



Lenovo XClarity Management Hub

Guida per l'utente e all'installazione



Versione 2.1

Nota

Prima di utilizzare queste informazioni e il prodotto supportato, consultare le [informazioni generali e legali nella documentazione online di XClarity Orchestrator](#).

Seconda edizione (Luglio 2024)

© Copyright Lenovo 2022.

NOTA SUI DIRITTI LIMITATI: se i dati o il software sono distribuiti secondo le disposizioni che regolano il contratto "GSA" (General Services Administration), l'uso, la riproduzione o la divulgazione si basa sulle limitazioni previste dal contratto n. GS-35F-05925.

Contenuto

Contenuto	i	Configurazione di data e ora di XClarity Management Hub per i dispositivi client Edge	14
Capitolo 1. Pianificazione per Lenovo XClarity Management Hub	1	Gestione dei certificati di sicurezza di Lenovo XClarity Management Hub per i dispositivi client Edge	16
Hardware e software supportati	1	Rigenerazione del certificato server autofirmato di XClarity Management Hub per i dispositivi client Edge.	17
Firewall e server proxy	2	Installazione di un certificato del server con firma esterna attendibile per XClarity Management Hub per i dispositivi client Edge	19
Disponibilità della porta	3	Importazione del certificato del server in un browser Web per Lenovo XClarity Management Hub per i dispositivi client Edge	21
Considerazioni sulla rete	5	Collegamento di XClarity Management Hub per i dispositivi client Edge a XClarity Orchestrator	23
Considerazioni sulla disponibilità elevata	6		
Capitolo 2. Configurazione di XClarity Management Hub per i dispositivi client Edge	9		
Accesso a XClarity Management Hub per i dispositivi client Edge	9		
Creazione di account utente per Lenovo XClarity Management Hub per i dispositivi client Edge	12		
Configurazione delle impostazioni di rete di XClarity Management Hub per i dispositivi client Edge	13		
		Capitolo 3. Disinstallazione di XClarity Management Hub per i dispositivi client Edge	25

Capitolo 1. Pianificazione per Lenovo XClarity Management Hub

Esaminare le considerazioni e i prerequisiti che seguono per pianificare l'installazione di Lenovo XClarity Management Hub.

Hardware e software supportati

Verificare che l'ambiente in uso soddisfi i requisiti hardware e software per Lenovo XClarity Management Hub.

Sistemi host

Requisiti hypervisor

Per l'installazione di Lenovo XClarity Management Hub sono supportati i seguenti hypervisor.

- VMware ESXi 7.0, U1, U2 e U3
- VMware ESXi 6.7, U1, U2¹ e U3

Per VMware ESXi, l'appliance virtuale è un template OVF.

Importante:

- Per VMware ESXi 6.7 U2, è necessario utilizzare l'immagine ISO VMware-ESXi-6.7.0.update02-13981272-LNV-20190630.iso o versione successiva.

Requisiti hardware

Nella seguente tabella sono elencate le configurazioni *minime consigliate* per XClarity Management Hub in base al numero di dispositivi client Edge. A seconda dell'ambiente, potrebbero essere necessarie risorse aggiuntive per assicurare prestazioni ottimali.

Numero di dispositivi client Edge gestiti	Processori	Memoria	Storage
0-100 dispositivi	6	32 GB	340 GB
100-200 dispositivi	8	34 GB	340 GB
200-400 dispositivi	10	36 GB	340 GB
400-600 dispositivi	12	40 GB	340 GB
600-800 dispositivi	14	44 GB	340 GB
800-1.000 dispositivi	16	48 GB	340 GB

1. Questa è la quantità minima di storage che l'appliance virtuale XClarity Management Hub può utilizzare come archivio dati SSD.

Requisiti software

XClarity Management Hub richiede il software che segue.

- **Server NTP.** È necessario utilizzare un server NTP (Network Time Protocol) per assicurare che i timestamp per tutti gli eventi e gli avvisi ricevuti dagli strumenti di gestione delle risorse e dai dispositivi gestiti siano sincronizzati con XClarity Management Hub. Verificare che il server NTP sia accessibile sulla rete di gestione (in genere, l'interfaccia Eth0).

Dispositivi gestibili

XClarity Management Hub è in grado di gestire, monitorare ed eseguire il provisioning di un massimo di 10,000 dispositivi client ThinkEdge (senza controller di gestione della scheda di base).

Un elenco completo di dispositivi client ThinkEdge e opzioni supportati (come I/O, DIMM e adattatori di storage), i livelli minimi di firmware richiesti e le considerazioni sulle limitazioni sono disponibili sul [Pagina Web del supporto XClarity Management Hub](#).

Per informazioni generali sulle configurazioni hardware e le opzioni per uno specifico dispositivo, vedere [Pagina Web di Lenovo Server Proven](#).

Browser Web

L'interfaccia Web XClarity Management Hub è supportata dai browser Web che seguono.

- Chrome 80.0 o versioni successive
- Firefox ESR 68.6.0 o versioni successive
- Microsoft Edge 40.0 o versioni successive
- Safari 13.0.4 o versioni successive (su macOS 10.13 o versioni successive)

Firewall e server proxy

Alcune funzioni di assistenza e supporto, tra cui lo stato Call Home e garanzia, richiedono l'accesso a Internet. Se la rete è protetta da firewall, configurarli per abilitare XClarity Orchestrator e gli strumenti di gestione delle risorse a eseguire queste operazioni. Se Lenovo XClarity Orchestrator e gli strumenti di gestione delle risorse non possono accedere direttamente a Internet, configurarli per utilizzare un server proxy.

Firewall

Verificare che i seguenti nomi e porte DNS siano aperti sul firewall per XClarity Orchestrator e gli strumenti di gestione delle risorse applicabili (Lenovo XClarity Management Hub 2.0, Lenovo XClarity Management Hub e Lenovo XClarity Administrator), a seconda dei casi. Ogni DNS rappresenta un sistema distribuito geograficamente con un indirizzo IP dinamico.

Nota: Gli indirizzi IP possono variare. Usare i nomi DNS quando possibile.

Nome DNS	Porte	Protocolli
Download degli aggiornamenti server di gestione, aggiornamenti firmware, UpdateXpress System Packs (driver di dispositivo del sistema operativo) e pacchetti del repository		
download.lenovo.com	443	https
support.lenovo.com	443 e 80	https e http
Inviare i dati di servizio al supporto Lenovo (Call Home): solo XClarity Orchestrator		
soaus.lenovo.com	443	https
esupportwebapi.lenovo.com (XClarity Orchestrator v2.0 e versioni successive)	443	https
rsgw-eservice.motorola.com (XClarity Orchestrator v1.6)		
supportwebapi.lenovo.com:443/luf.luf-web.prd/BLL/Logupload.ashx (XClarity Orchestrator v1.5 e versioni precedenti)		
Inviare i dati periodici a Lenovo: solo XClarity Orchestrator		

Nome DNS	Porte	Protocolli
esupportwebapi.lenovo.com (XClarity Orchestrator v2.0 e versioni successive)	443	https
rsgw-eservice.motorola.com (XClarity Orchestrator v1.6)		
supportwebapi.lenovo.com:443/luf.luf-web.prd/BLL/uploadSnapshot.ashx (XClarity Orchestrator v1.5 e versioni precedenti)		
Recupero delle informazioni sulla garanzia		
supportapi.lenovo.com	443	https e http

Server proxy

Se XClarity Orchestrator o gli strumenti di gestione delle risorse non hanno accesso diretto a Internet, verificare che siano configurati per utilizzare un server proxy HTTP (vedere [Configurazione della rete](#) nella documentazione online di XClarity Orchestrator).

- Accertarsi che il server proxy sia configurato per utilizzare l'autenticazione di base.
- Accertarsi che il server proxy sia configurato come proxy non ricevitore.
- Accertarsi che il server proxy sia configurato come proxy di inoltro.
- Accertarsi che i bilanciamenti del carico siano configurati in modo da mantenere sessioni con un solo server proxy e non scambiandole.

Attenzione: XClarity Management Hub deve disporre dell'accesso diretto a Internet. Un server proxy HTTP non è attualmente supportato.

Disponibilità della porta

Lenovo XClarity Orchestrator e gli strumenti di gestione delle risorse richiedono che alcune porte siano aperte per facilitare la comunicazione. Se le porte richieste sono bloccate o utilizzate da un altro processo, alcune funzioni potrebbero non essere eseguite correttamente.

XClarity Orchestrator, Lenovo XClarity Management Hub 2.0, Lenovo XClarity Management Hub e Lenovo XClarity Administrator sono applicazioni RESTful che comunicano in modo sicuro su TCP sulla porta 443.

XClarity Orchestrator

XClarity Orchestrator è in ascolto e risponde tramite le porte elencate nella seguente tabella. Se XClarity Orchestrator e tutte le risorse gestite sono protetti da un firewall e si intende accedere a tali risorse da un browser esterno al firewall, verificare che le porte richieste siano aperte.

Nota: XClarity Orchestrator può essere configurato facoltativamente per creare connessioni in uscita a servizi esterni, come LDAP, SMTP o syslog. Queste connessioni potrebbero richiedere porte aggiuntive che generalmente possono essere configurate dall'utente e non sono incluse in questo elenco. Potrebbero inoltre richiedere l'accesso a un server DNS (Domain Name Service) sulla porta TCP o UDP 53 per risolvere i nomi del server esterno.

Servizio	In uscita (porte aperte sui sistemi esterni)	In ingresso (porte aperte sull'appliance XClarity Orchestrator)
Appliance XClarity Orchestrator	<ul style="list-style-type: none"> • DNS: TCP/UDP sulla porta 53 	<ul style="list-style-type: none"> • HTTPS: TCP sulla porta 443
Server di autenticazione esterni	<ul style="list-style-type: none"> • LDAP: TCP sulla porta 389¹ 	Non applicabile

Servizio	In uscita (porte aperte sui sistemi esterni)	In ingresso (porte aperte sull'appliance XClarity Orchestrator)
Servizi di inoltro eventi	<ul style="list-style-type: none"> • Server e-mail (SMTP): UDP sulla porta 25¹ • Servizio Web REST (HTTP): UDP sulla porta 80¹ • Splunk: UDP su porta 8088¹, 8089¹ • Syslog: UDP sulla porta 514¹ 	Non applicabile
Servizi Lenovo (incluso Call Home)	<ul style="list-style-type: none"> • HTTPS (Call Home): TCP sulla porta 443 	Non applicabile

1. Questo è la porta predefinita. Questa porta può essere configurata dall'interfaccia utente di XClarity Orchestrator.

XClarity Management Hub 2.0

Lenovo XClarity Management Hub 2.0 richiede che alcune porte siano aperte per facilitare la comunicazione. Se le porte richieste sono bloccate o utilizzate da un altro processo, alcune funzioni dell'hub di gestione potrebbero non essere eseguite correttamente.

Se i dispositivi gestibili (come nodi di elaborazione o server rack) sono protetti da firewall e si intende gestirli da un hub di gestione non protetto dallo stesso firewall, è necessario verificare che tutte le porte interessate dalla comunicazione tra l'hub di gestione e il controller di gestione della scheda di base di ciascun dispositivo gestito siano aperte.

Servizio o componente	In uscita (porte aperte ai sistemi esterni)	In ingresso (porte aperte sui dispositivi di destinazione)
XClarity Management Hub 2.0	<ul style="list-style-type: none"> • DNS: UDP sulla porta 53 • NTP: UDP sulla porta 123 • HTTPS: TCP sulla porta 443 • SSDP: UDP sulla porta 1900 • DHCP: UDP sulla porta 67 	<ul style="list-style-type: none"> • HTTPS: TCP sulla porta 443 • Risposta SSDP: UDP sulle porte 32768-65535
Server ThinkSystem e ThinkAgile	<ul style="list-style-type: none"> • HTTPS: TCP sulla porta 443 • Rilevamento SSDP: UDP sulla porta 1900 	<ul style="list-style-type: none"> • HTTPS: TCP sulla porta 443

XClarity Management Hub

XClarity Management Hub è in ascolto e risponde tramite le porte elencate nella seguente tabella.

Servizio o componente	In uscita (porte aperte sui sistemi esterni)	In ingresso (porte aperte sull'appliance XClarity Management Hub)
Appliance XClarity Management Hub ¹	<ul style="list-style-type: none"> • DNS: TCP/UDP sulla porta 53² 	<ul style="list-style-type: none"> • HTTPS: TCP sulla porta 443 • MQTT: TCP sulla porta 8883
Dispositivi client ThinkEdge ³	Non applicabile	<ul style="list-style-type: none"> • MQTT: TCP sulla porta 8883

1. Quando si utilizza XClarity Management Hub per gestire i dispositivi tramite XClarity Orchestrator, alcune porte devono essere aperte per facilitare la comunicazione. Se le porte richieste sono bloccate o

utilizzate da un altro processo, alcune funzioni di XClarity Orchestrator potrebbero non essere eseguite correttamente.

2. XClarity Management Hub può essere configurato facoltativamente per creare connessioni in uscita a servizi esterni. Potrebbero inoltre richiedere l'accesso a un server DNS (Domain Name Service) sulla porta TCP o UDP 53 per risolvere i nomi del server esterno.
3. Se i dispositivi gestibili (come nodi di elaborazione o server rack) sono protetti da firewall e si intende gestirli da un XClarity Management Hub non protetto dallo stesso firewall, è necessario verificare che tutte le porte interessate dalla comunicazione tra XClarity Management Hub e i dispositivi Edge siano aperte.

XClarity Administrator

Quando si utilizza Lenovo XClarity Administrator per gestire i dispositivi tramite Lenovo XClarity Orchestrator, alcune porte devono essere aperte per facilitare la comunicazione. Se le porte richieste sono bloccate o utilizzate da un altro processo, alcune funzioni di XClarity Orchestrator potrebbero non essere eseguite correttamente.

Per informazioni sulle porte che devono essere aperte per XClarity Administrator, vedere [Disponibilità della porta](#) nella documentazione online di XClarity Administrator.

Considerazioni sulla rete

È possibile configurare Lenovo XClarity Management Hub per utilizzare una singola interfaccia di rete (eth0) o due interfacce di rete separate (eth0 e eth1) per la comunicazione.

Lenovo XClarity Management Hub comunica sulle seguenti reti.

- La *rete di gestione* viene utilizzata per le comunicazioni tra Lenovo XClarity Management Hub e i dispositivi gestiti.
- La *rete di dati* generalmente viene utilizzata per le comunicazioni tra i sistemi operativi installati sui server e l'Intranet aziendale, Internet o entrambe.

Singola interfaccia (eth0)

Quando si utilizza una singola interfaccia di rete (eth0), le comunicazioni di gestione, le comunicazioni di dati e la distribuzione del sistema operativo si verificano sulla stessa rete.

Quando si configura Lenovo XClarity Management Hub, definire l'interfaccia di rete eth0 utilizzando le seguenti considerazioni.

- L'interfaccia di rete deve essere configurata per supportare il rilevamento e la gestione dei dispositivi (inclusi gli aggiornamenti firmware). Lenovo XClarity Management Hub deve essere in grado di comunicare con tutti i dispositivi che gestirà dalla rete di gestione. Lenovo XClarity Management Hub deve essere in grado di comunicare con tutti i dispositivi che gestirà dalla rete.
- Per distribuire le immagini del sistema operativo, l'interfaccia eth0 deve disporre della connettività di rete IP all'interfaccia di rete del server utilizzato per accedere al sistema operativo host.
- **Important:** l'implementazione di una rete di gestione e di dati condivisi può causare interruzioni del traffico, come perdita di pacchetti o problemi di connettività della rete di gestione, a seconda della configurazione di rete (ad esempio, se il traffico dei server ha priorità elevata mentre il traffico del controller di gestione ha priorità bassa). La rete di gestione utilizza il traffico UDP e TCP. Il traffico UDP può avere priorità più bassa quando il traffico di rete è elevato.

Due interfacce separate (eth0 ed eth1)

Quando si utilizzano due interfacce di rete (eth0 ed eth1), è possibile configurare le reti in reti fisicamente separate o virtualmente separate.

Esaminare le seguenti considerazioni quando si definiscono le interfacce di rete eth0 ed eth1.

- L'interfaccia di rete eth0 deve essere connessa alla rete di gestione e configurata per supportare il rilevamento e la gestione dei dispositivi. Lenovo XClarity Management Hub deve essere in grado di comunicare con tutti i dispositivi che gestirà dalla rete di gestione.
- L'interfaccia di rete eth1 può essere configurata per comunicare con una rete di dati interna, una rete di dati pubblica o entrambe.
- Per distribuire le immagini del sistema operativo, l'interfaccia di rete eth1 deve disporre della connettività di rete IP sull'interfaccia di rete del server che viene utilizzata per accedere al sistema operativo host.
- Le funzioni possono essere eseguite su entrambe le reti.
- Per le reti virtualmente separate, i pacchetti dalla rete di gestione e dalla rete di dati vengono inviati sulla stessa connessione fisica. Utilizzare l'etichettatura VLAN su tutti i pacchetti di dati della rete di gestione per separare il traffico tra le due reti.

Considerazioni sull'indirizzo IP

Prima di configurare la rete, esaminare le seguenti considerazioni sull'indirizzo IP.

- La modifica dell'indirizzo IP dell'appliance virtuale dopo l'installazione e l'esecuzione di XClarity Management Hub causerà problemi di connettività con XClarity Orchestrator e tutti i dispositivi gestiti. Se è necessario modificare l'indirizzo IP, disconnettere XClarity Management Hub da XClarity Orchestrator e annullare la gestione di tutti i dispositivi gestiti prima di modificare l'indirizzo IP. Quindi gestire nuovamente i dispositivi e riconnettere XClarity Management Hub a XClarity Orchestrator, una volta completata la modifica dell'indirizzo IP.
- Configurare i dispositivi e i componenti in modo che le modifiche dell'indirizzo IP siano minime. Considerare la possibilità di utilizzare gli indirizzi IP statici invece di DHCP (DHCP). Se si utilizza DHCP, accertarsi che le modifiche dell'indirizzo IP siano minime, ad esempio basando l'indirizzo DHCP su un indirizzo MAC o configurando DHCP in modo che il lease non scada. Se l'indirizzo IP di un dispositivo gestito (diverso da un dispositivo client ThinkEdge) viene modificato, è necessario annullare la gestione del dispositivo e gestirlo nuovamente.
- NAT (Network Address Translation), che riesegue il mapping di uno spazio dell'indirizzo IP in un altro, non è supportato.
- Per gestire i seguenti dispositivi, le interfacce di rete devono essere configurate con un indirizzo IPv4. Gli indirizzi IPv6 non sono supportati.
 - Server ThinkServer
 - Dispositivi Lenovo Storage
- La gestione dei dispositivi RackSwitch utilizzando il collegamento locale IPv6 mediante una porta dati o una porta di gestione non è supportata.

Considerazioni sulla disponibilità elevata

Per configurare la disponibilità elevata di Lenovo XClarity Orchestrator, utilizzare le funzioni di disponibilità elevata integrate nel sistema operativo host.

Microsoft Hyper-V

Utilizzare la funzione di alta disponibilità fornita per l'ambiente Hyper-V.

VMware ESXi

In un ambiente VMware High Availability, più host vengono configurati come un unico cluster. Lo storage condiviso viene utilizzato per assicurare la disponibilità dell'immagine disco di una macchina virtuale (VM) agli host del cluster. Le VM possono essere eseguite solo su un host alla volta. Se si verifica un problema di una VM, viene avviata un'altra istanza della stessa VM su un host di backup.

VMware High Availability richiede i componenti che seguono.

- Almeno due host su cui è installato ESXi. Questi host diventano parte del cluster VMware.
- Un terzo host su cui è installato VMware vCenter.

Suggerimento: verificare di avere installato una versione di VMware vCenter compatibile con le versioni di ESXi installate sugli host da utilizzare nel cluster.

VMware vCenter può essere installato su uno degli host utilizzati nel cluster. Tuttavia, se tale host è spento o inutilizzabile, non sarà possibile accedere neanche all'interfaccia di VMware vCenter.

- È possibile accedere allo storage condiviso (archivio dati) da tutti gli host del cluster. È possibile utilizzare qualsiasi tipo di storage condiviso supportato da VMware. L'archivio dati viene utilizzato da VMware per determinare se è necessario eseguire il failover di una VM su un host differente (heartbeat).

Capitolo 2. Configurazione di XClarity Management Hub per i dispositivi client Edge

Al primo accesso di Lenovo XClarity Management Hub, è necessario effettuare alcuni passaggi per eseguire la configurazione iniziale di XClarity Management Hub.

Procedura

Per eseguire la configurazione iniziale di XClarity Management Hub, attenersi alla procedura descritta di seguito.

- Passo 1. Eseguire il login all'interfaccia Web di XClarity Management Hub.
- Passo 2. Leggere e accettare il contratto di licenza.
- Passo 3. Creare account utente aggiuntivi.
- Passo 4. Configurare l'accesso alla rete, inclusi gli indirizzi IP per le reti dati e di gestione.
- Passo 5. Configurare la data e l'ora.
- Passo 6. Registrare l'istanza di XClarity Management Hub con il server Orchestrator.

Accesso a XClarity Management Hub per i dispositivi client Edge

È possibile avviare l'interfaccia Web di XClarity Management Hub da qualsiasi computer con connettività di rete alla macchina virtuale XClarity Management Hub.

Prima di iniziare

Accertarsi di utilizzare uno dei seguenti browser Web supportati.

- Chrome 80.0 o versioni successive
- Firefox ESR 68.6.0 o versioni successive
- Microsoft Edge 40.0 o versioni successive
- Safari 13.0.4 o versioni successive (su macOS 10.13 o versioni successive)

L'accesso all'interfaccia Web avviene attraverso una connessione sicura. Accertarsi di utilizzare **https**.

se la configurazione di XClarity Management Hub viene eseguita in remoto, è necessario disporre della connettività alla stessa rete di livello 2. L'accesso deve essere eseguito da un indirizzo non instradato fino al completamento della configurazione iniziale. Pertanto, è consigliabile eseguire l'accesso a XClarity Management Hub da un'altra macchina virtuale che disponga della connettività a XClarity Management Hub. Ad esempio, è possibile accedere a XClarity Management Hub da un'altra macchina virtuale sull'host in cui è installato XClarity Management Hub.

XClarity Management Hub disconnette automaticamente le sessioni utente dopo 60 minuti, indipendentemente dall'attività.

Procedura

Per eseguire il login all'interfaccia Web di XClarity Management Hub, attenersi alla procedura descritta di seguito.

- Passo 1. Puntare il browser all'indirizzo IP di XClarity Management Hub.
`https://<IPv4_address>`

Ad esempio:

https://192.0.2.10

L'indirizzo IP utilizzato dipende dalla modalità di configurazione dell'ambiente.

- Se è stato specificato un indirizzo IPv4 in `eth0_config`, utilizzare tale indirizzo IPv4 per accedere a XClarity Management Hub.
- Se un server DHCP è configurato nello stesso dominio di broadcast di XClarity Management Hub, utilizzare l'indirizzo IPv4 visualizzato nella console della macchina virtuale di XClarity Management Hub per accedere a XClarity Management Hub.
- Se le reti `eth0` e `eth1` si trovano in sottoreti diverse, e in entrambe viene usato DHCP, utilizzare l'indirizzo IP `eth1` per accedere all'interfaccia Web ed eseguire la configurazione iniziale. Al primo avvio di XClarity Management Hub sia `eth0` che `eth1` ottengono un indirizzo IP assegnato da DHCP mentre il gateway predefinito di XClarity Management Hub viene impostato sul gateway assegnato da DHCP per `eth1`.

Verrà visualizzata la pagina di login iniziale di XClarity Management Hub:



Passo 2. Selezionare la lingua desiderata dall'elenco a discesa **Lingua**.

Nota: i valori e le impostazioni di configurazione forniti dai dispositivi gestiti potrebbero essere disponibili solo in inglese.

Passo 3. Immettere le credenziali utente e fare clic su **Accedi**.

Se si accede a XClarity Management Hub per la prima volta, immettere le credenziali predefinite **USERID** e **PASSWORD** (dove 0 è zero).

Passo 4. Leggere e accettare il contratto di licenza.

Passo 5. Se si è eseguito il login per la prima volta utilizzando le credenziali predefinite, viene richiesto di modificare la password. Per impostazione predefinita, le password devono contenere da **8 a 256** caratteri e devono soddisfare i criteri seguenti.

Importante: Si consiglia di utilizzare password sicure formate da almeno 16 caratteri.


- (1) Deve contenere almeno un carattere alfabetico maiuscolo
- (2) Deve contenere almeno un carattere alfabetico minuscolo
- (3) Deve contenere almeno un numero
- (4) Deve contenere almeno un carattere speciale
- (5) Non deve coincidere con il nome utente


Passo 6. Se si è eseguito il login per la prima volta, viene richiesto di scegliere se utilizzare il certificato autofirmato corrente o un certificato con firma CA esterna. Se si sceglie di usare un certificato con firma esterna, viene visualizzata la pagina Certificato server.

Attenzione: Il certificato autofirmato non è sicuro. Si consiglia di generare e installare un certificato con firma esterna personalizzato.

Per informazioni sull'utilizzo di un certificato con firma esterna, vedere [Installazione di un certificato del server con firma esterna attendibile per XClarity Management Hub per i dispositivi client Edge](#).

Al termine

È possibile effettuare le seguenti azioni dal menu **Account utente** () nell'angolo superiore destro dell'interfaccia Web di XClarity Management Hub.

- È possibile effettuare il logout dalla sessione corrente facendo clic su **Disconnetti**. Viene visualizzata la pagina di login di XClarity Management Hub.
- Porre domande e individuare risposte sul [Sito Web del forum della community dedicata a Lenovo XClarity](#).
- Per inviare idee su XClarity Management Hub fare clic su **Invia idee** dal menu **Account utente** () nell'interfaccia Web nell'angolo in alto a destra o visitando direttamente il [Sito Web di Lenovo XClarity Ideation](#).
- Visualizzare la documentazione online facendo clic su **Guida per l'utente**.
- È possibile visualizzare le informazioni sulla versione di XClarity Management Hub facendo clic su **Informazioni su**.
- È possibile modificare la lingua dell'interfaccia utente facendo clic su **Modifica lingua**. Sono supportate le seguenti lingue.
 - Inglese (en)
 - Cinese semplificato (zh-CN)
 - Cinese tradizionale (zh-TW)
 - Francese (fr)
 - Tedesco (de)
 - Italiano (it)
 - Giapponese (ja)
 - Coreano (ko)
 - Portoghese brasiliano (pt-BR)
 - Russo (ru)
 - Spagnolo (es)
 - Tailandese (th)

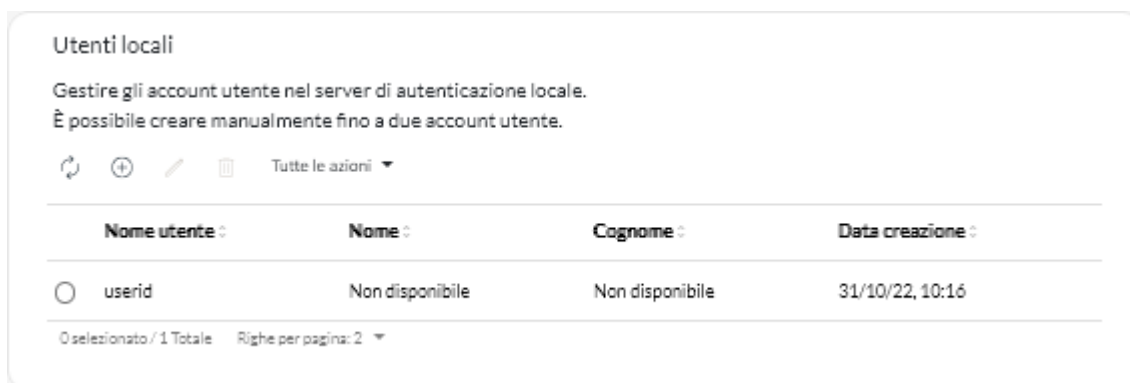
Creazione di account utente per Lenovo XClarity Management Hub per i dispositivi client Edge

È possibile creare fino a 10 account utente per Lenovo XClarity Management Hub.

Procedura

Per creare un account utente, completare le seguenti operazioni.

Passo 1. Sulla barra dei menu di Lenovo XClarity Management Hub fare clic su **Sicurezza** (🔒) → **Utenti locali** per visualizzare la scheda Utenti locali.



Passo 2. Fare clic sull'icona **Crea** (+) per creare un utente. Viene visualizzata la finestra di dialogo Crea nuovo utente.

Passo 3. Compilare le seguenti informazioni nella finestra di dialogo.

- Immettere un nome utente univoco. È possibile specificare fino a 32 caratteri, inclusi i caratteri alfanumerici, il punto (.), il trattino (-) e il carattere di sottolineatura (_).

Nota: per i nomi utente non viene fatta distinzione tra maiuscole e minuscole.

- Immettere e confermare le nuove password. Per impostazione predefinita, le password devono contenere da **8** a **256** caratteri e devono soddisfare i criteri seguenti.

Importante: Si consiglia di utilizzare password sicure formate da almeno 16 caratteri.

- (1) Deve contenere almeno un carattere alfabetico maiuscolo
- (2) Deve contenere almeno un carattere alfabetico minuscolo
- (3) Deve contenere almeno un numero
- (4) Deve contenere almeno un carattere speciale
- (5) Non deve coincidere con il nome utente

Passo 4. Fare clic su **Crea**.

L'account utente viene aggiunto alla tabella.

Al termine

Nella scheda Utenti locali è possibile effettuare le operazioni che seguono.

- Modificare la password e le proprietà dell'account utente facendo clic sull'icona **Modifica** (✎). Si tenga presente che le password non scadono.
- Eliminare un utente selezionato facendo clic sull'icona **Elimina** (🗑️).

Configurazione delle impostazioni di rete di XClarity Management Hub per i dispositivi client Edge

È possibile configurare una singola interfaccia di rete IPv4 e le impostazioni di routing Internet.

Prima di iniziare

Prima di configurare la rete, esaminare le relative considerazioni (vedere [Considerazioni sulla rete](#)).

Procedura

Per configurare le impostazioni di rete, fare clic su **Amministrazione** (🔧) → **Rete** sulla barra dei menu XClarity Management Hub ed effettuare una o più delle operazioni che seguono.

- **Configurare le impostazioni IP** Per l'interfaccia eth0 fare clic sulla scheda **Interfaccia Eth0**, configurare le impostazioni dell'indirizzo IPv4 applicabili e fare clic su **Applica**.

Attenzione:

- La modifica dell'indirizzo IP dell'appliance virtuale dopo l'installazione e l'esecuzione di XClarity Management Hub causerà problemi di connettività con XClarity Orchestrator e tutti i dispositivi gestiti. Se è necessario modificare l'indirizzo IP, disconnettere XClarity Management Hub da XClarity Orchestrator e annullare la gestione di tutti i dispositivi gestiti prima di modificare l'indirizzo IP. Quindi gestire nuovamente i dispositivi e riconnettere XClarity Management Hub a XClarity Orchestrator, una volta completata la modifica dell'indirizzo IP.

Attualmente, solo gli indirizzi IPv4 sono supportati.

- **Impostazioni IPv4.** È possibile configurare il metodo di assegnazione IP, l'indirizzo IPv4, la maschera di rete e il gateway predefinito. Per il metodo di assegnazione IP, è possibile scegliere di utilizzare un indirizzo IP assegnato staticamente oppure di ottenere un indirizzo IP da un server DHCP. Quando si utilizza un indirizzo IP statico, è necessario fornire un indirizzo IP, una maschera di rete e un gateway predefinito.

Il gateway predefinito, deve essere un indirizzo IP valido e utilizzare la stessa maschera di rete (la stessa sottorete) dell'interfaccia abilitata (eth0).

Se una delle due interfaccia utilizza DHCP per ottenere l'indirizzo IP, anche il gateway predefinito utilizza DHCP.

Interfaccia Eth0

Configurazione IPv4

Metodo: Ottieni indirizzo IP d...
 Maschera di rete IPv4: 255.255.255.0
 Intervallo IPv4: 10.241.54.20
 Gateway predefinito IPv4: 10.241.54.1

Applica Reimposta

Configurazione IPv6

Metodo: Utilizza configurazio...
 Lunghezza del prefisso IPv6:
 Indirizzo IPv6:
 Gateway predefinito IPv6:

Applica Reimposta

- **Configurare le impostazioni di routing di Internet** Configurare facoltativamente le impostazioni DNS (Domain Name System) dalla scheda Configurazione DNS. Fare quindi clic su **Applica**.

Attualmente, solo gli indirizzi IPv4 sono supportati.

È possibile modificare l'indirizzo IP per il server DNS.

Il nome FQDN (Fully-Qualified Domain Name) e il nome host del server DNS sono gli stessi del server XClarity Management Hub e non possono essere modificati.

Configurazione DNS

Tipo di indirizzi DNS preferiti: IPv4 IPv6

Indirizzo DNS*: 10.241.54.2
 FQDN: node-64021cc6.lenovo.com

Nome host: Imh

Applica Reimposta

Configurazione di data e ora di XClarity Management Hub per i dispositivi client Edge

È necessario impostare almeno uno (e fino a quattro) server NTP (Network Time Protocol) per sincronizzare i timestamp tra XClarity Management Hub e tutti i dispositivi gestiti.

Prima di iniziare

Ogni server NTP deve essere accessibile in rete. Valutare la possibilità di configurare il server NTP sul sistema locale in cui XClarity Management Hub è in esecuzione.

Se si modifica l'ora sul server NTP, la sincronizzazione di XClarity Management Hub con la nuova ora potrebbe richiedere tempo.

Attenzione: L'appliance virtuale XClarity Management Hub e il relativo host devono essere impostati per sincronizzarsi con la stessa origine dell'ora, in modo da impedire l'errata sincronizzazione oraria tra XClarity Management Hub e il relativo host. In genere, l'host è configurato per sincronizzarsi con l'ora delle rispettive appliance virtuali. Se XClarity Management Hub è impostato per sincronizzarsi con un'origine differente rispetto all'host, è necessario disabilitare la sincronizzazione oraria dell'host tra l'appliance virtuale XClarity Management Hub e il rispettivo host.

- Per ESXi, seguire le istruzioni sulla [VMware - Pagina Web sulla disabilitazione della sincronizzazione dell'ora](#).

Procedura

Per l'impostazione della data e dell'ora di XClarity Management Hub, completare le seguenti operazioni.

Passo 1. Dalla barra dei menu di XClarity Management Hub fare clic su **Amministrazione** (⚙️) → **Data e ora** per visualizzare la scheda Data e ora.

The screenshot shows the 'Data e ora' configuration page in XClarity Management Hub. At the top, it states 'Data e ora verranno sincronizzate automaticamente con il server NTP'. Below this, the current date is '04/10/22' and the time is '18:50:59'. The time zone is set to 'UTC -00:00, Coordinated Universal Time Universal'. A light blue notification box contains the text: 'Una volta applicate le modifiche, questa pagina verrà aggiornata automaticamente per ottenere la configurazione più recente.' Below the notification, there is a dropdown menu for 'Fuso orario' currently showing 'UTC -00:00, Coordinated Universal Time Universal'. Underneath is a text input field for 'Server NTP' with the placeholder 'Server NTP 1 Indirizzo FQDN o IP'. At the bottom left, there is a '+ Aggiungi nuovo server NTP' button. At the bottom center, there is an 'Applica' button.

Passo 2. Scegliere il fuso orario in cui si trova l'host per XClarity Management Hub.

Se il fuso orario selezionato osserva l'ora legale, l'ora viene automaticamente regolata di conseguenza.

Passo 3. Specificare il nome host o l'indirizzo IP di ciascun server NTP nella rete. È possibile definire fino a quattro server NTP.

Passo 4. Fare clic su **Applica**.

Gestione dei certificati di sicurezza di Lenovo XClarity Management Hub per i dispositivi client Edge

Lenovo XClarity Management Hub utilizza i certificati SSL per stabilire comunicazioni sicure e attendibili tra Lenovo XClarity Management Hub e i propri dispositivi gestiti, nonché comunicazioni con Lenovo XClarity Management Hub da parte degli utenti o con servizi diversi. Per impostazione predefinita, Lenovo XClarity Management Hub e XClarity Orchestrator utilizzano i certificati generati da XClarity Orchestrator, autofirmati e pubblicati da un'autorità di certificazione interna.

Prima di iniziare

Questa sezione è dedicata agli amministratori con nozioni di base sugli standard SSL e sui certificati SSL, che ne conoscono la definizione e sanno come gestirli. Per informazioni generali sui certificati di chiave pubblica, vedere [Pagina Web di X.509 su Wikipedia](#) e [Pagina Web - Profilo certificato di infrastruttura con chiave pubblica Internet X.509 e CRL \(Certificate Revocation List\) \(RFC5280\)](#).

Informazioni su questa attività

Il certificato server predefinito, generato in modo univoco in ogni istanza di Lenovo XClarity Management Hub, fornisce misure di sicurezza sufficienti per molti ambienti. È possibile delegare la gestione dei certificati a Lenovo XClarity Management Hub oppure avere un ruolo più attivo personalizzando e sostituendo i certificati server. Lenovo XClarity Management Hub fornisce le opzioni per personalizzare i certificati dell'ambiente. Ad esempio, è possibile scegliere di:

- Generare una nuova coppia di chiavi rigenerando l'autorità di certificazione interna e/o il certificato server finale che utilizzano i valori specifici dell'organizzazione.
- Generare una richiesta di firma del certificato (CSR) da inviare all'autorità di certificazione preferita per firmare un certificato personalizzato che può quindi essere caricato in Lenovo XClarity Management Hub ed essere utilizzato come certificato end-server per tutti i rispettivi servizi in hosting.
- Scaricare il certificato del server nel sistema locale in modo da importarlo nell'elenco del browser Web dei certificati attendibili.

Lenovo XClarity Management Hub fornisce diversi servizi che accettano le connessioni SSL/TLS in entrata. Quando un client, come un browser Web, si collega a uno di questi servizi, Lenovo XClarity Management Hub fornisce il rispettivo *certificato server* per essere identificato dal client che sta tentando di connettersi. Il client deve mantenere un elenco di certificati ritenuti attendibili. Se il certificato server di Lenovo XClarity Management Hub non è nell'elenco, il client si disconnette da Lenovo XClarity Management Hub per evitare lo scambio di informazioni di sicurezza riservate con un'origine non attendibile.

Lenovo XClarity Management Hub funge da client durante la comunicazione con dispositivi gestiti e servizi esterni. In questo caso, il dispositivo gestito o il servizio esterno sottopone il relativo certificato server a Lenovo XClarity Management Hub per la verifica. Lenovo XClarity Management Hub gestisce un elenco di certificati ritenuti attendibili. Se il *certificato attendibile* fornito dal dispositivo gestito o dal servizio esterni non è nell'elenco, Lenovo XClarity Management Hub si disconnette dal dispositivo gestito o dal servizio esterno al fine di evitare lo scambio di eventuali informazioni di sicurezza riservate con un'origine non attendibile.

La seguente categoria di certificati viene utilizzata dai servizi di Lenovo XClarity Management Hub e deve essere considerata attendibile da qualsiasi client che vi si connette.

- **Certificato server.** Durante l'avvio iniziale vengono generati una chiave univoca e un certificato autofirmato. Entrambi vengono utilizzati come autorità di certificazione radice predefinita, gestibile dalla pagina Autorità di certificazione tra le impostazioni di sicurezza di Lenovo XClarity Management Hub. Non è necessario rigenerare questo certificato radice, a meno che la chiave non sia stata compromessa o la politica della propria organizzazione non preveda la sostituzione periodica di tutti i certificati (vedere

[Rigenerazione del certificato server autofirmato di XClarity Management Hub per i dispositivi client Edge](#)). Durante la configurazione iniziale viene generata una chiave separata e un certificato server viene creato e sottoscritto dall'autorità di certificazione interna. Questo certificato viene utilizzato come certificato server predefinito di Lenovo XClarity Management Hub. Esso si rigenera automaticamente ogni volta che Lenovo XClarity Management Hub rileva che i rispettivi indirizzi di rete (indirizzi DNS o IP) sono stati modificati per garantire che il certificato contenga gli indirizzi corretti per il server. Può essere personalizzato e generato su richiesta (vedere [Rigenerazione del certificato server autofirmato di XClarity Management Hub per i dispositivi client Edge](#)).

È possibile scegliere di utilizzare un certificato del server con firma esterna invece del certificato server autofirmato predefinito, generando una richiesta di firma del certificato (CSR), disponendo di una CSR firmata da un'autorità di certificazione radice privata o commerciale e importando quindi la catena di certificati completa in Lenovo XClarity Management Hub (vedere [Installazione di un certificato del server con firma esterna attendibile per XClarity Management Hub per i dispositivi client Edge](#)).

Se si sceglie di utilizzare il certificato del server autofirmato predefinito, è consigliabile importare il certificato del server nel browser Web come autorità radice attendibile per evitare messaggi di errore del certificato nel browser (vedere [Importazione del certificato del server in un browser Web per Lenovo XClarity Management Hub per i dispositivi client Edge](#)).

- **Certificato di distribuzione del sistema operativo.** Un certificato separato viene utilizzato dal servizio di distribuzione del sistema operativo per garantire che il programma di installazione del sistema operativo possa connettersi in modo sicuro al servizio di distribuzione durante il processo di distribuzione. Se la chiave è stata compromessa, è possibile rigenerarla riavviando Lenovo XClarity Management Hub.

Rigenerazione del certificato server autofirmato di XClarity Management Hub per i dispositivi client Edge

È possibile generare un nuovo certificato del server per sostituire il certificato del server Lenovo XClarity Management Hub autofirmato corrente o per reintegrare un certificato generato da XClarity Management Hub se attualmente XClarity Management Hub utilizza un certificato personalizzato del server con firma esterna. Il nuovo certificato del server autofirmato viene usato da XClarity Management Hub per l'accesso HTTPS.

Prima di iniziare

Attenzione: Se si rigenera il certificato del server XClarity Management Hub utilizzando una nuova autorità di certificazione radice, la connessione di XClarity Management Hub ai dispositivi gestiti viene interrotta ed è necessario gestire di nuovo i dispositivi. Se si rigenera il certificato del server XClarity Management Hub senza modificare l'autorità di certificazione radice (ad esempio, quando il certificato è scaduto), non è necessario gestire nuovamente i dispositivi.

Informazioni su questa attività

Il certificato del server corrente, sia esso autofirmato o con firma esterna, rimane in uso finché non viene generato, firmato e installato un nuovo certificato del server.

Importante: Dopo avere modificato il certificato del server, l'hub di gestione viene riavviato e tutte le sessioni utente vengono terminate. Gli utenti devono eseguire di nuovo il login per continuare a utilizzare l'interfaccia Web.

Procedura

Per generare un certificato del server XClarity Management Hub autofirmato, completare le seguenti operazioni.

Passo 1. Sulla barra dei menu di XClarity Management Hub fare clic su **Sicurezza** (🔒) → **Certificato server** per visualizzare la nuova scheda **Rigenera certificato server autofirmato**.

Rigenera certificato server

Generare una nuova chiave e un nuovo certificato utilizzando i dati forniti per il certificato.

Paese/Area geografica*
UNITED STATES

Organizzazione*
Lenovo

Stato/Provincia*
NC

Unità organizzativa*
DCG

Città*
Raleigh

Nome comune*
Generated by Lenovo Management Ecosystem

Data Non valido prima
03/Ottobre/2022 13:21

Non valido dopo la data*
30/Settembre/2032 13:21

Rigenera certificato Salva certificato Reimposta certificato

Passo 2. Nella scheda **Rigenera certificato server autofirmato** compilare i campi per la richiesta.

- Codice ISO 3166 di due lettere per il paese o l'area geografica di origine da associare all'organizzazione del certificato (ad esempio, US per gli Stati Uniti).
- Nome completo dello stato o della provincia da associare al certificato (ad esempio, California o New Brunswick).
- Nome completo della città da associare al certificato (ad esempio, San Jose). La lunghezza del valore non può superare i 50 caratteri.
- Organizzazione (azienda) che deve possedere il certificato. In genere, questo è il nome giuridicamente riconosciuto di un'azienda. Dovrebbe includere un suffisso, quale Ltd., Inc. o Corp (ad esempio, ACME International Ltd.). La lunghezza di questo valore non può superare i 60 caratteri.
- (Facoltativo) Unità organizzativa che deve possedere il certificato (ad esempio, divisione ABC). La lunghezza di questo valore non può superare i 60 caratteri.
- Nome comune del proprietario del certificato. In genere, questo è il nome di dominio completo (FQDN) o l'indirizzo IP del server che utilizza il certificato (ad esempio, www.domainname.com o 192.0.2.0). La lunghezza di questo valore non può superare i 63 caratteri.

Nota: Attualmente questo attributo non ha alcun effetto sul certificato.

- Data e ora in cui il certificato del server non è più valido.

Nota: Attualmente questi attributi non hanno alcun effetto sul certificato.

Nota: Non è possibile cambiare i nomi alternativi dell'oggetto durante la rigenerazione del certificato del server.

Passo 3. Fare clic su **Rigenera certificato server autofirmato** per rigenerare il certificato autofirmato e selezionare **Rigenera certificato** per confermare. L'hub di gestione viene riavviato e tutte le sessioni utente consolidate vengono terminate.

Passo 4. Eseguire di nuovo il login al browser Web.

Al termine

Nella scheda Rigenera certificato server autofirmato è possibile effettuare le operazioni che seguono.

- Salvare il certificato corrente del server sul sistema locale in formato PEM facendo clic su **Salva certificato**.
- Rigenerare il certificato del server utilizzando l'impostazione predefinita facendo clic su **Reimposta certificato**. Quando richiesto, premere Ctrl + F5 per aggiornare il browser, quindi ristabilire la connessione all'interfaccia Web.

Installazione di un certificato del server con firma esterna attendibile per XClarity Management Hub per i dispositivi client Edge

È possibile scegliere di utilizzare un certificato del server attendibile firmato da un'autorità di certificazione (CA) privata o commerciale. Per utilizzare un certificato del server con firma esterna, generare una richiesta di firma del certificato (CSR) e importare il certificato server risultante per sostituire il certificato server esistente.

Prima di iniziare

Attenzione:

- Se si installa un certificato del server Lenovo XClarity Management Hub con firma esterna utilizzando una nuova autorità di certificazione radice, la connessione di XClarity Management Hub ai dispositivi gestiti viene interrotta ed è necessario gestire di nuovo i dispositivi. Se si installa un certificato del server Lenovo XClarity Management Hub con firma esterna senza modificare l'autorità di certificazione radice (ad esempio, quando il certificato è scaduto), non è necessario gestire nuovamente i dispositivi.
- Se si aggiungono nuovi dispositivi dopo la generazione della CSR e prima dell'importazione del certificato firmato del server, è necessario riavviare tali dispositivi per ricevere il nuovo certificato del server.

Informazioni su questa attività

Si consiglia di utilizzare sempre certificati con firma v3.

Il certificato del server con firma esterna deve essere creato tramite la richiesta di firma del certificato generata più di recente utilizzando il pulsante **Genera file CSR**.

Il contenuto del certificato del server con firma esterna deve essere un bundle di certificati contenente l'intera catena di firme della CA, come il certificato radice della CA, i certificati intermedi e il certificato del server.

Se il nuovo certificato del server non è stato firmato da una terza parte attendibile, alla successiva connessione a Lenovo XClarity Management Hub, nel browser Web, verranno visualizzati un avviso di sicurezza e una finestra di dialogo in cui verrà chiesto di accettare il nuovo certificato nel browser. Per evitare gli avvisi di sicurezza, è possibile importare il certificato del server nell'elenco dei certificati attendibili del browser Web (vedere [Importazione del certificato del server in un browser Web per Lenovo XClarity Management Hub per i dispositivi client Edge](#)).

XClarity Management Hub inizia a utilizzare il nuovo certificato del server senza terminare la sessione corrente. Le nuove sessioni verranno stabilite utilizzando il nuovo il certificato. Per utilizzare il nuovo certificato, riavviare il browser Web.

Importante: Quando il certificato del server viene modificato, in tutte le sessioni utente consolidate è necessario accettare il nuovo certificato facendo clic su Ctrl + F5 per aggiornare il browser Web e ristabilire la connessione a XClarity Management Hub.

Procedura

Per generare e installare un certificato del server con firma esterna, effettuare le operazioni che seguono.

Passo 1. Creare una richiesta di firma del certificato e salvare il file nel sistema locale.

1. Sulla barra dei menu di XClarity Management Hub fare clic su **Sicurezza** (🔒) → **Certificato server** per visualizzare la scheda Genera CSR (Certificate Signing Request).

Genera CSR (Certificate Signing Request)

Crea e salva una richiesta di firma del certificato utilizzando i valori forniti dall'utente.

Paese/Area geografica*
UNITED STATES

Organizzazione*
Lenovo

Stato/Provincia*
NC

Unità organizzativa*
DCG

Città*
Raleigh

Nome comune*
Generated by Lenovo Management Ecosystem

Nomi alternativi oggetto ?

Per aggiungere un nuovo nome alternativo dell'oggetto, fare clic su +

Genera file CSR Importa certificato

2. Nella scheda Genera CSR (Certificate Signing Request) compilare i campi per la richiesta.

- Codice ISO 3166 di due lettere per il paese o l'area geografica di origine associato all'organizzazione del certificato (ad esempio, US per gli Stati Uniti).
- Nome completo dello stato o della provincia da associare al certificato (ad esempio, California o New Brunswick).
- Nome completo della città da associare al certificato (ad esempio, San Jose). La lunghezza del valore non può superare i 50 caratteri.
- Organizzazione (azienda) che deve possedere il certificato. In genere, questo è il nome giuridicamente riconosciuto di un'azienda. Dovrebbe includere un suffisso, quale Ltd., Inc. o Corp (ad esempio, ACME International Ltd.). La lunghezza di questo valore non può superare i 60 caratteri.
- (Facoltativo) Unità organizzativa che deve possedere il certificato (ad esempio, divisione ABC). La lunghezza di questo valore non può superare i 60 caratteri.
- Nome comune del proprietario del certificato. Deve essere il nome host del server che utilizza il certificato. La lunghezza di questo valore non può superare i 63 caratteri.

Nota: Attualmente questo attributo non ha alcun effetto sul certificato.

- Facoltativo: i nomi alternativi dell'oggetto che vengono personalizzati, eliminati e aggiunti all'estensione "subjectAltName" X.509 quando viene generata una richiesta CSR. I nomi alternativi dell'oggetto specificati vengono convalidati (in base al tipo specificato) e aggiunti

al CSR solo dopo aver generato una richiesta CSR. Per impostazione predefinita, XClarity Management Hub definisce automaticamente i nomi alternativi dell'oggetto per la richiesta CSR in base all'indirizzo IP e al nome host rilevati dalle interfacce di rete del sistema operativo guest di XClarity Management Hub.

Attenzione: I nomi alternativi dell'oggetto devono includere il nome FQDN (Fully-Qualified Domain Name) o l'indirizzo IP dell'hub di gestione e il nome dell'oggetto deve essere impostato sul nome FQDN dell'hub di gestione. Verificare che questi campi obbligatori siano presenti e corretti prima di iniziare il processo CSR per assicurarsi che il certificato risultante sia completo. Eventuali dati mancanti nel certificato potrebbero avere come conseguenza connessioni non attendibili quando si tenta di connettere l'hub di gestione a Lenovo XClarity Orchestrator.

Il nome specificato deve essere valido per il tipo selezionato.

- **DNS** (utilizzare il nome FQDN, ad esempio, hostname.labs.company.com)
- **Indirizzo IP** (ad esempio, 192.0.2.0)
- **e-mail** (ad esempio, example@company.com)

Passo 2. Fornire la CSR a un'autorità di certificazione (CA) attendibile. L'autorità di certificazione firma la richiesta CSR e restituisce un certificato del server.

Passo 3. Importare il certificato del server con firma esterna e il certificato CA in XClarity Management Hub e sostituire il certificato corrente del server.

1. Nella scheda Genera CSR (Certificate Signing Request) fare clic su **Importa certificato** per visualizzare la finestra di dialogo Importa certificato.
2. Copiare e incollare il certificato del server e il certificato CA in formato PEM. È necessario fornire l'intera catena di certificati, a partire dal certificato del server per finire con il certificato CA radice.
3. Fare clic su **Importa** per archiviare il certificato del server nell'archivio attendibile di XClarity Management Hub.

Passo 4. Accettare il nuovo certificato premendo Ctrl + F5 per aggiornare il browser, quindi ristabilire la connessione all'interfaccia Web. Questa operazione deve essere eseguita in tutte le sessioni utente consolidate.

Importazione del certificato del server in un browser Web per Lenovo XClarity Management Hub per i dispositivi client Edge

È possibile salvare una copia del certificato corrente del server in formato PEM nel sistema locale. È quindi possibile importare il certificato nell'elenco dei certificati attendibili del browser Web o in altre applicazioni per evitare gli avvisi di sicurezza del browser Web durante l'accesso a Lenovo XClarity Management Hub.

Procedura

Per importare il certificato del server in un browser Web, effettuare le operazioni che seguono.

- **Chrome**

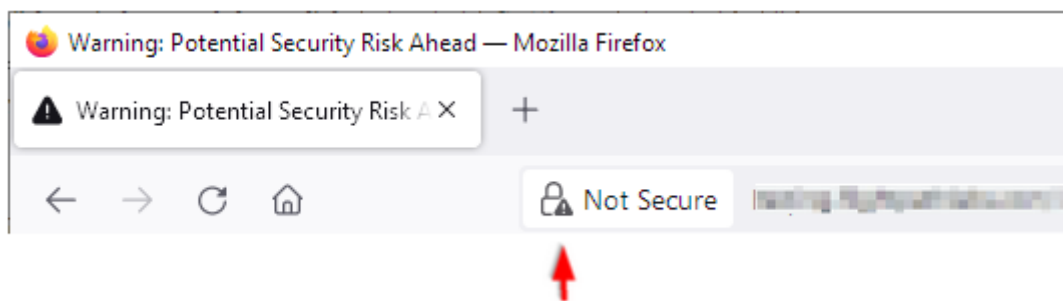
1. Esportare il certificato del server Lenovo XClarity Management Hub.
 - a. Fare clic sull'icona di avvertenza "Non sicuro" nella barra degli indirizzi superiore, ad esempio:



- b. Fare clic su **Certificato non valido** per visualizzare la finestra di dialogo Certificato.
 - c. Fare clic sulla scheda **Dettagli**.
 - d. Fare clic su **Esporta**.
 - e. Specificare il nome e la posizione del file del certificato, quindi selezionare **Salva** per esportare il certificato.
 - f. Chiudere la finestra di dialogo Visualizzazione certificati.
2. Importare il certificato del server Lenovo XClarity Management Hub nell'elenco dei certificati radice attendibili dell'autorità per il browser in uso.
 - a. Dal browser Chrome, fare clic sui tre punti nell'angolo superiore destro della finestra, quindi selezionare **Impostazioni** per aprire la pagina Impostazioni.
 - b. Fare clic su **Privacy e sicurezza**, quindi selezionare **Sicurezza** per visualizzare la pagina Sicurezza.
 - c. Scorrere fino alla sezione **Avanzate** e fare clic su **Gestisci certificati dispositivo**.
 - d. Fare clic su **Importa** e selezionare **Avanti**.
 - e. Selezionare il file del certificato esportato in precedenza, quindi fare clic su **Avanti**.
 - f. Scegliere la posizione in cui archiviare il certificato e fare clic su **Avanti**.
 - g. Fare clic su **Fine**.
 - h. Chiudere e riaprire il browser Chrome, quindi aprire Lenovo XClarity Management Hub.

- **Firefox**

1. Esportare il certificato del server Lenovo XClarity Management Hub.
 - a. Fare clic sull'icona di avvertenza "Non sicuro" nella barra degli indirizzi superiore, ad esempio:



- b. Fare clic su **Connessione non sicura**, quindi selezionare **Ulteriori informazioni**.
 - c. Fare clic su **Visualizza certificato**.
 - d. Scorrere verso il basso fino alla sezione **Varie** e fare clic sul collegamento **PEM (cert)** per salvare il file nel sistema locale.
2. Importare il certificato del server Lenovo XClarity Management Hub nell'elenco dei certificati radice attendibili dell'autorità per il browser in uso.
 - a. Aprire il browser e fare clic su **Strumenti** → **Impostazioni**, quindi selezionare **Privacy e sicurezza**.
 - b. Scorrere verso il basso alla sezione **Sicurezza**.

- c. Fare clic su **Visualizza certificati** per visualizzare la finestra di dialogo Gestione certificati.
- d. Fare clic sulla scheda **I tuoi certificati**.
- e. Fare clic su **Importa** e accedere alla posizione in cui è stato scaricato il certificato.
- f. Selezionare il certificato e fare clic su **Apri**.
- g. Chiudere la finestra di dialogo Gestione certificati.

Collegamento di XClarity Management Hub per i dispositivi client Edge a XClarity Orchestrator

Una volta registrato (connesso) Lenovo XClarity Management Hub con Lenovo XClarity Orchestrator, è possibile iniziare a gestire e monitorare i dispositivi.

Prima di iniziare

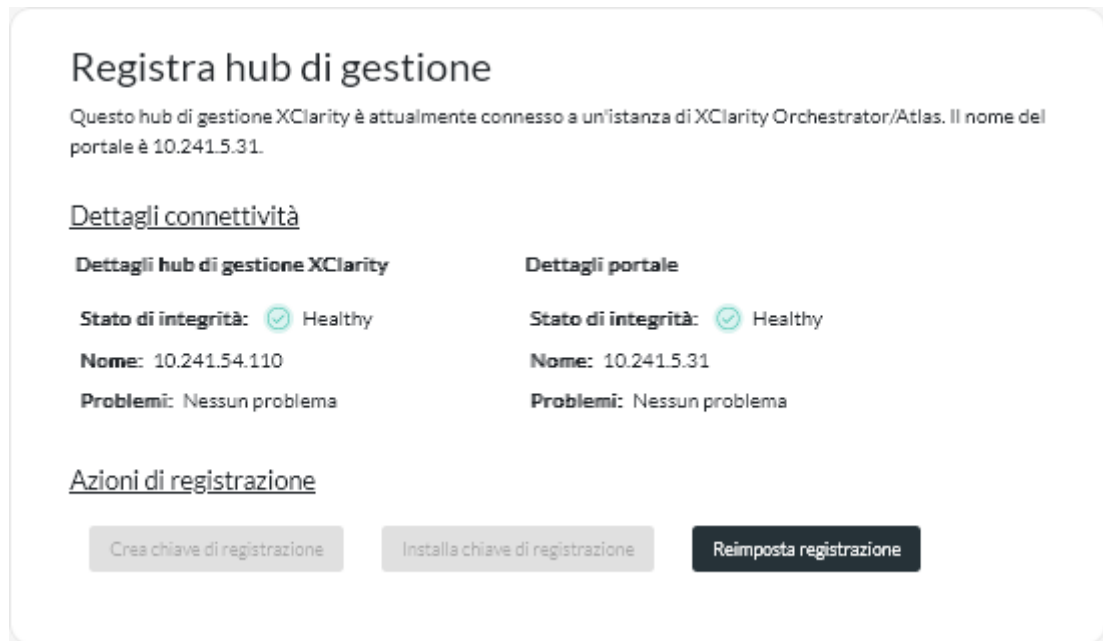
Accertarsi che XClarity Management Hub sia raggiungibile in rete da XClarity Orchestrator e che XClarity Orchestrator sia raggiungibile in rete da XClarity Management Hub.

Procedura

Per registrare XClarity Management Hub, completare i seguenti passaggi.

Passo 1. Creare la chiave di registrazione dell'hub di gestione.

1. Sulla barra dei menu del Management Hub fare clic su **Registrazione** per visualizzare la pagina Registrazione.




2. Fare clic su **Crea chiave di registrazione**.
3. Fare clic su **Copia negli Appunti** per copiare la chiave di registrazione e chiudere la finestra di dialogo.

Passo 2. Aggiungere la chiave di registrazione dell'hub di gestione a XClarity Orchestrator.

1. Dalla barra dei menu di XClarity Orchestrator, fare clic su **Risorse** (🔍) → **Strumenti di gestione delle risorse** per visualizzare la scheda Strumenti di gestione delle risorse.

2. Fare clic sull'icona **Connetti** (+) per visualizzare lo strumento di gestione delle risorse. Viene visualizzata la finestra di dialogo Connetti strumento di gestione delle risorse.



3. Selezionare **XClarity Management Hub** come strumento di gestione delle risorse.
4. Copiare la chiave di registrazione nel campo **Token di registrazione**.
5. Fare clic su **Connetti** per visualizzare la finestra di dialogo Connetti strumento di gestione delle risorse che contiene la chiave di registrazione di XClarity Orchestrator.
6. Fare clic su **Copia negli Appunti** per copiare la chiave di registrazione e chiudere la finestra di dialogo.

Passo 3. Aggiungere la chiave di registrazione di XClarity Orchestrator all'hub di gestione.

1. Dalla barra dei menu del Management Hub, fare clic su **Registrazione** per visualizzare la pagina Registrazione.
2. Fare clic su **Installa chiave di registrazione**.
3. Copiare la chiave di registrazione nel campo **Token di registrazione**.
4. Fare clic su **Connetti**.

Al termine

- Gestire i dispositivi mediante l'hub di gestione (vedere [Gestione dei dispositivi client ThinkEdge](#) nella documentazione online di XClarity Orchestrator).
- Eliminare la chiave di registrazione dell'hub di gestione corrente, facendo clic su **Reimposta registrazione**.

Capitolo 3. Disinstallazione di XClarity Management Hub per i dispositivi client Edge

Completare la seguente procedura per disinstallare un'appliance virtuale di XClarity Management Hub.

Procedura

Per disinstallare l'appliance virtuale di XClarity Management Hub, attenersi alla procedura descritta di seguito.

Passo 1. Annullare la gestione di tutti i dispositivi attualmente gestiti da XClarity Management Hub.

Passo 2. Disinstallare XClarity Management Hub, a seconda del sistema operativo.

- **ESXi**

1. Connettersi all'host tramite VMware vSphere Client.
2. Fare clic con il pulsante destro del mouse sulla macchina virtuale e scegliere **Alimentazione → Spegni**.
3. Fare nuovamente clic con il pulsante destro del mouse sulla macchina virtuale e scegliere **Elimina dal disco**.

Lenovo