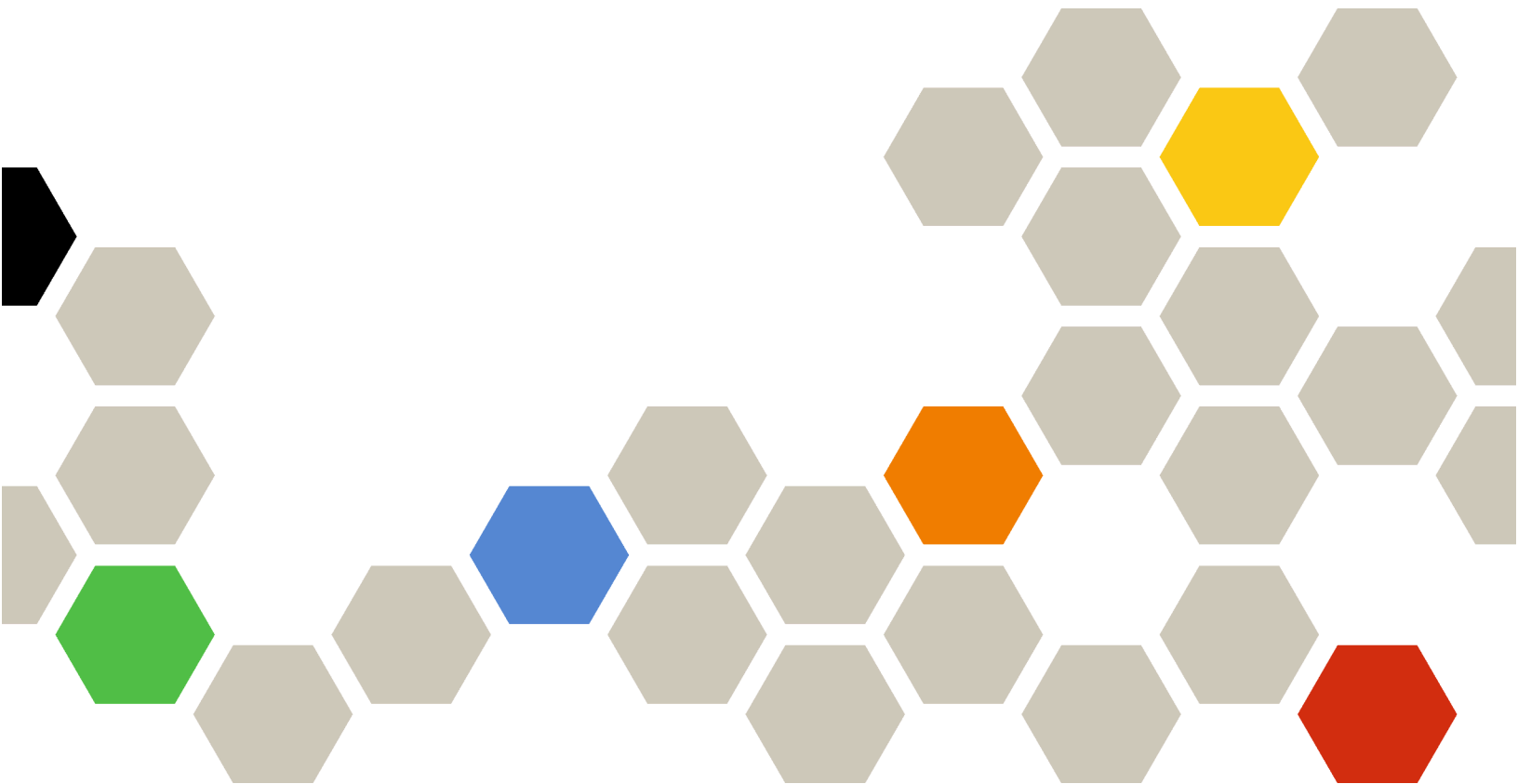




Lenovo XClarity Orchestrator

Guida all'installazione e alla pianificazione



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 2020, 2024.

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

Riepilogo delle modificheiii

Capitolo 1. Pianificazione per XClarity Orchestrator 1

Licenze	1
Hardware e software supportati	2
Firewall e server proxy	5
Disponibilità della porta	6
Considerazioni sulla rete	8
Considerazioni sulla sicurezza	8
Considerazioni su un ambiente sicuro	8
Considerazioni sulla crittografia	9
Considerazioni sui certificati di sicurezza	9
Considerazioni sul server di autenticazione	10
Considerazioni sul controllo degli accessi	10
Considerazioni sulla disponibilità elevata	10

Capitolo 2. Installazione di XClarity Orchestrator 13

Capitolo 3. Implementazione dell'alta disponibilità 17

Implementazione dell'alta disponibilità (Hyper-V)	17
Implementazione dell'alta disponibilità (ESXi)	18

Capitolo 4. Configurazione di XClarity Orchestrator per la prima volta 21

Primo accesso all'interfaccia Web di XClarity Orchestrator	21
Creazione di un utente locale	23
Configurazione della rete	25
Configurazione di data e ora	27
Configurazione del server di autenticazione	29
Configurazione delle impostazioni di sicurezza aggiuntive	32
Configurazione e abilitazione della notifica automatica dei problemi (Call Home)	33
Configurazione dell'inoltro dei dati degli eventi	35
Connessione degli strumenti di gestione delle risorse	36

Capitolo 5. Applicazione delle licenze per XClarity Orchestrator 41

Capitolo 6. Aggiornamento di XClarity Orchestrator 47

Capitolo 7. Disinstallazione di XClarity Orchestrator 53

Riepilogo delle modifiche

Le versioni successive del software di gestione Lenovo XClarity Orchestrator forniscono il supporto per i nuovi miglioramenti software e le correzioni.

Per informazioni sulle correzioni, fare riferimento al file di cronologia modifiche (*.chg) fornito nel pacchetto di aggiornamento.

Questa versione supporta i seguenti miglioramenti per la pianificazione e l'installazione. Per informazioni sulle modifiche delle versioni precedenti, vedere [Novità](#) nella documentazione online di XClarity Orchestrator.

Funzione	Descrizione
Pianificazione e installazione	XClarity Orchestrator richiede almeno 8 core del processore virtuale (vedere Hardware e software supportati).

Capitolo 1. Pianificazione per XClarity Orchestrator

Licenze

Lenovo XClarity Orchestrator è un'applicazione a pagamento. È possibile utilizzare XClarity Orchestrator gratuitamente per un massimo di 90 giorni con la licenza di prova gratuita; tuttavia, una volta terminata la prova gratuita, è necessario acquistare e installare le licenze appropriate per continuare a utilizzare le funzioni di assistenza e supporto di XClarity Orchestrator.

XClarity Orchestrator supporta le seguenti licenze.

- **XClarity Orchestrator.** Abilita le funzioni di Orchestrator e di gestione di base per server, chassis, switch e dispositivi di storage, nonché la licenza di assistenza e supporto per XClarity Orchestrator. Per le funzioni di Orchestrator, è richiesta una licenza in XClarity Orchestrator per ogni dispositivo che supporta la configurazione del server e la distribuzione del sistema operativo. Per il servizio e il supporto di XClarity Orchestrator, è richiesta una licenza per *ogni dispositivo gestito*.

La conformità della licenza viene determinata in base al numero di dispositivi gestiti. Il numero di dispositivi gestiti non deve superare il numero totale di licenze in tutte le chiavi di licenza attive di XClarity Orchestrator. Quando il numero di licenze di XClarity Orchestrator non è conforme al numero richiesto di licenze (ad esempio, se una licenza scade o se la gestione dei dispositivi aggiuntivi supera il numero totale di licenze attive), è necessario un periodo di tolleranza di 90 giorni per installare le licenze appropriate. Se il periodo di tolleranza (inclusa la versione di prova gratuita) delle licenze termina prima dell'installazione del numero di licenze richiesto, *tutte* le funzioni di XClarity Orchestrator (inclusi monitoraggio, gestione di base e analisi) vengono disabilitate. Quando si esegue il login, si viene reindirizzati alla pagina informativa della licenza in cui è possibile applicare licenze aggiuntive.

Ad esempio, se si gestiscono altri 100 server ThinkSystem e 20 switch rack mediante un'istanza esistente di XClarity Administrator gestita mediante XClarity Orchestrator, sono necessari 90 giorni per l'acquisto e l'installazione di 100 licenze aggiuntive di XClarity Orchestrator prima che tutte le funzioni siano disabilitate nell'interfaccia utente. Le licenze per i 20 switch rack non sono necessarie per utilizzare le funzioni di XClarity Orchestrator; tuttavia, sono richieste se si desidera assistenza e supporto per XClarity Orchestrator. Se le funzioni di XClarity Orchestrator sono disabilitate, vengono riabilite dopo aver installato una quantità di licenze sufficiente a ottenere nuovamente la conformità.

Importante: La licenza di base di XClarity Orchestrator è un prerequisito per le licenze di analisi di XClarity Pro e XClarity Orchestrator. Se il numero di licenze di XClarity Pro o XClarity Orchestrator è conforme, ma il numero di licenze di base attive *non lo* è, tutte le funzioni di XClarity Orchestrator (incluse le funzioni di analisi) sono disabilitate per tutti i dispositivi.

- **Lenovo XClarity Pro.** Abilita le funzioni di gestione avanzate (configurazione del server e distribuzione del sistema operativo). È richiesta una licenza in XClarity Orchestrator per ogni dispositivo che supporta le funzioni di gestione avanzate.

La conformità della licenza viene determinata in base al numero di dispositivi gestiti. Il numero di dispositivi gestiti non deve superare il numero totale di licenze in tutte le chiavi di licenza attive di XClarity Pro. Quando il numero di licenze di XClarity Pro non è conforme, si dispone di un periodo di tolleranza di 90 giorni per installare le licenze appropriate. Se il periodo di tolleranza (inclusa la versione di prova gratuita) termina prima dell'installazione del numero di licenze richiesto, le funzioni di configurazione e di distribuzione del sistema operativo vengono disabilitate per *tutti i dispositivi*.

Per ulteriori informazioni sulle licenze di XClarity Pro, vedere [Licenze e versione di prova gratuita per 90 giorni](#) nella documentazione online di XClarity Administrator.

- **XClarity Orchestrator Analisi.** Abilita le funzioni di analisi. È richiesta una licenza in XClarity Orchestrator per ogni dispositivo che supporta le funzioni di gestione avanzate.

La conformità della licenza viene determinata in base al numero di dispositivi gestiti. Il numero di dispositivi gestiti non deve superare il numero totale di licenze in tutte le chiavi di licenza di analisi attive di XClarity Orchestrator. Quando il numero di licenze di XClarity Orchestrator non è conforme al numero richiesto di licenze di analisi (ad esempio, se una licenza scade o se la gestione dei dispositivi aggiuntivi supera il numero totale di licenze attive), è necessario un periodo di tolleranza di 90 giorni per installare le licenze appropriate. Se il periodo di tolleranza (inclusa la versione di prova gratuita) per le licenze di analisi di termina prima dell'installazione del numero di licenze richiesto, i menu **Monitoraggio → Analisi** vengono disabilitati e non è possibile visualizzare i report di analisi o creare regole di avviso personalizzate e query per *tutti i dispositivi*.

Importante: Dopo aver installato le licenze di analisi di XClarity Orchestrator, è necessario aggiornare l'interfaccia utente.

Nota: Se si installano le licenze di analisi di XClarity Orchestrator scadute (che hanno superato la data di scadenza oltre il periodo di tolleranza di 90 giorni) e quindi si aggiorna l'interfaccia utente, le funzioni di analisi sono disabilitate. Ciò significa che un periodo di prova o di tolleranza attivo viene interrotto, che i servizi di analisi sono stati arrestati e che le funzioni di analisi sono disabilitate. La seguente operazione potrebbe richiedere alcuni minuti. È possibile riabilitare le funzioni di analisi importando nuove licenze valide.

Una licenza *non* è legata a dispositivi specifici.

Il periodo di attivazione viene avviato quando le licenze vengono riscattate.

Le licenze vengono installate mediante una *chiave di attivazione* della licenza. Una volta riscattate le licenze, è possibile creare una chiave di attivazione per tutte le licenze o per un sottoinsieme di licenze disponibili e quindi scaricare e installare la chiave di attivazione in XClarity Orchestrator.

Ogni volta che XClarity Orchestrator non è conforme, il periodo di tolleranza viene reimpostato su 90 giorni.

Se le licenze sono già installate, le nuove licenze *non* sono richieste per l'aggiornamento a una nuova versione di XClarity Orchestrator.

Se si utilizza una licenza di prova gratuita o si dispone di un periodo di tolleranza per diventare conformi e si esegue l'aggiornamento a una versione successiva di XClarity Orchestrator, la licenza di prova o il periodo di tolleranza viene reimpostato su 90 giorni.

Quando si aggiorna XClarity Orchestrator o si verifica una condizione di errore che richiede il ripristino delle chiavi di attivazione, è possibile utilizzare le chiavi esportate o scaricare tutte le chiavi di attivazione (per ciascun ID cliente) da [Portale Web Features on Demand](#) e quindi importarle (come chiavi di attivazione singole o un file ZIP delle chiavi) in XClarity Orchestrator.

Per informazioni sull'acquisto delle licenze, contattare un rappresentante Lenovo o un business partner autorizzato.

Hardware e software supportati

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

Sistemi host

XClarity Orchestrator viene eseguito in un'appliance virtuale su un sistema host.

Requisiti hypervisor

Per l'installazione di XClarity Orchestrator sono supportati i seguenti hypervisor.

- Microsoft Windows Server 2019 con Hyper-V
- Microsoft Windows Server 2022 con Hyper-V
- VMware ESXi 7.0
- VMware ESXi 6.7, U1, U2 e U3
- VMware ESXi 6.5, U1 e U2

Per Hyper-V, l'appliance virtuale è un'immagine VDI (Virtual-Disk Image). Per VMware ESXi, l'appliance virtuale è un template OVF.

Requisiti hardware

Devono essere rispettati i seguenti *requisiti minimi* per l'appliance virtuale. A seconda delle dimensioni dell'ambiente e dell'utilizzo delle funzioni di provisioning (come distribuzione del sistema operativo, aggiornamenti firmware e configurazione dei server), potrebbero essere richieste ulteriori risorse per garantire prestazioni ottimali.

- 8 core di processore virtuali
- 16 GB di memoria
- Storage 551 GB, su due dischi collegati.
 - 251 GB minimo per l'appliance virtuale (disco 0)
 - 100 GB per il repository degli aggiornamenti (disco 1)
 - 200 GB per il repository delle immagini del sistema operativo (disco 2)

Importante: Non è possibile aumentare o diminuire le dimensioni del disco utilizzato per il repository degli aggiornamenti e delle immagini del sistema operativo.

Requisiti software

XClarity Orchestrator richiede il software che segue.

- **Server di autenticazione.** Per impostazione predefinita, XClarity Orchestrator utilizza un server LDAP (Lightweight Directory Access Protocol) per l'autenticazione. Se si sceglie di utilizzare un server di autenticazione esterna, sono supportati i seguenti server LDAP:
 - Microsoft Active Directory in esecuzione su Windows Server 2008 o versione successiva
- **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 Orchestrator. Verificare che il server NTP sia accessibile sulla rete di gestione (in genere, l'interfaccia Eth0). Considerare la possibilità di utilizzare il sistema locale su cui è installato XClarity Orchestrator come server NTP. In tal caso, verificare che il sistema locale sia accessibile sulla rete di gestione.

Risorse gestibili

XClarity Orchestrator può supportare un numero illimitato di strumenti di gestione delle risorse che gestiscono collettivamente un massimo di 10,000 dispositivi.

XClarity Orchestrator supporta i seguenti strumenti di gestione delle risorse.

- **Lenovo XClarity Management Hub 2.0** XClarity Orchestrator gestisce e monitora i dispositivi gestiti da XClarity Management Hub 2.0. Ogni istanza XClarity Management Hub 2.0 può gestire fino a 5,000 dispositivi.

Importante: Le funzioni avanzate (come la distribuzione del sistema operativo e la configurazione dei server con l'utilizzo dei pattern di configurazione) non sono supportate da questo hub di gestione

Un elenco completo di dispositivi 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 2.0](#).

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

- **Lenovo XClarity Management Hub**XClarity Orchestrator gestisce, monitora ed esegue il provisioning dei dispositivi gestiti da XClarity Management Hub. Ogni istanza XClarity Management Hub può gestire fino a **10.000** dispositivi client ThinkEdge.

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](#).

- **Lenovo XClarity Administrator** v2.6 o versione successiva XClarity Orchestrator gestisce, monitora ed esegue il provisioning dei dispositivi fisici gestiti da XClarity Administrator. Ogni istanza XClarity Administrator può gestire fino a **1.000 dispositivi** (server, chassis, switch e storage).

XClarity Orchestrator supporta tutti i dispositivi supportati da XClarity Administrator e XClarity Management Hub, tranne se diversamente indicato. Un elenco completo di dispositivi e opzioni supportati (come I/O, DIMM e adattatori di storage), i livelli minimi di firmware richiesti e le considerazioni sulle limitazioni sono disponibili nelle seguenti pagine Web del supporto Lenovo XClarity.

- [Server ThinkAgile, ThinkEdge, ThinkSystem, System x, Converged HX e NeXtScale](#)
- [Dispositivi Flex System e ThinkSystem nello chassis](#)
- [Server ThinkServer](#)
- [Switch](#)
- [Dispositivi di storage](#)

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

Nota: La funzione di distribuzione del sistema operativo richiede XClarity Administrator 4.0 o versioni successive.

- **Schneider Electric EcoStruxure IT Expert**XClarity Orchestrator gestisce e monitora le risorse dell'infrastruttura, come PDU e UPS, gestite da Esperto EcoStruxure IT.
- **VMware vRealize Operations Manager**XClarity Orchestrator monitora le metriche dei carichi di lavoro virtuali da vRealize Operations Manager.

Nota: vRealize Operations Manager non è incluso nell'elenco degli strumenti di gestione delle risorse, poiché non gestisce i dispositivi in XClarity Orchestrator.

Browser Web

L'interfaccia Web XClarity Orchestrator 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)

Software di terze parti

XClarity Orchestrator si integra con il seguente software.

- Splunk v 7.0.3 e versione successiva (vedere la [Guida per l'utente dell'app XClarity Orchestrator per Splunk](#))

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) 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)	443	https
Inviare i dati periodici a Lenovo: solo XClarity Orchestrator		
esupportwebapi.lenovo.com (XClarity Orchestrator v2.0 e versioni successive) 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)	443	https
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
Servizi di inoltro eventi	<ul style="list-style-type: none"> • Server e-mail (SMTP): UDP sulla porta 25¹ • Servizio Web REST (HTTP): UPD 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

XClarity Orchestrator utilizza una singola sottorete (eth0) per la gestione e la comunicazione dei dati. Prima di configurare la rete, esaminare le seguenti considerazioni.

- L'interfaccia di rete viene utilizzata per il rilevamento e la gestione. Deve essere in grado di comunicare con tutti i dispositivi che si intende gestire.
- Se si desidera inviare manualmente i dati di servizio raccolti al Supporto Lenovo o utilizzare la funzione di notifica automatica dei problemi (Call Home), le interfacce devono essere connesse a Internet, preferibilmente tramite un firewall.
- Se si modifica l'indirizzo IP dell'appliance virtuale di XClarity Orchestrator dopo avere connesso gli strumenti di gestione delle risorse, XClarity Orchestrator non potrà più comunicare con gli strumenti di gestione delle risorse, che risulteranno offline. Se è necessario modificare l'indirizzo IP dell'appliance virtuale dopo che XClarity Orchestrator è attivo e in esecuzione, verificare che tutti gli strumenti di gestione delle risorse risultino disconnessi (eliminati) prima di procedere.
- 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 cambia, è necessario disconnettere (eliminare) i dispositivi gestiti e quindi connetterli nuovamente.
- NAT (Network Address Translation), che riesegue il mapping di uno spazio dell'indirizzo IP in un altro, non è supportato.

Considerazioni sulla sicurezza

Esaminare le seguenti considerazioni per semplificare la pianificazione della sicurezza di Lenovo XClarity Orchestrator e di tutte le risorse gestite.

Considerazioni su un ambiente sicuro

È importante valutare i requisiti di sicurezza dell'ambiente, comprendere e ridurre tutti i rischi per la sicurezza. Lenovo XClarity Orchestrator include diverse funzioni che semplificano la protezione dell'ambiente. Utilizzare le seguenti informazioni per facilitare l'implementazione di un piano di sicurezza per l'ambiente.

Importante: L'utente è responsabile della valutazione, della scelta e dell'implementazione delle funzioni di sicurezza, delle procedure di configurazione e dei controlli appropriati per il proprio ambiente. L'implementazione delle funzioni di sicurezza descritte in questa sezione non garantisce la protezione completa dell'ambiente.

Tenere presente le seguenti informazioni quando si valutano i requisiti di sicurezza dell'ambiente.

- La sicurezza fisica dell'ambiente è importante. Limitare l'accesso alle sale e ai rack in cui è custodito l'hardware di gestione dei sistemi.
- Utilizzare un firewall basato su software per proteggere i dati e l'hardware di rete da minacce per la sicurezza note ed emergenti, come virus e accessi non autorizzati.
- Non modificare le impostazioni di sicurezza predefinite degli switch di rete e i moduli pass-thru. Le impostazioni predefinite di fabbrica di questi componenti disabilitano l'uso dei protocolli non sicuri e abilitano il requisito di aggiornamenti firmware firmati.
- È necessario garantire almeno l'installazione degli aggiornamenti firmware critici. Dopo avere apportato eventuali modifiche, eseguire sempre il backup della configurazione.
- Verificare che tutti gli aggiornamenti relativi alla sicurezza dei server DNS siano prontamente installati e aggiornati.

- Avvisare gli utenti di non accettare i certificati non attendibili. Per ulteriori informazioni, vedere [Utilizzo dei certificati di sicurezza](#) nella documentazione online di XClarity Orchestrator.
- Se possibile, collocare l'hardware di gestione dei sistemi in una sottorete separata. In genere, solo i supervisori devono avere accesso all'hardware di gestione dei sistemi.
- Quando si scelgono le password, non utilizzare espressioni facili da indovinare, come "password" o il nome della propria azienda. Conservare le password in un luogo sicuro e accertarsi che l'accesso alle password sia limitato. Implementare i criteri per le password definiti dall'azienda.

Importante: Tutti gli utenti devono rispettare le regole delle password sicure.

- Stabilire le password di accensione per gli utenti come metodo di controllo per chi accede a dati e programmi di installazione sui server. Per ulteriori informazioni sulle password di accensione, consultare la documentazione fornita con l'hardware.

Considerazioni sulla crittografia

Lenovo XClarity Orchestrator supporta TLS 1.2 e algoritmi crittografici più avanzati per connessioni di rete sicure.

Per una maggiore sicurezza, sono supportate soltanto cifrature avanzate. Il sistema operativo del client e i browser Web devono supportare una delle suite di cifratura che seguono.

- ECDHE-ECDSA-AES128-GCM-SHA256
- ECDHE-RSA-AES128-GCM-SHA256
- ECDHE-ECDSA-AES256-GCM-SHA384
- ECDHE-RSA-AES256-GCM-SHA384
- ECDHE-ECDSA-CHACHA20-POLY1305
- ECDHE-RSA-CHACHA20-POLY1305
- DHE-RSA-AES128-GCM-SHA256
- DHE-RSA-AES256-GCM-SHA384

Considerazioni sui certificati di sicurezza

Lenovo XClarity Orchestrator utilizza i certificati SSL per stabilire comunicazioni sicure e attendibili tra XClarity Orchestrator e i propri strumenti di gestione delle risorse gestite (ad esempio Lenovo XClarity Administrator o Schneider Electric EcoStruxure IT Expert), nonché comunicazioni con XClarity Orchestrator da parte degli utenti o con servizi diversi. Per impostazione predefinita, XClarity Orchestrator e Lenovo XClarity Administrator utilizzano i certificati generati da XClarity Orchestrator, autofirmati e pubblicati da un'autorità di certificazione interna.

Il certificato server predefinito, generato in modo univoco in ogni istanza di XClarity Orchestrator, fornisce misure di sicurezza sufficienti per molti ambienti. È possibile delegare la gestione dei certificati a XClarity Orchestrator oppure avere un ruolo più attivo personalizzando e sostituendo i certificati server. XClarity Orchestrator 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 XClarity Orchestrator 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.

Per ulteriori informazioni sui certificati, vedere .

Considerazioni sul server di autenticazione

È possibile scegliere se utilizzare il server LDAP (Lightweight Directory Access Protocol) locale o un altro server LDAP esterno come server di autenticazione.

Il *server di autenticazione* è un registro utente utilizzato per autenticare le credenziali utente. Lenovo XClarity Orchestrator supporta due tipi di server di autenticazione:

- **Server di autenticazione locale.** Per impostazione predefinita, XClarity Orchestrator è configurato per utilizzare il server LDAP locale (incorporato) che risiede nel server Orchestrator.
- **Server LDAP esterno.** Microsoft Active Directory è supportato come server LDAP esterno. Questo server deve trovarsi in un server Microsoft Windows esterno connesso alla rete di gestione.

Per ulteriori informazioni sull'impostazione di server LDAP esterni, vedere .

Considerazioni sul controllo degli accessi

Lenovo XClarity Orchestrator utilizza *gli elenchi di controllo accessi (ACL)* per determinare a quali risorse (dispositivi, strumenti di gestione delle risorse e XClarity Orchestrator) possono accedere gli utenti. Quando un utente ha accesso a una serie specifica di risorse, l'utente può visualizzare i dati (ad esempio, inventario, eventi, avvisi e analisi) relativi solo a tali risorse

Informazioni su questa attività

Un elenco di controllo degli accessi è un insieme di gruppi di utenti e di risorse.

- I *gruppi di utenti* identificano gli utenti interessati da questo elenco di controllo degli accessi. L'elenco di controllo degli accessi deve contenere un singolo gruppo di utenti. Gli utenti che sono membri di un gruppo a cui è assegnato il ruolo predefinito di **Supervisore** hanno sempre accesso a tutte le risorse. Non è possibile limitare l'accesso alla risorsa per gli utenti supervisore.

Quando è abilitato l'accesso basato sulle risorse, gli utenti che *non sono* membri di un gruppo a cui è assegnato il ruolo predefinito di **Supervisore** non hanno accesso ad alcuna risorsa (dispositivi e strumenti di gestione delle risorse) per impostazione predefinita. È necessario aggiungere gli utenti non supervisore a un gruppo di utenti incluso in un elenco di controllo degli accessi per consentire a questi utenti di accedere a una serie specifica di risorse.

Quando l'accesso basato sulle risorse è disabilitato, tutti gli utenti hanno accesso a tutte le risorse (dispositivi e strumenti di gestione delle risorse) per impostazione predefinita.

- I *gruppi di risorse* identificano le risorse (dispositivi, strumenti di gestione delle risorse e XClarity Orchestrator) a cui è possibile accedere. L'elenco di controllo degli accessi deve contenere almeno un gruppo di risorse.

Nota: Un utente che ha accesso a un gruppo di strumenti di gestione non ottiene automaticamente l'accesso a tutti i dispositivi gestiti da questo strumento di gestione delle risorse. È necessario concedere l'accesso esplicito ai dispositivi che utilizzano i gruppi di dispositivi.

Per ulteriori informazioni sugli elenchi di controllo degli accessi, vedere [Controllo dell'accesso alle risorse](#) nella documentazione online di XClarity Orchestrator.

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. Installazione di XClarity Orchestrator

Installare e configurare l'appliance virtuale Lenovo XClarity Orchestrator su un sistema nell'ambiente locale.

Prima di iniziare

Accertarsi di aver esaminato i prerequisiti, inclusi i requisiti hardware e i suggerimenti per XClarity Orchestrator (vedere [Hardware e software supportati](#)).

Verificare che siano abilitate tutte le porte appropriate, tra cui le porte richieste da XClarity Orchestrator (vedere [Disponibilità della porta](#)).

Accertarsi che gli strumenti di gestione delle risorse che si intende gestire siano supportati e ai livelli di versione richiesti (vedere [Hardware e software supportati](#)).

Per informazioni sull'aggiornamento di un'appliance virtuale di XClarity Orchestrator già installata, vedere [Aggiornamento di XClarity Orchestrator](#).

Per informazioni sulla configurazione di un ambiente a elevata disponibilità, vedere [Implementazione dell'alta disponibilità](#).

Lenovo XClarity Orchestrator è un'applicazione a pagamento. È possibile utilizzare XClarity Orchestrator gratuitamente per un massimo di 90 giorni con la licenza di prova gratuita; tuttavia, una volta terminata la prova gratuita, è necessario acquistare e installare le licenze appropriate per continuare a utilizzare le funzioni di assistenza e supporto di XClarity Orchestrator. Per informazioni sull'acquisto delle licenze, contattare un rappresentante Lenovo o un business partner autorizzato. Per informazioni sull'installazione della licenza, vedere [Applicazione delle licenze per XClarity Orchestrator](#).

Informazioni su questa attività

È possibile assegnare l'indirizzo IP dell'appliance virtuale utilizzando un indirizzo IP statico sulla porta eth0 durante la configurazione.

Se non si assegna l'indirizzo IP durante la configurazione, le impostazioni IP vengono assegnate per impostazione predefinita mediante DHCP (Dynamic Host Configuration Protocol) all'avvio iniziale dell'appliance virtuale. È possibile configurare le impostazioni IP di XClarity Orchestrator durante l'avvio iniziale dell'appliance virtuale. Prima di iniziare, accertarsi di disporre delle informazioni richieste relative agli IP. Si hanno a disposizione massimo 60 secondi per immettere le impostazioni per ogni richiesta.

- Per le impostazioni IPv4 statiche, è possibile modificare l'indirizzo IP, la maschera di sottorete, l'indirizzo IP del gateway e gli indirizzi IP DNS 1 e DNS 2 (facoltativi).
- Per le impostazioni IPv6 statiche, è possibile cambiare l'indirizzo IP, la lunghezza del prefisso e gli indirizzi IP DNS 1 e DNS 2 (facoltativi).
- Per le impostazioni DHCP, è possibile cambiare le impostazioni delle interfacce loopback e primaria (auto lo, iface lo inet loopback, auto eth0 e iface eth0 inet dhcp).

Attenzione: Se si modifica l'indirizzo IP dell'appliance virtuale di XClarity Orchestrator dopo aver connesso gli strumenti di gestione delle risorse, XClarity Orchestrator non potrà più comunicare con gli strumenti di gestione delle risorse, che risulteranno offline. Se è necessario cambiare l'indirizzo IP dell'appliance virtuale dopo che XClarity Orchestrator è attivo e in esecuzione, verificare che tutti gli strumenti di gestione delle risorse risultino disconnessi (eliminati) prima di effettuare tale operazione. Per ulteriori informazioni sulla configurazione degli indirizzi IP, vedere [Configurazione della rete](#).

Procedura

Per installare l'appliance virtuale XClarity Orchestrator, attenersi alla procedura descritta di seguito.

Passo 1. Scaricare l'immagine di XClarity Orchestrator dalla [Pagina Web dei download di XClarity Orchestrator](#) nel sistema locale. Accedere al sito Web e utilizzare la chiave di accesso fornita per scaricare l'immagine.

Per Hyper-V, l'appliance virtuale è un'immagine VDI (Virtual-Disk Image). Per VMware ESXi, l'appliance virtuale è un template OVF.

Passo 2. Installare e configurare l'appliance virtuale nel sistema locale.

- **Per ESXi mediante VMware vSphere**

1. Connettersi all'host tramite VMware vSphere Client.
2. Fare clic con il pulsante destro del mouse su **Macchine virtuali** → **Crea/Registra VM** → **Distribuisci una macchina virtuale da un file OVF o OVA**.
3. Completare ogni passaggio della procedura guidata di distribuzione dell'appliance virtuale. Tenere presente quanto segue, durante l'esecuzione della procedura guidata.
 - **Nome appliance**. Scegliere un nome univoco per questo host.
 - **Storage**. Scegliere un archivio dati con almeno 551 GB di storage disponibile.
 - **Formato disco**. Scegliere il formato del disco che soddisfa le esigenze aziendali. Se non si è certi del formato da scegliere, selezionare **Thin provisioning**.
 - **Impostazioni aggiuntive**. Facoltativamente aggiornare la configurazione di rete per l'appliance virtuale per configurare l'indirizzo IP statico per l'interfaccia eth0.

- **Per ESXi mediante VMware vCenter**

1. Connettersi all'host tramite VMware vCenter.
2. In "Host e cluster" o "VM e modelli", fare clic con il pulsante destro del mouse sull'host, quindi selezionare **File** → **Distribuisci modello OVF**.
3. Completare ogni passaggio della procedura guidata di distribuzione dell'appliance virtuale. Tenere presente quanto segue, durante l'esecuzione della procedura guidata.
 - **Nome appliance**. Scegliere un nome univoco per questo host.
 - **Storage**. Scegliere un archivio dati con almeno 551 GB di storage disponibile.
 - **Formato disco**. Scegliere il formato del disco che soddisfa le esigenze aziendali. Se non si è certi del formato da scegliere, selezionare **Thin provisioning**.
 - **Personalizza modello**. Facoltativamente aggiornare la configurazione di rete per l'appliance virtuale per configurare l'indirizzo IP statico per l'interfaccia eth0.
4. Se si sceglie di configurare l'indirizzo IP statico per l'appliance virtuale, completare le seguenti operazioni.
 - a. Selezionare la VM nell'inventario.
 - b. Fare clic su **Configura** → **vApp**, quindi selezionare **Abilita opzioni vApp**.
 - c. Una volta abilitata l'opzione, selezionare **Ambiente OVF** per lo schema di allocazione IP.
 - d. Nella scheda **Dettagli OVF** selezionare "VMware Tools" per l'opzione **Trasferimento ambiente OVF**.

- **Per Microsoft Hyper-V**

1. Dal Dashboard Server Manager fare clic su **Hyper-V**.
2. Fare clic con il pulsante destro del mouse sul server e scegliere **Hyper-V Manager**.
3. In **Azioni** fare clic su **Nuovo** → **Macchina virtuale** per avviare Nuova procedura guidata macchina virtuale, quindi fare clic su **Avanti**.

4. Nella pagina Impostazione nome e percorso immettere un nome per la nuova macchina virtuale, (ad esempio, LXCO-*{version}*).
5. Nella pagina Specifica generazione, selezionare **Generazione 1**.
6. Nella pagina Assegna memoria selezionare almeno 16 GB di memoria da utilizzare per questa macchina virtuale (vedere [Hardware e software supportati](#)).
7. Nella pagina Configurazione della rete scegliere lo switch virtuale creato durante l'installazione e la configurazione dell'host.
8. Nella pagina Collega unità disco fisso virtuale fare clic su **Usa un disco fisso virtuale esistente**, passare alla posizione in cui si sono copiate le immagini in formato VHD di XClarity Orchestrator e selezionare l'immagine ***disk001*.vhd**.
9. Fare clic su **Fine**.
10. Fare clic con il pulsante destro del mouse sulla macchina virtuale appena creata e scegliere **Impostazioni**.
11. Configurare il numero di processori da assegnare alla macchina virtuale.
 - a. Selezionare **Processore** e specificare almeno 8 processori virtuali da utilizzare per questa macchina virtuale (vedere [Hardware e software supportati](#)).
 - b. Fare clic su **Applica** e quindi su **OK**.
12. Aggiungere la seconda unità disco fisso all'appliance virtuale.
 - a. Espandere **IDE Controller 0** e selezionare **Unità disco fisso**.
 - b. Dal campo **Unità disco fisso virtuale** passare alla posizione in cui si sono copiate le immagini in formato VHD di XClarity Orchestrator e selezionare l'immagine ***disk002*.vhd**.
 - c. Fare clic su **Applica** e quindi su **OK**.
13. Aggiungere la terza unità disco fisso all'appliance virtuale.
 - a. Espandere **IDE Controller 1** e selezionare **Unità disco fisso**.
 - b. Dal campo **Unità disco fisso virtuale** passare alla posizione in cui si sono copiate le immagini in formato VHD di XClarity Orchestrator e selezionare l'immagine ***disk003*.vhd**.
 - c. Fare clic su **Applica** e quindi su **OK**.
14. (Facoltativo) È possibile impostare un indirizzo MAC statico per ogni scheda di rete. A tal fine espandere **Scheda di rete** per lo switch virtuale, selezionare **Funzioni avanzate**, fare clic su **Statico in Indirizzo MAC** e specificare l'indirizzo MAC.

Passo 3. Avviare l'appliance virtuale.

All'avvio dell'appliance virtuale, verranno elencati gli indirizzi IPv4 e IPv6 assegnati da DHCP per ogni interfaccia, come riportato nell'esempio seguente.

```
Lenovo XClarity Orchestrator Version x.x.x
```

```
-----
```

```
eth0  Link encap:Ethernet  HWaddr 2001:db8:65:12:34:56
      inet addr: 192.0.2.10  Bcast 192.0.2.55  Mask 255.255.255.0
      inet6 addr: 2001:db8:56ff:fe80:bea3/64  Scope:Link
```

```
=====
```

```
You have 118 seconds to change IP settings. Enter one of the following:
 1. To set a static IP address for Lenovo XClarity virtual appliance eth0 port
 2. To use a DHCP address for Lenovo XClarity virtual appliance eth0 port
 3. To select subnet for Lenovo XClarity virtual appliance internal network
 x. To continue without changing IP settings
```

... ..

Passo 4. Facoltativamente, è possibile configurare le impostazioni IP dell'appliance virtuale dalla console. Se non si effettua una selezione entro il tempo specificato oppure si immette x, l'avvio iniziale continua a utilizzare le impostazioni IP predefinite assegnate.

- **Assegnare gli indirizzi IP statici per la porta eth0.** Immettere 1, quindi seguire le istruzioni per modificare le impostazioni.
- **Assegnare i nuovi indirizzi IP per la porta eth0 mediante DHCP.** Immettere 2, quindi seguire le istruzioni per modificare le impostazioni.
- **Selezionare la sottorete per la rete interna dell'appliance virtuale.** Immettere 3, quindi seguire le istruzioni per modificare le impostazioni. Per impostazione predefinita, XClarity Orchestrator utilizza la sottorete **192.168.252.0/24** per la rete interna. Se questa sottorete si sovrappone alla rete host, sostituire la sottorete con una delle altre opzioni disponibili per evitare problemi di rete.
 - 192.168.252.0/24
 - 172.31.252.0/24
 - 10.255.252.0/24

Importante: Se si specificano valori non validi, viene restituito un errore. Sono disponibili fino a quattro tentativi per immettere i valori validi.

Al termine

Eeguire il login e configurare XClarity Orchestrator.

Capitolo 3. Implementazione dell'alta disponibilità

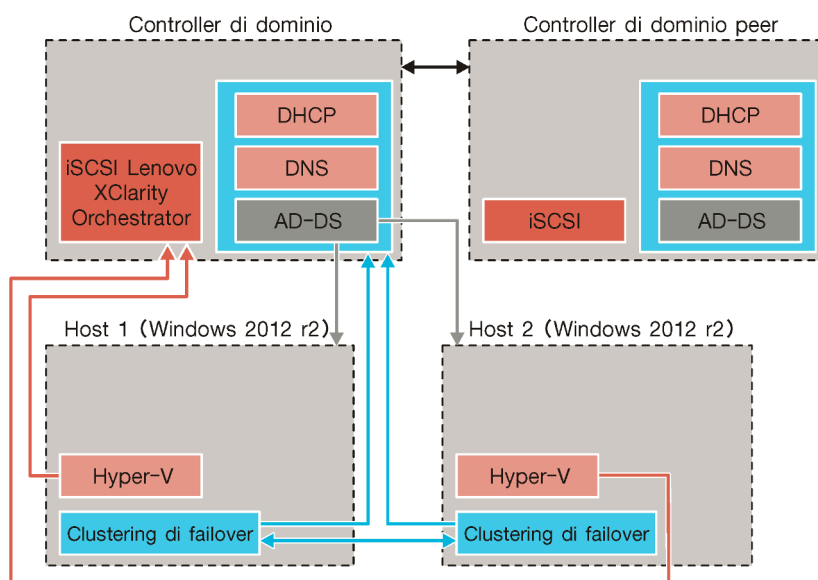
Per implementare l'alta disponibilità per Lenovo XClarity Orchestrator, utilizzare la funzione di alta disponibilità fornita dall'ambiente host.

Implementazione dell'alta disponibilità (Hyper-V)

Per implementare la disponibilità elevata per Lenovo XClarity Orchestrator in un ambiente Microsoft Hyper-V, utilizzare la funzione di disponibilità elevata fornita da Hyper-V.

Informazioni su questa attività

La seguente figura fornisce una panoramica di alto livello per implementare la disponibilità elevata per XClarity Orchestrator in un ambiente Hyper-V. In questo esempio, l'immagine di XClarity Orchestrator è installata nello storage condiviso e accessibile dal cluster.



Procedura

Per configurare un ambiente a disponibilità elevata, effettuare le operazioni che seguono.

Passo 1. Configurare il controller di dominio.

- a. Eseguire la configurazione DHCP iniziale.
- b. Configurare il DNS.
- c. Configurare Servizi di dominio Active Directory.
- d. Completare la configurazione DHCP.

Passo 2. Configurare il primo host.

- a. Installare Microsoft Windows 2012 r2.
- b. Eseguire l'aggiunta al dominio Servizi di dominio Active Directory.
- c. Aggiungere le funzioni che seguono.
 - Hyper-V
 - Clustering di failover

Passo 3. Configurare il secondo host.

- a. Installare Microsoft Windows 2012 r2.
- b. Eseguire l'aggiunta al dominio Servizi di dominio Active Directory.
- c. Aggiungere le funzioni che seguono.
 - Hyper-V
 - Clustering di failover

Passo 4. Configurare lo storage condiviso (ad esempio, iSCSI) nel controller di dominio e in entrambi gli host.

Passo 5. Configurare il clustering di failover.

Passo 6. Aggiungere l'immagine XClarity Orchestrator.

Implementazione dell'alta disponibilità (ESXi)

Per implementare la disponibilità elevata per Lenovo XClarity Orchestrator in un ambiente VMware ESXi, utilizzare la funzione di disponibilità elevata fornita da ESXi.

Informazioni su questa attività

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.

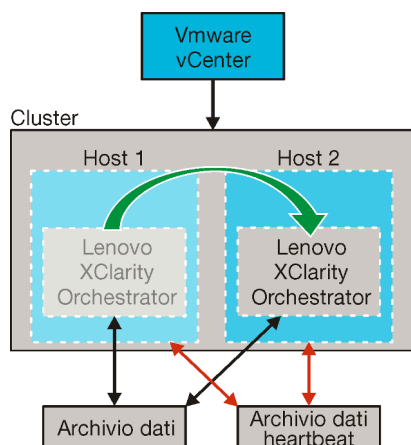
- Almeno due host su cui è installato ESXi. Questi host diventano parte del cluster VMware.
- Un terzo host su cui è installato VMware vCenter.

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).

La figura che segue illustra una procedura per implementare la disponibilità elevata per XClarity Orchestrator in un ambiente ESXi. In questo scenario, l'appliance virtuale XClarity Orchestrator è installata nello storage condiviso e accessibile dal cluster.



Per maggiori dettagli sulla configurazione del cluster VMware High Availability (VMware 5.0), vedere [Pagina Web sulla configurazione dell'alta disponibilità per VMware](#).

Procedura

Per configurare un ambiente a disponibilità elevata, effettuare le operazioni che seguono.

Passo 1. Configurare lo storage condiviso in modo che sia accessibile da tutti gli host nel cluster.

Passo 2. Installare ESXi su due server, ciascuno con indirizzi IP statici. Accertarsi che VMware vCenter sia configurato in un server distinto.

Passo 3. Avviare VMware vCenter.

Passo 4. Configurare gli altri due host da utilizzare con VMware vCenter.

- a. Creare il cluster.
- b. Aggiungere gli host al cluster.
- c. Aggiungere entrambi gli archivi dati agli host nel cluster.

Nota: Per l'heartbeating è necessario il secondo archivio dati.

Passo 5. Distribuire XClarity Orchestrator nel cluster.

Capitolo 4. Configurazione di XClarity Orchestrator per la prima volta

Quando si accede a Lenovo XClarity Orchestrator per la prima volta, è necessario effettuare alcuni passaggi per eseguire la configurazione iniziale.

Procedura

Per la configurazione iniziale di XClarity Orchestrator, effettuare le operazioni che seguono.

Passo 1. Accesso all'interfaccia Web di XClarity Orchestrator.

Passo 2. Cambiare la password iniziale.

Passo 3. Leggere e accettare il contratto di licenza.

Passo 4. Creare account utente aggiuntivi.

Passo 5. Configurare la data e l'ora.

Passo 6. Configurare l'accesso alla rete, inclusi gli indirizzi IP per la rete di dati e gestione.

Passo 7. Scegliere di utilizzare il server di autenticazione predefinito o di configurare un client LDAP esterno.

Passo 8. Configurare le impostazioni aggiuntive di sicurezza, come l'importazione di certificati attendibili per servizi interni ed esterni.

Passo 9. Configurare e abilitare la notifica automatica dei problemi, se applicabile

Passo 10. Configurare XClarity Orchestrator per inoltrare gli eventi a servizi e ad applicazioni specifici, se applicabili.

Passo 11. Connettere gli strumenti di gestione delle risorse.

Primo accesso all'interfaccia Web di XClarity Orchestrator

È possibile avviare l'interfaccia Web di Lenovo XClarity Orchestrator da qualsiasi sistema con connettività di rete alla macchina virtuale XClarity Orchestrator.

Prima di iniziare

Accertarsi di utilizzare uno dei seguenti browser Web supportati. Per ulteriori informazioni, vedere [Hardware e software 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**.

XClarity Orchestrator utilizza una singola sottorete, generalmente eth0.

se la configurazione di XClarity Orchestrator 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 Orchestrator da un'altra macchina virtuale che disponga della connettività a XClarity Orchestrator. Ad esempio, è possibile accedere a XClarity Orchestrator da un'altra macchina virtuale sull'host in cui è installato XClarity Orchestrator.

Procedura

Per accedere all'interfaccia Web di XClarity Orchestrator per la prima volta, attenersi alla procedura descritta di seguito.

1. Puntare il browser all'indirizzo IP dell'appliance virtuale XClarity Orchestrator.

- **Utilizzo di un indirizzo IPv4 statico** Se durante l'installazione è stato specificato un indirizzo IPv4, utilizzare tale indirizzo IPv4 per accedere all'interfaccia Web mediante il seguente URL.
`https://{IPv4_address}#/login.html`

Ad esempio:

`https://192.0.2.10/#/login.html`

- **Utilizzo di un server DHCP nello stesso dominio di broadcast di XClarity Orchestrator** Se un server DHCP è configurato nello stesso dominio di broadcast di XClarity Orchestrator, utilizzare l'indirizzo IPv4 visualizzato nella console dell'appliance virtuale di XClarity Orchestrator per accedere all'interfaccia Web mediante l'URL che segue.

`https://{IPv4_address}#/login.html`

Ad esempio:

`https://192.0.2.10/#/login.html`

Viene visualizzata la pagina di login iniziale.

Dalla pagina di login, è possibile completare le seguenti azioni:

- Inviare idee per XClarity Orchestrator sul [Sito Web di Lenovo XClarity Ideation](#) oppure facendo clic su **Invia idea**.

- Porre domande e individuare risposte sul [Sito Web del forum della community dedicata a Lenovo XClarity](#) facendo clic su **Forum utenti**.
 - Per informazioni sull'utilizzo di XClarity Orchestrator, fare clic su **Guida per l'utente**.
 - Individuare e gestire tutte le licenze Lenovo da [Portale Web Features on Demand](#) facendo clic su **Titolarità della licenza**.
 - Per informazioni sulle API disponibili, fare clic su **Toolkit**.
2. Selezionare la lingua desiderata dall'elenco a discesa della lingua.

Nota: Alcune impostazioni di configurazione e alcuni dati che vengono forniti dagli strumenti di gestione delle risorse e i dispositivi gestiti potrebbero essere disponibili solo in inglese.

3. Immettere le credenziali predefinite ID UTENTE e PASSWORD (dove 0 è zero) e fare clic su **Login**. La prima volta che si utilizzerà un account utente specifico per il login a XClarity Orchestrator, verrà richiesto di cambiare la password. Per impostazione predefinita, le password devono contenere da **8 a 256** caratteri e devono soddisfare i criteri che seguono.

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

- Deve contenere almeno un carattere alfabetico e non deve avere più di due caratteri sequenziali, tra cui sequenze di caratteri alfabetici, cifre e tasti della tastiera QWERTY (ad esempio, "abc", "123" e "asd" non sono consentiti)
- Deve contenere almeno un numero
- Deve contenere almeno due dei caratteri che seguono:
 - Caratteri alfabetici maiuscoli (A - Z)
 - Caratteri alfabetici minuscoli (a - z)
 - Caratteri speciali ; @ _ ! ' \$ & +
 Gli spazi non sono consentiti.
- Non deve essere una ripetizione o l'inversione del nome utente.
- Non deve contenere consecutivamente più di due degli stessi caratteri (ad esempio, "aaa", "111" e "... " non sono ammessi).

Al termine

Importante: Al primo accesso a XClarity Orchestrator si potrebbero ricevere avvertenze sulla sicurezza o sui certificati. È possibile ignorare tali avvertenze.

Continuare la configurazione iniziale consultando la sezione [Creazione di un utente locale](#).

Creazione di un utente locale


È possibile creare manualmente gli account utente nel server di autenticazione locale (incorporato). Gli *account utente locali* sono utilizzati per eseguire il login a Lenovo XClarity Orchestrator e autorizzare l'accesso alle risorse.

Informazioni su questa attività

Come misura aggiuntiva di sicurezza, creare almeno due account utente.

Procedura

Per creare un utente locale, effettuare le seguenti operazioni.

- Passo 1. Sulla barra dei menu di XClarity Orchestrator fare clic su **Amministrazione**  → **Sicurezza**, quindi su **Utenti locali** nel riquadro di navigazione sinistro per visualizzare la scheda Utenti locali.

Utenti locali				
Gestire gli account utente nel server di autenticazione locale.				
Nome utente :		Nome completo :	Ruoli :	Gruppi di utenti :
<input type="radio"/>	userid	Non disponibile	Supervisor	Supervisor Group

0 Selezionato/i / 1 Totale Righe per pagina: 10

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 che seguono.

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

- Deve contenere almeno un carattere alfabetico e non deve avere più di due caratteri sequenziali, tra cui sequenze di caratteri alfabetici, cifre e tasti della tastiera QWERTY (ad esempio, "abc", "123" e "asd" non sono consentiti)
- Deve contenere almeno un numero
- Deve contenere almeno due dei caratteri che seguono:
 - Caratteri alfabetici maiuscoli (A - Z)
 - Caratteri alfabetici minuscoli (a - z)
 - Caratteri speciali ; @ _ ! ' \$ & +
 Gli spazi non sono consentiti.
- Non deve essere una ripetizione o l'inversione del nome utente.
- Non deve contenere consecutivamente più di due degli stessi caratteri (ad esempio, "aaa", "111" e "... " non sono ammessi).
- (Facoltativo) Specificare le informazioni di contatto per l'account utente, tra cui il nome completo, l'indirizzo e-mail e il numero di telefono.

Suggerimento: Per il nome completo è possibile specificare fino a 128 caratteri, inclusi lettere, numeri, spazi, punti, trattini, apostrofi e virgole.

Passo 4. Fare clic sulla scheda **Gruppi di utenti** e selezionare i gruppi di utenti di cui deve essere membro questo utente.

Suggerimento: se non viene selezionato un gruppo di utenti, il ruolo **OperatorGroup** viene assegnato per impostazione predefinita

Passo 5. Fare clic su **Crea**.

L'account utente viene aggiunto alla tabella.

Al termine

Continuare la configurazione iniziale consultando la sezione [Configurazione della rete](#).

Configurazione della rete

Quando si configura inizialmente Lenovo XClarity Orchestrator, è necessario configurare una singola interfaccia di rete (mediante le impostazioni IPv4 e IPv6). È inoltre possibile configurare le impostazioni di routing di Internet.

Prima di iniziare


Nella scelta dell'interfaccia tenere in considerazione i seguenti punti.

- L'interfaccia deve essere configurata per supportare il rilevamento e la gestione. Deve essere in grado di comunicare con gli strumenti di gestione delle risorse e i dispositivi gestiti.
- Se si desidera inviare manualmente i dati di servizio raccolti al Supporto Lenovo o utilizzare la funzione di notifica automatica dei problemi (Call Home), le interfacce devono essere connesse a Internet, preferibilmente tramite un firewall.

Attenzione:

- Se si modifica l'indirizzo IP dell'appliance virtuale di XClarity Orchestrator dopo aver connesso gli strumenti di gestione delle risorse, XClarity Orchestrator non potrà più comunicare con gli strumenti di gestione delle risorse, che risulteranno offline. Se è necessario cambiare l'indirizzo IP dell'appliance virtuale dopo che XClarity Orchestrator è attivo e in esecuzione, verificare che tutti gli strumenti di gestione delle risorse risultino disconnessi (eliminati) prima di effettuare tale operazione.
- Se l'interfaccia di rete è configurata per utilizzare DHCP (Dynamic Host Configuration Protocol), l'indirizzo IP potrebbe cambiare alla scadenza del lease DHCP. Se l'indirizzo IP cambia, è necessario disconnettere (eliminare) gli strumenti di gestione delle risorse e connetterli nuovamente. Per evitare questo problema, modificare l'interfaccia di rete con un indirizzo IP statico oppure verificare che il server DHCP sia configurato in modo che l'indirizzo DHCP sia basato su un indirizzo MAC o che il protocollo DHCP non scada.
- NAT (Network Address Translation), che riesegue il mapping di uno spazio dell'indirizzo IP in un altro, non è supportato.

Procedura

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

- **Configurare le impostazioni IP** È possibile scegliere di utilizzare le impostazioni di rete IPv4 e IPv6 delle schede Configurazione IPv4 e Configurazione IPv6. Abilitare e modificare le impostazioni di configurazione IP applicabili, quindi fare clic su **Applica**.
 - **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 deve trovarsi nella stessa sottorete dell'interfaccia di rete.

Se si utilizza DHCP per ottenere un indirizzo IP, anche il gateway predefinito utilizzerà DHCP.
 - **Impostazioni IPv6.** È possibile configurare il metodo di assegnazione IP, l'indirizzo IPv6, la lunghezza del prefisso e il gateway predefinito. Per il metodo di assegnazione IP, è possibile scegliere di utilizzare un indirizzo IP assegnato staticamente, la configurazione dell'indirizzo con stato (DHCPv6) o la configurazione automatica dell'indirizzo IP senza stato. Quando si utilizza un indirizzo IP statico, è necessario fornire un indirizzo IPv6, una lunghezza del prefisso e un gateway. Il gateway deve essere un indirizzo IP valido e deve trovarsi nella stessa sottorete dell'interfaccia di rete.

Configurazione IPv4

Abilitato

Metodo Ottieni indirizzo IP da ... ▼	Maschera di rete IPv4 255.255.224.0
Intervallo IPv4 10.243.14.36	Gateway predefinito IPv4 10.243.0.1

Configurazione IPv6

Abilitato

Metodo Utilizza configurazio... ▼	Lunghezza del prefisso IPv6 64
Indirizzo IPv6 fd55:faaf:e1ab:2021:20c:2'	Gateway predefinito IPv6 fe80::5:73ff:fea0:2c

- **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.

Scegliere se utilizzare DHCP per ottenere gli indirizzi IP o per specificare gli indirizzi IP statici abilitando o disabilitando il **DNS DHCP**. Se si sceglie di utilizzare gli indirizzi IP statici, specificare l'indirizzo IP per almeno uno e massimo due server DNS.

Specificare il nome host DNS e il nome di dominio. È possibile scegliere di recuperare il nome di dominio da un server DHCP o specificare un nome di dominio personalizzato.

Nota:

- Se si sceglie di utilizzare un server DHCP per ottenere l'indirizzo IP, eventuali modifiche apportate ai campi Server DNS verranno sovrascritte al successivo rinnovo del lease DHCP da parte di XClarity Orchestrator.
- Quando si modificano le impostazioni DNS, è necessario riavviare manualmente la macchina virtuale per applicare le modifiche.
- Se si modifica l'impostazione DNS in modo da utilizzare un indirizzo IP statico invece del protocollo DHCP, accertarsi di modificare anche l'indirizzo IP del server DNS stesso.

Configurazione DNS

Se si modificano le impostazioni DNS, è necessario riavviare il server XClarity Orchestrator per applicare le modifiche.

Tipo di indirizzi DNS preferiti IPv4 IPv6

Abilitato

Primo indirizzo DNS: 10.240.0.10

Metodo: Utilizza il nome di d... ▼

Secondo indirizzo DNS: 10.240.0.11

Nome di dominio:

Nome Host: lxco

Applica Reimposta

- **Configurare le impostazioni proxy HTTP** Facoltativamente abilitare e specificare il nome host del server proxy, la porta e le credenziali facoltative nella scheda Configurazione proxy. Fare quindi clic su **Applica**.

Nota:

- 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.

Configurazione proxy

Disabilitato

Nome host server proxy

Nome utente

Porta server proxy

Password

Applica Reimposta

Al termine

Continuare la configurazione iniziale consultando la sezione [Configurazione di data e ora](#).

Configurazione di data e ora

È necessario configurare almeno uno (e fino a quattro) server NTP (Network Time Protocol) per sincronizzare i timestamp per Lenovo XClarity Orchestrator con eventi ricevuti tramite gli strumenti di gestione delle risorse.

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 Orchestrator è in esecuzione.

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

Attenzione: L'appliance virtuale XClarity Orchestrator 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 Orchestrator e il relativo host. In genere, l'host è configurato per sincronizzarsi con l'ora delle rispettive appliance virtuali. Se XClarity Orchestrator è impostato per sincronizzarsi con un'origine differente rispetto all'host, è necessario disabilitare la sincronizzazione oraria dell'host tra l'appliance virtuale XClarity Orchestrator e il rispettivo host.

- **ESXi** Seguire le istruzioni sulla [VMware - Pagina Web sulla disabilitazione della sincronizzazione dell'ora](#).
- **Hyper-V** Da Hyper-V Manager, fare clic con il pulsante destro del mouse sulla macchina virtuale XClarity Orchestrator, quindi selezionare **Impostazioni**. Nella finestra di dialogo fare clic su **Gestione** → **Servizi di integrazione** nel riquadro di navigazione, quindi deselezionare **Sincronizzazione ora**.

Procedura

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

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

The screenshot shows the 'Data e ora' (Date and Time) configuration page in XClarity Orchestrator. At the top, it states 'Data e ora verranno sincronizzate automaticamente con il server NTP'. Below this, the current settings are displayed: 'Data' (Date) is 04/10/22, 'Tempo' (Time) is 18:50:59, and 'Fuso orario' (Time Zone) is UTC -00:00, Coordinated Universal Time Universal. A light blue notification banner reads: 'Una volta applicate le modifiche, questa pagina verrà aggiornata automaticamente per ottenere la configurazione più recente.' Below the notification are three input fields: 'Fuso orario' (Time Zone) with a dropdown menu showing 'UTC -00:00, Coordinated Universal Time Universal'; 'Server NTP' (NTP Server) with a text input field containing 'Server NTP 1 Indirizzo FQDN o IP'; and a '+ Aggiungi nuovo server NTP' (Add new NTP server) button. At the bottom left is an 'Applica' (Apply) button.

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

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**.

Al termine

Continuare la configurazione iniziale consultando la sezione [Configurazione del server di autenticazione](#).

Configurazione del server di autenticazione

Lenovo XClarity Orchestrator include un server di autenticazione locale (integrato). È inoltre possibile scegliere di utilizzare un server LDAP Active Directory esterno.

Prima di iniziare

Prima che un utente LDAP esterno possa accedere a XClarity Orchestrator, l'utente deve essere un membro diretto di un gruppo di utenti LDAP clonato in XClarity Orchestrator. XClarity Orchestrator non riconosce gli utenti membri di gruppi di utenti nidificati nel gruppo di utenti LDAP clonato, definito nel server LDAP esterno.

Verificare che tutte le porte richieste per il server di autenticazione esterna siano aperte su rete e firewall. Per informazioni sui requisiti della porta, vedere [Disponibilità della porta](#).

Informazioni su questa attività


Se un server LDAP esterno non è configurato, XClarity Orchestrator autentica sempre un utente utilizzando il server di autenticazione locale.

Se un server LDAP esterno non è configurato, XClarity Orchestrator tenta prima di autenticare un utente utilizzando il server di autenticazione locale. Se l'autenticazione non riesce, XClarity Orchestrator prova quindi a eseguire l'autenticazione utilizzando l'indirizzo IP del primo server LDAP. Se l'autenticazione non riesce, il client LDAP tenta di eseguire l'autenticazione utilizzando l'indirizzo IP del successivo server LDAP.

Quando un utente LDAP esterno accede a XClarity Orchestrator per la prima volta, un account utente con nome <nomeutente>@<dominio> viene clonato automaticamente in XClarity Orchestrator. È possibile aggiungere utenti LDAP esterni clonati ai gruppi di utenti oppure utilizzare i gruppi LDAP per il controllo degli accessi. È inoltre possibile aggiungere i privilegi di supervisore a un utente LDAP esterno.

Procedura

Per configurare XClarity Orchestrator affinché utilizzi un server di autenticazione LDAP, effettuare le operazioni che seguono.

Passo 1. Sulla barra dei menu di XClarity Orchestrator fare clic su **Amministrazione**  → **Sicurezza**, quindi su **Client LDAP** nel riquadro di navigazione sinistro per visualizzare la scheda Client LDAP.

Client LDAP

È possibile configurare XClarity Orchestrator per utilizzare i server LDAP esterni per autenticare gli utenti. Il server di autenticazione locale esegue sempre prima l'autenticazione. Se l'autenticazione non riesce, il client LDAP tenta di eseguire l'autenticazione utilizzando il primo indirizzo IP del server LDAP esterno. Se l'autenticazione non riesce, il client LDAP tenta di eseguire l'autenticazione utilizzando l'indirizzo IP successivo.

Informazioni sul server

+
↑
↓

Active Directory
 LDAP personalizzato

LDAP su SSL

Configurazione

Credenziali di associazione

Recuperare il certificato o incollare il certificato in formato PEM (accertarsi di includere le righe BEGIN ed END):

```

-----BEGIN CERTIFICATE-----
contenuti del certificato
-----END CERTIFICATE-----
  
```

Passo 2. Configurare ogni server LDAP esterno completando la procedura seguente.

1. Fare clic sull'icona **Aggiungi** (+) per aggiungere un server LDAP.
2. Specificare il nome di dominio, l'indirizzo IP e la porta per il server LDAP esterno.

Se il numero di porta *non* è impostato in modo esplicito su 3268 o 3269, si presuppone che la voce identifichi un controller di dominio.

Quando il numero di porta è impostato su 3268 o 3269, si presuppone che la voce identifichi un catalogo globale. Il client LDAP tenta di eseguire l'autenticazione utilizzando il controller di dominio per il primo indirizzo IP configurato del server. In caso di errore, il client LDAP tenta di eseguire l'autenticazione utilizzando il controller di dominio per l'indirizzo IP successivo del server.

3. Facoltativamente, scegliere di abilitare la personalizzazione delle impostazioni di configurazione avanzate. Quando si sceglie di utilizzare una configurazione personalizzata, è possibile specificare il filtro di ricerca utente. Se non si specifica un filtro di ricerca utente, (&(objectClass=user)(!(userPrincipalName={0})(sAMAccountName={0}))) viene utilizzato per impostazione predefinita.

Se la configurazione avanzata è disabilitata, viene utilizzata la configurazione predefinita di Active Directory.

4. Specificare il nome distinto di base LDAP completo da cui il client LDAP avvia la ricerca per l'autenticazione utente.
5. Specificare il nome distinto di base LDAP completo da cui il client LDAP avvia la ricerca per i gruppi di utenti (ad esempio, `dc=company,dc=com`).
6. È possibile specificare le credenziali per collegare XClarity Orchestrator al server di autenticazione esterno. È possibile utilizzare uno dei due metodi di collegamento.
 - **Credenziali configurate.** Selezionare questo metodo di collegamento per utilizzare un nome e una password specifici del client per collegare XClarity Orchestrator al server di autenticazione esterno. Se il collegamento non riesce, anche il processo di autenticazione fallisce. Specificare il nome distinto LDAP completo (ad esempio, `cn=somebody,dc=company,dc=com`) o l'indirizzo e-mail (ad esempio, `somebody@company.com`) dell'account utente e la password da utilizzare per l'autenticazione LDAP per collegare XClarity Orchestrator al server LDAP. Se il collegamento non riesce, anche il processo di autenticazione fallisce.

Il nome distinto deve essere un account utente del dominio che disponga almeno dei privilegi di sola lettura.

Se il server LDAP non dispone di sottodomini, è possibile specificare il nome utente senza il dominio (ad esempio, `user1`). Tuttavia, se il server LDAP dispone di sottodomini (ad esempio, il sottodominio `new.company.com` nel dominio `company.com`), è necessario specificare il nome utente e il dominio (ad esempio, `user1@company.com`).

Attenzione: Se si cambia la password del client del server LDAP esterno, verificare che sia stata aggiornata anche la nuova password in XClarity Orchestrator (vedere [Impossibile eseguire il login a XClarity Orchestrator](#) nella documentazione online di XClarity Orchestrator).

- **Credenziali di login.** Selezionare questo metodo di collegamento per utilizzare il nome utente e la password di XClarity Orchestrator per LDAP per collegare XClarity Orchestrator al server di autenticazione esterno. Specificare il nome distinto LDAP completo di un account utente di *prova* e la password da utilizzare per l'autenticazione LDAP per convalidare la connessione al server di autenticazione.

Queste credenziali utente non vengono salvate. Se l'operazione riesce, tutti i futuri collegamenti utilizzeranno il nome utente e la password usati per eseguire il login a XClarity Orchestrator. Se il collegamento non riesce, anche il processo di autenticazione fallisce.

Nota: È necessario avere eseguito il login a XClarity Orchestrator utilizzando un ID utente completo (ad esempio, `administrator@domain.com`).

7. Se si sceglie di utilizzare l'autenticazione LDAP sicura, selezionare l'interruttore **LDAP su SSL** e fare clic su **Recupera** per recuperare e importare il certificato SSL attendibile. Quando viene visualizzata la finestra di dialogo Recupera certificato server, fare clic su **Accetta** per usare il certificato. Se si sceglie di utilizzare LDAP su SSL, XClarity Orchestrator utilizza il protocollo LDAPS per connettersi in modo sicuro al server di autenticazione esterna. Quando questa opzione è selezionata, vengono utilizzati certificati attendibili per abilitare il supporto LDAP sicuro.

Attenzione: Se si sceglie di disabilitare LDAP su SSL, XClarity Orchestrator utilizza un protocollo non sicuro per connettersi al server di autenticazione esterna. Se si seleziona questa impostazione, l'hardware potrebbe essere vulnerabile agli attacchi di sicurezza.

8. Facoltativamente ordinare di nuovo i server LDAP utilizzando le icone **Sposta verso l'alto** (↑) e **Sposta verso il basso** (↓). Il client LDAP tenta di eseguire l'autenticazione utilizzando il primo indirizzo IP del server. Se l'autenticazione non riesce, il client LDAP tenta di eseguire l'autenticazione utilizzando l'indirizzo IP successivo.

Importante: Per l'autenticazione LDAP sicura, utilizzare il certificato per l'autorità di certificazione (CA) radice del server LDAP o uno dei certificati intermedi del server. È possibile recuperare il certificato CA radice o intermedio da un prompt dei comandi eseguendo il comando che segue, dove *{FullyQualifiedHostNameOrIpAddress}* è il nome completo del server LDAP esterno. Il certificato CA radice o intermedio è in genere l'ultimo certificato nell'output, l'ultima sezione BEGIN - -END.

```
openssl s_client -showcerts -connect {FullyQualifiedHostNameOrIpAddress}:636
```

9. Fare clic su **Applica modifiche**. XClarity Orchestrator prova a verificare l'indirizzo IP, la porta, i certificati SSL e le credenziali di collegamento e convalida la connessione al server LDAP per rilevare gli errori comuni. Se la convalida riesce, l'autenticazione utente viene effettuata sul server di autenticazione esterna quando un utente esegue il login a XClarity Orchestrator. Se la convalida non riesce, vengono visualizzati i messaggi di errore che indicano l'origine degli errori.

Nota: Se la convalida riesce e le connessioni ai server LDAP vengono completate correttamente, l'autenticazione utente potrebbe avere esito negativo se il nome distinto della radice non è corretto.

Al termine

Continuare la configurazione iniziale consultando la sezione [Configurazione delle impostazioni di sicurezza aggiuntive](#).

Configurazione delle impostazioni di sicurezza aggiuntive

È possibile configurare le impostazioni di sicurezza aggiuntive, inclusi certificati e impostazioni di sicurezza degli account utente.

Procedura

Per configurare la sicurezza aggiuntiva, completare una o più delle seguenti operazioni.

- Lenovo XClarity Orchestrator utilizza i certificati SSL per stabilire comunicazioni sicure e attendibili tra XClarity Orchestrator e gli strumenti di gestione delle risorse (ad esempio Lenovo XClarity Administrator), nonché comunicazioni con XClarity Orchestrator da parte degli utenti. Per impostazione predefinita, XClarity Orchestrator e gli strumenti di gestione delle risorse utilizzano i certificati generati da XClarity Orchestrator, autofirmati ed emessi da un'autorità di certificazione (CA) interna. È possibile scegliere di generare una richiesta di firma del certificato (CSR) da far firmare a un'autorità di certificazione esterna, come l'autorità di certificazione della propria organizzazione o di terze parti (vedere [Installazione di un certificato attendibile del server XClarity Orchestrator con firma esterna](#) nella documentazione online di XClarity Orchestrator).
- È possibile importare certificati attendibili per servizi esterni nell'archivio attendibile di XClarity Orchestrator per stabilire una connessione sicura con gli strumenti di gestione delle risorse e i server d'inoltro di eventi, come Splunk (vedere [Aggiunta di un certificato attendibile per i servizi esterni](#) nella documentazione online di XClarity Orchestrator).
- È possibile importare certificati attendibili per servizi interni nell'archivio attendibile di XClarity Orchestrator per stabilire una connessione sicura con gli strumenti di gestione delle risorse e i server LDAP attendibili (vedere [Aggiunta di un certificato attendibile per i servizi interni](#) nella documentazione online di XClarity Orchestrator).
- Configurare le impostazioni di sicurezza per complessità della password, blocco dell'account e timeout di inattività della sessione Web. Per ulteriori informazioni su queste impostazioni, vedere [Configurazione delle impostazioni di sicurezza utente](#) nella documentazione online di XClarity Orchestrator.

Al termine

Continuare la configurazione iniziale consultando la sezione [Configurazione e abilitazione della notifica automatica dei problemi \(Call Home\)](#).

Configurazione e abilitazione della notifica automatica dei problemi (Call Home)

È possibile configurare Lenovo XClarity Orchestrator affinché apra automaticamente un ticket di assistenza e invii i dati di servizio raccolti al supporto Lenovo utilizzando la funzione Call Home quando un dispositivo genera determinati eventi che richiedono assistenza, come una memoria irrecuperabile, e il problema possa essere risolto.

Prima di iniziare

Accertarsi che tutte le porte richieste da XClarity Orchestrator e dalla funzione Call Home siano disponibili prima di abilitare la funzione. Per maggiori informazioni sulle porte, vedere [Disponibilità della porta](#) nella documentazione online di XClarity Orchestrator.

Accertarsi che sia stata stabilita una connessione agli indirizzi Internet richiesti da Call Home. Per informazioni sui firewall, vedere [Firewall e server proxy](#) nella documentazione online di XClarity Orchestrator.

Se XClarity Orchestrator accede a Internet con un proxy HTTP, accertarsi che il server proxy sia configurato per l'utilizzo dell'autenticazione di base e come proxy non ricevitore. Per ulteriori informazioni sulla configurazione del proxy, vedere [Configurazione delle impostazioni di rete](#) nella documentazione online di XClarity Orchestrator.

Importante: Se Call Home è abilitato sia su XClarity Orchestrator che su Lenovo XClarity Administrator, verificare che venga utilizzato Lenovo XClarity Administrator v2.7 o versioni successive per evitare di duplicare i ticket di assistenza. Se Call Home è abilitato su XClarity Orchestrator e disabilitato su Lenovo XClarity Administrator, Lenovo XClarity Administrator v2.6 o versioni successive è supportato.

Informazioni su questa attività

Quando la funzione Call Home è configurata e abilitata e si verifica un evento che richiede assistenza su un dispositivo specifico, XClarity Orchestrator apre *automaticamente* un ticket di assistenza e trasferisce i dati di servizio relativi a quel dispositivo al centro di assistenza Lenovo.


Importante: Lenovo è impegnata nella sicurezza. I dati di servizio che in genere vengono caricati manualmente nel centro di supporto Lenovo vengono inviati automaticamente al centro di supporto Lenovo su HTTPS mediante TLS 1.2 o versione successiva. I dati relativi all'azienda non vengono mai trasmessi. L'accesso ai dati di servizio nel centro di supporto Lenovo è limitato al personale di assistenza autorizzato.

Quando la funzione Call Home non è abilitata, è possibile aprire manualmente un ticket di assistenza e inviare file di servizio al centro di supporto Lenovo seguendo le istruzioni fornite sulla [Come aprire una pagina Web del ticket di assistenza](#). Per informazioni sulla raccolta di file di servizio, vedere [Apertura manuale di un ticket di assistenza nel centro di supporto Lenovo](#) nella documentazione online di XClarity Orchestrator.

Per informazioni sulla visualizzazione dei ticket di assistenza aperti automaticamente da Call Home, vedere [Visualizzazione di ticket di assistenza e stato](#) nella documentazione online di XClarity Orchestrator.

Procedura

Per configurare Call Home per la notifica automatica dei problemi, completare le seguenti operazioni.

Passo 1. Sulla barra dei menu di XClarity Orchestrator fare clic su **Amministrazione**  → **Assistenza e supporto**, quindi su **Configurazione Call Home** nel riquadro di navigazione sinistro per visualizzare la scheda Configurazione Call Home.

Configurazione Call Home

In questa pagina è possibile configurare una funzione Call Home per inviare automaticamente i dati di servizio per qualsiasi endpoint gestito al supporto Lenovo, quando si verificano determinati eventi che richiedono assistenza su un endpoint gestito.

[Informativa sulla privacy di Lenovo](#)

Accetto l'informativa sulla privacy Lenovo

Dettagli cliente

Numero cliente


Contatto primario da utilizzare da più assegnazioni di gruppi

Assegnazione del primo gruppo
 Assegnazione dell'ultimo gruppo

Contatto predefinito

Stato Call Home:

Nome del contatto <input type="text"/>	Indirizzo <input type="text"/>
E-mail <input type="text"/>	Città <input type="text"/>
Numero di telefono <input type="text"/>	Stato/Provincia <input type="text"/>
Nome società <input type="text"/>	Paese/Area geografica <input type="text"/>
Metodo di contatto <input type="text"/>	Codice postale/CAP <input type="text"/>

Posizione del sistema 

Passo 2. Leggere l' [Informativa sulla privacy di Lenovo](#), quindi fare clic su **Accetto l'Informativa sulla privacy di Lenovo**.

Passo 3. Specificare il numero cliente Lenovo predefinito da utilizzare quando si segnalano problemi.

Il numero cliente è indicato nell'e-mail di abilitazione ricevuta al momento dell'acquisto della licenza per XClarity Orchestrator.

Passo 4. Modificare lo stato di Call Home su **Abilita**.

Passo 5. Selezionare il contatto primario da utilizzare da più assegnazioni di gruppo.

È possibile assegnare un contatto primario di supporto a un gruppo di dispositivi. Se un dispositivo è membro di più gruppi, è possibile che a ciascun gruppo sia assegnato un contatto primario differente. È possibile scegliere di utilizzare l'assegnazione del contatto principale per il primo gruppo o l'ultimo gruppo a cui è stato assegnato il dispositivo.

Passo 6. Compilare le informazioni sul contatto e il metodo di contatto preferito dal supporto Lenovo.

Se un dispositivo non è membro di un gruppo con un contatto primario assegnato, il contatto predefinito viene utilizzato per Call Home.

Passo 7. Compilare le informazioni sulla posizione.

Passo 8. Fare clic su **Test della connessione Call Home** per verificare che XClarity Orchestrator possa comunicare con il centro di supporto Lenovo.

Passo 9. Fare clic su **Applica**.

Al termine

Continuare la configurazione iniziale consultando la sezione [Configurazione dell'inoltro dei dati degli eventi](#).

Configurazione dell'inoltro dei dati degli eventi

È possibile inoltrare i dati di eventi, inventari e metriche da Lenovo XClarity Orchestrator alle applicazioni esterne, utilizzabili per monitorare e analizzare i dati.

Informazioni su questa attività

Dati di eventi

XClarity Orchestrator può inoltrare eventi che si verificano nel proprio ambiente a strumenti esterni, in base a criteri (filtri) specificati. Ogni evento generato viene monitorato per verificarne la corrispondenza ai criteri. Se c'è corrispondenza, l'evento viene inoltrato alla posizione specificata utilizzando il protocollo indicato.

XClarity Orchestrator supporta l'inoltro dei dati degli eventi ai seguenti strumenti esterni.

- **E-mail.** I dati di evento vengono inoltrati a uno o più indirizzi e-mail tramite SMTP.
- **Intelligent Insights.** I dati degli eventi vengono inoltrati in un formato predefinito a SAP Data Intelligence. È quindi possibile utilizzare SAP Data Intelligence per gestire e monitorare i dati degli eventi.
- **REST.** I dati di evento vengono inoltrati in rete a un Web Service REST.
- **Syslog.** I dati di evento vengono inoltrati in rete a un server log centrale in cui gli strumenti nativi possono essere utilizzati per monitorare il syslog.

XClarity Orchestrator utilizza *filtri globali* per definire l'ambito dei dati di evento da inoltrare. È possibile creare filtri eventi per inoltrare solo eventi con proprietà specifiche, inclusi codici di eventi, classi di eventi, gravità degli eventi e tipi di assistenza. È inoltre possibile creare filtri per dispositivi per inoltrare solo gli eventi generati da determinati dispositivi.

Dati dell'inventario e degli eventi

XClarity Orchestrator consente di inoltrare tutti i dati di inventario ed eventi per tutti i dispositivi alle applicazioni esterne, che è possibile utilizzare per monitorare e analizzare i dati.

- **Splunk.** I dati degli eventi vengono inoltrati in un formato predefinito a un'applicazione Splunk. È possibile quindi utilizzare Splunk per creare grafici e diagrammi basati sui dati degli eventi. È possibile definire più configurazioni Splunk, ma XClarity Orchestrator può inoltrare gli eventi a una sola configurazione Splunk. Pertanto, è possibile abilitare solo una configurazione Splunk alla volta.

Dati di metrica

XClarity Orchestrator può inoltrare i dati di metrica raccolti sui dispositivi gestiti al seguente strumento esterno.

- **TruScale Infrastructure Services.** I dati di metrica vengono inoltrati in un formato predefinito a Lenovo TruScale Infrastructure Services. È quindi possibile utilizzare TruScale Infrastructure Services per gestire e monitorare i dati di metrica.

Attenzione: Le informazioni sul server d'inoltro TruScale Infrastructure Services sono destinate solo ai rappresentanti dell'assistenza Lenovo.

È possibile definire più server d'inoltro TruScale Infrastructure Services. Tuttavia XClarity Orchestrator può inoltrare i dati di metrica a un solo server d'inoltro TruScale Infrastructure Services. Pertanto è possibile abilitare solo un server d'inoltro TruScale Infrastructure Services alla volta.

Ulteriori informazioni:  [Per conoscere Lenovo TruScale Infrastructure Services](#)

Per ulteriori informazioni sull'inoltro dei dati degli eventi, vedere [Inoltro di dati di eventi, inventario e metrica](#) nella documentazione online di XClarity Orchestrator.

Al termine

Continuare la configurazione iniziale consultando la sezione [Connessione degli strumenti di gestione delle risorse](#).

Connessione degli strumenti di gestione delle risorse

Lenovo XClarity Orchestrator monitora e gestisce i dispositivi tramite gli strumenti di gestione delle risorse e delle applicazioni.

Prima di iniziare

XClarity Orchestrator può supportare un numero illimitato di strumenti di gestione delle risorse che gestiscono collettivamente un massimo di 10,000 dispositivi.

Assicurarsi che gli strumenti di gestione delle risorse siano supportati (vedere [Hardware e software supportati](#) nella documentazione online di XClarity Orchestrator).

Verificare che gli strumenti di gestione delle risorse siano online e raggiungibili in rete da XClarity Orchestrator.

Assicurarsi che l'account utente utilizzato per l'autenticazione allo strumento di gestione delle risorse disponga dei privilegi corretti. Per XClarity Administrator, gli account utente devono essere assegnati al ruolo **lxc-supervisor**, **lxc-admin**, **lxc-security-admin**, **lxc-hw-admin** o **lxc-recovery**.

Verificare che lo strumento di gestione delle risorse non abbia raggiunto il numero massimo di server d'inoltro degli eventi supportati. XClarity Orchestrator crea un server d'inoltro degli eventi nello strumento di gestione delle risorse quando viene creata una connessione allo strumento di gestione delle risorse.

Quando si connette uno strumento di gestione delle risorse che dispone di un certificato con firma esterna:

- Verificare che sia un certificato X.509 v3. XClarity Orchestrator non può connettersi a uno strumento di gestione delle risorse che dispone di un certificato v1 con firma esterna.
- Verificare che i dettagli del certificato includano i seguenti requisiti.
 - Utilizzo chiavi deve contenere
 - Accordo chiave
 - Firma digitale
 - Crittografia a chiave
 - Utilizzo chiavi avanzato deve contenere
 - Server di autenticazione (1.3.6.1.5.5.7.3.1)
 - Autenticazione client (1.3.6.1.5.5.7.3.2)

Informazioni su questa attività

XClarity Orchestrator supporta i seguenti strumenti di gestione delle risorse e delle applicazioni.

- **Lenovo XClarity Management Hub 2.0.** Gestisce, monitora ed esegue il provisioning dei dispositivi ThinkSystem e ThinkAgile. È necessario installare un agente UDC in ciascun dispositivo client ThinkEdge per consentire la comunicazione tra il dispositivo e XClarity Orchestrator.

Importante: Il processo di registrazione XClarity Management Hub 2.0 è diverso da quello di un altro strumento di gestione delle risorse. Per istruzioni dettagliate, vedere .

- **Lenovo XClarity Management Hub.** Gestisce, monitora ed esegue il provisioning dei dispositivi client ThinkEdge. È necessario installare un agente UDC in ciascun dispositivo client ThinkEdge per consentire la comunicazione tra il dispositivo e XClarity Orchestrator.

Importante: Il processo di registrazione XClarity Management Hub è diverso da quello di un altro strumento di gestione delle risorse. Per istruzioni dettagliate, vedere .

- **Lenovo XClarity Administrator.** Gestisce, monitora ed esegue il provisioning dei dispositivi Lenovo con controller di gestione della scheda di base.
- **Schneider Electric EcoStruxure IT Expert.** Gestisce e monitora le risorse dell'infrastruttura.
- **VMware vRealize Operations Manager.**

Quando si connette uno strumento di gestione delle risorse di XClarity Management Hub o XClarity Administrator, XClarity Orchestrator:

- Recupera le informazioni su tutti i dispositivi gestiti dallo strumento di gestione delle risorse.
- Crea e abilita un server d'inoltro degli eventi (per un servizio Web REST) nel server di gestione per monitorare e inoltrare gli eventi a XClarity Orchestrator.

L'indirizzo di rete (indirizzo IP o nome host) fornito viene utilizzato come nome dello strumento di gestione.

Procedura

Per connettere uno strumento di gestione delle risorse o delle applicazioni, completare le seguenti operazioni.

- Passo 1. Sulla barra dei menu di XClarity Orchestrator fare clic su **Risorse** (🔗) → **Strumenti di gestione delle risorse** per visualizzare la scheda Strumenti di gestione delle risorse.

Strumenti di gestione delle risorse

Definire gli strumenti di gestione delle risorse che XClarity Orchestrator può utilizzare per ricevere le informazioni sui dispositivi ed eseguire le funzioni di gestione.

Tutte le azioni Filtri Cerca

<input type="checkbox"/>	Strumento di	Stato di inte	Tipo	Versione	Build	Connesso	Dati di analis	Gruppi
<input type="checkbox"/>	XClarity...	● No...	XClarity...	2.0.0	279	Non dispor	Non dispor	Non dispor
<input type="checkbox"/>	host-10-...	● No...	XClarity...	3.6.0	108	16/02/23,	<input checked="" type="checkbox"/> 1	Non dispor

0 selezionato / 2 Totale Righe per pagina: 10

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

Connetti strumento di gestione delle risorse

Strumento di gestione delle risorse
XClarity Administrator

Indirizzo FQDN o IP*

Porta sicura*
443

Autenticazione a Lenovo XClarity Administrator

Account utente*

Password*

Raccolta dei dati di analisi unità Disabilitato

Connetti

Passo 3. Selezionare il tipo di strumento di gestione delle risorse e inserire le informazioni richieste.

- **XClarity Management Hub 2.0 o XClarity Management Hub**
 1. Immettere la chiave di registrazione generata dall'istanza dell'hub di gestione e fare clic su **Connetti**. Per ottenere il token di richiesta della registrazione, eseguire l'accesso al portale dell'hub di gestione, fare clic su **Registrazione** e selezionare **Crea chiave di registrazione**.
 2. Copiare la chiave di registrazione generata da XClarity Orchestrator.

3. Dal portale dell'hub di gestione, fare clic su **Registrazione** e selezionare **Installa chiave di registrazione**, incollare il token di registrazione di XClarity Orchestrator e fare clic su **Connetti**.

- **XClarity Administrator**

- Specificare il nome di dominio completo o l'indirizzo IP (IPv4 o IPv6).L'utilizzo del nome host senza il nome di dominio non è supportato.
- Facoltativamente è possibile modificare la porta dello strumento di gestione delle risorse. Il valore predefinito è 443.
- Specificare l'account utente e la password da utilizzare per eseguire il login a strumento di gestione delle risorse.
- È possibile abilitare **Raccolta dei dati di analisi unità**. Se abilitata, i dati di analisi dell'unità vengono raccolti quotidianamente per i dispositivi ThinkSystem e ThinkAgile e utilizzati per l'analisi predittiva.La raccolta dei dati di analisi dell'unità è supportata solo per gli strumenti di gestione delle risorse XClarity Administrator v3.3.0 e successive.

Attenzione: La raccolta dei dati potrebbe incidere sulle prestazioni del sistema.

- **Esperto EcoStruxure IT.** Specificare il nome, la chiave token e l'URL da utilizzare per la connessione.

- **vRealize Operations Manager**

- Specificare il nome di dominio completo o l'indirizzo IP (IPv4 o IPv6).L'utilizzo del nome host senza il nome di dominio non è supportato.
- Facoltativamente è possibile modificare la porta dello strumento di gestione delle risorse. Il valore predefinito è 443.
- Selezionare facoltativamente l'origine dell'autorizzazione per utenti e gruppi.
- Specificare l'account utente e la password da utilizzare per eseguire il login a vRealize Operations Manager.

Passo 4. Fare clic su **Connetti**.

Viene creato un processo per eseguire questa operazione. È possibile monitorare l'avanzamento del processo dalla scheda **Monitoraggio** (📧) → **Processi**. Se il processo non è stato completato correttamente, fare clic sul relativo collegamento per visualizzare i dettagli sul processo (vedere).

Quando viene stabilita una connessione con lo strumento di gestione delle risorse, lo strumento viene aggiunto alla tabella.

Passo 5. Se si sceglie di collegarsi a XClarity Management Hub, verrà visualizzata una finestra di dialogo con una chiave di registrazione.

Per completare la connessione, fare clic su **Copia negli Appunti** per copiare la chiave di registrazione. Eseguire quindi l'accesso a XClarity Management Hub, fare clic su **Amministrazione** → **Configurazione hub** e selezionare **Installa chiave di registrazione**. Incollare quindi la chiave di registrazione e fare clic su **Invia**.

Al termine

La configurazione iniziale è completata.

Capitolo 5. Applicazione delle licenze per XClarity Orchestrator

Lenovo XClarity Orchestrator è un'applicazione a pagamento. È possibile utilizzare XClarity Orchestrator gratuitamente per un massimo di 90 giorni con la licenza di prova gratuita; tuttavia, una volta terminata la prova gratuita, è necessario acquistare e installare le licenze appropriate per continuare a utilizzare le funzioni di assistenza e supporto di XClarity Orchestrator.

Prima di iniziare

Per informazioni sull'acquisto delle licenze, contattare un rappresentante Lenovo o un business partner autorizzato.

È necessaria una licenza per ogni dispositivo gestito che supporta le funzioni avanzate (configurazione di server e distribuzione del sistema operativo).

- Una licenza dello chassis fornisce licenze per 14 dispositivi.
- Per i server complessi scalabili System x3850 X6 (6241), ogni server richiede una licenza specifica, indipendentemente dalle partizioni.
- Per i server complessi scalabili System x3950 X6 (6241), se non esistono partizioni, ogni server richiede una licenza specifica. Se esistono partizioni, ogni partizione necessita di una licenza specifica.
- I seguenti dispositivi *non supportano* le funzioni avanzate e pertanto *non richiedono* licenze per queste funzioni; è necessario tuttavia acquistare una licenza per ognuno di questi dispositivi per ottenere assistenza e supporto per XClarity Orchestrator XClarity Administrator.
 - Server ThinkServer
 - Server System x M4
 - Server System x X5
 - Server System x3850 X6 e x3950 X6 (3837)
 - Dispositivi di storage
 - Switch

È necessario essere membro di un gruppo di utenti a cui è assegnato il ruolo predefinito di **Supervisore**.

Informazioni su questa attività

XClarity Orchestrator supporta le seguenti licenze.

- **XClarity Orchestrator.** Abilita le funzioni di Orchestrator e di gestione di base per server, chassis, switch e dispositivi di storage, nonché la licenza di assistenza e supporto per XClarity Orchestrator. Per le funzioni di Orchestrator, è richiesta una licenza in XClarity Orchestrator per ogni dispositivo che supporta la configurazione del server e la distribuzione del sistema operativo. Per il servizio e il supporto di XClarity Orchestrator, è richiesta una licenza per *ogni dispositivo gestito*.

La conformità della licenza viene determinata in base al numero di dispositivi gestiti. Il numero di dispositivi gestiti non deve superare il numero totale di licenze in tutte le chiavi di licenza attive di XClarity Orchestrator. Quando il numero di licenze di XClarity Orchestrator non è conforme al numero richiesto di licenze (ad esempio, se una licenza scade o se la gestione dei dispositivi aggiuntivi supera il numero totale di licenze attive), è necessario un periodo di tolleranza di 90 giorni per installare le licenze appropriate. Se il periodo di tolleranza (inclusa la versione di prova gratuita) delle licenze termina prima dell'installazione del numero di licenze richiesto, *tutte* le funzioni di XClarity Orchestrator (inclusi monitoraggio, gestione di base e analisi) vengono disabilitate. Quando si esegue il login, si viene reindirizzati alla pagina informativa della licenza in cui è possibile applicare licenze aggiuntive.

Ad esempio, se si gestiscono altri 100 server ThinkSystem e 20 switch rack mediante un'istanza esistente di XClarity Administrator gestita mediante XClarity Orchestrator, sono necessari 90 giorni per l'acquisto e l'installazione di 100 licenze aggiuntive di XClarity Orchestrator prima che tutte le funzioni siano disabilitate nell'interfaccia utente. Le licenze per i 20 switch rack non sono necessarie per utilizzare le funzioni di XClarity Orchestrator; tuttavia, sono richieste se si desidera assistenza e supporto per XClarity Orchestrator. Se le funzioni di XClarity Orchestrator sono disabilitate, vengono riabilitate dopo aver installato una quantità di licenze sufficiente a ottenere nuovamente la conformità.

Importante: La licenza di base di XClarity Orchestrator è un prerequisito per le licenze di analisi di XClarity Pro e XClarity Orchestrator. Se il numero di licenze di XClarity Pro o XClarity Orchestrator è conforme, ma il numero di licenze di base attive *non lo è*, tutte le funzioni di XClarity Orchestrator (incluse le funzioni di analisi) sono disabilitate per tutti i dispositivi.

- **Lenovo XClarity Pro.** Abilita le funzioni di gestione avanzate (configurazione del server e distribuzione del sistema operativo). È richiesta una licenza in XClarity Orchestrator per ogni dispositivo che supporta le funzioni di gestione avanzate.

La conformità della licenza viene determinata in base al numero di dispositivi gestiti. Il numero di dispositivi gestiti non deve superare il numero totale di licenze in tutte le chiavi di licenza attive di XClarity Pro. Quando il numero di licenze di XClarity Pro non è conforme, si dispone di un periodo di tolleranza di 90 giorni per installare le licenze appropriate. Se il periodo di tolleranza (inclusa la versione di prova gratuita) termina prima dell'installazione del numero di licenze richiesto, le funzioni di configurazione e di distribuzione del sistema operativo vengono disabilitate per *tutti i dispositivi*.

Per ulteriori informazioni sulle licenze di XClarity Pro, vedere [Licenze e versione di prova gratuita per 90 giorni](#) nella documentazione online di XClarity Administrator.

- **XClarity Orchestrator Analisi.** Abilita le funzioni di analisi. È richiesta una licenza in XClarity Orchestrator per ogni dispositivo che supporta le funzioni di gestione avanzate.

La conformità della licenza viene determinata in base al numero di dispositivi gestiti. Il numero di dispositivi gestiti non deve superare il numero totale di licenze in tutte le chiavi di licenza di analisi attive di XClarity Orchestrator. Quando il numero di licenze di XClarity Orchestrator non è conforme al numero richiesto di licenze di analisi (ad esempio, se una licenza scade o se la gestione dei dispositivi aggiuntivi supera il numero totale di licenze attive), è necessario un periodo di tolleranza di 90 giorni per installare le licenze appropriate. Se il periodo di tolleranza (inclusa la versione di prova gratuita) per le licenze di analisi di termina prima dell'installazione del numero di licenze richiesto, i menu **Monitoraggio → Analisi** vengono disabilitati e non è possibile visualizzare i report di analisi o creare regole di avviso personalizzate e query per *tutti i dispositivi*.

Importante: Dopo aver installato le licenze di analisi di XClarity Orchestrator, è necessario aggiornare l'interfaccia utente.

Nota: Se si installano le licenze di analisi di XClarity Orchestrator scadute (che hanno superato la data di scadenza oltre il periodo di tolleranza di 90 giorni) e quindi si aggiorna l'interfaccia utente, le funzioni di analisi sono disabilitate. Ciò significa che un periodo di prova o di tolleranza attivo viene interrotto, che i servizi di analisi sono stati arrestati e che le funzioni di analisi sono disabilitate. La seguente operazione potrebbe richiedere alcuni minuti. È possibile riabilitare le funzioni di analisi importando nuove licenze valide.

Una licenza *non* è legata a dispositivi specifici.

Il periodo di attivazione viene avviato quando le licenze vengono riscattate.

Le licenze vengono installate mediante una *chiave di attivazione* della licenza. Una volta riscattate le licenze, è possibile creare una chiave di attivazione per tutte le licenze o per un sottoinsieme di licenze disponibili e quindi scaricare e installare la chiave di attivazione in XClarity Orchestrator.

Ogni volta che XClarity Orchestrator non è conforme, il periodo di tolleranza viene reimpostato su 90 giorni.

Se le licenze sono già installate, le nuove licenze *non* sono richieste per l'aggiornamento a una nuova versione di XClarity Orchestrator.

Se si utilizza una licenza di prova gratuita o si dispone di un periodo di tolleranza per diventare conformi e si esegue l'aggiornamento a una versione successiva di XClarity Orchestrator, la licenza di prova o il periodo di tolleranza viene reimpostato su 90 giorni.

Quando si aggiorna XClarity Orchestrator o si verifica una condizione di errore che richiede il ripristino delle chiavi di attivazione, è possibile utilizzare le chiavi esportate o scaricare tutte le chiavi di attivazione (per ciascun ID cliente) da [Portale Web Features on Demand](#) e quindi importarle (come chiavi di attivazione singole o un file ZIP delle chiavi) in XClarity Orchestrator.

È possibile visualizzare un elenco delle licenze software correnti dal [Portale Web Features on Demand](#).

Procedura

Per installare licenze per XClarity Orchestrator, effettuare le operazioni che seguono.

Passo 1. Contattare il rappresentante Lenovo o il business partner autorizzato per acquistare le licenze in base al numero di dispositivi che si desidera gestire.

Una volta acquistate le licenze, viene inviato un codice di autorizzazione in un'e-mail di *prova di titolarità elettronica*. È inoltre possibile recuperare il codice di autorizzazione dal [Portale Web Features on Demand](#) facendo clic su **Recupera codice di autorizzazione**. Se non si riceve l'e-mail e la licenza è stata acquistata tramite un business partner, contattare il business partner per richiedere il codice di autorizzazione.

Il codice di autorizzazione è una stringa alfanumerica di 22 caratteri. Per completare il passaggio successivo, è necessario il codice di autorizzazione.

Passo 2. Recuperare le chiavi di attivazione per le licenze.

- **Creazione delle chiavi di attivazione da un codice di autorizzazione**

1. Accedere al [Portale Web Features on Demand](#) da un browser Web ed eseguire il login al portale utilizzando l'indirizzo e-mail come ID utente.
2. Fare clic su **Richiedi chiave di attivazione**.
3. Selezionare **Inserisci un codice di autorizzazione singolo**.
4. Immettere il codice di autorizzazione di 22 caratteri e fare clic su **Continua**.
5. Immettere il numero cliente Lenovo nel campo **Numero cliente Lenovo**.
6. Immettere il numero di licenze che si desidera riscattare nel campo **Riscatta quantità**, quindi fare clic su **Continua**. Per riscattare tutte le licenze disponibili in questa chiave, inserire il numero corrispondente nel campo **Licenze disponibili**.

Se si riscatta un sottoinsieme di licenze disponibili, è possibile riscattare le licenze rimanenti in un'altra chiave di attivazione utilizzando lo stesso codice di autorizzazione.

7. Seguire le istruzioni per immettere i dettagli del prodotto e le informazioni di contatto, quindi fare clic su **Continua** per generare la chiave di attivazione.
8. Facoltativamente, specificare i destinatari aggiuntivi cui inviare le chiavi di attivazione.
9. Fare clic su **Invia** per inviare le chiavi di attivazione. La persona assegnata all'ordine di acquisto e i destinatari aggiuntivi riceveranno un'e-mail con la chiave di attivazione. La chiave di attivazione è un file in formato .KEY.

Nota: È inoltre possibile scaricare le chiavi di attivazione (singolarmente o in batch) dal [Portale Web Features on Demand](#) facendo clic sul **Collegamento per il download**.

- **Download delle chiavi di attivazione esistenti**

1. Accedere al [Portale Web Features on Demand](#) da un browser Web ed eseguire il login al portale utilizzando l'indirizzo e-mail come ID utente.
2. Fare clic su **Recupera cronologia**.
3. Selezionare "Cerca cronologia tramite il numero cliente Lenovo" come **Tipo di ricerca**.
4. Immettere il numero cliente Lenovo nel campo **Cerca valore**. Il formato del numero cliente è 121XXXXXXX.
5. Fare clic su **Seleziona tutto** per scaricare tutte le chiavi di attivazione oppure selezionare le singole chiavi di attivazione dall'elenco.
6. Fare clic su **E-mail** per inviare le chiavi all'utente oppure fare clic su **Scarica** per scaricare le chiavi nel sistema locale.

Passo 3. Applicare le licenze in XClarity Orchestrator.

1. Sulla barra dei menu di XClarity Orchestrator fare clic su **Manutenzione** (🔧) e selezionare la scheda **Licenze** per visualizzare la scheda Informazioni sulla licenza.

Prodotto	Descrizione chiave di	Numero di licenze	Data di scadenza	Stato
XClarity Orchestr...	Lenovo SYSTEM...	Illimitato	01/03/22	Scaduto
XClarity Orchestr...	Lenovo SYSTEM...	100000	01/03/20	Scaduto

2. Fare clic sull'icona **Importa e applica** (📁) per applicare le licenze.
3. Trascinare e rilasciare il file della chiave di attivazione per le licenze che si desidera applicare nella finestra di dialogo Importa oppure fare clic su **Sfoggia** per individuare il file.

Per importare più chiavi di attivazione, comprimere i file .KEY in un file ZIP e selezionare il file ZIP per l'importazione.

4. Fare clic sull'icona **Importa** per importare e applicare le licenze. Al termine dell'installazione, la chiave di attivazione (licenza) viene elencata nella tabella con il numero di licenze installate e il periodo di attivazione (data di inizio e di scadenza).

Passo 4. Se sono state applicate licenze valide dopo che alcune funzioni sono state disabilitate, scollegarsi ed eseguire nuovamente il login per abilitare le funzioni applicabili.

Al termine

Nella scheda Informazioni sulla licenza è possibile effettuare le operazioni che seguono.

- Salvare una o più chiavi di attivazione selezionate nel sistema locale facendo clic sull'icona **Salva** (↓).

Quando si esportano più chiavi di attivazione, i file vengono scaricati come un singolo file ZIP.

- Eliminare una chiave di attivazione specifica facendo clic sull'icona **Elimina** (🗑️).

Richiesta di supporto

- Se si verificano problemi ed è stato utilizzato un business partner, contattare il business partner per verificare la transazione e la titolarità.
- Se non si riceve la prova di titolarità elettronica, i codici di autorizzazione o le chiavi di attivazione o se queste informazioni sono state inviate a un utente sbagliato, contattare un responsabile regionale in base all'area geografica.
 - ESDNA@lenovo.com (Paesi del Nord America)
 - ESDAP@lenovo.com (paesi dell'Asia Pacifico)
 - ESDEMEA@lenovo.com (paesi europei, mediorientali e asiatici)
 - ESDLA@lenovo.com (Paesi dell'America Latina)
 - ESDChina@Lenovo.com (Cina)
- Se le informazioni personali sulla titolarità non sono corrette, contattare il supporto Lenovo all'indirizzo SW_override@lenovo.com e includere le seguenti informazioni.
 - Numero dell'ordine
 - Le informazioni di contatto, tra cui l'indirizzo e-mail
 - L'indirizzo fisico
 - Le modifiche desiderate
- In caso di problemi o domande relative al download della licenza, contattare il supporto Lenovo all'indirizzo -eSupport_-_Ops@lenovo.com.

Capitolo 6. Aggiornamento di XClarity Orchestrator

È possibile aggiornare Lenovo XClarity Orchestrator per utilizzare il software Orchestrator più recente.

Prima di iniziare

Ulteriori informazioni:  [Come aggiornare XClarity Orchestrator](#)

È necessario essere membro di un gruppo di utenti a cui è assegnato il ruolo predefinito di **Supervisore**.

Un bundle di correzioni di XClarity Orchestrator (ad esempio, v1.4.2) può essere applicato solo a una versione (ad esempio, v1.4.0 o v1.4.1). Un bundle di correzioni contiene tutte le correzioni precedenti (ad esempio, v1.4.2 contiene le stesse correzioni di v1.4.1, oltre a correzioni aggiuntive); tuttavia, un bundle di correzioni non contiene l'intera base di codice.

Attenzione: Esaminare le seguenti considerazioni prima di aggiornare XClarity Orchestrator.

- **A XClarity Orchestrator 2.0** Lo storage minimo richiesto per l'appliance virtuale è pari a un **totale di 551 GB** con tre dischi collegati. È inoltre necessario collegare un terzo disco (disco 2) con un minimo di 200 GB.

L'appliance virtuale XClarity Orchestrator deve essere spenta prima di aggiungere un nuovo disco fisso.

Per aggiungere un nuovo disco fisso all'appliance virtuale, attenersi alla procedura descritta di seguito.

– Per ESXi mediante VMware vSphere

1. Connettersi all'host tramite VMware vSphere Client.
2. Spegnerne la macchina virtuale XClarity Orchestrator.
3. Fare clic con il pulsante destro del mouse sulla macchina virtuale e scegliere **Modifica impostazioni**.
4. Selezionare **Aggiungi un nuovo dispositivo → Disco fisso**.
5. Modificare le dimensioni e impostarle su 200 GB.
6. Fare clic su **OK**.
7. Accendere la macchina virtuale XClarity Orchestrator.

– Per ESXi mediante VMware vCenter

1. Connettersi all'host tramite VMware vCenter.
2. Spegnerne la macchina virtuale.
3. Accedere alle impostazioni della macchina virtuale e fare clic su **Aggiungi**.
4. Fare clic su **Disco fisso → Crea un nuovo disco virtuale**.
5. Selezionare **SCSI** per il formato del disco.
6. Configurare la capacità dell'unità disco fisso su 200 GB.
7. Fare clic su **OK**.
8. Accendere la macchina virtuale.

– Per Microsoft Hyper-V

1. Dal dashboard Server Manager fare clic su **Hyper-V**.
2. Fare clic con il pulsante destro del mouse sul server e scegliere **Hyper-V Manager**.
3. Selezionare la macchina virtuale XClarity Orchestrator e fare clic su **Arresta** nel riquadro Azioni.
4. Fare clic su **Impostazioni** per visualizzare la finestra di dialogo Impostazioni.
5. Selezionare **IDE Controller 1**.
6. Dal riquadro destro, selezionare **Unità disco fisso**, quindi fare clic su **Aggiungi** per aggiungere un nuovo disco fisso.

7. Dal riquadro destro, selezionare **File disco fisso virtuale (.vhd)** e fare clic su **Nuovo** per visualizzare la Creazione guidata nuovo disco fisso virtuale.
 8. Completare la procedura guidata come richiesto. Accertarsi di specificare un nome dell'unità disco utilizzando il formato .vhd (ad esempio, LXC0-disk3.vhd) e impostare le dimensioni su 200 GB.
 9. Selezionare la macchina virtuale XClarity Orchestrator e fare clic su **Avvia** nel riquadro Azioni.
- **A XClarity Orchestrator v1.6.** L'aggiornamento a XClarity Orchestrator v1.6 richiede XClarity Orchestrator v1.5. Se non si sta eseguendo XClarity Orchestrator v1.5, è necessario eseguire l'aggiornamento a XClarity Orchestrator v1.5 prima di eseguire l'aggiornamento a XClarity Orchestrator v1.6.
 - **A XClarity Orchestrator v1.5.** L'aggiornamento a XClarity Orchestrator v1.5 richiede XClarity Orchestrator v1.4. Se non si sta eseguendo XClarity Orchestrator v1.4, è necessario eseguire l'aggiornamento a XClarity Orchestrator v1.4 prima di eseguire l'aggiornamento a XClarity Orchestrator v1.5.
 - **A XClarity Orchestrator v1.4.** L'aggiornamento a XClarity Orchestrator v1.4 richiede XClarity Orchestrator v1.3. Se non si sta eseguendo XClarity Orchestrator v1.3, è necessario eseguire l'aggiornamento a XClarity Orchestrator v1.3 prima di eseguire l'aggiornamento a XClarity Orchestrator v1.4.
 - **A XClarity Orchestrator 1.3**
 - L'aggiornamento a XClarity Orchestrator v1.3 potrebbe richiedere almeno due ore. Per determinare se l'aggiornamento è stato completato, fare clic su **Manutenzione → Aggiornamenti del server Orchestrator** e verificare che la nuova versione sia elencata e che lo stato applicato non sia più "Applicazione".
 - **Attenzione:** Prima di aggiornare XClarity Orchestrator a v1.3, verificare che il nome host dell'appliance virtuale XClarity Orchestrator sia **lxco** e che nella scheda Configurazione DNS non sia impostato alcun dominio sulla pagina **Amministrazione (⚙️) → Rete**.
 - Gli utenti assegnati al ruolo di **Supervisore** vengono aggiunti al gruppo di utenti **SupervisorGroup** durante l'aggiornamento
 - Gli utenti assegnati al ruolo di **Operatore** vengono aggiunti al gruppo di utenti **OperatorLegacyGroup** durante l'aggiornamento. Il gruppo di utenti **OperatorLegacyGroup** è associato al ruolo **Legacy operatore**, che fornisce agli utenti gli stessi privilegi del ruolo **Operatore** nelle versioni precedenti. Il ruolo **Legacy operatore** e il gruppo di utenti **OperatorLegacyGroup** verranno deprecati in una versione successiva i gruppi di utenti esistenti vengono assegnati al ruolo **Operatore** durante l'aggiornamento
 - La creazione di regole per la generazione di avvisi di analisi personalizzate è semplificata in XClarity Orchestrator v1.3. Le regole di avviso personalizzate esistenti non vengono migrate nel nuovo formato e andranno perse una volta completato l'aggiornamento.
 - **Da XClarity Orchestrator v1.1**
 - Gli utenti assegnati al ruolo di **Supervisore** vengono aggiunti al gruppo di utenti **SupervisorGroup** durante l'aggiornamento
 - Gli utenti assegnati al ruolo di **Operatore** vengono aggiunti al gruppo di utenti **OperatorLegacyGroup** durante l'aggiornamento. Il gruppo di utenti **OperatorLegacyGroup** è associato al ruolo **Legacy operatore**, che fornisce agli utenti gli stessi privilegi del ruolo **Operatore** nelle versioni precedenti. Il ruolo **Legacy operatore** e il gruppo di utenti **OperatorLegacyGroup** verranno deprecati in una versione successiva i gruppi di utenti esistenti vengono assegnati al ruolo **Operatore** durante l'aggiornamento.
 - La creazione di regole per la generazione di avvisi di analisi personalizzate è semplificata in XClarity Orchestrator v1.3. Le regole di avviso personalizzate esistenti non vengono migrate nel nuovo formato e andranno perse una volta completato l'aggiornamento.

- Lo storage minimo richiesto per l'appliance virtuale è pari a un totale di **301 GB** con due dischi collegati. È necessario aumentare lo storage per il disco 0 a un minimo di 251 GB. È inoltre necessario collegare un secondo disco (disco 1) con un minimo di 100 GB. L'appliance virtuale XClarity Orchestrator deve essere spenta prima di aggiungere un nuovo disco fisso.

Per aggiungere un nuovo disco fisso all'appliance virtuale, attenersi alla procedura descritta di seguito.

- **Per ESXi mediante VMware vSphere**

1. Connettersi all'host tramite VMware vSphere Client.
2. Spegnerla macchina virtuale XClarity Orchestrator.
3. Fare clic con il pulsante destro del mouse sulla macchina virtuale e scegliere **Modifica impostazioni**.
4. Selezionare **Aggiungi un nuovo dispositivo → Disco fisso**.
5. Modificare le dimensioni e impostarle su 100 GB.
6. Fare clic su **OK**.
7. Accendere la macchina virtuale XClarity Orchestrator.

- **Per ESXi mediante VMware vCenter**

1. Connettersi all'host tramite VMware vCenter.
2. Spegnerla macchina virtuale.
3. Accedere alle impostazioni della macchina virtuale e fare clic su **Aggiungi**.
4. Fare clic su **Disco fisso → Crea un nuovo disco virtuale**.
5. Selezionare **SCSI** per il formato del disco.
6. Configurare la capacità dell'unità disco fisso su 100 GB.
7. Fare clic su **OK**.
8. Accendere la macchina virtuale.

- **Per Microsoft Hyper-V**

1. Dal dashboard Server Manager fare clic su **Hyper-V**.
2. Fare clic con il pulsante destro del mouse sul server e scegliere **Hyper-V Manager**.
3. Selezionare la macchina virtuale XClarity Orchestrator e fare clic su **Arresta** nel riquadro Azioni.
4. Fare clic su **Impostazioni** per visualizzare la finestra di dialogo Impostazioni.
5. Selezionare **Controller IDE 0**.
6. Dal riquadro destro, selezionare **Unità disco fisso**, quindi fare clic su **Aggiungi** per aggiungere un nuovo disco fisso.
7. Dal riquadro destro, selezionare **File disco fisso virtuale (.vhd)** e fare clic su **Nuovo** per visualizzare la Creazione guidata nuovo disco fisso virtuale.
8. Completare la procedura guidata come richiesto. Accertarsi di specificare un nome dell'unità disco utilizzando il formato .vhd (ad esempio, LXC0-disk2.vhd) e impostare le dimensioni su 100 GB.
9. Selezionare la macchina virtuale XClarity Orchestrator e fare clic su **Avvia** nel riquadro Azioni.

- **A XClarity Orchestrator v1.1**

- Tutti gli utenti vengono aggiunti automaticamente al gruppo di utenti **SupervisorGroup**. Tutti gli utenti hanno privilegi di supervisore per impostazione predefinita al termine dell'aggiornamento. Un utente supervisore può rimuovere i privilegi di supervisore per altri utenti che non devono disporre di tali privilegi
- Le configurazioni LDAP esterne esistenti vengono rimosse. Dopo aver completato l'aggiornamento è necessario riconfigurare i server di autenticazione LDAP esterni

Durante il processo di aggiornamento tutti gli utenti vengono disconnessi quando il server Orchestrator viene riavviato. È necessario attendere alcuni minuti per il completamento del riavvio. Al termine dell'aggiornamento e del riavvio, cancellare la cache del browser Web e aggiornare il browser Web prima di accedere di nuovo.

Assicurarsi di eseguire il backup dell'appliance virtuale di XClarity Orchestrator prima di installare un aggiornamento (vedere [Backup e ripristino dei dati del server di gestione](#) nella documentazione online di nella documentazione online di XClarity Orchestrator).

Verificare che tutte le porte e gli indirizzi Internet richiesti siano disponibili prima di tentare di aggiornare XClarity Orchestrator. Per ulteriori informazioni, vedere [Disponibilità della porta](#) e [Firewall e server proxy](#).

Procedura

Per aggiornare XClarity Orchestrator, completare le seguenti operazioni:

Passo 1. Scaricare il file del pacchetto di aggiornamento del server Orchestrator (.tgz) dalla [Pagina Web dei download di XClarity Orchestrator](#) in una workstation con connessione di rete nell'host XClarity Orchestrator.

Il file del pacchetto di aggiornamento contiene tutti i file richiesti: file payload (.tar.gz), metadati (.xml), cronologia delle modifiche (.chg) e leggimi (.txt).

Passo 2. Dal menu principale di XClarity Orchestrator fare clic su **Manutenzione** (🔧), quindi su **Aggiornamenti del server Orchestrator** per visualizzare la scheda Aggiornamenti del server Orchestrator.

Gli aggiornamenti del server Orchestrator precedenti alla versione attualmente installata sono elencati nella tabella con lo stato "Non applicabile" e non possono essere applicati al server Orchestrator.

File	Nota sulla	Versione	Numero di	Data di ril	Stato appl	Riavvio ob	Tipo	Dimension
Non d...	[blue square icon]	Non d...	Non d...	Non d...	Not A...	Non d...	Non d...	0.004...

Passo 3. Fare clic sull'icona **Importa** (📁) per visualizzare la finestra di dialogo Importa.

Passo 4. Trascinare e rilasciare il file intero del pacchetto di aggiornamento (.tgz) nella finestra di dialogo Importa oppure fare clic su **Sfogli** per individuare il file.

Passo 5. Fare clic su **Importa**.

Attenzione: L'importazione dei file di aggiornamento potrebbe richiedere tempo. È necessario restare sulla scheda Aggiornamenti del server Orchestrator finché non viene completato il processo di importazione. Chiudendo la scheda Aggiornamenti del server Orchestrator, il processo di importazione viene interrotto.

Una volta completata l'importazione, l'aggiornamento del server Orchestrator viene elencato nella tabella sulla scheda File del server Orchestrator.

Per monitorare l'avanzamento dell'importazione, fare clic su **Monitoraggio** (📈) → **Processi** sulla barra del menu di XClarity Orchestrator.

Passo 6. Nella scheda File del server Orchestrator selezionare il pacchetto di aggiornamento che si desidera installare.

Passo 7. Fare clic sull'icona **Applica aggiornamento** (E✓).

Per monitorare l'avanzamento dell'aggiornamento, fare clic su **Monitoraggio** (📊) → **Processi** sulla barra dei menu di XClarity Orchestrator.

Passo 8. Attendere il completamento dell'aggiornamento e il riavvio di XClarity Orchestrator. Il processo di aggiornamento potrebbe richiedere tempo.

Se si dispone dell'accesso all'host dell'appliance virtuale, è possibile monitorare l'avanzamento dalla console dell'appliance virtuale, ad esempio:

```
Lenovo XClarity Orchestrator Version x.x.x
```

```
-----
```

```
eth0    Link encap:Ethernet  HWaddr 2001:db8:65:12:34:56
        inet addr: 192.0.2.10  Bcast 192.0.2.55  Mask 255.255.255.0
        inet6 addr: 2001:db8:56ff:fe80:bea3/64  Scope:Link
```

```
=====
=====
```

```
You have 118 seconds to change IP settings. Enter one of the following:
 1. To set a static IP address for Lenovo XClarity virtual appliance eth0 port
 2. To use a DHCP address for Lenovo XClarity virtual appliance eth0 port
 3. To select subnet for Lenovo XClarity virtual appliance internal network
 x. To continue without changing IP settings
... ..
```

Passo 9. Cancellare la cache del browser Web e aggiornare il browser.

Una volta completata l'operazione, la colonna **Stato applicato** cambia in "Applicato".

Al termine

Nella scheda File del server Orchestrator è possibile effettuare le operazioni che seguono.

- Visualizzare la versione corrente e il numero della build per l'istanza di XClarity Orchestrator facendo clic sul menu **Account utente** (👤) sulla barra del titolo di XClarity Orchestrator, quindi su **Informazioni su**.
- Visualizzare la cronologia degli aggiornamenti per un aggiornamento specifico applicato a XClarity Orchestrator facendo clic sul collegamento di aggiornamento dello stato nella colonna **Stato applicato**.
- Salvare un aggiornamento del server Orchestrator selezionato nel sistema locale facendo clic sull'icona **Salva con nome** (💾).
- Eliminare un aggiornamento di un server Orchestrator selezionato, facendo clic sull'icona **Elimina** (🗑️).

Capitolo 7. Disinstallazione di XClarity Orchestrator

È possibile disinstallare l'appliance virtuale Lenovo XClarity Orchestrator utilizzando gli strumenti di gestione della macchina virtuale.

Procedura

Per disinstallare XClarity Orchestrator, effettuare le operazioni che seguono.

Passo 1. Disconnettere e rimuovere tutti gli strumenti di gestione delle risorse.

- a. Dalla barra dei menu di XClarity Orchestrator, fare clic su **Risorse** (🌐) → **Strumento di gestione delle risorse** per visualizzare la scheda Strumenti di gestione delle risorse.
- b. Selezionare tutti gli strumenti di gestione delle risorse.
- c. Fare clic sull'icona **Elimina** (🗑️).

Passo 2. Disinstallare XClarity Orchestrator utilizzando gli strumenti di gestione della macchina virtuale.

- **ESXi mediante VMware vCenter**

1. Connettersi all'host tramite VMware vCenter.
2. Fare clic con il pulsante destro del mouse sulla macchina virtuale XClarity Orchestrator nell'inventario del client **Host VMware** e selezionare **Sistema operativo guest** dal menu a comparsa.
3. Fare clic su **Arresta**.
4. Fare clic con il pulsante destro del mouse sulla macchina virtuale nell'inventario del client **Host VMware** e selezionare **Sistema operativo guest** dal menu a comparsa.
5. Fare clic su **Elimina**.

- **ESXi mediante VMware vSphere**

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

- **Hyper-V**

1. Dal dashboard **Server Manager** fare clic su **Hyper-V**.
2. Fare clic con il pulsante destro del mouse sul server e scegliere **Hyper-V Manager**.
3. Fare clic con il pulsante destro del mouse sulla macchina virtuale XClarity Orchestrator e scegliere **Arresta**.
4. Fare nuovamente clic con il pulsante destro del mouse sulla macchina virtuale e scegliere **Elimina**.

Lenovo