Eseguire attività amministrative e di configurazione

Active IQ Unified Manager 9.9

NetApp
April 05, 2024

Sommario

Eseguire attività amministrative e di configurazione

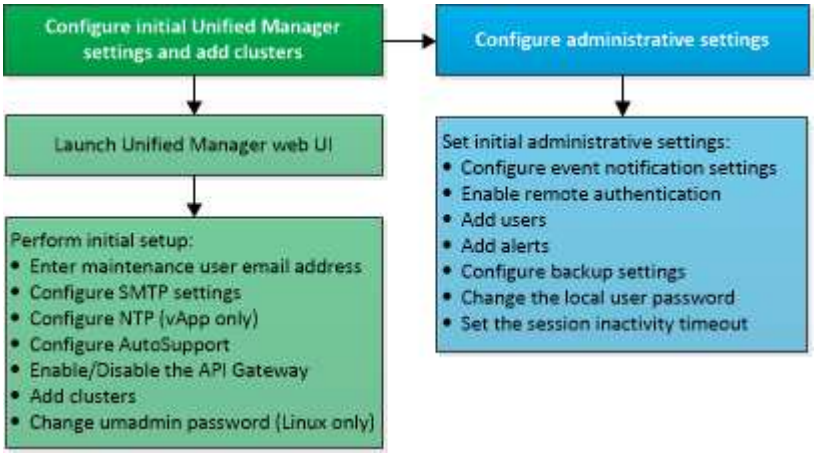
Configurazione di Active IQ Unified Manager

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

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

Panoramica della sequenza di configurazione

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



Accesso all'interfaccia utente Web di Unified Manager

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

Prima di iniziare

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

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

Fasi

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

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

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

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

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

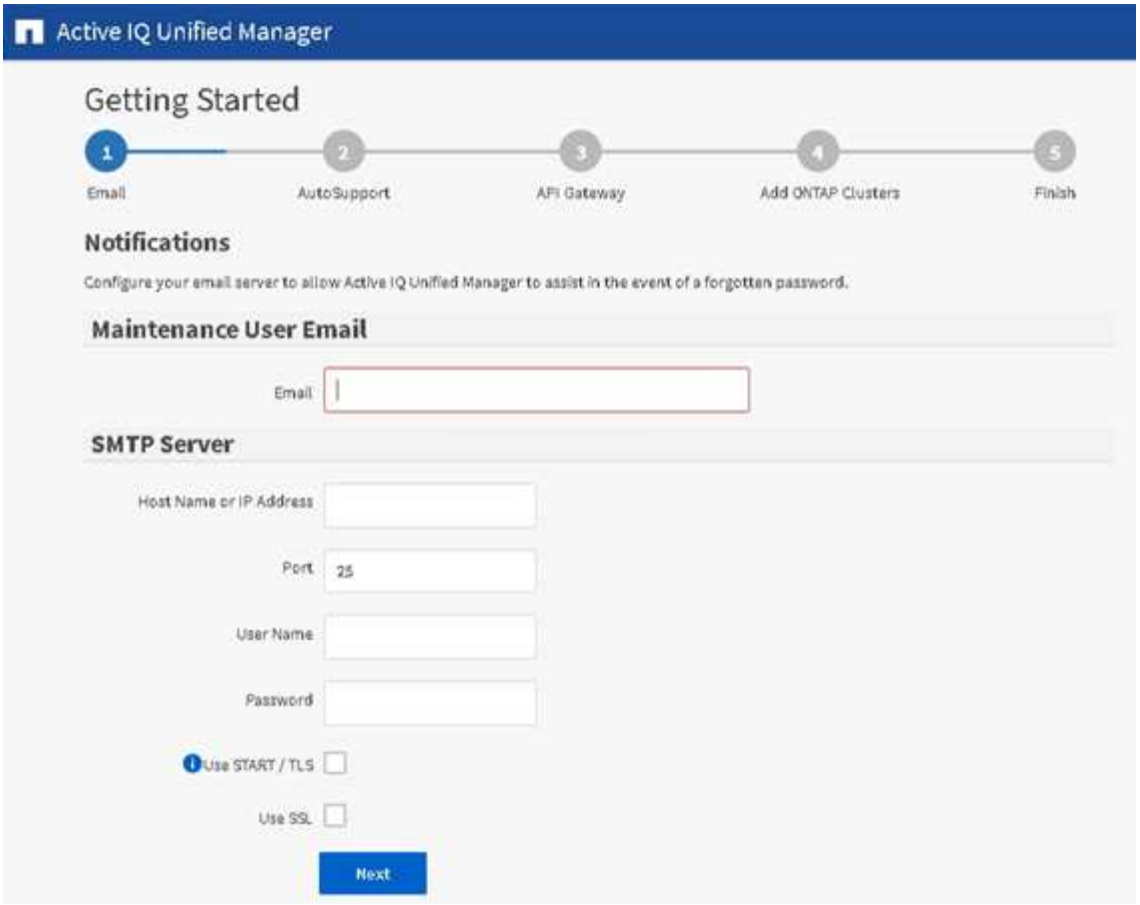
Prima di iniziare

È necessario aver eseguito le seguenti operazioni:

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

A proposito di questa attività

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



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

Fasi

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

   Se è necessario designare un proxy per fornire l'accesso a Internet per inviare contenuti AutoSupport o se si desidera disattivare AutoSupport, utilizzare l'opzione **Generale** > **AutoSupport** dall'interfaccia utente Web.

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

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

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

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

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

Risultati

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

Aggiunta di cluster

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

Prima di iniziare

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

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

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

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

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

  - Il numero di porta per la connessione al cluster utilizzando il protocollo HTTPS (generalmente la porta 443).
  - Si dispone dei certificati richiesti. Sono necessari due tipi di certificati:

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

Certificati client: Utilizzati per l'autenticazione. Per aggiungere un cluster è necessario un certificato valido. Non è possibile aggiungere un cluster a Unified Manager con un certificato scaduto e, se il certificato client è già scaduto, è necessario rigenerarlo prima di aggiungere il cluster. Tuttavia, se il certificato scade per un cluster già aggiunto e viene utilizzato da Unified Manager, la messaggistica EMS continua a funzionare con il certificato scaduto. Non è necessario rigenerare il certificato client.

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

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

A proposito di questa attività

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

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

Fasi

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

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

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

   Unified Manager controlla il certificato solo quando il cluster viene aggiunto inizialmente. Unified Manager non controlla il certificato per ogni chiamata API a ONTAP.

Risultati

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

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

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

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

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

Prima di iniziare

È necessario disporre del ruolo di amministratore dell'applicazione.

A proposito di questa attività

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

Fasi

1. Configurare le impostazioni di notifica degli eventi

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

2. Abilitare l'autenticazione remota

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

3. Aggiungere server di autenticazione

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

4. Aggiungere utenti

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

5. Aggiungere avvisi

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

Configurazione delle impostazioni di notifica degli eventi

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

Prima di iniziare

È necessario disporre delle seguenti informazioni:

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

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

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

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

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

Fasi

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

   Note:

   - Se l'indirizzo da è pre-compilato con l'indirizzo "ActiveIQUnifiedManager@localhost.com", devi cambiarlo in un indirizzo e-mail reale e funzionante per assicurarti che tutte le notifiche e-mail siano inviate correttamente.
   - Se il nome host del server SMTP non può essere risolto, è possibile specificare l'indirizzo IP (IPv4 o IPv6) del server SMTP invece del nome host.

Attivazione dell'autenticazione remota

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

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 come SSSD (System Security Services Daemon) o NSLCD (Name Service LDAP Caching Daemon).

A proposito di questa attività

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

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

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

Fasi

1. Nel riquadro di spostamento di sinistra, fare clic su **Generale** > **autenticazione remota**.
2. Selezionare la casella **Enable remote Authentication…** (attiva autenticazione remota…).
3. Nel campo **Servizio di autenticazione**, selezionare il tipo di servizio e configurare il servizio di autenticazione.

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

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

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

1. Aggiungere server di autenticazione e verificare l'autenticazione.
2. Fare clic su **Save** (Salva).

Disattivazione dei gruppi nidificati dall'autenticazione remota

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

Prima di iniziare

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

A proposito di questa attività

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

Fasi

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

Aggiunta di server di autenticazione

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

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 attivato l'autenticazione remota e configurato il servizio di autenticazione in modo che il server di gestione possa autenticare utenti o gruppi remoti nel server di autenticazione.
- È necessario disporre del ruolo di amministratore dell'applicazione.

A proposito di questa attività

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

Fasi

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

Se si desidera…	Quindi…
Abilitarlo	1. Selezionare l'opzione **Usa connessione protetta**. 2. Nella sezione Authentication Servers (Server di autenticazione), fare clic su **Add** (Aggiungi) 3. Nella finestra di dialogo Add Authentication Server (Aggiungi server di autenticazione), immettere il nome di autenticazione o l'indirizzo IP (IPv4 o IPv6) del server. 4. Nella finestra di dialogo autorizza host, fare clic su Visualizza certificato. 5. Nella finestra di dialogo Visualizza certificato, verificare le informazioni del certificato, quindi fare clic su **Chiudi**. 6. Nella finestra di dialogo autorizza host, fare clic su **Sì**. Quando si attiva l'opzione **Usa autenticazione connessione sicura**, Unified Manager comunica con il server di autenticazione e visualizza il certificato. Unified Manager utilizza 636 come porta predefinita per comunicazioni sicure e il numero di porta 389 per comunicazioni non sicure.
Disattivarlo	1. Deselezionare l'opzione **Usa connessione protetta**. 2. Nella sezione Authentication Servers (Server di autenticazione), fare clic su **Add** (Aggiungi) 3. Nella finestra di dialogo Add Authentication Server (Aggiungi server di autenticazione), specificare il nome host o l'indirizzo IP (IPv4 o IPv6) del server e i dettagli della porta. 4. Fare clic su **Aggiungi**.

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

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

Verifica della configurazione dei server di autenticazione

È possibile convalidare la configurazione dei server di autenticazione per garantire che il server di gestione sia in grado di comunicare con essi. È possibile convalidare la configurazione ricercando un utente remoto o un gruppo remoto dai server di autenticazione e autenticandoli utilizzando le impostazioni configurate.

Prima di iniziare

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

A proposito di questa attività

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

Fasi

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

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

Aggiunta di utenti

È possibile aggiungere utenti locali o utenti di database utilizzando la pagina utenti. È inoltre possibile aggiungere utenti o gruppi remoti appartenenti a un server di autenticazione. È possibile assegnare ruoli a questi utenti e, in base ai privilegi dei ruoli, gli utenti possono gestire gli oggetti e i dati di storage con Unified Manager o visualizzare i dati in un database.

Prima di iniziare

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

  L'accesso all'interfaccia utente non è consentito per gli utenti di tipo "local" o "maintenance" quando l'autenticazione SAML è attivata.

A proposito di questa attività

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

Fasi

1. Nel riquadro di navigazione a sinistra, fare clic su **Generale** > **utenti**.
2. Nella pagina **utenti**, fare clic su **Aggiungi**.
3. Nella finestra di dialogo **Aggiungi utente**, selezionare il tipo di utente che si desidera aggiungere e immettere le informazioni richieste.

   Quando si immettono le informazioni utente richieste, è necessario specificare un indirizzo e-mail univoco per l'utente. Evitare di specificare indirizzi e-mail condivisi da più utenti.
4. Fare clic su **Aggiungi**.

Aggiunta di avvisi

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

Prima di iniziare

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

A proposito di questa attività

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

Fasi

1. Nel riquadro di navigazione a sinistra, fare clic su **Storage Management** > **Alert Setup**.
2. Nella pagina **Alert Setup**, fare clic su **Add** (Aggiungi).
3. Nella finestra di dialogo **Aggiungi avviso**, fare clic su **Nome** e immettere un nome e una descrizione per l'avviso.
4. Fare clic su **risorse** e selezionare le risorse da includere o escludere dall'avviso.

   È possibile impostare un filtro specificando una stringa di testo nel campo **Nome contiene** per selezionare

un gruppo di risorse. In base alla stringa di testo specificata, l'elenco delle risorse disponibili visualizza solo le risorse corrispondenti alla regola di filtro. La stringa di testo specificata fa distinzione tra maiuscole e minuscole.

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

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

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

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

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

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

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

Esempio di aggiunta di un avviso

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

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

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

1. Fare clic su **Nome** e digitare `HealthTest` Nel campo **Nome avviso**.
2. Fare clic su **Resources** (risorse) e nella scheda include (Includi) selezionare **Volumes** (volumi) dall'elenco a discesa.
   a. Invio `abc` Nel campo **Nome contiene** per visualizzare i volumi il cui nome contiene "abc".
   b. Selezionare **<<All Volumes whose name contains 'abc'>>** dall'area risorse disponibili e spostarla nell'area risorse selezionate.
   c. Fare clic su **Escludi** e digitare `xyz` Nel campo **Nome contiene**, quindi fare clic su **Aggiungi**.
3. Fare clic su **Eventi** e selezionare **critico** dal campo gravità evento.
4. Selezionare **All Critical Events** (tutti gli eventi critici) dall'area Matching Events (Eventi corrispondenti) e spostarla nell'area Selected Events (Eventi selezionati).
5. Fare clic su **azioni** e digitare `sample@domain.com` Nel campo Alert these users (Avvisa questi utenti).

6. Selezionare **promemoria ogni 15 minuti** per avvisare l'utente ogni 15 minuti.

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

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

Eventi EMS aggiunti automaticamente a Unified Manager

I seguenti eventi EMS di ONTAP vengono aggiunti automaticamente a Unified Manager. Questi eventi verranno generati quando vengono attivati su qualsiasi cluster monitorato da Unified Manager.

I seguenti eventi EMS sono disponibili durante il monitoraggio dei cluster con software ONTAP 9.5 o superiore:

Nome evento di Unified Manager	Nome evento EMS	Risorsa interessata	Severità di Unified Manager
Accesso al livello cloud negato per il trasferimento aggregato	arl.netra.ca.check.failed	Aggregato	Errore
Accesso di livello cloud negato per il trasferimento aggregato durante il failover dello storage	gb.netra.ca.check.failed	Aggregato	Errore
Risincronizzazione replica mirror FabricPool completata	wafl.ca.resync.complete	Cluster	Errore
Spazio FabricPool quasi pieno	fabricpool.nehly.full	Cluster	Errore
Inizio del periodo NVMe-of Grace	nvmf.graceperiod.start	Cluster	Attenzione
Periodo di tolleranza NVMe attivo	nvmf.graceperiod.active	Cluster	Attenzione
Periodo di tolleranza NVMe scaduto	nvmf.graceperiod.expired	Cluster	Attenzione
LUN distrutta	lun.destroy	LUN	Informazioni
Cloud AWS MetaDataConnFail	Cloud.aws.metadataConnFail	Nodo	Errore

Nome evento di Unified Manager	Nome evento EMS	Risorsa interessata	Severità di Unified Manager
Cloud AWS IAMCredsExpired	Cloud.aws.iamCredsExpired	Nodo	Errore
Cloud AWS IAMCredsInvalid (IAMCrediti AWS cloud non	Cloud.aws.iamCredsInvalid	Nodo	Errore
Cloud AWS IAMCredsNotFound	Cloud.aws.iamCredsNotFound	Nodo	Errore
Cloud AWS IAMCredsNotInitialized	Cloud.aws.iamNotInitialized	Nodo	Informazioni
Cloud AWS IAMRoleInvalid (IAMRoleInvalid	Cloud.aws.iamRoleInvalid	Nodo	Errore
Cloud AWS IAMRoleNotFound	Cloud.aws.iamRoleNotFound	Nodo	Errore
Host di livello cloud irrisolvibile	objstore.host.unresolvable	Nodo	Errore
Livello cloud LIF Intercluster inattivo	objstore.interclusterlifDown	Nodo	Errore
Richiesta di una firma del livello cloud non corrispondente	osc.signatureMismatch	Nodo	Errore
Uno dei pool NFSv4 esaurito	Nblade.nfsV4PoolExhaust	Nodo	Critico
Memoria monitor QoS massima	qos.monitor.memory.maxed	Nodo	Errore
Memoria monitor QoS esaurita	qos.monitor.memory.abated	Nodo	Informazioni
NVMeNS distruggere	NVMeNS.destroy	Namespace	Informazioni
NVMeNS online	NVMeNS.offline	Namespace	Informazioni
NVMNS non in linea	NVMeNS.online	Namespace	Informazioni

Nome evento di Unified Manager	Nome evento EMS	Risorsa interessata	Severità di Unified Manager
NVMeNS fuori spazio	NVMeNS.out.of.space	Namespace	Attenzione
Replica sincrona fuori sincronizzazione	sms.status.out.of.sync	Relazione di SnapMirror	Attenzione
Replica sincrona ripristinata	sms.status.in.sync	Relazione di SnapMirror	Informazioni
Risincronizzazione automatica replica sincrona non riuscita	sms.resync.tentativo.non riuscito	Relazione di SnapMirror	Errore
Molte connessioni CIFS	Nblade.cifsManyAuths	SVM	Errore
Connessione CIFS massima superata	Nblade.cifsMaxOpenSameFile	SVM	Errore
È stato superato il numero massimo di connessioni CIFS per utente	Nblade.cifsMaxSessPerUsrConn	SVM	Errore
Conflitto nome NetBIOS CIFS	Nblade.cifsNbNameConflict	SVM	Errore
Tentativi di connessione di una condivisione CIFS inesistente	Nblade.cifsNoPrivShare	SVM	Critico
Operazione di copia shadow CIFS non riuscita	cifs.shadowcopy.failure	SVM	Errore
Virus rilevato dal server AV	Nblade.vscanVirusDetected	SVM	Errore
Nessuna connessione al server AV per Virus Scan	Nblade.vscanNoSannerConn	SVM	Critico
Nessun server AV registrato	Nblade.vscanNoRegdscanner	SVM	Errore
Nessuna connessione al server AV reattiva	Nblade.vscanConnInactive	SVM	Informazioni

Nome evento di Unified Manager	Nome evento EMS	Risorsa interessata	Severità di Unified Manager
Server AV troppo occupato per accettare una nuova richiesta di scansione	Nblade.vscanConnBackPressure	SVM	Errore
Tentativo di utente non autorizzato di accedere al server AV	Nblade.vscanBadUserPrivAccess	SVM	Errore
I componenti FlexGroup presentano problemi di spazio	flexgroup.costituenti.hanno.spazio.problemi	Volume	Errore
Stato dello spazio dei componenti FlexGroup OK	flexgroup.costituenti.spazio.stato.tutto.ok	Volume	Informazioni
I componenti FlexGroup presentano problemi di nodi	flexgroup.constituents.have.inodes.issues	Volume	Errore
FlexGroup costituenti nodi Stato tutto OK	flexgroup.constituents.inodes.status.all.ok	Volume	Informazioni
Volume Logical Space quasi pieno	monitor.vol.nearFull.inc.sav	Volume	Attenzione
Volume Logical Space Full (spazio logico volume pieno)	monitor.vol.full.inc.sav	Volume	Errore
Volume Logical Space Normal (spazio logico volume normale)	monitor.vol.one.ok.inc.sav	Volume	Informazioni
Errore di dimensionamento automatico del volume WAFL	wafl.vol.autoSize.fail	Volume	Errore
Dimensione automatica volume WAFL completata	wafl.vol.autoSize.done	Volume	Informazioni
Timeout operazione file READDIR WAFL	wafl.readdir.expired	Volume	Errore

Iscrizione a eventi EMS ONTAP

È possibile iscriversi per ricevere gli eventi del sistema di gestione degli eventi (EMS) generati dai sistemi installati con il software ONTAP. Un sottoinsieme di eventi EMS viene segnalato automaticamente a Unified Manager, ma vengono segnalati eventi EMS aggiuntivi solo se si è abbonati a questi eventi.

Prima di iniziare

Non sottoscrivere gli eventi EMS che sono già stati aggiunti automaticamente a Unified Manager, in quanto ciò potrebbe causare confusione quando si ricevono due eventi per lo stesso problema.

A proposito di questa attività

È possibile iscriversi a qualsiasi numero di eventi EMS. Tutti gli eventi a cui si è abbonati sono validati e solo gli eventi validati vengono applicati ai cluster monitorati in Unified Manager. Il *Catalogo eventi EMS di ONTAP 9* fornisce informazioni dettagliate su tutti i messaggi EMS per la versione specificata del software ONTAP 9. Individuare la versione appropriata del *Catalogo eventi EMS* dalla pagina della documentazione del prodotto ONTAP 9 per un elenco degli eventi applicabili.

"Libreria di prodotti ONTAP 9"

È possibile configurare gli avvisi per gli eventi EMS di ONTAP a cui si è abbonati ed è possibile creare script personalizzati da eseguire per questi eventi.

> Se non si ricevono gli eventi EMS di ONTAP a cui si è abbonati, potrebbe esserci un problema con la configurazione DNS del cluster che impedisce al cluster di raggiungere il server di Unified Manager. Per risolvere questo problema, l'amministratore del cluster deve correggere la configurazione DNS del cluster, quindi riavviare Unified Manager. In questo modo, gli eventi EMS in sospeso verranno reincisi sul server Unified Manager.

Fasi

1. Nel riquadro di navigazione a sinistra, fare clic su **Storage Management** > **Event Setup**.
2. Nella pagina **Setup evento**, fare clic sul pulsante **Subscribe to EMS events** (Iscriviti agli eventi EMS).
3. Nella finestra di dialogo **Iscriviti agli eventi EMS**, immettere il nome dell'evento EMS ONTAP a cui si desidera iscriversi.

   Per visualizzare i nomi degli eventi EMS a cui è possibile iscriversi, dalla shell del cluster ONTAP, è possibile utilizzare `event route show` (Prima di ONTAP 9) o il `event catalog show` Command (ONTAP 9 o versioni successive).

   "Come configurare e ricevere avvisi dall'abbonamento eventi EMS ONTAP in Active IQ Unified Manager"

4. Fare clic su **Aggiungi**.

   L'evento EMS viene aggiunto all'elenco degli eventi EMS registrati, ma nella colonna applicabile al cluster viene visualizzato lo stato "Sconosciuto" per l'evento EMS aggiunto.

5. Fare clic su **Save and Close** (Salva e chiudi) per registrare l'abbonamento agli eventi EMS nel cluster.
6. Fare nuovamente clic su **Subscribe to EMS events** (Iscriviti agli eventi EMS).

Lo stato “Sì” viene visualizzato nella colonna applicabile al cluster per l’evento EMS aggiunto.

Se lo stato non è “Sì”, controllare l’ortografia del nome dell’evento EMS ONTAP. Se il nome non viene inserito correttamente, rimuovere l’evento errato e aggiungerlo di nuovo.

Al termine

Quando si verifica l’evento EMS ONTAP, l’evento viene visualizzato nella pagina Eventi. È possibile selezionare l’evento per visualizzare i dettagli relativi all’evento EMS nella pagina Dettagli evento. È inoltre possibile gestire l’eliminazione dell’evento o creare avvisi per l’evento.

Gestione delle impostazioni di autenticazione SAML

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

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

Requisiti del provider di identità

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

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

Standard di crittografia supportati

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

Provider di identità validati

- Shibboleth
- Active Directory Federation Services (ADFS)

Requisiti di configurazione di ADFS

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

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

- È necessario impostare il metodo di autenticazione su “Forms Authentication” (autenticazione moduli), altrimenti gli utenti potrebbero ricevere un errore durante la disconnessione da Unified Manager . Attenersi alla seguente procedura:
  a. Aprire la console di gestione ADFS.
  b. Fare clic sulla cartella Authentication Policies (Criteri di autenticazione) nella vista ad albero a sinistra.
  c. Nella sezione azioni a destra, fare clic su Modifica policy di autenticazione primaria globale.
  d. Impostare il metodo di autenticazione Intranet su “Forms Authentication” invece di “Windows Authentication” predefinito.
- In alcuni casi, l’accesso tramite IdP viene rifiutato quando il certificato di sicurezza di Unified Manager è firmato dalla CA. Esistono due soluzioni alternative per risolvere questo problema:
  - Seguire le istruzioni indicate nel collegamento per disattivare il controllo di revoca sul server ADFS per la parte di base associata al certificato CA concatenato:

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

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

Altri requisiti di configurazione

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

Attivazione dell’autenticazione SAML

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

Prima di iniziare

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

A proposito di questa attività

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

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

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

Fasi

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

   Vengono visualizzati i campi necessari per configurare la connessione IdP.
3. Immettere l'URI IdP e i metadati IdP richiesti per connettere il server Unified Manager al server IdP.

   Se il server IdP è accessibile direttamente dal server Unified Manager, è possibile fare clic sul pulsante **Fetch IdP Metadata** (Scarica metadati IdP) dopo aver immesso l'URI IdP per popolare automaticamente il campo IdP Metadata (metadati IdP).
4. Copiare l'URI dei metadati host di Unified Manager o salvare i metadati host in un file di testo XML.

   In questo momento è possibile configurare il server IdP con queste informazioni.
5. Fare clic su **Save** (Salva).

   Viene visualizzata una finestra di messaggio per confermare che si desidera completare la configurazione e riavviare Unified Manager.
6. Fare clic su **Confirm and Logout** (Conferma e Disconnetti) per riavviare Unified Manager.

Risultati

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

Al termine

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

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

Modifica della password utente locale

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

Prima di iniziare

Devi essere connesso come utente locale.

A proposito di questa attività

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

Fasi

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

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

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

Al termine

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

Impostazione del timeout di inattività della sessione

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

Prima di iniziare

È necessario disporre del ruolo di amministratore dell'applicazione.

A proposito di questa attività

Questa impostazione ha effetto su tutte le sessioni utente registrate.

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

Fasi

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

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

Modifica del nome host di Unified Manager

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

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

Modifica del nome host dell'appliance virtuale Unified Manager

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

Prima di iniziare

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

A proposito di questa attività

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

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

generare un nuovo certificato di protezione.

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

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

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

Fasi

1. Generare un certificato di protezione HTTPS

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

2. Riavviare la macchina virtuale di Unified Manager

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

Generazione di un certificato di protezione HTTPS

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

Prima di iniziare

È necessario disporre del ruolo di amministratore dell'applicazione.

A proposito di questa attività

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

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

Fasi

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

   Viene visualizzata la finestra di dialogo Rigenera certificato HTTPS.

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

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

4. Fare clic su **Sì** per rigenerare il certificato.
5. Riavviare il server Unified Manager in modo che il nuovo certificato abbia effetto.

Al termine

Verificare le informazioni sul nuovo certificato visualizzando il certificato HTTPS.

Riavvio della macchina virtuale di Unified Manager

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

Prima di iniziare

L'appliance virtuale è accesa.

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

A proposito di questa attività

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

Fasi

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

Modifica del nome host di Unified Manager sui sistemi Linux

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

Prima di iniziare

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

A proposito di questa attività

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

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

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

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

Fasi

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

3. Modificare il nome host utilizzando Linux `hostnamectl` comando: `hostnamectl set-hostname new_FQDN`

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

4. Rigenerare il certificato HTTPS per il server:`/opt/netapp/essentials/bin/cert.sh create`
5. Riavviare il servizio di rete: `service network restart`
6. Una volta riavviato il servizio, verificare se il nuovo nome host è in grado di eseguire il ping: `ping new_hostname`

   ```
   ping nuhost
   ```

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

7. Dopo aver completato e verificato la modifica del nome host, riavviare Unified Manager immettendo il seguente comando: `systemctl start mysqld ocie ocieau`

Attivazione e disattivazione della gestione dello storage basata su policy

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

Prima di iniziare

È necessario disporre del ruolo di amministratore dell'applicazione.

A proposito di questa attività

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

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

Nuovi contenuti	Posizione
Una pagina per il provisioning di nuovi workload	Disponibile da **attività comuni** > **Provisioning**
Una pagina per creare policy sui livelli di servizio per le performance	Disponibile in **Impostazioni** > **politiche** > **livelli di servizio delle performance**
Una pagina per creare policy di efficienza dello storage per le performance	Disponibile in **Impostazioni** > **politiche** > **efficienza dello storage**

Nuovi contenuti	Posizione
Pannelli che descrivono gli IOPS correnti relativi a workload Performance e workload	Disponibile nella dashboard

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

Fasi

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

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

Configurazione del backup di Unified Manager

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

Per informazioni sulle procedure di configurazione, vedere “Moperazioni di backup e ripristino” in *Guida al flusso di lavoro di Unified Manager Active IQ® per la gestione dello stato dei cluster*.

Utilizzando la console di manutenzione

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

Quali funzionalità offre la console di manutenzione

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

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

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

Manager non è disponibile

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

Cosa fa l'utente che effettua la manutenzione

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

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

Funzionalità diagnostiche per l'utente

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

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

Accesso alla console di manutenzione

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

Prima di iniziare

Unified Manager deve essere installato e configurato.

A proposito di questa attività

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

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

Fasi

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

Su questo sistema operativo…	Attenersi alla procedura descritta di seguito…
VMware	1. Utilizzando Secure Shell, connettersi all'indirizzo IP o al nome di dominio completo dell'appliance virtuale Unified Manager. 2. Accedere alla console di manutenzione utilizzando il nome utente e la password di manutenzione.
Linux	1. Utilizzando Secure Shell, connettersi all'indirizzo IP o al nome di dominio completo del sistema Unified Manager. 2. Accedere al sistema con il nome utente di manutenzione (umadmin) e la password. 3. Immettere il comando `maintenance_console` E premere Invio.
Windows	1. Accedere al sistema Unified Manager con le credenziali di amministratore. 2. Avviare PowerShell come amministratore di Windows. 3. Immettere il comando `maintenance_console` E premere Invio.

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

Accesso alla console di manutenzione mediante la console vSphere VM

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

Prima di iniziare

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

Fasi

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

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

Menu della console di manutenzione

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

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

- Upgrade di Unified Manager (solo VMware)
- Configurazione di rete (solo VMware)
- Configurazione del sistema (solo VMware)
- Supporto/Diagnostica
- Reimposta certificato server
- Provider di dati esterno
- Configurazione dell'intervallo di polling delle performance

Menu Network Configuration (Configurazione di rete)

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

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

Sono disponibili le seguenti opzioni di menu.

- **Visualizza impostazioni indirizzo IP**

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

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

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

- **Visualizza impostazioni di ricerca nome dominio**

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

- **Modifica impostazioni di ricerca nome dominio**

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

- **Visualizza percorsi statici**

Visualizza i percorsi di rete statici correnti.

- **Modifica percorsi statici**

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

- **Aggiungi percorso**

Consente di aggiungere un percorso statico.

- **Elimina percorso**

Consente di eliminare un percorso statico.

- **Indietro**

Consente di tornare al **Menu principale**.

- **Esci**

Consente di uscire dalla console di manutenzione.

- **Disattiva interfaccia di rete**

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

- **Attiva interfaccia di rete**

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

- **Conferma modifiche**

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

- **Ping di un host**

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

- **Ripristina impostazioni predefinite**

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

- **Indietro**

Consente di tornare al **Menu principale**.

- **Esci**

Consente di uscire dalla console di manutenzione.

Menu Configurazione di sistema

Il menu System Configuration (Configurazione di sistema) consente di gestire l'appliance

virtuale fornendo varie opzioni, ad esempio la visualizzazione dello stato del server, il riavvio e l'arresto della macchina virtuale.

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

Sono disponibili le seguenti opzioni di menu:

- **Visualizza stato server**

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

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

- **Riavviare la macchina virtuale**

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

- **Spegnere la macchina virtuale**

Arresta la macchina virtuale, interrompendo tutti i servizi.

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

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

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

- **Aumentare le dimensioni del disco dati**

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

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

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

- **Modifica fuso orario**

Consente di modificare il fuso orario in base alla posizione.

- **Cambia server NTP**

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

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

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

- **Ripristina certificato server**

Ripristina il certificato di sicurezza del server.

- **Modifica nome host**

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

- **Indietro**

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

- **Esci**

Consente di uscire dal menu della console di manutenzione.

Menu Support and Diagnostics (supporto e diagnostica)

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

Sono disponibili le seguenti opzioni di menu:

- **Genera bundle di supporto leggero**

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

- **Genera bundle di supporto**

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

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

Opzioni di menu aggiuntive

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

Sono disponibili le seguenti opzioni di menu:

- **Ripristina certificato server**

Rigenera il certificato del server HTTPS.

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

- **Disattiva autenticazione SAML**

Disattiva l'autenticazione SAML in modo che il provider di identità (IdP) non fornisca più l'autenticazione di accesso per gli utenti che accedono alla GUI di Unified Manager. Questa opzione della console viene

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

- **Fornitore di dati esterno**

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

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

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

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

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

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

- **Visualizza/Modifica porte applicazione**

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

- **Esci**

Consente di uscire dal menu della console di manutenzione.

Modifica della password utente per la manutenzione in Windows

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

Fasi

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

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

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

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

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

Modifica della password di umadmin sui sistemi Linux

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

Prima di iniziare

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

Fasi

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

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

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

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

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.

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

A proposito di questa attività

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

Fasi

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

   Vengono visualizzati i prompt della console di Unified Managermaintenance.

2. Digitare il numero dell'opzione di menu **View/Change Application Ports** (Visualizza/Modifica porte applicazione), quindi premere Invio.

3. Se richiesto, inserire nuovamente la password utente per la manutenzione.
4. Digitare i nuovi numeri di porta per le porte HTTP e HTTPS, quindi premere Invio.

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

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

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

Risultati

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

Aggiunta di interfacce di rete

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

Prima di iniziare

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

L'appliance virtuale deve essere accesa.

A proposito di questa attività

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

Fasi

1. Nella console vSphere **Menu principale**, selezionare **Configurazione di sistema** > **riavviare il sistema operativo**.

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

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

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

1. Digitare **y** per attivare l'interfaccia di rete.
2. Immettere le impostazioni di rete.

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

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

1. Selezionare **Conferma modifiche**.

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

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

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

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

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

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

Aggiunta di spazio alla directory dei dati dell'host Linux

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

Prima di iniziare

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

A proposito di questa attività

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

Fasi

1. Accedere come utente root alla macchina Linux su cui si desidera aggiungere spazio su disco.
2. Arrestare il servizio Unified Manager e il software MySQL associato nell'ordine indicato: `systemctl stop ocieau ocie mysqld`
3. Creare una cartella di backup temporanea (ad esempio, `/backup-data`) con spazio su disco sufficiente per contenere i dati nella corrente `/opt/netapp/data` directory.
4. Copiare il contenuto e la configurazione dei privilegi dell'esistente `/opt/netapp/data` directory nella directory dei dati di backup: `cp -arp /opt/netapp/data/* /backup-data`
5. Se Linux è attivato:

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

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

Il sistema restituisce una conferma simile a quanto segue:

```
echo $se_type
mysqld_db_t
```

a. Eseguire `chcon` Per impostare il tipo di se Linux per la directory di backup: `chcon -R --type=mysqld_db_t /backup-data`

6. Rimuovere il contenuto di `/opt/netapp/data` directory:
   a. `cd /opt/netapp/data`
   b. `rm -rf *`
7. Espandere le dimensioni di `/opt/netapp/data` Directory fino a un minimo di 150 GB tramite comandi LVM o aggiungendo dischi aggiuntivi.

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

1. Verificare che il `/opt/netapp/data` il proprietario della directory (mysql) e il gruppo (root) rimangono invariati: `ls -ltr /opt/netapp/ | grep data`

Il sistema restituisce una conferma simile a quanto segue:

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

1. Se Linux è attivato, verificare che il contesto per `/opt/netapp/data` la directory è ancora impostata su mysqld_db_t:
   a. `touch /opt/netapp/data/abc`
   b. `ls -Z /opt/netapp/data/abc`

Il sistema restituisce una conferma simile a quanto segue:

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

1. Eliminare il file `abc` in modo che questo file estraneo non causi un errore di database in futuro.
2. Copiare il contenuto da `backup-data` torna all'expanded `/opt/netapp/data` directory: `cp -arp /backup-data/* /opt/netapp/data/`
3. Se Linux è attivato, eseguire il seguente comando: `chcon -R --type=mysqld_db_t /opt/netapp/data`

4. Avviare il servizio MySQL: `systemctl start mysqld`
5. Una volta avviato il servizio MySQL, avviare i servizi ocie e ocieau nell'ordine indicato: `systemctl start ocie ocieau`
6. Una volta avviati tutti i servizi, eliminare la cartella di backup `/backup-data`: `rm -rf /backup-data`

Aggiunta di spazio al disco dati della macchina virtuale VMware

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

Prima di iniziare

- È necessario disporre dell'accesso al client vSphere.
- La macchina virtuale non deve contenere snapshot memorizzate localmente.
- È necessario disporre delle credenziali utente di manutenzione.

A proposito di questa attività

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

Fasi

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

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

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

Aggiunta di spazio all'unità logica del server Microsoft Windows

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

Prima di iniziare

È necessario disporre dei privilegi di amministratore di Windows.

A proposito di questa attività

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

Fasi

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

Opzione	Descrizione
Su un server fisico, aggiungere capacità all'unità logica su cui è installato il server Unified Manager.	Seguire la procedura descritta nell'argomento Microsoft: "Estensione di un volume di base"
Su un server fisico, aggiungere un disco rigido.	Seguire la procedura descritta nell'argomento Microsoft: "Aggiunta di dischi rigidi"
Su una macchina virtuale, aumentare le dimensioni di una partizione del disco.	Seguire la procedura descritta nell'argomento VMware: "Aumento delle dimensioni di una partizione del disco"