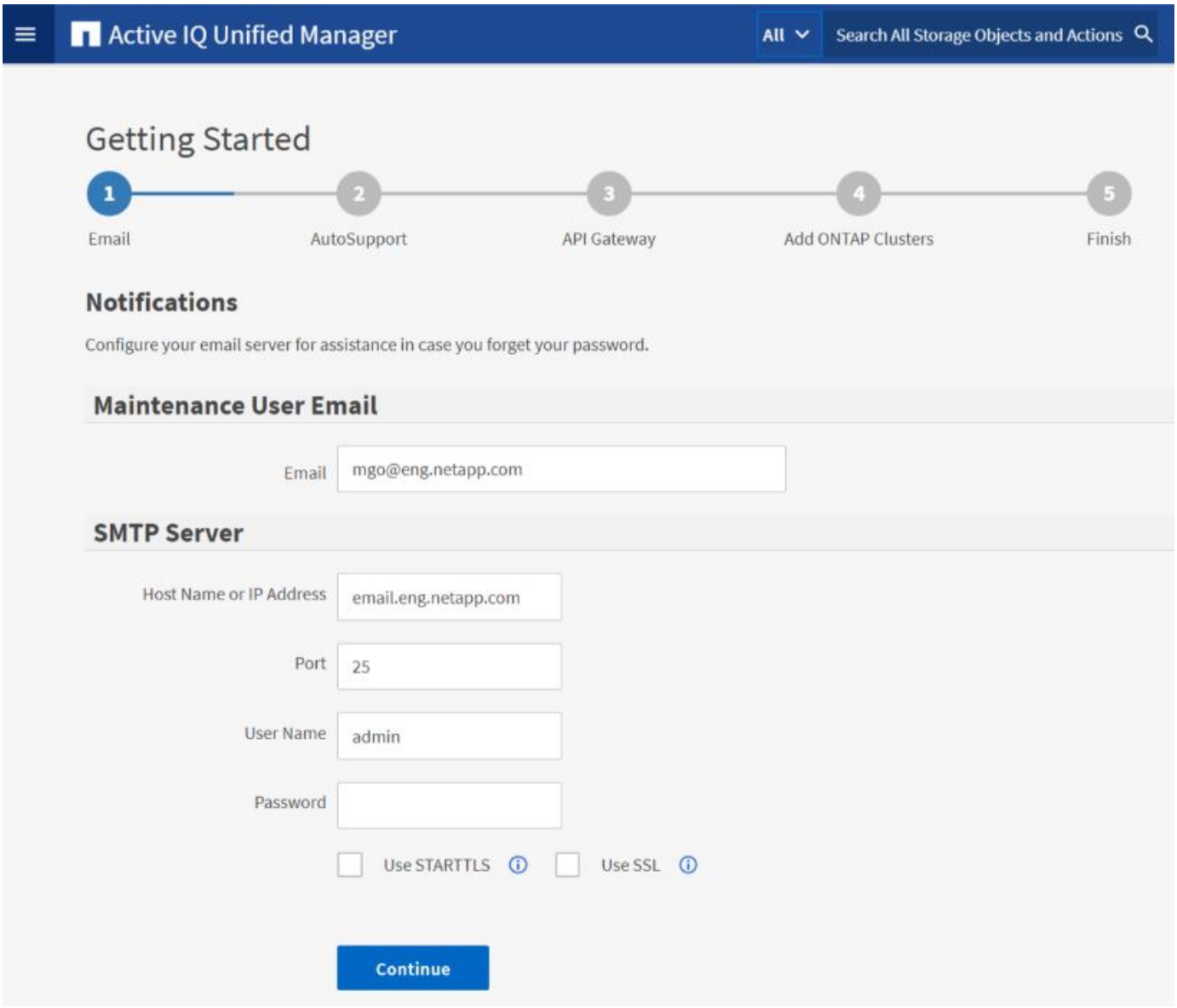
Per utilizzare Unified Manager, è necessario innanzitutto configurare le opzioni di configurazione iniziale, tra cui il server NTP, l'indirizzo e-mail dell'utente addetto alla manutenzione, l'host del server SMTP e l'aggiunta di cluster ONTAP .

Prima di iniziare

Devi aver eseguito le seguenti operazioni:

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

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



Se in seguito desideri modificare una di queste opzioni, puoi selezionarla dalle opzioni Generali nel riquadro di navigazione a sinistra di Unified Manager. Si noti 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.

Passi

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

   Se hai selezionato l'opzione **Usa STARTTLS** o **Usa SSL**, dopo aver cliccato sul pulsante **Continua** verrà visualizzata una pagina del certificato. Verificare i dettagli del certificato e accettare il certificato per continuare con le impostazioni di configurazione iniziale dell'interfaccia utente Web.

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

   Se è necessario designare un proxy per fornire l'accesso a Internet per inviare contenuti AutoSupport , oppure se si desidera disattivare AutoSupport, utilizzare l'opzione **Generale** > * AutoSupport*

dall'interfaccia utente Web.

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

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

5. Aggiungere i cluster che si desidera vengano gestiti da Unified Manager, quindi fare clic su **Avanti**. Per ogni cluster che intendi gestire, devi disporre del nome host o dell'indirizzo IP di gestione del cluster (IPv4 o IPv6) insieme alle credenziali di nome utente e password; l'utente deve avere il ruolo "admin".

   Questo passaggio è facoltativo. È possibile aggiungere cluster in un secondo momento nell'interfaccia utente Web da **Gestione archiviazione** > **Configurazione cluster**.

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

La pagina Introduzione si chiude e viene visualizzata la pagina Dashboard di Unified Manager.

Aggiungi cluster

È possibile aggiungere un cluster ad Active IQ Unified Manager in modo da poterlo monitorare. Ciò include la possibilità di ottenere informazioni sul cluster, quali integrità, capacità, prestazioni e configurazione del cluster, in modo da poter individuare e risolvere eventuali problemi che potrebbero verificarsi.

Prima di iniziare

- È necessario disporre del ruolo di Amministratore dell'applicazione o Amministratore dell'archiviazione.
- È necessario disporre delle seguenti informazioni:
  - Unified Manager supporta cluster ONTAP on-premise, ONTAP Select Cloud Volumes ONTAP.
  - Nome host o indirizzo IP di gestione del cluster

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

    L'indirizzo IP di gestione del cluster deve essere il LIF di gestione del cluster della macchina virtuale di archiviazione amministrativa (SVM). Se si utilizza un LIF di gestione dei nodi, l'operazione fallisce.

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

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

  - Il numero di porta per connettersi al cluster tramite il protocollo HTTPS (in genere la porta 443)
  - Hai i certificati richiesti:

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

Certificato EMS: Questo certificato è di proprietà di Unified Manager. Viene utilizzato 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 certificato è abilitata per un cluster, in base alla versione ONTAP . Se il cluster che esegue la versione ONTAP è precedente alla 9.5, l'autenticazione basata su certificato non è abilitata.

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

- È possibile aggiungere un cluster dall'interfaccia utente Web e l'autenticazione basata su certificato verrà abilitata automaticamente.
- È possibile aggiungere un cluster tramite Unified Manager CLI; l'autenticazione basata su certificato non è abilitata per impostazione predefinita. Se si aggiunge un cluster tramite Unified Manager CLI, è necessario modificare il cluster tramite l'interfaccia utente di Unified Manager. Puoi vedere"Comandi CLI di Unified Manager supportati" per aggiungere un cluster utilizzando Unified Manager CLI.
- Se per un cluster è abilitata l'autenticazione basata su certificato e si esegue il backup di Unified Manager da un server e lo si ripristina su un altro server Unified Manager in cui il nome host o l'indirizzo IP è stato modificato, il monitoraggio del cluster potrebbe non riuscire. Per evitare il fallimento, modificare e salvare i dettagli del cluster. Per ulteriori informazioni sulla modifica dei dettagli del cluster, vedere"Modifica dei cluster" .

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

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

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

Passi

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

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

4. Fare clic su **Invia**.
5. Nella finestra di dialogo Autorizza host, fare clic su **Visualizza certificato** per visualizzare le informazioni sul certificato del cluster.
6. Fare clic su **Sì**.

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

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

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

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

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

Informazioni correlate

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

Configurare Unified Manager per inviare notifiche di avviso

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

Prima di iniziare

È necessario disporre del ruolo di amministratore dell'applicazione.

Dopo aver distribuito Unified Manager e completato la configurazione iniziale, dovresti prendere in considerazione la possibilità di configurare l'ambiente in modo da attivare avvisi e generare e-mail di notifica o trap SNMP in base alla ricezione di eventi.

Passi

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

   Se si desidera che vengano inviate notifiche di avviso quando si verificano determinati eventi nel proprio ambiente, è necessario configurare un server SMTP e fornire un indirizzo e-mail da cui verrà inviata la notifica di avviso. Se si desidera utilizzare trap SNMP, è possibile selezionare tale opzione e fornire le informazioni necessarie.

2. "Abilita l'autenticazione remota".

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

3. "Aggiungi server di autenticazione".

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

4. "Aggiungi utenti".

   È possibile aggiungere diversi tipi di utenti locali o remoti e assegnare ruoli specifici. Quando si crea un avviso, si assegna un utente che riceverà le notifiche di avviso.

5. "Aggiungi avvisi".

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

Configurare le impostazioni di notifica degli eventi

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

Prima di iniziare

È necessario disporre delle seguenti informazioni:

- Indirizzo email da cui viene inviata la notifica di avviso

  L'indirizzo email appare nel campo "Da" nelle notifiche di avviso inviate. Se per qualsiasi motivo l'e-mail non può essere recapitata, questo indirizzo e-mail viene utilizzato anche come destinatario per la posta non recapitata.

- Nome host del server SMTP e nome utente e password per accedere al server
- Nome host o indirizzo IP per l'host di destinazione della trappola che riceverà la trappola SNMP, insieme alla versione SNMP, alla porta della trappola in uscita, alla community e ad altri valori di configurazione SNMP richiesti

  Per specificare più destinazioni trap, separare ogni host con una virgola. In questo caso, tutte le altre impostazioni SNMP, come la versione e la porta trap in uscita, devono essere le stesse per tutti gli host nell'elenco.

È necessario disporre del ruolo di Amministratore dell'applicazione o Amministratore dell'archiviazione.

Passi

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

   Note:

   - Se l'indirizzo del mittente è precompilato con l'indirizzo "ActiveIQUnifiedManager@localhost.com", dovresti modificarlo con un indirizzo email reale e funzionante per assicurarti che tutte le notifiche email vengano recapitate correttamente.
   - Se non è possibile risolvere il nome host del server SMTP, è possibile specificare l'indirizzo IP (IPv4 o IPv6) del server SMTP anziché il nome host.
3. Fare clic su **Salva**.
4. Se hai selezionato l'opzione **Usa STARTTLS** o **Usa SSL**, dopo aver fatto clic sul pulsante **Salva** verrà visualizzata una pagina del certificato. Verificare i dettagli del certificato e accettare il certificato per salvare le impostazioni di notifica.

   È possibile 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

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

Prima di iniziare

È necessario disporre del ruolo di amministratore dell'applicazione.

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

È possibile abilitare l'autenticazione remota utilizzando 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 (Secure LDAP). Unified Manager utilizza 389 come porta predefinita per le comunicazioni non sicure e 636 come porta predefinita per le comunicazioni sicure.

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

Passi

1. Nel riquadro di navigazione a sinistra, fare clic su **Generale** > **Autenticazione remota**.
2. Seleziona la casella **Abilita 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…
Directory attiva	• Nome dell'amministratore del server di autenticazione in uno dei seguenti formati: ◦ `domainname\username` ◦ `username@domainname` ◦ `Bind Distinguished Name`(utilizzando la notazione LDAP appropriata) • Password dell'amministratore • Nome distinto di base (utilizzando la notazione LDAP appropriata)
Apri LDAP	• Associa nome distinto (nella notazione LDAP appropriata) • Password di collegamento • Nome distinto di base

Se l'autenticazione di un utente di Active Directory richiede molto tempo o scade, è probabile che il server di autenticazione stia impiegando molto tempo a rispondere. La disattivazione del supporto per i gruppi nidificati in Unified Manager potrebbe ridurre il tempo di autenticazione.

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

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

Disabilita i gruppi nidificati dall'autenticazione remota

Se è abilitata l'autenticazione remota, è possibile disabilitare l'autenticazione di gruppo nidificata in modo che solo i singoli utenti, e non i membri del gruppo, possano autenticarsi in remoto su Unified Manager. È possibile disabilitare i gruppi nidificati quando si desidera migliorare il tempo di risposta dell'autenticazione di Active Directory.

Prima di iniziare

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

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

Passi

1. Nel riquadro di navigazione a sinistra, fare clic su **Generale** > **Autenticazione remota**.
2. Seleziona la casella **Disabilita ricerca gruppi annidati**.

3. Fare clic su **Salva**.

Impostare i servizi di autenticazione

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

Prima di iniziare

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

Passi

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

Se selezioni…	Allora fai così…
Directory attiva	a. Inserisci il nome e la password dell'amministratore. b. Specificare il nome distinto di base del server di autenticazione. Ad esempio, se il nome di dominio del server di autenticazione è ou@domain.com, il nome distinto di base è **cn=ou,dc=domain,dc=com**.
OpenLDAP	a. Immettere il nome distinto e la password di associazione. b. Specificare il nome distinto di base del server di autenticazione. Ad esempio, se il nome di dominio del server di autenticazione è ou@domain.com, il nome distinto di base è **cn=ou,dc=domain,dc=com**.

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

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

3. Fare clic su **Salva**.

Aggiungi server di autenticazione

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

Prima di iniziare

- Devono essere disponibili le seguenti informazioni:
  - Nome host o indirizzo IP del server di autenticazione
  - Numero di porta del server di autenticazione
- È necessario aver 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.
- È necessario disporre del ruolo di amministratore dell'applicazione.

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

Passi

1. Nel riquadro di navigazione a sinistra, fare clic su **Generale** > **Autenticazione remota**.
2. Abilita o disabilita l'opzione **Usa connessione sicura**:

Se lo desidera…	Allora fai così…
Abilitalo	a. Selezionare l'opzione **Usa connessione protetta**. b. Nell'area Server di autenticazione, fare clic su **Aggiungi**. c. Nella finestra di dialogo Aggiungi server di autenticazione, immettere il nome di autenticazione o l'indirizzo IP (IPv4 o IPv6) del server. d. Nella finestra di dialogo Autorizza host, fare clic su Visualizza certificato. e. Nella finestra di dialogo Visualizza certificato, verificare le informazioni sul certificato, quindi fare clic su **Chiudi**. f. Nella finestra di dialogo Autorizza host, fare clic su **Sì**. Quando si abilita l'opzione **Usa autenticazione connessione protetta**, Unified Manager comunica con il server di autenticazione e visualizza il certificato. Unified Manager utilizza la porta 636 come porta predefinita per le comunicazioni protette e la porta 389 per le comunicazioni non protette.
Disabilitarlo	a. Deselezionare l'opzione **Usa connessione protetta**. b. Nell'area Server di autenticazione, fare clic su **Aggiungi**. c. Nella finestra di dialogo Aggiungi server di autenticazione, specificare il nome host o l'indirizzo IP (IPv4 o IPv6) del server e i dettagli della porta. d. Fare clic su **Aggiungi**.

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

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

Testare la configurazione dei server di autenticazione

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

configurazione cercando un utente o un gruppo remoto dai server di autenticazione e autenticandolo tramite le impostazioni configurate.

Prima di iniziare

- È necessario 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.
- È necessario aver aggiunto i server di autenticazione affinché il server di gestione possa cercare l'utente o il gruppo remoto da questi server e autenticarli.
- È necessario disporre del ruolo di amministratore dell'applicazione.

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

Passi

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

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

Aggiungi avvisi

È possibile configurare degli avvisi per essere avvisati quando viene generato un evento specifico. È possibile configurare gli avvisi per una singola risorsa, per un gruppo di risorse o per eventi di un tipo di gravità specifico. È possibile specificare la frequenza con cui si desidera ricevere la notifica e associare uno script all'avviso.

Prima di iniziare

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

È possibile creare un avviso direttamente dalla pagina Dettagli evento dopo aver ricevuto un evento, oltre a creare un avviso dalla pagina Impostazione avviso, come descritto qui.

Passi

1. Nel riquadro di navigazione a sinistra, fare clic su **Gestione archiviazione** > **Configurazione avvisi**.
2. Nella pagina Impostazione avvisi, fare clic su **Aggiungi**.
3. Nella finestra di dialogo Aggiungi avviso, fare clic su **Nome** e immettere un nome e una descrizione per l'avviso.

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

   È possibile impostare un filtro specificando una stringa di testo nel campo **Il nome contiene** per selezionare un gruppo di risorse. In base alla stringa di testo specificata, l'elenco delle risorse disponibili visualizza solo le risorse che corrispondono alla regola del filtro. La stringa di testo specificata è sensibile alla distinzione tra maiuscole e minuscole.

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

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

   Per selezionare più di un evento, premere il tasto Ctrl mentre si effettuano le selezioni.

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

   Se si modifica l'indirizzo email specificato per l'utente e si riapre l'avviso per modificarlo, il campo Nome appare vuoto perché l'indirizzo email modificato non è più associato all'utente precedentemente selezionato. Inoltre, se hai modificato l'indirizzo email dell'utente selezionato dalla pagina Utenti, l'indirizzo email modificato non verrà aggiornato per l'utente selezionato.

   È anche possibile scegliere di avvisare gli utenti tramite trap SNMP.

7. Fare clic su **Salva**.

Esempio di aggiunta di un avviso

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

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

Eseguire i seguenti passaggi nella finestra di dialogo Aggiungi avviso:

Passi

1. Fare clic su **Nome** e immettere **HealthTest** nel campo **Nome avviso**.
2. Fare clic su **Risorse** e, nella scheda Includi, selezionare **Volumi** dall'elenco a discesa.
   a. Immettere **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 spostarlo nell'area Risorse selezionate.
   c. Fare clic su **Escludi** e immettere **xyz** nel campo **Il nome contiene**, quindi fare clic su **Aggiungi**.
3. Fare clic su **Eventi** e selezionare **Critico** dal campo Gravità evento.

4. Seleziona **Tutti gli eventi critici** dall'area Eventi corrispondenti e spostalo nell'area Eventi selezionati.
5. Fare clic su **Azioni** e immettere **sample@domain.com** nel campo Avvisa questi utenti.
6. Seleziona **Ricorda ogni 15 minuti** per avvisare l'utente ogni 15 minuti.

   È possibile configurare un avviso in modo che invii ripetutamente notifiche ai destinatari per un periodo di tempo specificato. È necessario stabilire l'orario a partire dal quale la notifica dell'evento è attiva per l'avviso.

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

Cambia la password dell'utente locale

È possibile 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 per l'utente addetto alla manutenzione e per gli utenti remoti non possono essere modificate seguendo questi passaggi. Per modificare la password di un utente remoto, contattare l'amministratore delle password. Per modificare la password dell'utente addetto alla manutenzione, vedere"Utilizzo della console di manutenzione" .

Passi

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

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

3. Nella finestra di dialogo Cambia password, immettere la password corrente e quella nuova.
4. Fare clic su **Salva**.

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

Imposta il timeout di inattività della sessione

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

Prima di iniziare

È necessario disporre del ruolo di amministratore dell'applicazione.

Questa impostazione ha effetto su tutte le sessioni utente registrate.

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

Passi

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

Se lo desidera…	Allora fai così…
Non impostare alcun timeout in modo che la sessione non venga mai chiusa automaticamente	Nel pannello **Timeout di inattività**, spostare il cursore verso sinistra (off) e fare clic su **Applica**.
Imposta un numero specifico di minuti come valore di timeout	Nel pannello **Timeout di inattività**, spostare il cursore verso destra (on), specificare il valore del timeout di inattività in minuti e fare clic su **Applica**.

Imposta il timeout della sessione tramite CLI

È possibile impostare un valore massimo di timeout della sessione per Unified Manager tramite la CLI, in modo che la sessione venga terminata 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 questo compito

È necessario disporre del ruolo di amministratore dell'applicazione.

L'impostazione del timeout della sessione ha effetto su tutte le sessioni degli utenti registrati.

Passi

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

Cambiare il nome host di Unified Manager

A un certo punto, potresti voler modificare il nome host del sistema 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 monitorati.

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

Modificare il nome host dell'appliance virtuale Unified Manager

All'host di rete viene assegnato un nome quando l'appliance virtuale Unified Manager viene distribuita per la prima volta. È possibile modificare il nome host dopo la

distribuzione. Se si modifica il nome host, è necessario rigenerare anche il certificato HTTPS.

Prima di iniziare

Per eseguire queste attività, è necessario aver effettuato l'accesso a Unified Manager come utente addetto alla manutenzione oppure avere il ruolo di amministratore dell'applicazione assegnato.

È possibile utilizzare il nome host (o l'indirizzo IP host) per accedere all'interfaccia utente Web di Unified Manager. Se hai configurato un indirizzo IP statico per la tua rete durante la distribuzione, allora avrai designato un nome per l'host di rete. Se hai configurato la rete tramite DHCP, il nome host dovrebbe essere preso dal DNS. Se DHCP o DNS non sono configurati correttamente, il nome host "Unified Manager" viene assegnato automaticamente e associato al certificato di sicurezza.

Indipendentemente da come è stato assegnato il nome host, se si modifica il nome host e si intende utilizzare il nuovo nome host per accedere all'interfaccia utente Web di Unified Manager, è necessario generare un nuovo certificato di sicurezza.

Se si accede all'interfaccia utente Web utilizzando l'indirizzo IP del server anziché il nome host, non è necessario generare un nuovo certificato se si modifica il nome host. Tuttavia, è consigliabile aggiornare il certificato in modo che il nome host nel certificato corrisponda al nome host effettivo.

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

Il nuovo certificato non avrà effetto finché non verrà riavviata la macchina virtuale Unified Manager.

Passi

1. Genera un certificato di sicurezza HTTPS

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

2. Riavviare la macchina virtuale Unified Manager

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

Genera un certificato di sicurezza HTTPS

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

Prima di iniziare

È necessario disporre del ruolo di amministratore dell'applicazione.

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

Se non si ha accesso all'interfaccia utente Web di Unified Manager, è possibile rigenerare il certificato HTTPS con gli stessi valori utilizzando la console di manutenzione. Durante la rigenerazione dei certificati, è possibile definire la dimensione della chiave e la durata di validità della chiave. Se usi il `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 dimensione 2048 bit.

Passi

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

   Viene visualizzata la finestra di dialogo Rigenera certificato HTTPS.

3. Selezionare una delle seguenti opzioni a seconda di come si desidera generare il certificato:

Se lo desidera…	Fai questo…
Rigenera il certificato con i valori correnti	Fare clic sull'opzione **Rigenera utilizzando gli attributi del certificato corrente**.

Se lo desidera…	Fai questo…
Generare il certificato utilizzando valori diversi	Fare clic sull'opzione **Aggiorna gli attributi del certificato corrente**. Se non si immettono nuovi valori, i campi Nome comune e Nomi alternativi utilizzeranno i valori del certificato esistente. Il ``Nome comune' dovrebbe essere impostato sul nome di dominio completo (FQDN) dell'host. Gli altri campi non richiedono valori, ma è possibile immettere valori, ad esempio, per EMAIL, AZIENDA, REPARTO, Città, Stato e Paese se si desidera che tali valori vengano compilati nel certificato. È anche possibile selezionare tra le DIMENSIONI DELLA CHIAVE disponibili (l'algoritmo della chiave è "RSA") e il PERIODO DI VALIDITÀ. • I valori consentiti per la dimensione della chiave sono `2048` , `3072` E `4096` . • I periodi di validità vanno da un minimo di 1 giorno a un massimo di 36500 giorni. Sebbene sia consentito un periodo di validità di 36.500 giorni, si consiglia di utilizzare un periodo di validità non superiore a 397 giorni o 13 mesi. Poiché se selezioni un periodo di validità superiore a 397 giorni e intendi esportare una CSR per questo certificato e farla firmare da una CA nota, la validità del certificato firmato restituito dalla CA verrà ridotta a 397 giorni. • È possibile selezionare la casella di controllo "Escludi informazioni di identificazione locali (ad esempio localhost)" se si desidera rimuovere le informazioni di identificazione locali dal campo Nomi alternativi nel certificato. Quando questa casella di controllo è selezionata, nel campo Nomi alternativi verrà utilizzato solo ciò che inserisci nel campo. Se lasciato vuoto, il certificato risultante non avrà alcun campo Nomi alternativi.

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

Riavviare la macchina virtuale Unified Manager

È possibile riavviare la macchina virtuale dalla console di manutenzione di Unified Manager. È necessario 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 addetto alla manutenzione.

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

Passi

1. Accedere alla console di manutenzione.
2. Selezionare **Configurazione di sistema** > **Riavvia macchina virtuale**.

Modificare il nome host di Unified Manager sui sistemi Linux

A un certo punto, potresti voler modificare il nome host del computer 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 monitorati quando elenchi i tuoi computer Linux.

Prima di iniziare

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

È possibile utilizzare il nome host (o l'indirizzo IP host) per accedere all'interfaccia utente Web di Unified Manager. Se hai configurato un indirizzo IP statico per la tua rete durante la distribuzione, allora avrai designato un nome per l'host di rete. Se hai configurato la rete tramite DHCP, il nome host dovrebbe essere preso dal server DNS.

Indipendentemente da come è stato assegnato il nome host, se si modifica il nome host e si intende utilizzare il nuovo nome host per accedere all'interfaccia utente Web di Unified Manager, è necessario generare un nuovo certificato di sicurezza.

Se si accede all'interfaccia utente Web utilizzando l'indirizzo IP del server anziché il nome host, non è necessario generare un nuovo certificato se si modifica il nome host. Tuttavia, è consigliabile aggiornare il certificato in modo che il nome host nel certificato corrisponda al nome host effettivo. Il nuovo certificato non avrà effetto finché non verrà riavviato il computer Linux.

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

Passi

1. Accedi come utente root al sistema Unified Manager che desideri modificare.

2. Arrestare il software Unified Manager e il software MySQL associato immettendo il seguente comando:

   ```
   systemctl stop ocieau ocie mysqld
   ```

3. Cambia il nome host usando Linux `hostnamectl` comando:

   ```
   hostnamectl set-hostname new_FQDN
   ```

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

4. Rigenerare il certificato HTTPS per il server:

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

5. Riavviare il servizio di rete:

   ```
   systemctl restart NetworkManager.service
   ```

6. Dopo aver riavviato il servizio, verificare se il nuovo nome host è in grado di eseguire il ping su se stesso:

   ```
   ping new_hostname
   ```

   ```
   ping nuhost
   ```

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

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

   ```
   systemctl start mysqld ocie ocieau
   ```

Abilitare e disabilitare la gestione dell'archiviazione basata su policy

A partire da Unified Manager 9.7, è possibile eseguire il provisioning di carichi di lavoro di archiviazione (volumi e LUN) sui cluster ONTAP e gestire tali 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 quando applicata tramite Unified Manager è possibile eseguire il provisioning e gestire i carichi di lavoro su tutti i cluster monitorati dall'istanza di Unified Manager.

È necessario disporre del ruolo di amministratore dell'applicazione.

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

Se abilitata, 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**
Una pagina per creare policy di livello di servizio delle prestazioni	Disponibile da **Impostazioni** > **Criteri** > **Livelli di servizio delle prestazioni**
Una pagina per creare policy di efficienza di archiviazione delle prestazioni	Disponibile da **Impostazioni** > **Criteri** > **Efficienza di archiviazione**
Pannelli che descrivono le prestazioni del carico di lavoro e gli IOPS del carico di lavoro attuali	Disponibile dalla Dashboard

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

Passi

1. Nel riquadro di navigazione a sinistra, fare clic su **Generale** > **Impostazioni funzionalità**.
2. Nella pagina **Impostazioni funzionalità**, disabilita o abilita la gestione dell'archiviazione basata su criteri scegliendo una delle seguenti opzioni:

Se lo desidera…	Allora fai così…
Disabilitare la gestione dell'archiviazione basata su policy	Nel pannello **Gestione dell'archiviazione basata su criteri**, spostare il cursore verso sinistra.
Abilita la gestione dell'archiviazione basata su policy	Nel pannello **Gestione dell'archiviazione basata su criteri**, spostare il cursore verso destra.

Configurare il backup di Unified Manager

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

Per informazioni sui passaggi di configurazione, vedere"Gestione delle operazioni di backup e ripristino" .

Gestisci le impostazioni delle funzionalità

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

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

Per informazioni sul caricamento degli script, vedere"Abilitazione e disabilitazione del caricamento degli script" .

Abilita la gestione dell'archiviazione basata su policy

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

Attivando questa funzionalità, è possibile eseguire il provisioning dei carichi di lavoro di archiviazione sui cluster ONTAP aggiunti all'istanza di Active IQ Unified Manager e gestire tali carichi di lavoro in base ai livelli di servizio delle prestazioni assegnati e ai criteri di efficienza dell'archiviazione.

Puoi scegliere di attivare o disattivare questa funzionalità da **Generale** > **Impostazioni funzionalità** > **Gestione dell'archiviazione basata su criteri**. Attivando questa funzione, sono disponibili le seguenti pagine per il funzionamento e il monitoraggio:

- Provisioning (provisioning del carico di lavoro di archiviazione)
- **Politiche** > **Livelli di servizio prestazionali**
- **Politiche** > **Efficienza di archiviazione**
- Colonna Carichi di lavoro gestiti dal livello di servizio delle prestazioni nella pagina Configurazione cluster
- Pannello Prestazioni del carico di lavoro nella **Dashboard**

È possibile utilizzare le schermate per creare livelli di servizio delle prestazioni e policy di efficienza dell'archiviazione, nonché per eseguire il provisioning dei carichi di lavoro di archiviazione. È inoltre possibile monitorare i carichi di lavoro di archiviazione conformi ai livelli di servizio delle prestazioni assegnati, nonché quelli non conformi. Il pannello Prestazioni del carico di lavoro e IOPS del carico di lavoro consente inoltre 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 in essi forniti.

Dopo aver attivato questa funzionalità, è possibile eseguire le API REST di Unified Manager per svolgere alcune di queste funzioni dalla categoria **Barra dei menu** > **Pulsante Guida** > **Documentazione API** > **provider di archiviazione**. In alternativa, puoi immettere il nome host o l'indirizzo IP e l'URL per accedere alla pagina REST API nel formato https://<hostname>/docs/api/

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

Abilita API Gateway

La funzionalità API Gateway consente ad Active IQ Unified Manager di essere un unico piano di controllo da cui è possibile gestire più cluster ONTAP , senza doverli accedere singolarmente.

È possibile abilitare questa funzionalità dalle pagine di configurazione che vengono visualizzate al primo accesso a Unified Manager. In alternativa, puoi abilitare o disabilitare questa funzione da **Generale** > **Impostazioni funzione** > **API Gateway**.

Le API REST di Unified Manager sono diverse dalle API REST ONTAP e non tutte le funzionalità delle API

REST ONTAP possono essere sfruttate utilizzando le API REST di Unified Manager. Tuttavia, se si ha un requisito aziendale specifico di accesso alle API ONTAP per la gestione di funzionalità specifiche non esposte a Unified Manager, è possibile abilitare la funzionalità API Gateway ed eseguire le API ONTAP . Il gateway funge da proxy per incanalare le richieste API mantenendo l'intestazione e il corpo delle richieste nello stesso formato delle API ONTAP . È possibile utilizzare le credenziali di Unified Manager ed eseguire le API specifiche per accedere e gestire i cluster ONTAP senza dover passare le credenziali individuali del cluster. Unified Manager funge da singolo punto di gestione per l'esecuzione delle API sui cluster ONTAP gestiti dall'istanza di Unified Manager. La risposta restituita dalle API è la stessa della risposta restituita dalle rispettive API REST ONTAP eseguite direttamente da ONTAP.

Dopo aver abilitato questa funzionalità, è possibile eseguire le API REST di Unified Manager dalla **Barra dei menu** > **Pulsante Guida** > **Documentazione API** > categoria **gateway**. In alternativa, puoi immettere il nome host o l'indirizzo IP e l'URL per accedere alla pagina REST API nel formato `https://<hostname>/docs/api/`

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

Specificare il timeout di inattività

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

È possibile disattivare questa funzione o modificare il tempo da **Generale** > **Impostazioni funzione** > **Timeout di inattività**. Una volta attivata questa funzione, è necessario specificare il limite di tempo di inattività (in minuti) nel campo **DISCONNETTITI DOPO**, dopo il quale il sistema si disconnetterà automaticamente. Il valore predefinito è 4320 minuti (72 ore).

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

Abilita gli eventi del portale Active IQ

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

Abilitando 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 archiviazione monitorati. Questi eventi sono diversi dagli altri eventi di Unified Manager e identificano incidenti o rischi correlati alla configurazione del sistema, al cablaggio, alle best practice e ai problemi di disponibilità.

Puoi scegliere di attivare o disattivare questa funzione da **Generale** > **Impostazioni funzione** > **Eventi Active IQ *. Nei siti senza accesso alla rete esterna, è necessario caricare manualmente le regole da *Gestione archiviazione** > **Impostazione evento** > **Carica regole**.

Questa funzione è abilitata per impostazione predefinita. La disattivazione di questa funzione impedisce che gli eventi Active IQ vengano rilevati o visualizzati su Unified Manager. Se disabilitata, l'abilitazione di questa funzionalità consente a Unified Manager di ricevere gli eventi Active IQ su un cluster all'ora predefinita 00:15 per quel fuso orario del cluster.

Abilita e disabilita le impostazioni di sicurezza per la conformità

Utilizzando il pulsante **Personalizza** nel pannello **Dashboard di sicurezza** della pagina Impostazioni funzionalità, è possibile abilitare o disabilitare i parametri di sicurezza per il monitoraggio della conformità su Unified Manager.

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

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

I criteri di sicurezza per i cluster ONTAP , le VM di archiviazione e i volumi vengono valutati in base alle raccomandazioni definite in"Guida al rafforzamento della sicurezza per NetApp ONTAP 9" . Il pannello Sicurezza nella dashboard e la pagina Sicurezza mostrano lo stato di conformità di sicurezza predefinito dei cluster, delle VM di archiviazione e dei volumi. Vengono inoltre generati eventi di sicurezza e abilitate 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 per il monitoraggio della conformità in base al tuo ambiente ONTAP , segui questi passaggi:

Passi

1. Fare clic su **Generale > Impostazioni funzionalità > Dashboard di sicurezza > Personalizza**. Viene visualizzata la finestra pop-up **Personalizza impostazioni dashboard di sicurezza**.

   I parametri di conformità alla sicurezza abilitati o disabilitati possono influire direttamente sulle visualizzazioni di sicurezza predefinite, sui report e sui report pianificati nelle schermate Cluster e VM di archiviazione. Se hai caricato un report Excel da queste schermate prima di modificare i parametri di sicurezza, i report Excel scaricati potrebbero essere difettosi.

2. Per abilitare o disabilitare le impostazioni personalizzate per i cluster ONTAP , selezionare l'impostazione generale richiesta in **Cluster**. Per informazioni sulle opzioni per la personalizzazione della conformità del cluster, vedere"Categorie di conformità del cluster" .
3. Per abilitare o disabilitare le impostazioni personalizzate per le VM di archiviazione, selezionare l'impostazione generale richiesta in **VM di archiviazione**. Per informazioni sulle opzioni per la personalizzazione della conformità della VM di archiviazione, vedere"Categorie di conformità delle VM di archiviazione" .

Personalizza le impostazioni di AutoSupport e autenticazione

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

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

Abilita e disabilita il caricamento degli script

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 disattivare questa funzionalità.

Prima di iniziare

È necessario disporre del ruolo di amministratore dell'applicazione.

Passi

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

Se lo desidera…	Allora fai così…
Disabilita gli script	Nel pannello **Caricamento script**, spostare il cursore verso sinistra.
Abilita gli script	Nel pannello **Caricamento script**, spostare il cursore verso destra.

Aggiungi banner di accesso

L'aggiunta di un banner di accesso consente alla tua organizzazione di visualizzare qualsiasi informazione, ad esempio chi è autorizzato ad accedere al sistema e i termini e le condizioni d'uso durante l'accesso e la disconnessione.

Qualsiasi utente, come gli operatori o gli amministratori di storage, può visualizzare questo banner pop-up di accesso durante l'accesso, la disconnessione e il timeout della sessione.

Utilizzare la console di manutenzione

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

Quali funzionalità fornisce la console di manutenzione

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

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

- Risolvi eventuali problemi con il tuo dispositivo virtuale, soprattutto se l'interfaccia web di Unified Manager non è disponibile

- Aggiorna alle versioni più recenti di Unified Manager
- Genera pacchetti di supporto da inviare al supporto tecnico
- Configurare le impostazioni di rete
- Cambia la password dell'utente addetto alla manutenzione
- Connettiti a un fornitore di dati esterno per inviare statistiche sulle prestazioni
- Modificare la raccolta dati sulle prestazioni interna
- Ripristinare il database e le impostazioni di configurazione di Unified Manager da una versione precedentemente sottoposta a backup.

Cosa fa l'utente addetto alla manutenzione

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

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

Capacità diagnostiche dell'utente

Lo scopo dell'accesso diagnostico è consentire al supporto tecnico di assisterti nella risoluzione dei problemi e dovresti utilizzarlo solo quando indicato dal supporto tecnico.

L'utente diagnostico può eseguire comandi a livello di sistema operativo quando richiesto dal supporto tecnico, per scopi di risoluzione dei problemi.

Accedi alla console di manutenzione

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

Prima di iniziare

È necessario aver installato e configurato Unified Manager.

Dopo 15 minuti di inattività, la console di manutenzione effettua la disconnessione.

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

Fare un passo

1. Per accedere alla console di manutenzione, seguire questi passaggi:

Su questo sistema operativo…	Segui questi passaggi…
VMware	a. Utilizzando Secure Shell, connettersi all'indirizzo IP o al nome di dominio completo dell'appliance virtuale Unified Manager. b. Accedi alla console di manutenzione utilizzando il tuo nome utente e la tua password di manutenzione.
Linux	a. Utilizzando Secure Shell, connettersi all'indirizzo IP o al nome di dominio completo del sistema Unified Manager. b. Accedi al sistema con il nome utente di manutenzione (umadmin) e la password. c. Inserisci il comando `maintenance_console` e premere Invio.
Finestre	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 premere Invio.

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

Accedi alla console di manutenzione tramite la console vSphere VM

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

Prima di iniziare

- Devi essere l'utente addetto alla manutenzione.
- Per accedere alla console di manutenzione, l'appliance virtuale deve essere accesa.

Passi

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

   Dopo 15 minuti di inattività, la console di manutenzione effettua la disconnessione.

Menu della console di manutenzione

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

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

- Aggiorna Unified Manager (solo VMware)
- Configurazione di rete (solo VMware)
- Configurazione del sistema (solo VMware)
  a. Supporto/Diagnostica
  b. Reimposta il certificato del server
  c. Fornitore di dati esterno
  d. Backup Ripristino
  e. Configurazione dell'intervallo di polling delle prestazioni
  f. Disabilitare l'autenticazione SAML
  g. Visualizza/modifica le porte dell'applicazione
  h. Configurazione del registro di debug
  i. Controlla l'accesso alla porta MySQL 3306
  j. Uscita

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

Menu di configurazione di rete

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

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

Sono disponibili le seguenti opzioni di menu.

- **Visualizza impostazioni indirizzo IP**

  Visualizza le impostazioni di rete correnti per l'appliance virtuale, tra cui indirizzo IP, rete, indirizzo broadcast, netmask, gateway e server DNS.

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

  Consente di modificare qualsiasi impostazione di rete per l'appliance virtuale, tra cui l'indirizzo IP, la maschera di rete, il gateway o i server DNS. Se si modificano le impostazioni di rete da DHCP a rete statica tramite la console di manutenzione, non è possibile modificare il nome host. Per rendere effettive le modifiche, è necessario selezionare **Importa modifiche**.

- **Visualizza impostazioni di ricerca del nome di dominio**

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

- **Modifica le impostazioni di ricerca del nome di dominio**

  Consente di modificare i nomi di dominio che si desidera cercare durante la risoluzione dei nomi host. Per rendere effettive le modifiche, è necessario selezionare **Importa modifiche**.

- **Visualizza percorsi statici**

  Visualizza le rotte di rete statiche correnti.

- **Modifica percorsi statici**

  Consente di aggiungere o eliminare percorsi di rete statici. Per rendere effettive le modifiche, è necessario selezionare **Importa modifiche**.

  - **Aggiungi percorso**

    Consente di aggiungere una route statica.

  - **Elimina percorso**

    Consente di eliminare una route statica.

  - **Indietro**

    Ti riporta al **Menu principale**.

  - **Uscita**

    Esce dalla console di manutenzione.

- **Disabilita interfaccia di rete**

  Disabilita tutte le interfacce di rete disponibili. Se è disponibile una sola interfaccia di rete, non è possibile disattivarla. Per rendere effettive le modifiche, è necessario selezionare **Importa modifiche**.

- **Abilita interfaccia di rete**

  Abilita le interfacce di rete disponibili. Per rendere effettive le modifiche, è necessario selezionare **Importa modifiche**.

- **Applica modifiche**

  Applica tutte le modifiche apportate alle impostazioni di rete per l’appliance virtuale. È necessario selezionare questa opzione per rendere effettive le modifiche apportate, altrimenti le modifiche non verranno applicate.

- **Ping un host**

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

- **Ripristina le impostazioni predefinite**

  Ripristina tutte le impostazioni ai valori predefiniti di fabbrica. Per rendere effettive le modifiche, è

necessario selezionare **Importa modifiche**.

- **Indietro**

  Ti riporta al **Menu principale**.

- **Uscita**

  Esce dalla console di manutenzione.

Menu di configurazione del sistema

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

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

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, potrebbe essere necessario contattare l'assistenza tecnica.

- **Riavvia la macchina virtuale**

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

- **Spegnimento della macchina virtuale**

  Arresta la macchina virtuale, interrompendo tutti i servizi.

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

- **Cambia la password dell'utente <utente registrato>**

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

- **Aumenta la dimensione del disco dati**

  Aumenta la dimensione del disco dati (disco 3) nella macchina virtuale.

- **Aumenta la dimensione del disco di swap**

  Aumenta la dimensione del disco di swap (disco 2) nella macchina virtuale.

- **Cambia fuso orario**

  Modifica il fuso orario in base alla tua posizione.

- **Cambia server NTP**

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

- **Cambia servizio NTP**

  Passa tra `ntp` E `systemd-timesyncd` servizi.

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

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

- **Reimposta certificato server**

  Reimposta il certificato di sicurezza del server.

- **Cambia nome host**

  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.

Menu Supporto e Diagnostica

Il menu Supporto e diagnostica consente di generare un pacchetto di supporto da inviare al supporto tecnico per ricevere assistenza nella risoluzione dei problemi.

Sono disponibili le seguenti opzioni di menu:

- **Genera pacchetto di supporto leggero**

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

- **Genera pacchetto di supporto**

  Consente di creare un pacchetto di supporto completo (file 7-Zip) contenente informazioni diagnostiche nella directory home 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 Unified Manager, dati dettagliati sugli elementi interni del server Unified Manager e registri dettagliati normalmente non inclusi nei messaggi AutoSupport o nel bundle di supporto leggero.

Opzioni di menu aggiuntive

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

Sono disponibili le seguenti opzioni di menu:

- **Reimposta certificato server**

  Rigenera il certificato del server HTTPS.

  È possibile rigenerare il certificato del server nell'interfaccia utente grafica di Unified Manager facendo clic su **Generale** > **Certificati HTTPS** > **Rigenera certificato HTTPS**.

- **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 la configurazione SAML impedisce agli utenti di accedere all'interfaccia utente grafica di Unified Manager.

- **Fornitore di dati esterno**

  Fornisce opzioni per connettere Unified Manager a un fornitore di dati esterno. Dopo aver stabilito la connessione, i dati sulle prestazioni vengono inviati a un server esterno in modo che gli esperti delle prestazioni di archiviazione possano tracciare le metriche delle prestazioni utilizzando software di terze parti. Vengono visualizzate le seguenti opzioni:

  - **Visualizza configurazione server**: visualizza le impostazioni di connessione e configurazione correnti per un fornitore di dati esterno.
  - **Aggiungi/Modifica connessione server**: consente di immettere nuove impostazioni di connessione per un fornitore di dati esterno o di modificare le impostazioni esistenti.
  - **Modifica configurazione server**: consente di immettere nuove impostazioni di configurazione per un fornitore di dati esterno o di modificare le impostazioni esistenti.
  - **Elimina connessione al server**: elimina la connessione a un fornitore di dati esterno.

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

- **Backup e ripristino**

  Per informazioni, vedere gli argomenti sotto"Gestione delle operazioni di backup e ripristino" .

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

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

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

- **Visualizza/Modifica porte applicazione**

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

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

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

- **Uscita**

  Esce dal menu della console di manutenzione.

Cambiare la password dell'utente di manutenzione su Windows

È possibile modificare la password dell'utente addetto alla manutenzione di Unified Manager quando necessario.

Passi

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

   Viene visualizzata una pagina in cui viene richiesto il nome dell'utente di cui si desidera reimpostare la password.

2. Inserisci il nome utente e clicca su **Invia**.

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

3. Fare clic sul **link per reimpostare la password** nell'e-mail e definire la nuova password.
4. Torna all'interfaccia utente Web e accedi a Unified Manager utilizzando la nuova password.

Cambiare la password umadmin sui sistemi Linux

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

Prima di iniziare

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

Passi

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

   ```
   passwd umadmin
   ```

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

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

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

Prima di iniziare

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

> Ci sono alcune porte considerate non sicure quando si utilizzano i browser Mozilla Firefox o Google Chrome. Prima di assegnare un nuovo numero di porta per il traffico HTTP e HTTPS, verifica con il tuo browser. Selezionando una porta non sicura il sistema potrebbe risultare inaccessibile e in tal caso sarebbe necessario contattare l'assistenza clienti per risolvere il problema.

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

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

   Vengono visualizzati i prompt della console di manutenzione di Unified Manager.

2. Digitare il numero dell'opzione di menu denominata **Visualizza/Modifica porte applicazione**, quindi premere Invio.
3. Se richiesto, immettere nuovamente la password dell'utente addetto alla manutenzione.
4. Digitare i nuovi numeri di porta per le porte HTTP e HTTPS, quindi premere Invio.

   Lasciando vuoto il numero di porta si assegna la porta predefinita per il protocollo.

   Ti verrà chiesto se desideri modificare le porte e riavviare Unified Manager ora.

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

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

Aggiungere interfacce di rete

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

Prima di iniziare

È necessario aver aggiunto l'interfaccia di rete all'appliance virtuale tramite vSphere.

L'appliance virtuale deve essere accesa.

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

Passi

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

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

2. Accedere alla console di manutenzione.
3. Selezionare **Configurazione di rete** > **Abilita interfaccia di rete**.
4. Selezionare la nuova interfaccia di rete e premere **Invio**.

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

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

   Se si utilizza un'interfaccia statica o se non viene rilevato DHCP, verrà richiesto di immettere le impostazioni di rete.

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

7. Seleziona **Applica modifiche**.

   È necessario confermare le modifiche per aggiungere l'interfaccia di rete.

Aggiungere spazio su disco alla directory del database Unified Manager

La directory del database Unified Manager contiene tutti i dati sullo stato e sulle prestazioni raccolti dai sistemi ONTAP . In alcune circostanze potrebbe essere necessario aumentare le dimensioni della directory del database.

Ad esempio, la directory del database potrebbe riempirsi se Unified Manager raccoglie dati da un numero elevato di cluster, ognuno dei quali ha 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 dati aggiuntivi dai cluster dopo che la directory raggiunge il 95% di riempimento.

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

Aggiungere spazio alla directory dati dell'host Linux

Se hai assegnato spazio su disco insufficiente al `/opt/netapp/data` directory per supportare Unified Manager quando hai originariamente configurato l'host Linux e poi installato Unified Manager, puoi aggiungere spazio su disco dopo l'installazione aumentando lo spazio su disco su `/opt/netapp/data` elenco.

Prima di iniziare

È necessario disporre dell'accesso come utente root al computer Red Hat Enterprise Linux su cui è installato Unified Manager.

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

Passi

1. Accedi come utente root al computer Linux su cui desideri aggiungere spazio su disco.
2. Arrestare il servizio Unified Manager e il software MySQL associato nell'ordine mostrato:

   ```
   systemctl stop ocieau ocie mysqld
   ```

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

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

5. Se SE Linux è abilitato:

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

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

      Il sistema restituisce una conferma simile alla seguente:

   ```
   echo $se_type
   mysqld_db_t
   ```

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

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

6. Rimuovere il contenuto del `/opt/netapp/data` elenco:

   a. `cd /opt/netapp/data`

   b. `rm -rf *`

7. Espandi le dimensioni del `/opt/netapp/data` directory a un minimo di 150 GB tramite comandi LVM o aggiungendo dischi extra.

   > Se hai creato `/opt/netapp/data` da un disco, allora non dovresti provare a montarlo `/opt/netapp/data` come quota NFS o CIFS. Perché, in questo caso, se si tenta di espandere lo spazio su disco, alcuni comandi LVM, come `resize` E `extend` potrebbe non funzionare come previsto.

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

invariati:

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

Il sistema restituisce una conferma simile alla seguente:

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

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

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

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

      Il sistema restituisce una conferma simile alla seguente:

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

10. Eliminare il file abc in modo che questo file estraneo non causi un errore del database in futuro.
11. Copia il contenuto dai dati di backup all'espanso `/opt/netapp/data` elenco:

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

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

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

13. Avviare il servizio MySQL:

```
systemctl start mysqld
```

14. Dopo aver avviato il servizio MySQL, avviare i servizi ocie e ocieau nell'ordine mostrato:

```
systemctl start ocie ocieau
```

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

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

Aggiungere spazio al disco dati della macchina virtuale VMware

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

Prima di iniziare

- È necessario avere accesso a vSphere Client.

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

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

Passi

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

   In alcuni rari casi la distribuzione di Unified Manager utilizza “Hard Disk 2” per il disco dati anziché “Hard Disk 3”. Se questo si è verificato nella distribuzione, aumentare lo spazio del disco più grande. Il disco dati avrà sempre più spazio rispetto all’altro disco.

2. Nel client vSphere, seleziona la macchina virtuale Unified Manager, quindi seleziona la scheda **Console**.
3. Fare clic nella finestra della console, quindi accedere alla console di manutenzione utilizzando il nome utente e la password.
4. Nel menu principale, immettere il numero per l’opzione **Configurazione del sistema**.
5. Nel menu Configurazione di sistema, immettere il numero per l’opzione **Aumenta dimensione disco dati**.

Aggiungere spazio all’unità logica del server Microsoft Windows

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

Prima di iniziare

È necessario disporre dei privilegi di amministratore di Windows.

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

Passi

1. Accedi come amministratore al server Windows su cui desideri aggiungere spazio su disco.
2. Segui il passaggio che corrisponde al metodo che vuoi utilizzare per aggiungere più spazio:

Opzione	Descrizione
Su un server fisico, aggiungere capacità all’unità logica su cui è installato il server Unified Manager.	Seguire i passaggi indicati nell’argomento Microsoft: "Estendi un volume di base"
Su un server fisico, aggiungere un’unità disco rigido.	Seguire i passaggi indicati nell’argomento Microsoft: "Aggiunta di unità disco rigido"
Su una macchina virtuale, aumentare le dimensioni di una partizione del disco.	Seguire i passaggi descritti nell’argomento VMware: "Aumento delle dimensioni di una partizione del disco"

Gestisci l’accesso degli utenti

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

Aggiungi utenti

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

Prima di iniziare

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

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

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

Passi

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

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

4. Fare clic su **Aggiungi**.

Creare un utente del database

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

Prima di iniziare

È necessario disporre del ruolo di amministratore dell'applicazione.

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

Passi

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

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

6. Fare clic su **Aggiungi**.

Modifica le impostazioni utente

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

Prima di iniziare

È necessario disporre del ruolo di amministratore dell'applicazione.

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

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

Passi

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

Visualizza utenti

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

Prima di iniziare

È necessario disporre del ruolo di amministratore dell'applicazione.

Fare un passo

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

Elimina utenti o gruppi

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

Prima di iniziare

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

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

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

Passi

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

Che cosa è RBAC

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

Cosa fa il controllo degli accessi basato sui ruoli

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

Il server di gestione utilizza RBAC per l'accesso degli utenti e le autorizzazioni dei ruoli. Se non hai modificato le impostazioni predefinite del server di gestione per l'accesso degli utenti amministrativi, non è necessario effettuare l'accesso per visualizzarle.

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

Definizioni dei tipi di utente

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

I tipi di utenti di Unified Manager sono i seguenti:

- **Utente addetto alla manutenzione**

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

- **Utente locale**

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

- **Gruppo remoto**

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

- **Utente remoto**

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

- **Utente del database**

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

Definizioni dei ruoli utente

L'utente addetto alla manutenzione o l'amministratore dell'applicazione assegna un ruolo a ogni utente. Ogni ruolo contiene determinati privilegi. L'ambito delle attività che puoi svolgere in Unified Manager dipende dal ruolo che ti è stato assegnato e dai privilegi che il ruolo contiene.

Unified Manager include i seguenti ruoli utente predefiniti:

- **Operatore**

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

- **Amministratore di archiviazione**

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

- **Amministratore dell'applicazione**

  Configura le impostazioni non correlate alla gestione dell'archiviazione. Questo ruolo consente la gestione degli utenti, dei certificati di sicurezza, dell'accesso al database e delle opzioni amministrative, tra cui autenticazione, SMTP, networking e AutoSupport.

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

- **Schema di integrazione**

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

- **Schema del report**

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

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

Ruoli e capacità degli utenti di Unified Manager

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

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

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

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

Gestisci le impostazioni di autenticazione SAML

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

Si noti che solo gli utenti remoti avranno accesso all'interfaccia utente grafica di Unified Manager dopo aver

abilitato l'autenticazione SAML. Gli utenti locali e gli utenti di manutenzione non potranno accedere all'interfaccia utente. Questa configurazione non ha alcun impatto sugli utenti che accedono alla console di manutenzione.

Requisiti del fornitore di identità

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

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

Standard di crittografia supportati

- Standard di crittografia avanzata (AES): AES-128 e AES-256
- Algoritmo hash sicuro (SHA): SHA-1 e SHA-256

Fornitori di identità convalidati

- Shibboleth
- Servizi federativi di Active Directory (ADFS)

Requisiti di configurazione ADFS

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

Regola di rivendicazione	Valore
Nome account SAM	ID nome
Nome account SAM	urna:oid:0.9.2342.19200300.100.1.1
Gruppi di token — Nome non qualificato	urna:oid:1.3.6.1.4.1.5923.1.5.1.1

- È necessario impostare il metodo di autenticazione su "Autenticazione tramite moduli" altrimenti gli utenti potrebbero ricevere un errore quando escono da Unified Manager. Segui questi passaggi:
  a. Aprire la console di gestione ADFS.
  b. Fare clic sulla cartella Criteri di autenticazione nella vista ad albero a sinistra.
  c. In Azioni sulla destra, fare clic su Modifica criterio di autenticazione primaria globale.
  d. Impostare il metodo di autenticazione Intranet su "Autenticazione basata su moduli" anziché sul valore predefinito "Autenticazione Windows".
- In alcuni casi l'accesso tramite IdP viene rifiutato quando il certificato di sicurezza di Unified Manager è firmato da una CA. Esistono due soluzioni alternative per risolvere questo problema:
  - Seguire le istruzioni identificate nel collegamento per disattivare il controllo di revoca sul server ADFS

per la parte affidabile associata al certificato CA concatenato:

"Disabilita il controllo di revoca per trust della parte affidabile"

- Fare in modo 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 sfasamento 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 fallirà.

Abilita l'autenticazione SAML

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

Prima di iniziare

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

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

Solo gli utenti remoti avranno accesso all'interfaccia utente grafica di Unified Manager dopo aver abilitato l'autenticazione SAML. Gli utenti locali e gli utenti di manutenzione non potranno accedere all'interfaccia utente. Questa configurazione non ha alcun impatto sugli utenti che accedono alla console di manutenzione, ai comandi di Unified Manager o alle ZAPI.

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

Passi

1. Nel riquadro di navigazione a sinistra, fare clic su **Generale** > **Autenticazione SAML**.
2. Selezionare la casella di controllo **Abilita autenticazione SAML**.

   Vengono visualizzati i campi necessari per configurare la connessione IdP.

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

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

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

   È possibile configurare il server IdP con queste informazioni in questo momento.

5. Fare clic su **Salva**.

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

6. Fare clic su **Conferma e disconnetti** e Unified Manager verrà riavviato.

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

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

Quando si utilizza ADFS come provider di identità, l'interfaccia utente grafica di Unified Manager non rispetta il timeout di ADFS e continuerà a funzionare finché non verrà raggiunto il timeout della sessione di Unified Manager. È possibile modificare il timeout della sessione GUI facendo clic su **Generale** > **Impostazioni funzionalità** > **Timeout di inattività**.

Cambia il provider di identità utilizzato per l'autenticazione SAML

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

Prima di iniziare

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

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

Passi

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

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

3. Copiare l'URI dei metadati di Unified Manager oppure salvare i metadati in un file di testo XML.
4. Fare clic su **Salva configurazione**.

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

5. Fare clic su **OK**.

Accedi al nuovo IdP e inserisci l'URI e i metadati del server Unified Manager 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 IdP anziché nella vecchia pagina di accesso IdP.

Aggiorna le impostazioni di autenticazione SAML dopo la modifica del certificato di sicurezza di Unified Manager

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

Dopo aver modificato il certificato di sicurezza e riavviato il server Unified Manager, l'autenticazione SAML non funzionerà e gli utenti non saranno in grado di accedere all'interfaccia grafica di Unified Manager. È necessario aggiornare le impostazioni di autenticazione SAML sia sul server IdP che sul server Unified Manager per riabilitare l'accesso all'interfaccia utente.

Passi

1. Accedi alla console di manutenzione.
2. Nel **Menu principale**, immettere il numero per l'opzione **Disabilita autenticazione SAML**.

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

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

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

7. Fare clic su **Conferma e disconnetti** e Unified Manager verrà riavviato.
8. Accedi al tuo server IdP e inserisci l'URI e i metadati del server Unified Manager per completare la configurazione.

Fornitore di identità	Fasi di configurazione
ADFS	a. Eliminare la voce di trust della relying party esistente nell'interfaccia utente grafica di gestione ADFS. b. Aggiungere una nuova voce di trust della parte affidabile utilizzando `saml_sp_metadata.xml` dal server Unified Manager aggiornato. c. Definire le tre regole di claim necessarie affinché Unified Manager analizzi le risposte SAML di ADFS per questa voce di trust della relying party. d. Riavviare il servizio ADFS di Windows.
Shibboleth	a. Aggiorna il nuovo FQDN del server Unified Manager in `attribute-filter.xml` E `relying-party.xml` file. b. Riavviare il server web Apache Tomcat e attendere che la porta 8005 torni online.

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

Disabilitare l'autenticazione SAML

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

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

È anche possibile disabilitare l'autenticazione SAML tramite la console di manutenzione di Unified Manager se non si ha accesso all'interfaccia utente grafica.

Unified Manager viene riavviato automaticamente dopo aver disabilitato l'autenticazione SAML.

Passi

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

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

4. Fare clic su **Conferma e disconnetti** e Unified Manager verrà riavviato.

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

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

Disabilitare l'autenticazione SAML dalla console di manutenzione

Potrebbe essere necessario disabilitare l'autenticazione SAML dalla console di manutenzione quando non è possibile accedere all'interfaccia utente grafica di Unified Manager. Ciò potrebbe verificarsi in caso di configurazione errata o se l'IdP non è accessibile.

Prima di iniziare

È necessario avere accesso alla console di manutenzione come utente addetto alla 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, gli utenti locali e gli utenti di manutenzione potranno accedere all'interfaccia utente grafica.

È anche possibile disabilitare l'autenticazione SAML dalla pagina Configurazione/Autenticazione nell'interfaccia utente.

Unified Manager viene riavviato automaticamente dopo aver disabilitato l'autenticazione SAML.

Passi

1. Accedi alla console di manutenzione.
2. Nel **Menu principale**, immettere il numero per l'opzione **Disabilita autenticazione SAML**.

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

3. Digitare **y**, quindi premere Invio; Unified Manager verrà riavviato.

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

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

Pagina di autenticazione SAML

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

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

Dopo aver configurato l'autenticazione remota e gli utenti remoti, è possibile 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.

  URI di esempio ADFS:

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

  Esempio di URI di Shibboleth:

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

- **Metadati IdP**

  Metadati IdP in formato XML.

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

- **Sistema host (FQDN)**

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

- **URI host**

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

- **Metadati host**

  Metadati del sistema host in formato XML.

Gestisci l'autenticazione

È possibile abilitare l'autenticazione tramite LDAP o Active Directory sul server Unified Manager e configurarlo in modo che funzioni con i server per autenticare gli utenti remoti.

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

Modifica i server di autenticazione

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

Prima di iniziare

È necessario disporre del ruolo di amministratore dell'applicazione.

Passi

1. Nel riquadro di navigazione a sinistra, fare clic su **Generale** > **Autenticazione remota**.
2. Selezionare la casella **Disabilita ricerca gruppi annidati**.
3. Nell'area **Server di autenticazione**, seleziona il server di autenticazione che desideri modificare, quindi fai clic su **Modifica**.
4. Nella finestra di dialogo **Modifica server di autenticazione**, modificare i dettagli della porta.
5. Fare clic su **Salva**.

Elimina i server di autenticazione

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

Prima di iniziare

È necessario disporre del ruolo di amministratore dell'applicazione.

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

Passi

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

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

Autenticazione con Active Directory o OpenLDAP

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

È possibile utilizzare uno dei seguenti servizi di autenticazione predefiniti oppure specificare un proprio servizio di autenticazione:

- Microsoft Active Directory

  Non è possibile utilizzare Microsoft Lightweight Directory Services.

- OpenLDAP

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

autenticazione configurato.

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

Registrazione di controllo

È possibile rilevare se i registri di controllo sono stati compromessi utilizzando i registri di controllo. Tutte le attività svolte da un utente vengono monitorate e registrate nei registri di controllo. Gli audit vengono eseguiti per tutte le funzionalità dell'interfaccia utente e delle API esposte pubblicamente di Active IQ Unified Manager.

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

Stato	Descrizione
ATTIVO	File in cui vengono attualmente registrati i log.
NORMALE	File inattivo, compresso e memorizzato nel sistema.
MANOMESTRI	File compromesso da un utente che lo ha modificato manualmente.
ELIMINA_MANUALE	File eliminato da un utente autorizzato.
ROLLOVER_ELIMINA	File eliminato a causa del roll-off basato sulla politica di configurazione rolling.
ELIMINAZIONE_INATTESA	File eliminato per motivi sconosciuti.

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

- Configurare
- Eliminare
- Scaricamento

Il pulsante **ELIMINA** consente di eliminare uno qualsiasi dei registri di controllo elencati nella vista Registri di controllo. È possibile eliminare un registro di controllo e, facoltativamente, specificare un motivo per eliminare il file, che aiuterà in futuro a determinare un'eliminazione valida. Nella colonna MOTIVO è elencato il motivo insieme al nome dell'utente che ha eseguito l'operazione di eliminazione.

L'eliminazione di un file di registro comporterà l'eliminazione del file dal sistema, ma la voce nella tabella del database non verrà eliminata.

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

I file di registro di controllo vengono archiviati periodicamente e salvati nel database per riferimento. Prima dell'archiviazione, i registri di controllo 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 registro di controllo archiviati che quelli attivi. Tuttavia, quando viene generato un pacchetto di supporto leggero, include solo i log di controllo attivi. I registri di controllo archiviati non sono inclusi.

Configurare i registri di controllo

È possibile utilizzare il pulsante **Configura** nella sezione Registri di controllo per configurare la policy di rotazione per i file dei registri di controllo e per abilitare anche la registrazione remota per i registri di controllo.

È possibile impostare i valori in **DIMENSIONE MASSIMA FILE** e **GIORNI DI CONSERVAZIONE REGISTRO DI CONTROLLO** in base alla quantità e alla frequenza desiderate dei dati che si desidera archiviare nel sistema. Il valore nel campo **DIMENSIONE TOTALE REGISTRO DI CONTROLLO** è la dimensione totale dei dati del registro di controllo presenti nel sistema. La politica di rollover è determinata dai valori nei campi **GIORNI DI CONSERVAZIONE DEL REGISTRO DI CONTROLLO**, **DIMENSIONE MASSIMA DEL FILE** e **DIMENSIONE TOTALE DEL REGISTRO DI CONTROLLO**. Quando la dimensione del backup del registro di controllo raggiunge il valore configurato in **DIMENSIONE TOTALE REGISTRO DI CONTROLLO**, il file archiviato per primo viene eliminato. Ciò significa che il file più vecchio viene eliminato. Tuttavia, la voce del file continua a essere disponibile nel database ed è contrassegnata come "Eliminazione rollover". Il valore **GIORNI DI CONSERVAZIONE DEL REGISTRO DI CONTROLLO** indica il numero di giorni in cui vengono conservati i file del registro di controllo. Tutti i file più vecchi del valore impostato in questo campo vengono riportati al valore precedente.

Passi

1. Fare clic su **Registri di controllo** > > **Configura**.
2. Immettere i valori in **DIMENSIONE MASSIMA DEL FILE**, **DIMENSIONE TOTALE DEL REGISTRO DI CONTROLLO** e **GIORNI DI CONSERVAZIONE DEL REGISTRO DI CONTROLLO**.

   Se si desidera abilitare la registrazione remota, è necessario selezionare **Abilita registrazione remota**. /// 2025-6-11, OTHERDOC-133

Abilita la registrazione remota dei log di controllo

È possibile selezionare la casella di controllo **Abilita registrazione remota** nella finestra di dialogo Configura registri di controllo per abilitare la registrazione di controllo remota. È possibile utilizzare questa funzionalità per trasferire i registri di controllo a un server Syslog remoto. Ciò ti consentirà di gestire i registri di controllo quando ci sono vincoli di spazio.

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

Passi

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

   Vengono visualizzati campi aggiuntivi per configurare la registrazione remota.

2. Inserisci **HOSTNAME** e **PORT** del server remoto a cui vuoi connetterti.
3. Nel campo **CERTIFICATO CA DEL SERVER**, fare clic su **SFOGLIA** per selezionare un certificato pubblico del server di destinazione.

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

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

   Per questi campi i valori devono essere espressi in millisecondi.

5. Selezionare il formato Syslog e la versione del protocollo TLS richiesti nei campi **FORMATO** e **PROTOCOLLO**.
6. Selezionare la casella di controllo **Abilita autenticazione client** se il server Syslog di destinazione richiede l'autenticazione basata su certificato.

   Sarà necessario scaricare il certificato di autenticazione client e caricarlo sul server Syslog prima di salvare la configurazione del registro di controllo, altrimenti la connessione non riuscirà. A seconda del tipo di server Syslog, potrebbe essere necessario creare un hash del certificato di autenticazione client.

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

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

   Verrai reindirizzato alla pagina Registri di controllo.

> Il valore **Timeout connessione** può influire sulla configurazione. Se la configurazione impiega più tempo per rispondere rispetto al valore definito, potrebbe verificarsi un errore di configurazione a causa di un errore di connessione. Per stabilire una connessione riuscita, aumentare il valore **Timeout connessione** e riprovare la configurazione.

Pagina di autenticazione remota

È possibile utilizzare 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 all'interfaccia utente Web di Unified Manager.

È necessario disporre del ruolo di Amministratore dell'applicazione o Amministratore dell'archiviazione.

Dopo aver selezionato la casella di controllo Abilita autenticazione remota, è possibile abilitare l'autenticazione remota tramite un server di autenticazione.

- **Servizio di autenticazione**

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

- **Directory attiva**
  - 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 nome di dominio 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 annidati. Per impostazione predefinita questa opzione è disabilitata. Se si utilizza Active Directory, è possibile velocizzare l'autenticazione disabilitando il supporto per i gruppi nidificati.

  - Utilizza una connessione sicura

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

- **OpenLDAP**
  - Associa nome distinto

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

  - Password di associazione

    Specifica la password per accedere al server di autenticazione.

  - Nome distinto di base

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

  - Utilizza una connessione sicura

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

- **Altri**
  - Associa nome distinto

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

- Password di associazione

  Specifica la password per accedere al server di autenticazione.

- Nome distinto di base

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

- Versione del protocollo

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

- Attributo nome utente

  Specifica il nome dell'attributo nel server di autenticazione che contiene i nomi di accesso utente da autenticare tramite il 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 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 annidati. Per impostazione predefinita questa opzione è disabilitata. Se si utilizza Active Directory, è possibile velocizzare l'autenticazione disabilitando il supporto per i gruppi nidificati.

- Membro

  Specifica il nome dell'attributo utilizzato dal server di autenticazione 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 di oggetti di gruppo

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

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

- Utilizza una connessione sicura

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

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

Area server di autenticazione

L'area Server di autenticazione visualizza i server di autenticazione con cui il server di gestione comunica per trovare e autenticare gli utenti remoti. Le credenziali per gli utenti o i gruppi remoti sono gestite dal server di autenticazione.

- **Pulsanti di comando**

  Consente di aggiungere, modificare o eliminare server di autenticazione.

  - Aggiungere

    Consente di aggiungere un server di autenticazione.

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

  - Modificare

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

  - Eliminare

    Elimina i server di autenticazione selezionati.

- **Nome o indirizzo IP**

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

- **Porta**

  Visualizza il numero di porta del server di autenticazione.

- **Test di autenticazione**

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

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

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

Gestire i certificati di sicurezza

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

Visualizza il certificato di sicurezza HTTPS

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

Prima di iniziare

È necessario disporre del ruolo di Operatore, Amministratore dell'applicazione o Amministratore dell'archiviazione.

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

Fare un passo

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

   Il certificato HTTPS viene visualizzato nella parte superiore della pagina

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

Scarica una richiesta di firma del certificato HTTPS

È possibile scaricare una richiesta di firma della certificazione per l'attuale certificato di sicurezza HTTPS, in modo da poter fornire il file a un'autorità di certificazione per la firma. Un certificato firmato da una CA aiuta a prevenire gli attacchi man-in-the-middle e offre una migliore protezione di sicurezza rispetto a un certificato autofirmato.

Prima di iniziare

È necessario disporre del ruolo di amministratore dell'applicazione.

Passi

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

È possibile fornire il file a un'autorità di certificazione affinché lo firmi e quindi installare il certificato firmato.

Installa un certificato HTTPS firmato e restituito da una CA

È possibile 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 una CA

aiuta a prevenire gli attacchi man-in-the-middle e fornisce una migliore protezione di sicurezza rispetto a un certificato autofirmato.

*Cosa. Prima di iniziare

Devi aver completato le seguenti azioni:

- Ho scaricato il file di richiesta di firma del certificato e l'ho fatto firmare da un'autorità di certificazione
- Salvata la catena di certificati in formato PEM
- Inclusi tutti i certificati nella catena, dal certificato del server Unified Manager al certificato di firma radice, inclusi tutti i certificati intermedi presenti

È necessario disporre del ruolo di amministratore dell'applicazione.

Se la validità del certificato per il quale è stato creato un CSR è superiore a 397 giorni, la validità verrà ridotta a 397 giorni dalla CA prima di firmare e restituire il certificato

Passi

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

   Per informazioni, vedere"Installazione di un certificato HTTPS generato tramite 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-----
```

Installa un certificato HTTPS generato utilizzando strumenti esterni

È possibile installare certificati autofirmati o firmati da una CA e generati tramite uno strumento esterno come OpenSSL, BoringSSL, LetsEncrypt.

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

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

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

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

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

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

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

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

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

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

Controlli durante il caricamento di certificati generati esternamente

Il sistema esegue controlli durante il caricamento di un certificato generato tramite strumenti esterni. Se uno qualsiasi dei controlli fallisce, il certificato viene rifiutato. Sono incluse anche le convalide per i certificati generati dal CSR all'interno del prodotto e per i certificati generati tramite strumenti esterni.

- La chiave privata nell'input viene convalidata rispetto al certificato host nell'input.
- Il nome comune (CN) nel certificato host viene confrontato con l'FQDN dell'host.
- Il nome comune (CN) del certificato host non deve essere vuoto e non deve essere impostato su localhost.
- La data di inizio della validità del certificato non deve essere nel futuro e la data di scadenza della validità del certificato non deve essere nel passato.
- Se esiste una CA intermedia o una CA, la data di inizio validità del certificato non deve essere futura e la data di scadenza della validità non deve essere passata.

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

Esempio 1

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

Esempio 2

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

Esempio 3

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

Se l'installazione del certificato non riesce, consultare l'articolo della Knowledge Base (KB):https://kb.netapp.com/mgmt/AIQUM/AIQUM_fails_to_install_externally_generated_certificate["ActiveIQ Unified Manager non riesce a installare un certificato generato esternamente"^]

Descrizioni delle pagine per la gestione dei certificati

È possibile utilizzare la pagina Certificato HTTPS per visualizzare i certificati di sicurezza correnti e per generare nuovi certificati HTTPS.

Pagina del certificato HTTPS

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 chiede di salvare il file <hostname>.csr in modo da poterlo fornire a un'autorità di certificazione per la firma.

- **Installa il certificato HTTPS**

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

- **Rigenera il certificato HTTPS**

  Consente di generare un nuovo certificato HTTPS autofirmato, che sostituisce l'attuale certificato di sicurezza. Il nuovo certificato sarà effettivo dopo il riavvio di Unified Manager.

Finestra di dialogo Rigenera certificato HTTPS

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

Le informazioni attuali sul certificato vengono visualizzate in questa pagina.

Le selezioni “Rigenera utilizzando gli attributi del certificato corrente” e “Aggiorna gli attributi del certificato corrente” consentono di rigenerare il certificato con le informazioni correnti o di generare un certificato con nuove informazioni.

- **Nome comune**

  Necessario. Il nome di dominio completamente qualificato (FQDN) che desideri proteggere.

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

- **E-mail**

  Opzionale. Un indirizzo email per contattare la tua organizzazione; in genere l’indirizzo email dell’amministratore del certificato o del reparto IT.

- **Azienda**

  Opzionale. Solitamente è il nome della società.

- **Dipartimento**

  Opzionale. Il nome del reparto della tua azienda.

- **Città**

  Opzionale. La sede della tua azienda in città.

- **Stato**

  Opzionale. La sede della tua azienda, non in forma abbreviata, nello stato o nella provincia.

- **Paese**

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

- **Nomi alternativi**

  Necessario. Nomi di dominio aggiuntivi, non primari, che possono essere utilizzati per accedere a questo server oltre all’indirizzo localhost o ad altri indirizzi di rete esistenti. Separare ogni nome alternativo con una virgola.

  Selezionare la casella di controllo "Escludi informazioni di identificazione locali (ad esempio localhost)" se si desidera rimuovere le informazioni di identificazione locali dal campo Nomi alternativi nel certificato. Quando questa casella di controllo è selezionata, nel campo Nomi alternativi verrà utilizzato solo ciò che inserisci nel campo. Se lasciato vuoto, il certificato risultante non avrà alcun campo Nomi alternativi.

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

  L'algoritmo chiave è impostato su RSA. È possibile 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 397 giorni. Se hai effettuato l'aggiornamento da una versione precedente, potresti notare che la validità del certificato precedente è rimasta invariata.

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

Informazioni sul copyright

Informazioni sul marchio commerciale