Lenovo XClarity Administrator
Guida alla pianificazione e all'installazione per ambienti Docker

Versione 4.0.0

Nota

Prima di utilizzare queste informazioni e il prodotto supportato, consultare le informazioni generali e legali nella documentazione online di XClarity Administrator.

Prima edizione (Febbraio 2023)

Contenuto

Figure

Tabelle

Riepilogo delle modifiche

Le versioni successive del software di gestione Lenovo XClarity Administrator forniscono il supporto di nuovi miglioramenti hardware e software, con l'aggiunta di nuove correzioni.

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

Per informazioni su tutti i componenti hardware supportati (come server, chassis e switch Flex), vedere Prerequisiti hardware e software.

Per informazioni sulle modifiche nelle release precedenti, vedere Novità nella documentazione online di XClarity Administrator.

In questa versione è supportato il seguente hardware.

- **Server e appliance**
  - ThinkAgile HX630 V3 (7D6M)
  - ThinkAgile HX645 V3 (7D9M)
  - ThinkAgile HX650 V3 (7D6N)
  - ThinkAgile HX665 V3 (7D9N)
  - ThinkAgile MX630 V3 (7D6U)
  - ThinkAgile MX650 V3 (7D6S)
  - ThinkAgile VX630 V3 (7D6X, 7Z63)
  - ThinkAgile VX635 V3 (7D9V)
  - ThinkAgile VX645 V3 (7D9K)
  - ThinkAgile VX650 V2-DPU (7Z63)
  - ThinkAgile VX650 V3 (7D6W)
  - ThinkAgile VX650 V3-DPU (7D6W)
  - ThinkAgile VX655 V3 (7D9W)
  - ThinkAgile VX665 V3 (7D9L)
  - ThinkAgile VX850 V3 (7DDK)
  - ThinkEdge SE350 V2 (7DA9)
  - ThinkEdge SE455 V3 (7DBY)
  - ThinkEdge SE360 V2 (7DAM)
  - ThinkSystem SD555 V3 (7DDP, 7DDQ)
  - ThinkSystem SD650 V3 (7D7M)
  - ThinkSystem SD650-I V3 (7D7L)
  - ThinkSystem SD650-N V3 (7D7L)
  - ThinkSystem SD665 V3 (7D9P)
  - ThinkSystem SD665-N V3 (7DAZ)
  - ThinkSystem SR630 V3 (7D72, 7D73, 7D74)
  - ThinkSystem SR635 V3 (7D9G, 7D9H)
  - ThinkSystem SR645 V3 (7D9C, 7D9D)
  - ThinkSystem SR650 V3 (7D75, 7D76, 7D77)
  - ThinkSystem SR655 V3 (7D9E, 7D9F)
  - ThinkSystem SR665 V3 (7D9B, 7D9A)
  - ThinkSystem SR675 V3 (7D9Q, 7D9R)
  - ThinkSystem SR850 V3 (7D96, 7D97, 7D98)
  - ThinkSystem SR860 V3 (7D93, 7D94, 7D95)
  - ThinkSystem SR950 V3 (7DC4, 7DC5, 7DC6)
  - ThinkSystem ST650 V3 (7D7A, 7D7B)
- **Dispositivi di storage**

  - Array completamente flash ThinkSystem DE6400F (7DB6)
  - Array flash ibrido ThinkSystem DE6400H (7DB6)
  - Array completamente flash ThinkSystem DE6600F (7DB7)
  - Array flash ibrido ThinkSystem DE6600H (7DB7)
- **Switch**
  - Switch ThinkSystem DB730S FC SAN (7D9J)
  - ThinkSystem DB400D FC SAN Director (6684)
  - ThinkSystem DB800D FC SAN Director (6682)

Questa versione supporta i seguenti miglioramenti alla pianificazione o all'installazione del software di gestione.

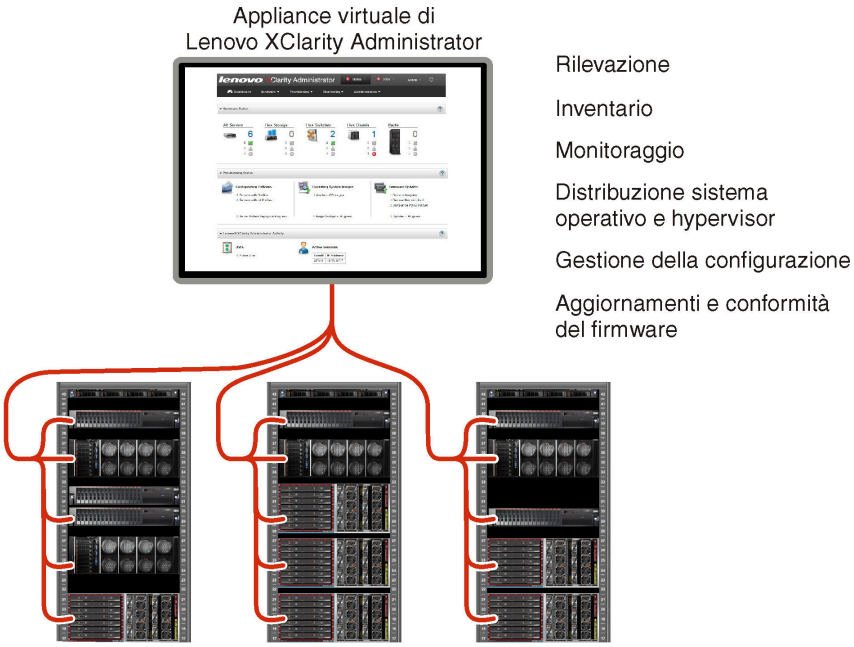
Funzione	Descrizione
Pianificazione e installazione	Rimosso ssh-rsa e aggiunti ssh-ed25519, ecdsa-sha2-nistp256, ecdsa-sha2-nistp384 e ecdsa-sha2-nistp521 all'elenco degli algoritmi delle chiavi host supportati (vedere Gestione della crittografia).

Capitolo 1. Panoramica di Lenovo XClarity Administrator

Lenovo XClarity Administrator è una soluzione centralizzata, per la gestione delle risorse, che semplifica la gestione dell'infrastruttura, velocizza i tempi di risposta e ottimizza la disponibilità dei sistemi e delle soluzioni per i server Lenovo®. Viene eseguita come un'appliance virtuale in grado di automatizzare il rilevamento, l'inventario, la tracciatura, il monitoraggio e il provisioning per server, rete e hardware di storage in un ambiente sicuro.

Ulteriori informazioni:

- XClarity Administrator: gestire l'hardware come il software
- XClarity Administrator: panoramica



XClarity Administrator dispone di un'interfaccia centrale che permette di eseguire le seguenti funzioni per tutti i dispositivi gestiti.

Gestione dell'hardware

XClarity Administrator consente una gestione dell'hardware senza agente. È in grado di rilevare automaticamente i dispositivi gestibili, inclusi il server, la rete e l'hardware di storage. La raccolta di dati dell'inventario per i dispositivi gestiti permette di disporre di un colpo d'occhio immediato dell'inventario dell'hardware gestito e del relativo stato.

Esistono varie attività di gestione per ogni dispositivo supportato, tra cui visualizzazione di stato e proprietà, configurazione di sistema e impostazioni di rete, avvio delle interfacce di gestione, accensione e spegnimento e controllo remoto. Per ulteriori informazioni sulla gestione di dispositivi, vedere Gestione dello chassis, Gestione dei server e Gestione degli switch nella documentazione online di XClarity Administrator.

Suggerimento: server, rete e hardware di storage che possono essere gestiti da XClarity Administrator vengono definiti *dispositivi*. Gli elementi hardware gestiti da XClarity Administrator vengono definiti *dispositivi gestiti*.

È possibile utilizzare la vista rack in XClarity Administrator per raggruppare i dispositivi gestiti in modo da riprodurre la configurazione del rack fisico nel data center. Per ulteriori informazioni sui rack, vedere Gestione dei rack nella documentazione online di XClarity Administrator.

Ulteriori informazioni:

- XClarity Administrator: rilevamento
- XClarity Administrator: inventario
- XClarity Administrator: controllo remoto

Monitoraggio dell'hardware

XClarity Administrator offre una vista centralizzata di tutti gli eventi e gli avvisi generati dai dispositivi gestiti. Un evento o un avviso viene passato a XClarity Administrator e visualizzato nel log eventi o nel log avvisi. Un riepilogo di tutti gli eventi e gli avvisi è visibile dal Dashboard e dalla barra di stato. Gli eventi e gli avvisi per un dispositivo specifico sono disponibili nella pagina dei dettagli di avvisi ed eventi per tale dispositivo.

Per ulteriori informazioni sul monitoraggio dell'hardware, vedere Utilizzo degli eventi e Gestione degli avvisi nella documentazione online di XClarity Administrator.

Ulteriori informazioni: XClarity Administrator: monitoraggio

Gestione della configurazione

È possibile eseguire rapidamente il provisioning e il pre-provisioning di tutti i server utilizzando una configurazione coerente. Le impostazioni di configurazione (come storage locale, adattatori I/O, impostazioni di avvio, firmware, porte, controller di gestione e impostazioni UEFI) vengono salvate come pattern server che è possibile applicare a uno o più server gestiti. Una volta aggiornati i pattern server, le modifiche vengono distribuite automaticamente ai server applicati.

I pattern server integrano inoltre il supporto per la virtualizzazione degli indirizzi I/O, pertanto è possibile virtualizzare le connessioni fabric Flex System oppure reimpiegare i server senza interruzione ne fabric.

Per ulteriori informazioni sulla configurazione dei server, vedere Configurazione dei server mediante XClarity Administrator nella documentazione online di XClarity Administrator.

Ulteriori informazioni:

- XClarity Administrator: dal bare metal al cluster
- XClarity Administrator: pattern di configurazione

Aggiornamenti e conformità del firmware

La gestione del firmware è semplificata dall'assegnazione di criteri di conformità del firmware ai dispositivi gestiti. Una volta creato e assegnato un criterio di conformità ai dispositivi gestiti, XClarity Administrator monitora le modifiche apportate all'inventario per tali dispositivi e contrassegna i dispositivi non conformi.

Quando un dispositivo non è conforme, è possibile utilizzare XClarity Administrator per applicare e attivare gli aggiornamenti firmware per tutti i dispositivi nel suddetto dispositivo da un repository di aggiornamenti firmware gestiti.

Nota: L'aggiornamento del repository e il download di aggiornamenti firmware richiedono una connessione Internet. Se XClarity Administrator non dispone di una connessione Internet, è possibile importare manualmente gli aggiornamenti firmware nel repository.

Per ulteriori informazioni sull'aggiornamento del firmware, vedere Aggiornamento del firmware sui dispositivi gestiti nella documentazione online di XClarity Administrator.

Ulteriori informazioni:

- XClarity Administrator: dal bare metal al cluster
- XClarity Administrator: aggiornamenti firmware
- XClarity Administrator: provisioning degli aggiornamenti di sicurezza del firmware

Distribuzione del sistema operativo

È possibile utilizzare XClarity Administrator per gestire un repository di immagini del sistema operativo e per distribuire immagini del sistema operativo a un massimo di 28 server gestiti contemporaneamente.

Per ulteriori informazioni sulla distribuzione di sistemi operativi, vedere Distribuzione di un'immagine del sistema operativo nella documentazione online di XClarity Administrator.

Ulteriori informazioni:

- XClarity Administrator: dal bare metal al cluster
- XClarity Administrator: distribuzione del sistema operativo

Gestione utenti

XClarity Administrator offre un server di autenticazione centralizzato per creare e gestire gli account utente e gestire e autenticare le credenziali degli utenti. Il server di autenticazione viene creato automaticamente quando si avvia il server di gestione per la prima volta. Gli account utente creati per XClarity Administrator possono essere utilizzati anche per eseguire il login ai server e allo chassis gestiti in modalità di autenticazione gestita. Per ulteriori informazioni sugli utenti, vedere Gestione degli account utente nella documentazione online di XClarity Administrator.

XClarity Administrator supporta tre tipi di server di autenticazione:

- **Server di autenticazione locale**. Per impostazione predefinita, XClarity Administrator è configurato in modo da utilizzare il server di autenticazione locale che si trova sul nodo di gestione.
- **Server LDAP esterno**. Attualmente, è supportato solo Microsoft Active Directory. Questo server deve trovarsi in un server Microsoft Windows esterno connesso alla rete di gestione.Quando viene utilizzato un server LDAP esterno, il server di autenticazione locale è disabilitato.
- **provider di identità SAML 2.0 esterno**. Attualmente, è supportato solo Microsoft Active Directory Federation Services (AD FS). Oltre all'immissione di un nome utente e una password, l'autenticazione a più fattori può essere configurata in modo da garantire un'ulteriore protezione attraverso la richiesta di un codice PIN, la lettura di una smart card e un certificato client.

Per ulteriori informazioni sui tipi di autenticazione, vedere Gestione del server di autenticazione nella documentazione online di XClarity Administrator.

Quando si crea un account utente, si assegna un gruppo di ruoli predefinito o personalizzato all'account utente per controllare il livello di accesso di tale utente. Per ulteriori informazioni sui gruppi di ruoli, vedere Creazione di un gruppo di ruoli nella documentazione online di XClarity Administrator.

XClarity Administrator include un log di controllo che fornisce un record cronologico degli interventi dell'utente, come il login, la creazione di nuovi utenti o la modifica delle password utente. Per ulteriori informazioni sul log di controllo, vedere Utilizzo degli eventi nella documentazione online di XClarity Administrator.

Autenticazione dispositivo

XClarity Administrator utilizza i seguenti metodi per l'autenticazione con i server e gli chassis gestiti.

- **Autenticazione gestita**. Quando l'autenticazione gestita è abilitata, gli account utente creati in XClarity Administrator vengono utilizzati per autenticare i server e gli chassis gestiti.

  Per ulteriori informazioni sugli utenti, vedere Gestione degli account utente nella documentazione online di XClarity Administrator.

- **Autenticazione locale**. Quando l'autenticazione gestita è disabilitata, le credenziali memorizzate definite in XClarity Administrator vengono utilizzate per autenticare i server gestiti. Le credenziali memorizzate devono corrispondere a un account utente attivo sul dispositivo o in Active Directory.

  Per ulteriori informazioni sulle credenziali memorizzate, vedere Gestione delle credenziali memorizzate nella documentazione online di XClarity Administrator.

Protezione

Se l'ambiente deve essere conforme agli standard NIST SP 800-131A, XClarity Administrator consente di disporre di un ambiente completamente conforme.

XClarity Administrator supporta certificati SSL autofirmati (emessi da un'autorità di certificazione interna) e certificati SSL esterni (emessi da un'autorità di certificazione privata o commerciale).

I firewall su chassis e server possono essere configurati per accettare richieste in entrata solo da XClarity Administrator.

Per ulteriori informazioni sulla protezione, vedere Implementazione di un ambiente sicuro nella documentazione online di XClarity Administrator.

Assistenza e supporto

XClarity Administrator può essere configurato in modo da raccogliere e inviare file di diagnostica automaticamente al fornitore di servizi preferito quando si verificano determinati eventi che richiedono assistenza in XClarity Administrator e nei dispositivi gestiti. È possibile scegliere di inviare i file di diagnostica al Supporto Lenovo utilizzando Call Home o a un altro fornitore di servizi utilizzando SFTP. È inoltre possibile raccogliere manualmente i file di diagnostica, aprire un record del problema e inviare i file di diagnostica al Centro assistenza clienti Lenovo.

Ulteriori informazioni:  XClarity Administrator: assistenza e supporto

Automatizzazione delle attività con gli script

XClarity Administrator può essere integrato in piattaforme di automazione e gestione esterne di livello superiore tramite API REST aperte. Utilizzando le API REST, XClarity Administrator può integrarsi facilmente con l'infrastruttura di gestione esistente.

Il toolkit PowerShell fornisce una libreria di cmdlet per l'automatizzazione del provisioning e la gestione delle risorse da una sessione di Microsoft PowerShell. Il toolkit Python fornisce una libreria di API e comandi basata su Python per automatizzare il provisioning e la gestione delle risorse da un ambiente OpenStack, come Ansible o Puppet. Entrambi i toolkit forniscono un'interfaccia per le API REST di XClarity Administrator che consente di automatizzare funzioni come:

- Login a XClarity Administrator
- Gestione e annullamento della gestione di chassis, server, dispositivi di storage e switch TOR (Top-of-Rack) (dispositivi)
- Raccolta e visualizzazione di dati di inventario per dispositivi e componenti
- Distribuzione di un'immagine del sistema operativo in uno o più server
- Configurazione di server attraverso l'utilizzo di pattern di configurazione
- Applicazione di aggiornamenti firmware ai dispositivi

Integrazione con un altro software gestito

I moduli XClarity Administrator integrano XClarity Administrator con il software di gestione di terze parti per fornire funzioni di rilevamento, monitoraggio, configurazione e gestione che consentono di ridurre il costo e la complessità dell'amministrazione ordinaria del sistema per i dispositivi supportati.

Per ulteriori informazioni su XClarity Administrator, vedere i documenti seguenti:

- Lenovo XClarity Integrator per Microsoft System Center

- Lenovo XClarity Integrator per VMware vCenter

Per ulteriori considerazioni, vedere Considerazioni sulla gestione.

Ulteriori informazioni:
- Panoramica di Lenovo XClarity Integrator per Microsoft System Center
- Lenovo XClarity Integrator per VMware vCenter

Documentazione

La XClarity Administrator documentazione online viene regolarmente aggiornata in inglese. Vedere Documentazione online di XClarity Administrator per le informazioni e le procedure più recenti.

La documentazione online è disponibile nelle seguenti lingue:
- Tedesco (de)
- Inglese (en)
- Spagnolo (es)
- Francese (fr)
- Italiano (it)
- Giapponese (ja)
- Coreano (ko)
- Portoghese brasiliano (pt_BR)
- Russo (ru)
- Tailandese (th)
- Cinese semplificato (zh_CN)
- Cinese tradizionale (zh_TW)

È possibile modificare la lingua della documentazione online nei seguenti modi:

- Modificare l'impostazione della lingua nel browser Web
- Aggiungere ?`lang=`<*language_code*> alla fine dell'URL, ad esempio, per visualizzare la documentazione online in cinese semplificato:
  `http://sysmgt.lenovofiles.com/help/topic/com.lenovo.lxca.doc/aug_product_page.html`**?lang=zh_CN**

Capitolo 2. Pianificazione per XClarity Administrator

Prima di installare Lenovo XClarity Administrator, esaminare le seguenti considerazioni per pianificare l'installazione e la gestione quotidiana.

Licenze e versione di prova gratuita per 90 giorni

Lenovo XClarity Administrator offre una licenza di prova gratuita per 90 giorni che consente di utilizzare tutte le funzioni disponibili per un periodo di tempo limitato.

È possibile determinare lo stato delle licenze, incluso il numero di giorni rimasti per la licenza di prova, facendo clic sul menu azioni utente (

) sulla barra del titolo XClarity Administrator, quindi selezionando **Informazioni su**.

XClarity Administrator supporta la seguente licenza.

- **Lenovo XClarity Pro**. Ogni licenza fornisce i diritti che seguono per un singolo dispositivo.
  - Assistenza e supporto per Lenovo XClarity Integrator
  - Assistenza e supporto per XClarity Administrator
  - Funzioni avanzate in XClarity Administrator:
    - Configurazione dei server mediante i pattern di configurazione
    - Distribuzione dei sistemi operativi
    - Segnalazione dei problemi di XClarity Administrator mediante Call Home (Call Home per avvisi hardware non è interessato).

È necessario acquistare una licenza per ogni dispositivo gestito che supporta le funzioni avanzate. Una licenza non è legata a un dispositivo specifico.

La conformità della licenza viene determinata in base al numero di dispositivi gestiti che supportano le funzioni avanzate. Il numero di dispositivi gestiti non deve superare il numero totale di licenze in tutte le chiavi di licenza attive. Se XClarity Administrator non è conforme alle licenze installate (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. Ogni volta che XClarity Administrator non è conforme, il periodo di tolleranza viene reimpostato su 90 giorni. Se il periodo di tolleranza (inclusa la versione di prova gratuita) termina prima che le licenze siano conformi, le funzioni avanzate sono disabilitate per tutti i dispositivi.

Nota:

- Le funzioni di configurazione del server e di distribuzione del sistema operativo vengono disabilitate alla scadenza del periodo di tolleranza.
- Call Home per i problemi di XClarity Administrator (funzione Call Home software) è disabilitata quando le licenze non sono conformi. Non è previsto un periodo di tolleranza per questa funzione. Tuttavia, la funzione Call Home per gli avvisi hardware non è interessata.

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

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

Per informazioni sull'installazione della licenza, vedere Installazione della licenza di abilitazione di tutte le funzionalità nella documentazione online di XClarity Administrator.

Prerequisiti hardware e software

L'appliance di gestione Lenovo XClarity Administrator viene eseguita in una macchina virtuale di un sistema host.

Requisiti hypervisor

Ambienti contenitori

L'ambiente contenitore seguente è supportato per l'esecuzione di XClarity Administrator come contenitore.

- Docker v20.10.9
- Docker-compose v1.29.2

Hypervisor

Sono supportati i seguenti hypervisor per l'esecuzione di XClarity Administrator come appliance virtuale.

- Citrix Hypervisor v8.2
- Citrix XenServer v7.6
- CentOS 7 e 8[1]
- Microsoft Windows Server 2022 con Hyper-V
- Microsoft Windows Server 2019 con Hyper-V
- Microsoft Windows Server 2016 con Hyper-V
- Microsoft Windows Server 2012 R2 con Hyper-V
- Microsoft Windows Server 2012 con Hyper-V
- Nutanix Acropolis Hypervisor (AHV)
- Red Hat v8.x con Kernel-based Virtual Machine (KVM) v2.12.0 installato
- Red Hat v7.x con KVM v1.2.17 installato
- Ubuntu 20.04.2 LTS con KVM v4.2.3 installato
- VMware ESXi 7.0, U1, U2 e U3
- VMware ESXi 6.7, U1, U2[2] e U3

Nota:

1. CentOS Linux non è più aggiornato da Red Hat. Valutare la possibilità di eseguire la migrazione a Red Hat Enterprise Linux (vedere Red Hat: pagina Web su come eseguire la conversione da CentOS o Oracle Linux in RHEL).
2. Per VMware ESXi 6.7 U2, è necessario utilizzare l'immagine ISO VMware-ESXi-6.7.0.update02-13981272-LNV-20190630.iso o versione successiva.

Per VMware e Citrix, la macchina virtuale è disponibile come modello OVF. Per Hyper-V e Nutanix AHV, la macchina virtuale è un'immagine VDI (Virtual-Disk Image). Per CentOS e KVM, la macchina virtuale è disponibile in formato qcow2.

Importante: Per gli ambienti Hyper-V in esecuzione su guest Linux con kernel 2.6, che utilizzano grandi quantità di memoria per l'appliance virtuale, è necessario disabilitare l'uso dell'accesso NUMA (Non-Uniform Memory Access) nel pannello delle impostazioni Hyper-V di Hyper-V Manager. La modifica di questa impostazione richiede il riavvio del servizio Hyper-V, che comporta anche il riavvio di tutte le macchine virtuali in esecuzione. Se questa impostazione non è disabilitata, potrebbero verificarsi problemi dell'appliance virtuale XClarity Administrator durante l'avvio iniziale.

Requisiti hardware

Devono essere rispettati i seguenti *requisiti minimi* per XClarity Administrator. A seconda delle dimensioni dell'ambiente e dell'utilizzo di Pattern di configurazione, potrebbero essere richieste ulteriori risorse per assicurare prestazioni ottimali.

- Due microprocessori virtuali
- 8 GB di memoria
- 192 GB di storage che verranno utilizzati dall'appliance virtuale XClarity Administrator.
- Da visualizzare con una risoluzione minima di 1.024 pixel in larghezza (XGA)

Nella seguente tabella sono elencate le configurazioni minime consigliate per un determinato numero di dispositivi. Tenere presente che se si esegue la configurazione minima, i tempi di completamento delle attività di gestione potrebbero essere più lunghi del previsto. Per le attività di provisioning, come distribuzione del sistema operativo, aggiornamenti firmware e configurazione dei server, potrebbe essere necessario aumentare temporaneamente le risorse.

Numero di dispositivi gestiti	Configurazione memoria/CPU virtuale
0-100 dispositivi	2 vCPU, 8 GB di RAM
100-200 dispositivi	4 vCPU, 10 GB di RAM
200-400 dispositivi	6 vCPU, 12 GB di RAM
400-600 dispositivi	8 vCPU, 16 GB di RAM
600-800 dispositivi	10 vCPU, 20 GB di RAM
800-1.000 dispositivi	12 vCPU, 24 GB di RAM

Nota:

- Una singola istanza XClarity Administrator può supportare fino a 1.000 dispositivi.
- Per i suggerimenti più recenti e ulteriori considerazioni sulle prestazioni, vedere XClarity Administrator: guida alle prestazioni (white paper).
- In base alla dimensione dell'ambiente gestito e dei pattern di utilizzo dell'installazione, potrebbe essere necessario aggiungere ulteriori risorse per garantire prestazioni accettabili. Se spesso viene riscontrato un utilizzo elevato o molto elevato del processore nel dashboard delle risorse di sistema, considerare la possibilità di aggiungere 1-2 core di processore virtuale. Se l'utilizzo minimo della memoria supera l'80%, considerare la possibilità di aggiungere 1-2 GB di RAM. Se il sistema rientra tra le configurazioni definite nella tabella, si consiglia di eseguire la macchina virtuale per un periodo maggiore di tempo per valutare le prestazioni del sistema.
- Per informazioni su come liberare spazio su disco eliminando le risorse di XClarity Administrator non più necessarie, vedere Gestione dello spazio su disco nella documentazione online di XClarity Administrator.

Requisiti software

- **Server Orchestrator**

  Se si gestisce un numero elevato di dispositivi utilizzando più istanze di XClarity Administrator è possibile centralizzare monitoraggio, gestione, provisioning e analisi mediante Lenovo XClarity Orchestrator. XClarity Orchestrator supporta un numero illimitato di istanze di XClarity Administrator che gestiscono complessivamente un massimo di **10.000** dispositivi client non ThinkEdge.

  Per gestire istanze v4.0 o successive XClarity Administrator mediante Lenovo XClarity Orchestrator, è necessario XClarity Orchestrator v2.0 o versioni successive.

- **Server di autenticazione**

Se si decide di utilizzare un server di autenticazione esterna, viene supportata l'esecuzione solo di Microsoft Active Directory su Windows Server 2008 o versioni successive.

Se si decide di utilizzare un provider di identificazione SAML, viene supportata l'esecuzione solo delle versioni 2.0 o successive di Microsoft Active Directory Federation Services (AD FS) su Windows Server 2012.

- **Server NTP**

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

  Suggerimento: considerare la possibilità di utilizzare il sistema host su cui è installato XClarity Administrator come server NTP. In tal caso, verificare che il sistema host sia accessibile dalla rete di gestione.

Risorse gestibili

Una singola istanza XClarity Administrator può gestire, monitorare ed eseguire il provisioning di un massimo di **1.000** dispositivi fisici.

È possibile trovare un elenco completo di opzioni e dispositivi supportati (come I/O, DIMM e adattatori di storage), livelli minimi di firmware richiesti e considerazioni sulle limitazioni sul Supporto XClarity Administrator - Pagina Web sulla compatibilità facendo clic sulla scheda **Compatibilità** e quindi selezionando il collegamento per i tipi di dispositivi appropriati.

Per informazioni generali sulla configurazione hardware e le opzioni per uno specifico dispositivo, vedere Pagina Web di Lenovo Server Proven.

Limitazione: se il sistema host su cui è installato XClarity Administrator è un server rack gestito, non è possibile utilizzare XClarity Administrator per applicare gli aggiornamenti firmware al sistema host o all'intero chassis contemporaneamente. Quando gli aggiornamenti firmware vengono applicati al sistema host, è necessario riavviarlo. Riavviando il sistema host, viene riavviato anche XClarity Administrator, pertanto XClarity Administrator non può completare gli aggiornamenti sul sistema host.

Browser Web supportati

L'interfaccia Web XClarity Administrator è supportata dai browser Web che seguono.
- Chrome™ 48.0 o versioni successive (55.0 o versioni successive per la console remota)
- Firefox® ESR 38.6.0 o versioni successive
- Microsoft® Internet Explorer® 11
- Microsoft Edge
- Safari® 9.0.2 o versioni successive (IOS7 o versioni successive e OS X)

Firewall e server proxy

Alcune funzioni di Lenovo XClarity Administrator, come aggiornamenti del server di gestione, aggiornamenti del firmware, assistenza e supporto, richiedono l'accesso a Internet. Se la rete è protetta da firewall, configurarli per abilitare il server di gestione XClarity Administrator a eseguire queste operazioni. Se il server di gestione non può accedere direttamente a Internet, configurare XClarity Administrator per utilizzare un server proxy.

Firewall

Verificare che i seguenti nomi DNS e porte siano aperti nel firewall.

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

Tabella 1. Connessione Internet richiesta

Nome DNS	Indirizzo IPv4	Indirizzo IPv6	Porte	Protocolli
Scaricamento delle chiavi di attivazione della licenza				
fod.lenovo.com	N/D	N/D	443	https
Scaricamento dei comunicati di servizio				
download.lenovo.com/servers/LXCA_Bulletin_Service.json	N/D	N/D	443 e 80	https
Download degli aggiornamenti del server di gestione, degli aggiornamenti firmware, di UpdateXpress System Packs (driver di dispositivo del sistema operativo) e dei pacchetti del repository				
datacentersupport.lenovo.com	N/D	N/D	443 e 80	https
download.lenovo.com	N/D	N/D	443 e 80	https
filedownload.lenovo.com	N/D	N/D	443 e 80	https
support.lenovo.com	N/D	N/D	443 e 80	https e http
supportapi.lenovo.com	N/D	N/D	443 e 80	https
Download del firmware (Flex System x220, x222, x240, x280 X6, x440, x480 X6, x880 X6, alcuni switch Flex e solo i CMM di prima generazione)				
www.ibm.com	129.42.56.216, 129.42.58.216, 129.42.60.216, 129.42.160.51, 207.25.252.19-7	N/D	443 e 80	https e http
www-03.ibm.com	204.146.30.17	N/D	443 e 80	https e http
download3.boulder.ibm.com	170.225.126.2-4	N/D	443	https
download4.boulder.ibm.com	170.225.126.4-3	N/D	443 e 80	https e http
delivery04-bld.dhe.ibm.com	170.225.126.4-5	N/D	443 e 80	https e http
delivery04-mul.dhe.ibm.com	170.225.126.4-6	N/D	443 e 80	https e http
delivery04.dhe.ibm.com	170.225.126.4-4	N/D	443 e 80	https e http
Caricamento dei dati di servizio al supporto Lenovo (Call Home)				
soaus.lenovo.com	3.222.8.29, 52.6.14.20	N/D	443	https
logupload.lenovo.com/BLL/Logupload.ashx	N/D	N/D	443 e 80	https
Caricamento dei dati di servizio a Funzione aggiornamento Lenovo				
logupload.lenovo.com/BLL/Logupload.ashx	N/D	N/D	443 e 80	https
Scaricamento delle informazioni sulla garanzia				

Tabella 1. Connessione Internet richiesta (continua)

Nome DNS	Indirizzo IPv4	Indirizzo IPv6	Porte	Protocolli
ibase.lenovo.com (worldwide)	N/D	N/D	443 e 80	https e http
service.lenovo.com.cn (solo Cina)	114.247.140.2-12 (solo Cina)	N/D	83	http
supportapi.lenovo.com	N/D	N/D	443 e 80	https e http

Attenzione: Per gli utenti della Cina, per recuperare le informazioni sulla garanzia per i dispositivi gestiti mediante XClarity Administrator, è necessario effettuare l'aggiornamento a XClarity Administrator v1.3.1 o versioni successive.

Server proxy

Se il server di gestione non ha accesso diretto a Internet, verificare che il server di gestione sia configurato per utilizzare un server proxy HTTP (vedere Configurazione dell'accesso alla rete).
- 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.

Disponibilità della porta

Devono essere disponibili diverse porte, a seconda delle modalità di implementazione dei firewall nell'ambiente. Se le porte richieste sono bloccate o utilizzate da un altro processo, alcune funzioni di Lenovo XClarity Administrator potrebbe non funzionare.

Per determinare le porte da aprire in base all'ambiente, esaminare le seguenti sezioni. Le tabelle di queste sezioni includono informazioni sulla modalità di utilizzo di ciascuna porta in XClarity Administrator, sul dispositivo gestito interessato, sul protocollo (TCP o UDP) e sulla direzione del flusso di traffico. Il traffico *in ingresso* identifica i flussi provenienti dal dispositivo gestito o dai sistemi esterni verso XClarity Administrator, pertanto le porte devono essere aperte sull'appliance XClarity Administrator. Il traffico *in uscita* va da XClarity Administrator al dispositivo gestito.

- Accesso al server XClarity Administrator
- Accesso tra XClarity Administrator e i dispositivi gestiti
- Accesso tra XClarity Administrator e la rete di dati per la distribuzione del sistema operativo e gli aggiornamenti dei driver di dispositivo

Accesso al server XClarity Administrator

Se il server XClarity Administrator e tutti i dispositivi gestiti sono protetti da firewall e si intende accedere a questi dispositivi da un browser esterno al firewall, è necessario verificare che le porte di XClarity Administrator siano aperte. Se si utilizzano SNMP e SMTP per la gestione eventi, potrebbe essere necessario verificare che anche le porte utilizzate dal server XClarity Administrator per l'inoltro eventi siano aperte.

Il server XClarity Administrator è in ascolto e risponde tramite le porte elencate nella tabella che segue.

Nota:

- XClarity Administrator è un'applicazione RESTful che comunica in modo sicuro su TCP sulla porta 443.

- XClarity Administrator 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.

Comunicazioni	Appliance XClarity Administrator	Server di autenticazione esterni	Servizi di inoltro eventi	Servizi Lenovo (incluso Call Home)
In uscita (porte aperte sui sistemi esterni)	• DNS: TCP/UDP sulla porta **53**	• LDAP: TCP sulla porta **389**[1] • LDAPS: TCP sulla porta **636** • Autenticazione SAML: TCP sulle porte **3268, 3269**	• Server FTP: TCP sulla porta **21**[1] • Server e-mail (SMTP): UDP sulla porta **25**[1] • Servizio Web REST (HTTP): UDP sulla porta **80**[1] • SNMP Manager: UDP sulla porta **161**[2], **162**[1] • MS Azure: UDP o porta **443**[1] • Syslog: UDP sulla porta **514**[1] • Push Apple[3]: TCP sulle porte **443, 2195, 5223** • Push Google[4]: TCP sulle porte **443, 5288, 5299, 5230**	• Garanzia (solo Cina): TCP sulla porta **83**[5] • HTTPS (Call Home): TCP sulla porta **443**
In ingresso (porte aperte sull'appliance XClarity Administrator)	• HTTPS: TCP sulla porta **443**	Non applicabile	• SNMP: UDP sulla porta **161**	Non applicabile

1. Questo è la porta predefinita. Questa porta è configurabile dall'interfaccia utente.
2. Questa porta viene utilizzata quando è configurato l'inoltro eventi SNMP con l'autenticazione utente.
3. Questa porta deve essere aperta quando il Wi-Fi è protetto da firewall o APN (Access Point Name) privato per i dati dei cellulari. Per i server APN su questa porta è richiesta una connessione diretta senza proxy. Questa porta viene utilizzata come failback solo per il Wi-Fi, quando i dispositivi non possono raggiungere il servizio di notifiche push di Apple sulla porta 5223. L'intervallo dell'indirizzo IP è 17.0.0.0/8.
4. Per l'intervallo di indirizzi IP, vedere Google ASN 15169. Il dominio è android.googleapis.com.
5. Sebbene non sia necessario al di fuori della Cina, XClarity Administrator potrebbe tentare di connettersi a questo servizio in altri paesi.

Accesso tra XClarity Administrator e i dispositivi gestiti

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

Se si desidera installare i sistemi operativi sui dispositivi gestiti utilizzando XClarity Administrator, verificare l'elenco delle porte in Accesso tra XClarity Administrator e la rete di dati per la distribuzione del sistema operativo e gli aggiornamenti dei driver di dispositivo.

- **CMM dello chassis Flex**

Comunicazioni	CMM dello chassis Flex
In uscita (porte aperte sui sistemi esterni)	– SLP: UDP/TCP sulla porta **427** – CIM HTTP - TCP sulla porta **5988**[2] – HTTPS CIM: TCP sulla porta **5989** – Comando TCP: TCP sulla porta **6090**[2] – Comando TCP sicuro: TCP sulla porta **6091**
In ingresso (porte aperte sull'appliance XClarity Administrator)	– SFTP - TCP sulla porta **22**[1] – HTTPS per le indicazioni CIM: TCP **9090** – LDAPS: TCP sulle porte **50637**

1. Questa porta viene utilizzata per trasferire gli aggiornamenti firmware utilizzando SFTP.
2. Per impostazione predefinita, la gestione viene eseguita sulle porte sicure. Le porte non sicure sono facoltative.

- **Server e nodi di elaborazione**

Comunicazioni	ThinkSystem e ThinkAgile	System x	Flex System	ThinkServer
In uscita (porte aperte sui sistemi esterni)	– SFTP: TCP sulla porta **115** – SLP: UDP/TCP sulla porta **427** – HTTPS: TCP sulla porta **443** – Rilevamento SSDP: UDP sulla porta **1900** – Controllo remoto: TCP sulla porta **3888**[4] – KVM remoto: TCP sulla porta **3889**[4] – HTTPS CIM: TCP sulla porta **5989** – Aggiornamenti firmware: TCP sulla porta **6990**[5]	– SLP: UDP/TCP sulla porta **427** – HTTPS: TCP sulla porta **443** – IPMI: TCP sulla porta **623** – Controllo remoto: TCP sulla porta **3888**[4] – KVM remoto: TCP sulla porta **3889**[4] – HTTP CIM: TCP sulla porta **5988**[3] – HTTPS CIM: TCP sulla porta **5989**[3] – Aggiornamenti firmware: TCP sulla porta **6990**[5]	– SLP: UDP/TCP sulla porta **427** – Controllo remoto: TCP sulla porta **3888**[4] – KVM remoto: TCP sulla porta **3889**[1, 4] – HTTP CIM: TCP sulla porta **5988**[3] – HTTPS CIM: TCP sulla porta **5989**[3] – Aggiornamenti firmware: TCP sulla porta **6990**[5]	– Trap SNMP: UDP sulla porta **162** – IPMI: UDP sulla porta **623**
In ingresso (porte aperte sull'appliance XClarity Administrator)	– SFTP: TCP sulla porta **22**[2] – HTTPS: TCP sulla porta **443** – Rilevamento SSDP: UDP sulla porta **1900** – Aggiornamenti firmware: TCP sulla porta **6990**[5] – HTTPS per le indicazioni CIM: TCP **9090** – LDAPS: TCP sulle porte **50636**[6]**,50637**	– SFTP: TCP sulla porta **22**[2] – HTTPS: TCP sulla porta **443** – Aggiornamenti firmware: TCP sulla porta **6990**[5] – HTTPS per le indicazioni CIM: TCP **9090** – LDAPS: TCP sulle porte **50636**[6]**,50637**	– SFTP: TCP sulla porta **22**[2] – HTTPS: TCP sulla porta **443** – Aggiornamenti firmware: TCP sulla porta **6990**[5] – HTTPS per le indicazioni CIM: TCP **9090** – LDAPS: TCP sulle porte **50636**[6]**,50637**	– Trap SNMP: UDP sulla porta **162**

1. È necessario che questa porta sia aperta solo per i server con IMM2.
2. Questa porta viene utilizzata per trasferire gli aggiornamenti firmware utilizzando SFTP.
3. Per impostazione predefinita, la gestione viene eseguita sulle porte sicure. Le porte non sicure sono facoltative.
4. Il controllo remoto e KVM remoto vengono avviati dal browser Web e non dal server XClarity Administrator.
5. Questa porta consente di collegarsi al sistema operativo BMU per trasferire file ed eseguire i comandi di aggiornamento.
6. Questa porta è necessaria per configurare i server utilizzando i modelli di configurazione.

- **Switch Flex e Rack**

Comunicazioni	Switch Rack	Switch Flex
In uscita (porte aperte sui sistemi esterni)	– SSH: TCP sulla porta **22**[1,3] – SNMP: UDP sulla porta **161**[2] – SLP: UDP/TCP sulla porta **427**[6] – HTTPS: TCP sulla porta **443**[7]	– SSH: TCP sulla porta **22**[3] – SNMP: UDP sulla porta **161**[5]
In ingresso (porte aperte sull'appliance XClarity Administrator)	– SFTP: TCP sulla porta **22**[4] – Trap SNMP: TCP sulle porte **162**[2]	– SFTP: TCP sulla porta **22**[4] – Trap SNMP: TCP sulla porta **162**[2]

1. Per quanto riguarda gli switch ENOS, questa porta viene utilizzata per configurare le credenziali HoS (Head of Stack) utilizzate tra gli switch CMM e Flex, attivare lo slot del firmware e cancellare le chiavi dell'host SSH prima delle operazioni di trasferimento dei file SFTP.
2. Questa porta deve essere aperta sull'appliance XClarity Administrator (in ingresso) quando gli switch si trovano su una rete diversa da XClarity Administrator, in modo che XClarity Administrator possa ricevere eventi per tali dispositivi.
3. Questa porta viene utilizzata per la gestione (SSH).
4. Questa porta viene utilizzata per trasferire gli aggiornamenti firmware utilizzando SFTP.
5. Per gli switch rack ENOS, questa porta consente di trasferire i dati di inventario.
6. Questa porta viene utilizzata per il rilevamento.
7. Questa porta consente di applicare gli aggiornamenti firmware.

- **Dispositivi di storage**

Comunicazioni	Dispositivi di storage
In uscita (porte aperte sui sistemi esterni)	– FTP: TCP sulla porta **21** – SFTP: TCP sulla porta **22**[2] – SLP: UDP/TCP sulla porta **427** – HTTPS: TCP sulla porta **443**[1]
In ingresso (porte aperte sull'appliance XClarity Administrator)	– HTTPS: TCP sulla porta **443**[2] – Trap SNMP: UDP sulla porta **115**

1. Questa porta consente di trasferire gli aggiornamenti firmware.
2. Questa porta consente di trasferire e applicare gli aggiornamenti firmware.

Accesso tra XClarity Administrator e la rete di dati per la distribuzione del sistema operativo e gli aggiornamenti dei driver di dispositivo

Comunicazioni	Distribuzione del sistema operativo[1, 2, 3]	Aggiornamenti dei driver di dispositivo del sistema operativo[2]
In uscita (porte aperte sui sistemi esterni)		• WinRM su HTTP: TCP sulla porta **5985**[5] • WinRM su HTTPS: TCP sulla porta **5986**[6]
In ingresso (porte aperte sull'appliance XClarity Administrator)	• Comunicazione SMB: TCP sulla porta **445**[4] • HTTPS (ad eccezione di ThinkServer): TCP sulla porta **8443**[6]	• Comunicazione SMB: TCP sulla porta **445**[4]

1. Se l'appliance XClarity Administrator è stata configurata per l'utilizzo di una rete di distribuzione del sistema operativo, le porte devono essere aperte su quella rete.
2. Per un elenco di porte che devono essere disponibili per la distribuzione dei sistemi operativi, vedere Disponibilità della porta per i sistemi operativi distribuiti nella documentazione online di XClarity Administrator. Ad esempio, se la distribuzione del sistema operativo è stata configurata per l'utilizzo di una rete di dati (eth1), queste porte devono essere aperte su quella rete.
3. Ogni istanza XClarity Administrator dispone di un'autorità di certificazione univoca, utilizzata solo per la distribuzione del sistema operativo. L'autorità di certificazione firma un certificato che viene utilizzato per il server di destinazione sulla porta 8443. Quando viene avviata la distribuzione del sistema operativo, il certificato CA viene incluso nell'immagine del sistema operativo che verrà inviata al server di destinazione. Durante il processo di distribuzione, il server si collega alla porta 8443 per verificare il certificato fornito dalla porta 8443 durante l'handshake, poiché in possesso del certificato CA.
4. Questa porta consente di trasferire i file dei driver di Windows.
5. Questa porta consente di collegare al server di destinazione WinRM.
6. Questa porta viene utilizzata per scambiare i dati tra il sistema operativo di destinazione e XClarity Administrator, incluse le immagini e lo stato del sistema operativo.

Considerazioni sulla gestione

Per la gestione dei dispositivi sono disponibili diverse alternative tra cui scegliere. A seconda dei dispositivi gestiti, potrebbe essere necessario eseguire contemporaneamente diverse soluzioni di gestione.

Un dispositivo può essere gestito da una sola istanza di Lenovo XClarity Administrator. È anche possibile utilizzare un altro software di gestione (come VMware vRealize Operations Manager) con Lenovo XClarity Administrator per *monitorare* i dispositivi gestiti da XClarity Administrator.

Attenzione: Prestare particolare attenzione quando si utilizzano più strumenti di gestione per gestire i dispositivi e prevenire conflitti imprevisti. Ad esempio, l'invio di modifiche dello stato di alimentazione mediante un altro strumento potrebbe determinare un conflitto con i processi di aggiornamento o configurazione in esecuzione su XClarity Administrator.

Dispositivi ThinkSystem, ThinkServer e System x

Se si intende utilizzare un altro software di gestione per monitorare i dispositivi gestiti, creare un nuovo utente locale con le impostazioni SNMP o IPMI corrette dall'interfaccia IMM. Verificare che siano stati concessi i privilegi SNMP o IPMI, a seconda delle specifiche esigenze.

Dispositivi Flex System

Se si intende utilizzare un altro software di gestione per monitorare i dispositivi gestiti e questo software di gestione utilizza la comunicazione SNMPv3 o IPMI, è necessario preparare l'ambiente eseguendo le seguenti operazioni per ciascun modulo CMM gestito:

1. Accedere all'interfaccia Web del controller di gestione dello chassis utilizzando nome utente e password di `RECOVERY_ID`.
2. Se i criteri di sicurezza sono impostati su **Protetto**, modificare il metodo di autenticazione utente.
   a. Fare clic su **Gestione del modulo di gestione → Account utente**.
   b. Fare clic sulla scheda **Account**.
   c. Fare clic su **Impostazioni di login globali**.
   d. Fare clic sulla scheda **Generale**.
   e. Selezionare **Prima autenticazione esterna, poi locale** per il metodo di autenticazione utente.
   f. Fare clic su **OK**.
3. Creare un nuovo utente locale con le impostazioni SNMP o IPMI corrette dall'interfaccia Web del controller di gestione.
4. Se i criteri di sicurezza sono impostati su **Protetto**, scollegarsi e accedere all'interfaccia Web del controller di gestione utilizzando il nuovo nome utente e la password. Quando richiesto, modificare la password per il nuovo utente.

È ora possibile utilizzare il nuovo utente come utente SNMP o IPMI attivo.

Nota: Se si annulla la gestione e quindi si gestisce nuovamente lo chassis, questo nuovo account utente viene bloccato e disabilitato. In questo caso, ripetere queste operazioni per creare un nuovo account utente.

Considerazioni sulla rete

Quando si pianifica l'installazione di Lenovo XClarity Administrator, considerare la topologia di rete implementata nell'ambiente e le modalità in cui XClarity Administrator viene integrato nella topologia.

Importante: 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 viene utilizzato DHCP, verificare che le modifiche dell'indirizzo IP siano minime.

Limitazioni della configurazione IP

Per i seguenti dispositivi gestiti e funzioni, le interfacce di rete devono essere configurate con un indirizzo IPv4. Gli indirizzi IPv6 non sono supportati.

- Aggiornamenti firmware per dispositivi Lenovo Storage
- Server ThinkServer
- Dispositivi Lenovo Storage

La gestione dei dispositivi RackSwitch utilizzando il collegamento locale IPv6 mediante una porta dati o una porta di gestione non è supportata.

NAT (Network Address Translation), che riesegue il mapping di uno spazio dell'indirizzo IP in un altro, non è supportato.

Tipi di rete

Generalmente, molti ambienti implementano i seguenti tipi di reti. In base ai requisiti, è possibile implementare solo una di queste reti o tutte e tre.

- **Rete di gestione**

La rete di gestione è generalmente riservata per le comunicazioni tra Lenovo XClarity Administrator e i processori di gestione dei dispositivi gestiti. Ad esempio, la rete di gestione potrebbe essere configurata per includere XClarity Administrator, i moduli CMM di ogni chassis gestito e il controller di gestione della scheda di base di ciascun server gestito da XClarity Administrator.

- **Rete di dati**

  La rete di dati generalmente viene utilizzata per le comunicazioni tra i sistemi operativi installati sui server e l'Intranet aziendale, Internet o entrambe.

- **Rete di distribuzione del sistema operativo**

  In alcuni casi, viene configurata una rete di distribuzione del sistema operativo per separate le comunicazioni richieste per distribuire i sistemi operativi sui server. Se implementata, questa rete generalmente include XClarity Administrator e tutti gli host del server.

  Invece di implementare una rete di distribuzione del sistema operativo separata, è possibile scegliere di integrare questa funzionalità nella rete di gestione o nella rete di dati.

Configurazioni di rete

È possibile configurare Lenovo XClarity Administrator per utilizzare uno o due interfacce di rete.

Attenzione:

- La modifica dell'indirizzo IP di XClarity Administrator dopo la gestione dei dispositivi potrebbe determinare l'attivazione dello stato offline dei dispositivi in XClarity Administrator. Verificare che tutti i dispositivi risultino non gestiti prima di modificare l'indirizzo IP.
- È possibile abilitare o disabilitare il controllo degli indirizzi IP duplicati nella stessa sottorete, facendo clic sull'interruttore **Controllo dell'indirizzo IP duplicato**. L'opzione è disabilitata per impostazione predefinita. Quando l'opzione è abilitata, XClarity Administrator genera un avviso se si tenta di modificare l'indirizzo IP di XClarity Administrator o di gestire un dispositivo con lo stesso indirizzo IP di un altro dispositivo gestito o presente nella stessa sottorete.

  Nota: Se abilitato, XClarity Administrator esegue una scansione ARP per individuare i dispositivi IPv4 attivi nella stessa sottorete. Per evitare la scansione ARP, disabilitare **Controllo dell'indirizzo IP duplicato**.
- Quando si esegue XClarity Administrator come appliance virtuale, se l'interfaccia di rete per la rete di gestione è configurata per utilizzare il protocollo DHCP (Dynamic Host Configuration Protocol), l'indirizzo IP dell'interfaccia di gestione potrebbe cambiare alla scadenza del protocollo DHCP. Se l'indirizzo IP cambia, è necessario annullare la gestione di chassis, rack e server tower e quindi gestirli nuovamente. Per evitare questo problema, modificare l'interfaccia di gestione con un indirizzo IP statico oppure verificare che la configurazione del server DHCP sia impostata in modo che l'indirizzo DHCP sia basato su un indirizzo MAC o che il protocollo DHCP non scada.
- Se *non* si intende utilizzare XClarity Administrator per distribuire il sistema operativo o aggiornare i driver di dispositivo del sistema operativo, è possibile disabilitare i server Samba e Apache modificando l'interfaccia di rete per utilizzare l'opzione **rileva e gestisci solo l'hardware**. Tenere presente che il server di gestione viene riavviato una volta modificata l'interfaccia di rete.
- Quando si esegue XClarity Administrator come contenitore.
  - È possibile abilitare o disabilitare solo il controllo degli indirizzi IP duplicati, modificare i ruoli dell'interfaccia di rete e cambiare le impostazioni del proxy. Tutte le altre impostazioni di rete (come indirizzo IP, gateway e DNS) vengono definite nella configurazione del contenitore.
  - Verificare che sul sistema host sia impostata una rete macvlan.

XClarity Administrator dispone di due interfacce di rete separate che possono essere definite in base all'ambiente, a seconda della topologia di rete implementata. Per le appliance virtuali, queste reti sono denominata eth0 ed eth1. Per i contenitori, è possibile scegliere nomi personalizzati.

- Se è presente solo un'interfaccia di rete (eth0):
  - L'interfaccia deve essere configurata per supportare il rilevamento dei dispositivi e la gestione (ad esempio, configurazione del server e aggiornamenti firmware). Deve essere in grado di comunicare con i moduli CMM e gli switch Flex di ogni chassis gestito, con il controller di gestione della scheda di base di ciascun server gestito e con ogni switch RackSwitch.
  - Se si intende acquistare gli aggiornamenti relativi a firmware e driver di dispositivo del sistema operativo mediante XClarity Administrator, almeno una delle interfacce di rete deve essere connessa a Internet, preferibilmente tramite un firewall. In caso contrario, è necessario importare gli aggiornamenti nel repository.
  - Se si desidera raccogliere i dati di servizio o utilizzare la notifica automatica dei problemi (come Call Home e Funzione Caricamento Lenovo), almeno una delle interfacce di rete deve essere collegata a Internet, preferibilmente tramite un firewall.
  - Se si intende distribuire le immagini del sistema operativo e aggiornare i driver di dispositivo del sistema operativo, l'interfaccia di rete deve disporre della connettività di rete IP all'interfaccia di rete del server utilizzata per accedere al sistema operativo host.

    Nota: Se si implementa una rete separata per la distribuzione del sistema operativo e gli aggiornamenti dei driver di dispositivo del sistema operativo, è possibile configurare la seconda interfaccia di rete per il collegamento a questa rete invece che alla rete di dati. Tuttavia, se il sistema operativo di ciascun server non ha accesso alla rete di dati, è necessario configurare un'interfaccia aggiuntiva sui server per fornire la connettività dal sistema operativo host alla rete di dati, per la distribuzione del sistema operativo e gli aggiornamenti dei driver di dispositivo del sistema operativo
- Se sono presenti due interfacce di rete (eth0 e eth1):
  - La prima interfaccia di rete (in genere, l'interfaccia Eth0) deve essere collegata alla rete di gestione e configurata per supportare il rilevamento dei dispositivi e la gestione (come configurazione del server e aggiornamenti firmware). Deve essere in grado di comunicare con i moduli CMM e gli switch Flex di ogni chassis gestito, con il controller di gestione di ciascun server gestito e con ogni switch RackSwitch.
  - La seconda interfaccia di rete (generalmente l'interfaccia eth1) può essere configurata per comunicare con una rete di dati interna, una rete di dati pubblica o entrambe.
  - Se si intende acquistare gli aggiornamenti relativi a firmware e driver di dispositivo del sistema operativo mediante XClarity Administrator, almeno una delle interfacce di rete deve essere connessa a Internet, preferibilmente tramite un firewall. In caso contrario, è necessario importare gli aggiornamenti nel repository.
  - Se si desidera raccogliere i dati di servizio o utilizzare la notifica automatica dei problemi (come Call Home e Funzione Caricamento Lenovo), almeno una delle interfacce di rete deve essere collegata a Internet, preferibilmente tramite un firewall.
  - Se si intende distribuire le immagini del sistema operativo e aggiornare i driver di dispositivo, è possibile scegliere di utilizzare l'interfaccia eth1 o eth0. Tuttavia, l'interfaccia utilizzata deve disporre della connettività di rete IP all'interfaccia di rete del server utilizzato per accedere al sistema operativo host.

    Nota: Se si implementa una rete separata per la distribuzione del sistema operativo e gli aggiornamenti dei driver di dispositivo del sistema operativo, è possibile configurare la seconda interfaccia di rete per il collegamento a questa rete invece che alla rete di dati. Tuttavia, se il sistema operativo di ciascun server non ha accesso alla rete di dati, è necessario configurare un'interfaccia aggiuntiva sui server per fornire la connettività dal sistema operativo host alla rete di dati, per la distribuzione del sistema operativo e gli aggiornamenti dei driver di dispositivo del sistema operativo

Nella seguente tabella sono riportate le possibili configurazioni per le interfacce di rete di XClarity Administrator in base al tipo di topologia di rete implementata nell'ambiente. Utilizzare questa tabella per determinare le modalità di definizione di ciascuna interfaccia di rete.

Tabella 2. Ruolo di ciascuna interfaccia di rete basata sulla topologia di rete

Topologia di rete	**Ruolo dell'interfaccia 1 (eth0)**	**Ruolo dell'interfaccia 2 (eth1)**
Rete convergente (rete di dati e gestione con supporto per la distribuzione del sistema operativo e degli aggiornamenti dei driver di dispositivo del sistema operativo)	Rete di gestione • Rilevamento e gestione • Configurazione server • Aggiornamenti firmware • Raccolta dei dati di servizio • Notifica automatica dei problemi (ad esempio, Call Home e Funzione Aggiornamento Lenovo) • Recupero dei dati sulla garanzia • Distribuzione sistema operativo • Aggiornamenti dei driver di dispositivo del sistema operativo	Nessuna
Rete di gestione separata con supporto per la distribuzione del sistema operativo, degli aggiornamenti dei driver di dispositivo del sistema operativo e della rete di dati	Rete di gestione • Rilevamento e gestione • Configurazione server • Aggiornamenti firmware • Raccolta dei dati di servizio • Notifica automatica dei problemi (ad esempio, Call Home e Funzione Aggiornamento Lenovo) • Recupero dei dati sulla garanzia • Distribuzione sistema operativo • Aggiornamenti dei driver di dispositivo del sistema operativo	Rete di dati • Nessuna
Rete di gestione separata e rete di dati con supporto per la distribuzione del sistema operativo e degli aggiornamenti dei driver di dispositivo	Rete di gestione • Rilevamento e gestione • Configurazione server • Aggiornamenti firmware • Raccolta dei dati di servizio • Notifica automatica dei problemi (ad esempio, Call Home e Funzione Aggiornamento Lenovo) • Recupero dei dati sulla garanzia	Rete di dati • Distribuzione sistema operativo • Aggiornamenti dei driver di dispositivo del sistema operativo

Tabella 2. Ruolo di ciascuna interfaccia di rete basata sulla topologia di rete (continua)

Topologia di rete	Ruolo dell'interfaccia 1 (eth0)	Ruolo dell'interfaccia 2 (eth1)
Rete di gestione separata e rete di dati senza supporto per la distribuzione del sistema operativo e degli aggiornamenti dei driver di dispositivo	Rete di gestione • Rilevamento e gestione • Configurazione server • Aggiornamenti firmware • Raccolta dei dati di servizio • Notifica automatica dei problemi (ad esempio, Call Home e Funzione Aggiornamento Lenovo) • Recupero dei dati sulla garanzia	Rete di dati • Nessuna
Rete di sola gestione (la distribuzione del sistema operativo e dei driver di dispositivo del sistema operativo non è supportata)	Rete di gestione • Rilevamento e gestione • Configurazione server • Aggiornamenti firmware • Raccolta dei dati di servizio • Notifica automatica dei problemi (ad esempio, Call Home e Funzione Aggiornamento Lenovo) • Recupero dei dati sulla garanzia	Nessuna

Rete singola di dati e gestione

In questa topologia di rete, le comunicazioni di gestione, le comunicazioni di dati e la distribuzione del sistema operativo si verificano sulla stessa rete. Questa topologia viene denominata rete *convergente.*

Importante: L'implementazione di una rete di gestione e di dati condivisi può causare interruzioni del traffico, come perdita di pacchetti o problemi di connettività della rete di gestione, a seconda della configurazione di rete (ad esempio, se il traffico dei server ha priorità elevata mentre il traffico del controller di gestione ha priorità bassa). La rete di gestione utilizza il traffico UDP e TCP. Il traffico UDP può avere priorità più bassa quando il traffico di rete è elevato.

Quando si installa Lenovo XClarity Administrator, definire l'interfaccia di rete eth0 utilizzando le seguenti considerazioni:

- L'interfaccia deve essere configurata per supportare il rilevamento dei dispositivi e la gestione (ad esempio, configurazione del server e aggiornamenti firmware). Deve essere in grado di comunicare con i moduli CMM e gli switch Flex di ogni chassis gestito, con il controller di gestione della scheda di base di ciascun server gestito e con ogni switch RackSwitch.
- Se si intende acquistare gli aggiornamenti relativi a firmware e driver di dispositivo del sistema operativo mediante XClarity Administrator, almeno una delle interfacce di rete deve essere connessa a Internet, preferibilmente tramite un firewall. In caso contrario, è necessario importare gli aggiornamenti nel repository.
- Se si desidera raccogliere i dati di servizio o utilizzare la notifica automatica dei problemi (come Call Home e Funzione Caricamento Lenovo), almeno una delle interfacce di rete deve essere collegata a Internet, preferibilmente tramite un firewall.
- Se si intende distribuire le immagini del sistema operativo e aggiornare i driver di dispositivo del sistema operativo, l'interfaccia di rete deve disporre della connettività di rete IP all'interfaccia di rete del server utilizzata per accedere al sistema operativo host.

  Nota: Se si implementa una rete separata per la distribuzione del sistema operativo e gli aggiornamenti dei driver di dispositivo del sistema operativo, è possibile configurare la seconda interfaccia di rete per il collegamento a questa rete invece che alla rete di dati. Tuttavia, se il sistema operativo di ciascun server non ha accesso alla rete di dati, è necessario configurare un'interfaccia aggiuntiva sui server per fornire la

connettività dal sistema operativo host alla rete di dati, per la distribuzione del sistema operativo e gli aggiornamenti dei driver di dispositivo del sistema operativo

- È possibile installare XClarity Administrator su qualsiasi sistema che soddisfa i requisiti di XClarity Administrator, incluso un server gestito, solo se viene implementata una topologia di rete singola di dati e gestione o una topologia di rete virtualmente separata di dati e gestione; tuttavia, non è possibile utilizzare XClarity Administrator per applicare gli aggiornamenti firmware a questo server gestito. Inoltre, solo alcuni firmware vengono applicati con attivazione immediata e XClarity Administrator forza il riavvio del server di destinazione, determinando il riavvio di XClarity Administrator. Se gli aggiornamenti vengono applicati con attivazione posticipata, solo parte del firmware viene applicata al riavvio dell'host XClarity Administrator.

Inoltre, è possibile configurare una seconda interfaccia di rete in modo da connettersi alla stessa rete di XClarity Administrator per supportare la ridondanza.

La seguente figura mostra un'implementazione di esempio per una topologia di rete convergente.

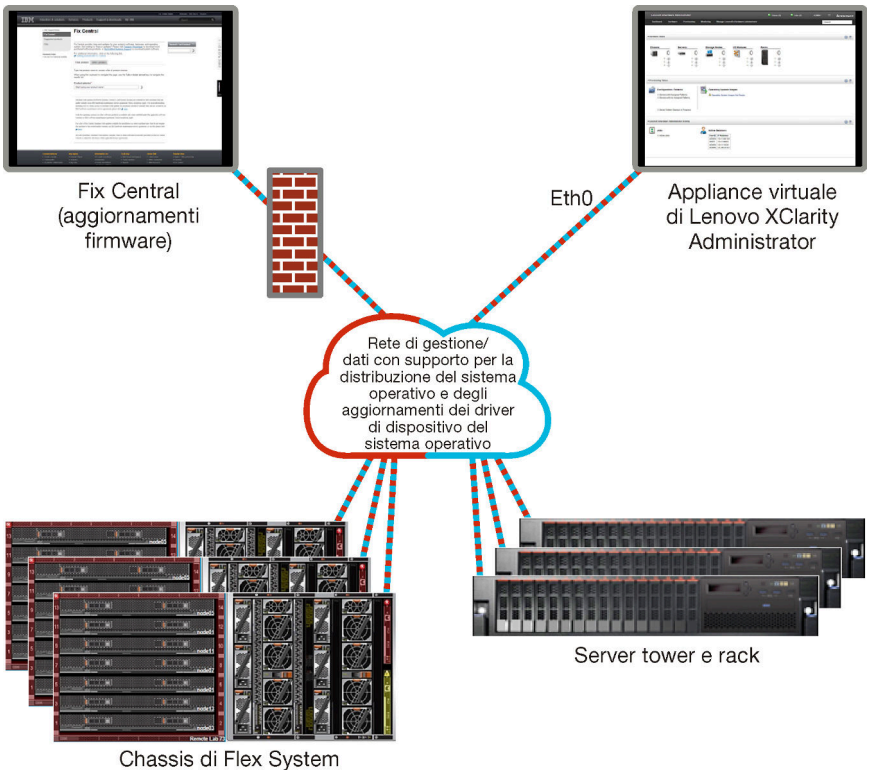


Figura 1. Implementazione di esempio di una singola rete per gestione, dati e distribuzione del sistema operativo

Rete fisicamente separata di dati e gestione

In questa topologia di rete, la rete di gestione e la rete di dati sono reti separate fisicamente e la rete di distribuzione del sistema operativo è configurata come parte della rete di gestione o della rete di dati.

Quando si installa Lenovo XClarity Administrator, definire le impostazioni di rete utilizzando le seguenti considerazioni:

- La prima interfaccia di rete (in genere, l'interfaccia Eth0) deve essere collegata alla rete di gestione e configurata per supportare il rilevamento dei dispositivi e la gestione (come configurazione del server e aggiornamenti firmware). Deve essere in grado di comunicare con i moduli CMM e gli switch Flex di ogni chassis gestito, con il controller di gestione di ciascun server gestito e con ogni switch RackSwitch.

- La seconda interfaccia di rete (generalmente l'interfaccia eth1) può essere configurata per comunicare con una rete di dati interna, una rete di dati pubblica o entrambe.
- Se si intende acquistare gli aggiornamenti relativi a firmware e driver di dispositivo del sistema operativo mediante XClarity Administrator, almeno una delle interfacce di rete deve essere connessa a Internet, preferibilmente tramite un firewall. In caso contrario, è necessario importare gli aggiornamenti nel repository.
- Se si desidera raccogliere i dati di servizio o utilizzare la notifica automatica dei problemi (come Call Home e Funzione Caricamento Lenovo), almeno una delle interfacce di rete deve essere collegata a Internet, preferibilmente tramite un firewall.
- Se si intende distribuire le immagini del sistema operativo e aggiornare i driver di dispositivo, è possibile scegliere di utilizzare l'interfaccia eth1 o eth0. Tuttavia, l'interfaccia utilizzata deve disporre della connettività di rete IP all'interfaccia di rete del server utilizzato per accedere al sistema operativo host.

  Nota: Se si implementa una rete separata per la distribuzione del sistema operativo e gli aggiornamenti dei driver di dispositivo del sistema operativo, è possibile configurare la seconda interfaccia di rete per il collegamento a questa rete invece che alla rete di dati. Tuttavia, se il sistema operativo di ciascun server non ha accesso alla rete di dati, è necessario configurare un'interfaccia aggiuntiva sui server per fornire la connettività dal sistema operativo host alla rete di dati, per la distribuzione del sistema operativo e gli aggiornamenti dei driver di dispositivo del sistema operativo

Figura 2 "Implementazione di esempio di reti di gestione e dati separati fisicamente con la rete del sistema operativo come parte della rete di dati" a pagina 24 mostra un'implementazione di esempio delle reti di dati e di gestione separate in cui la rete di distribuzione del sistema operativo è configurata come parte della rete di dati.

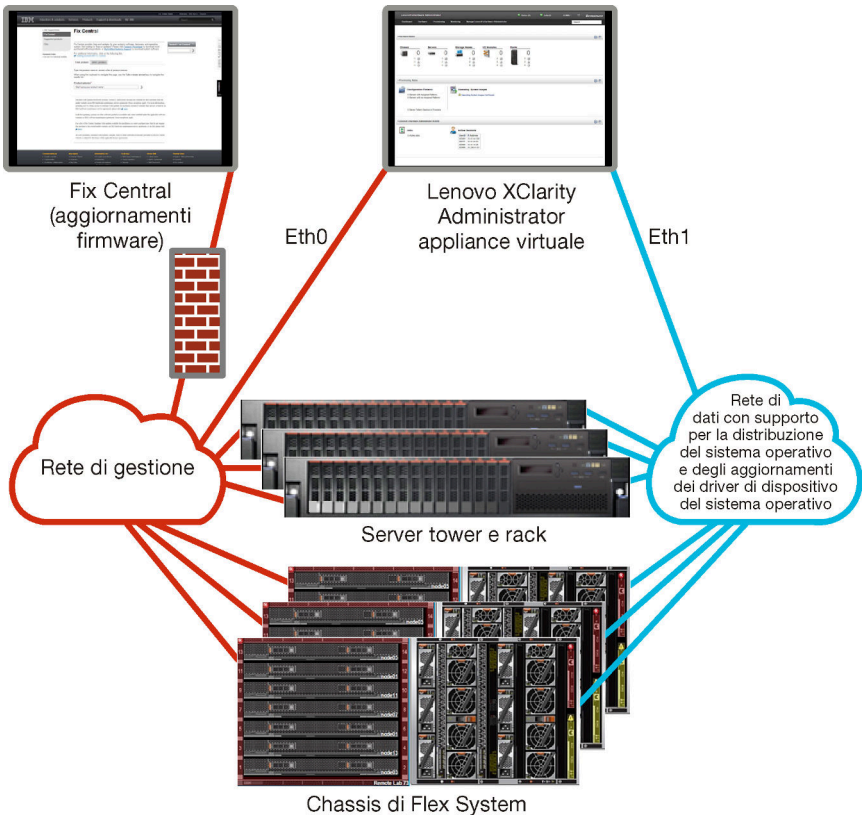


Figura 2. Implementazione di esempio di reti di gestione e dati separati fisicamente con la rete del sistema operativo come parte della rete di dati

Figura 3 "Implementazione di esempio di reti di gestione e dati separati fisicamente con la rete del sistema operativo come parte della rete di gestione" a pagina 25 mostra un'altra implementazione di esempio delle reti di dati e di gestione separate in cui la rete di distribuzione del sistema operativo è configurata come parte della rete di gestione. In questa implementazione, XClarity Administrator non richiede la connettività alla rete di dati.

Nota: Se la rete di distribuzione del sistema operativo non ha accesso alla rete di dati, configurare un'interfaccia aggiuntiva sui server per fornire la connettività dal sistema operativo host sul server alla rete di dati, se necessario.

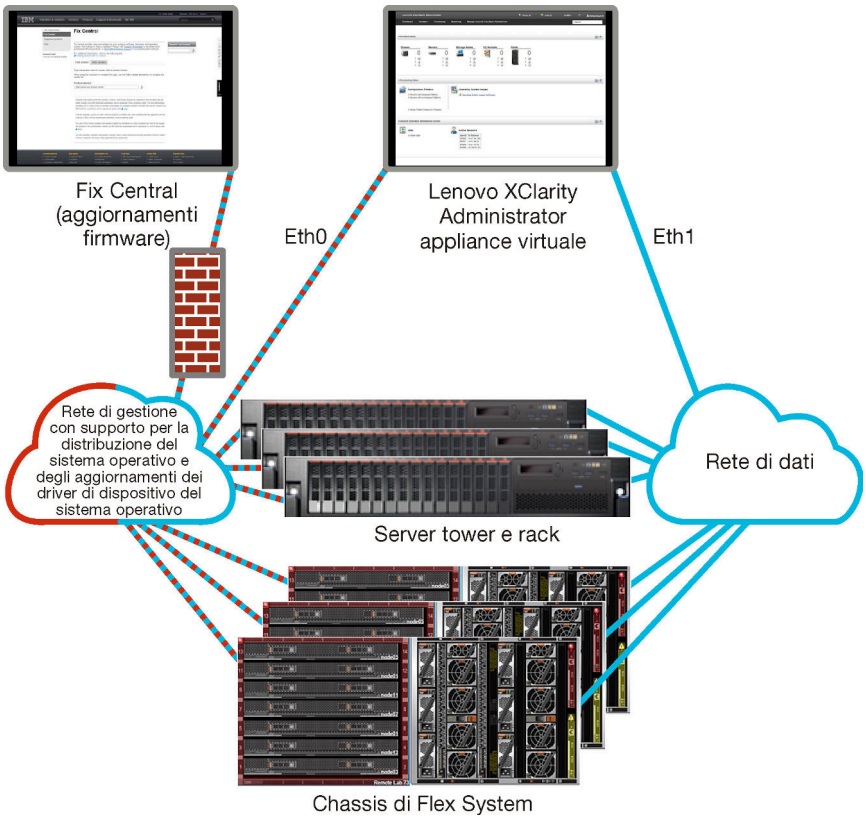


Figura 3. Implementazione di esempio di reti di gestione e dati separati fisicamente con la rete del sistema operativo come parte della rete di gestione

Rete virtualmente separata di dati e gestione

In questa topologia, la rete di dati e la rete di gestione sono virtualmente separate. I pacchetti dalla rete di dati e dalla rete di gestione vengono inviati sulla stessa connessione fisica. L'etichettatura VLAN viene utilizzata per tutti i package di dati della rete di gestione per separare il traffico tra le due reti.

Nota: Se Lenovo XClarity Administrator è installato su un host in esecuzione su un server gestito in uno chassis, non è possibile utilizzare XClarity Administrator per applicare contemporaneamente gli aggiornamenti firmware all'intero chassis. Quando gli aggiornamenti firmware vengono applicati, il sistema host deve essere riavviato.

Quando si installa XClarity Administrator, definire le impostazioni di rete utilizzando le seguenti considerazioni:

- La prima interfaccia di rete (in genere, l'interfaccia Eth0) deve essere collegata alla rete di gestione e configurata per supportare il rilevamento dei dispositivi e la gestione (come configurazione del server e aggiornamenti firmware). Deve essere in grado di comunicare con i moduli CMM e gli switch Flex di ogni chassis gestito, con il controller di gestione di ciascun server gestito e con ogni switch RackSwitch.

- La seconda interfaccia di rete (generalmente l'interfaccia eth1) può essere configurata per comunicare con una rete di dati interna, una rete di dati pubblica o entrambe.
- Se si intende acquistare gli aggiornamenti relativi a firmware e driver di dispositivo del sistema operativo mediante XClarity Administrator, almeno una delle interfacce di rete deve essere connessa a Internet, preferibilmente tramite un firewall. In caso contrario, è necessario importare gli aggiornamenti nel repository.
- Se si desidera raccogliere i dati di servizio o utilizzare la notifica automatica dei problemi (come Call Home e Funzione Caricamento Lenovo), almeno una delle interfacce di rete deve essere collegata a Internet, preferibilmente tramite un firewall.
- Se si intende distribuire le immagini del sistema operativo e aggiornare i driver di dispositivo, è possibile scegliere di utilizzare l'interfaccia eth1 o eth0. Tuttavia, l'interfaccia utilizzata deve disporre della connettività di rete IP all'interfaccia di rete del server utilizzato per accedere al sistema operativo host.

  Nota: Se si implementa una rete separata per la distribuzione del sistema operativo e gli aggiornamenti dei driver di dispositivo del sistema operativo, è possibile configurare la seconda interfaccia di rete per il collegamento a questa rete invece che alla rete di dati. Tuttavia, se il sistema operativo di ciascun server non ha accesso alla rete di dati, è necessario configurare un'interfaccia aggiuntiva sui server per fornire la connettività dal sistema operativo host alla rete di dati, per la distribuzione del sistema operativo e gli aggiornamenti dei driver di dispositivo del sistema operativo
- È possibile installare XClarity Administrator su qualsiasi sistema che soddisfa i requisiti di XClarity Administrator, incluso un server gestito, solo se viene implementata una topologia di rete singola di dati e gestione o una topologia di rete virtualmente separata di dati e gestione; tuttavia, non è possibile utilizzare XClarity Administrator per applicare gli aggiornamenti firmware a questo server gestito. Inoltre, solo alcuni firmware vengono applicati con attivazione immediata e XClarity Administrator forza il riavvio del server di destinazione, determinando il riavvio di XClarity Administrator. Se gli aggiornamenti vengono applicati con attivazione posticipata, solo parte del firmware viene applicata al riavvio dell'host XClarity Administrator.

Figura 4 "Implementazione di esempio di rete virtualmente separata di dati e gestione con la rete del sistema operativo come parte della rete di dati" a pagina 27 mostra un'implementazione di esempio delle reti virtualmente separate di dati e gestione in cui la rete di distribuzione del sistema operativo è configurata come parte della rete di dati. In questo esempio, XClarity Administrator è installato su un server gestito in uno chassis.

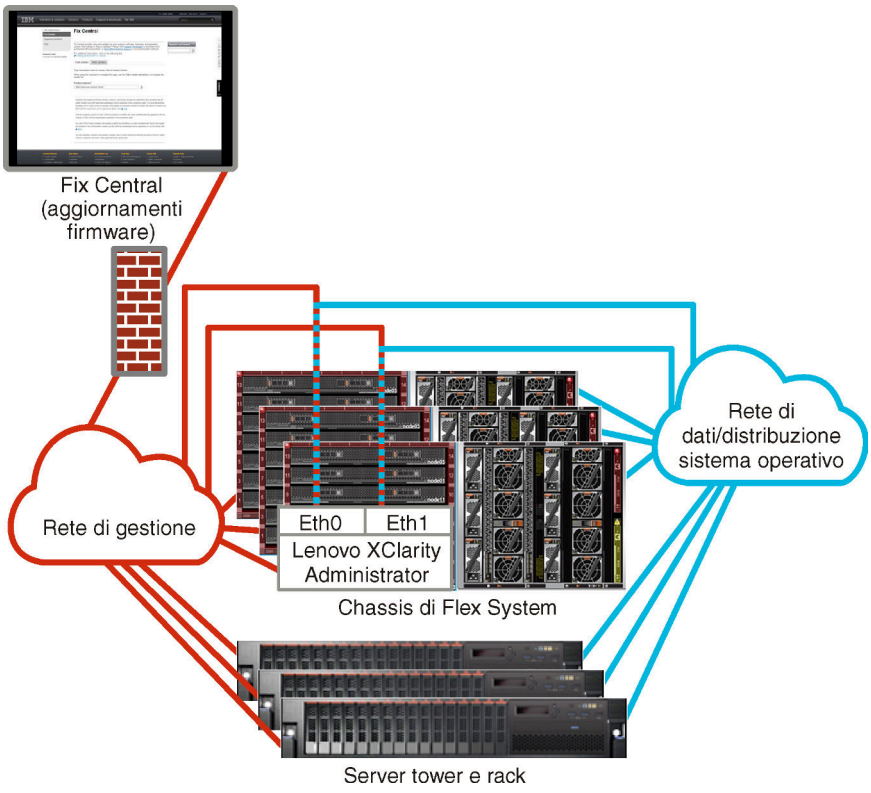


Figura 4. Implementazione di esempio di rete virtualmente separata di dati e gestione con la rete del sistema operativo come parte della rete di dati

Figura 5 "Implementazione di esempio di una rete virtualmente separata di dati e gestione con la rete del sistema operativo come parte della rete di gestione" a pagina 28 mostra un'implementazione di esempio delle reti virtualmente separate di dati e gestione in cui la rete di distribuzione del sistema operativo è configurata come parte della rete di gestione e XClarity Administrator è installato su un server gestito in uno chassis. In questa implementazione, XClarity Administrator non richiede la connettività alla rete di dati.

Nota: Se la rete di distribuzione del sistema operativo non ha accesso alla rete di dati, configurare un'interfaccia aggiuntiva sui server per fornire la connettività dal sistema operativo host sul server alla rete di dati, se necessario.

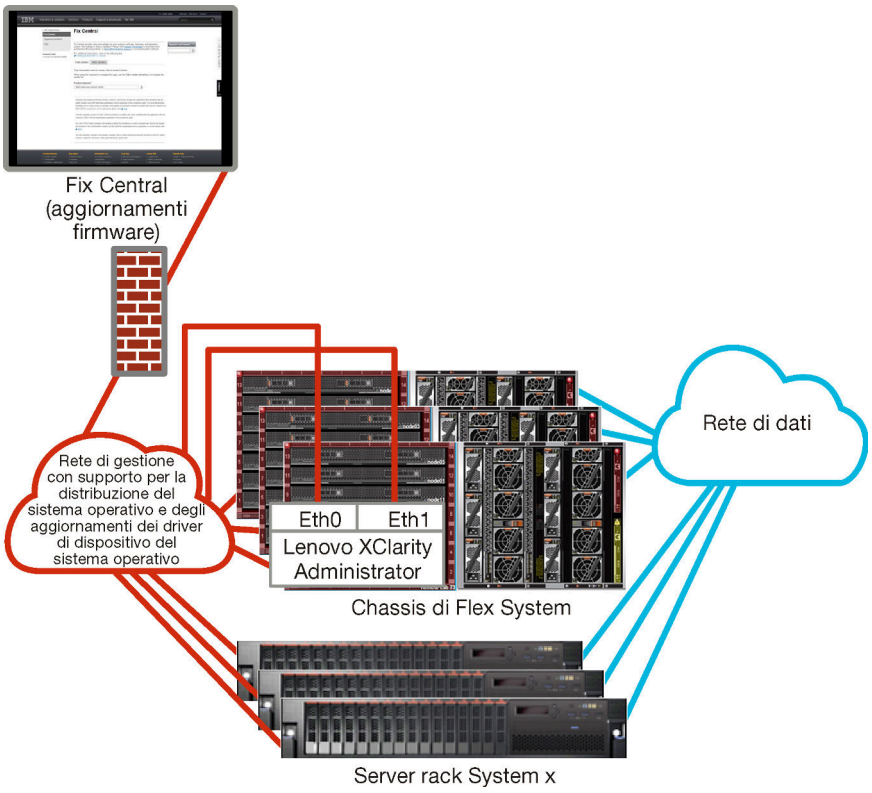


Figura 5. Implementazione di esempio di una rete virtualmente separata di dati e gestione con la rete del sistema operativo come parte della rete di gestione

Rete di sola gestione

In questa topologia, Lenovo XClarity Administrator dispone dell'accesso solo della rete di gestione e non alla rete di dati. Tuttavia, XClarity Administrator deve disporre dell'accesso alla rete di distribuzione del sistema operativo se si desidera distribuire le immagini del sistema operativo dai server gestiti di XClarity Administrator.

Quando si installa XClarity Administrator e si definiscono le impostazioni di rete, l'interfaccia di rete eth0 deve essere configurata in modo da:

- L'interfaccia deve essere configurata per supportare il rilevamento dei dispositivi e la gestione (ad esempio, configurazione del server e aggiornamenti firmware). Deve essere in grado di comunicare con i moduli CMM e gli switch Flex di ogni chassis gestito, con il controller di gestione della scheda di base di ciascun server gestito e con ogni switch RackSwitch.
- Se si intende acquistare gli aggiornamenti relativi a firmware e driver di dispositivo del sistema operativo mediante XClarity Administrator, almeno una delle interfacce di rete deve essere connessa a Internet, preferibilmente tramite un firewall. In caso contrario, è necessario importare gli aggiornamenti nel repository.
- Se si desidera raccogliere i dati di servizio o utilizzare la notifica automatica dei problemi (come Call Home e Funzione Caricamento Lenovo), almeno una delle interfacce di rete deve essere collegata a Internet, preferibilmente tramite un firewall.
- Se si intende distribuire le immagini del sistema operativo e aggiornare i driver di dispositivo del sistema operativo, l'interfaccia di rete deve disporre della connettività di rete IP all'interfaccia di rete del server utilizzata per accedere al sistema operativo host.

  Nota: Se si implementa una rete separata per la distribuzione del sistema operativo e gli aggiornamenti dei driver di dispositivo del sistema operativo, è possibile configurare la seconda interfaccia di rete per il

collegamento a questa rete invece che alla rete di dati. Tuttavia, se il sistema operativo di ciascun server non ha accesso alla rete di dati, è necessario configurare un'interfaccia aggiuntiva sui server per fornire la connettività dal sistema operativo host alla rete di dati, per la distribuzione del sistema operativo e gli aggiornamenti dei driver di dispositivo del sistema operativo

Inoltre, è possibile configurare una seconda interfaccia di rete in modo da connettersi alla stessa rete di XClarity Administrator per supportare la ridondanza.

Figura 6 "Implementazione di esempio di una rete di sola gestione che non supporta la distribuzione del sistema operativo" a pagina 29 mostra un'implementazione di esempio per una rete di sola gestione in cui la distribuzione del sistema operativo da XClarity Administrator non è supportata.

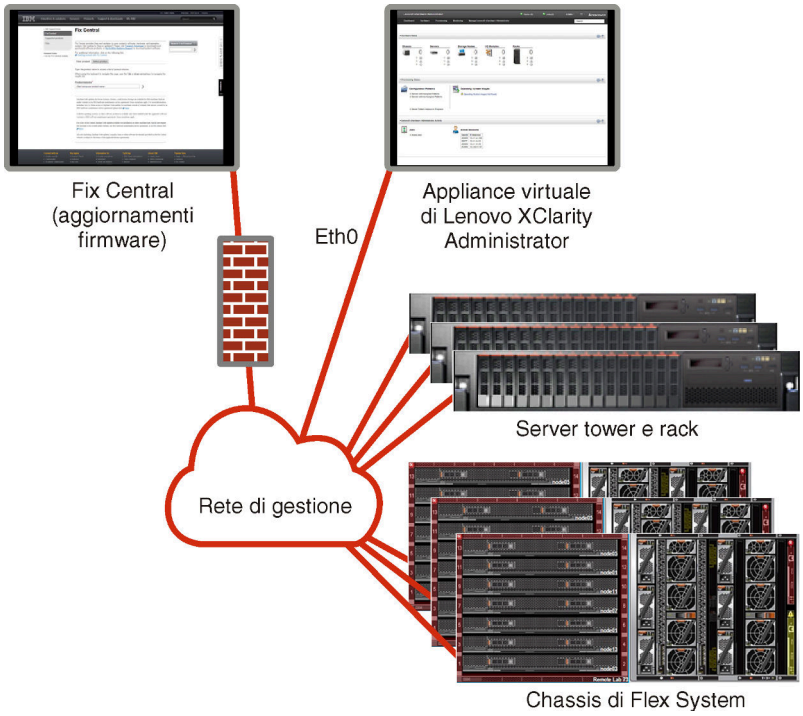


Figura 6. Implementazione di esempio di una rete di sola gestione che non supporta la distribuzione del sistema operativo

Figura 6 "Implementazione di esempio di una rete di sola gestione che non supporta la distribuzione del sistema operativo" a pagina 29 mostra un'implementazione di esempio per una rete di sola gestione in cui la distribuzione del sistema operativo da XClarity Administrator è supportata.

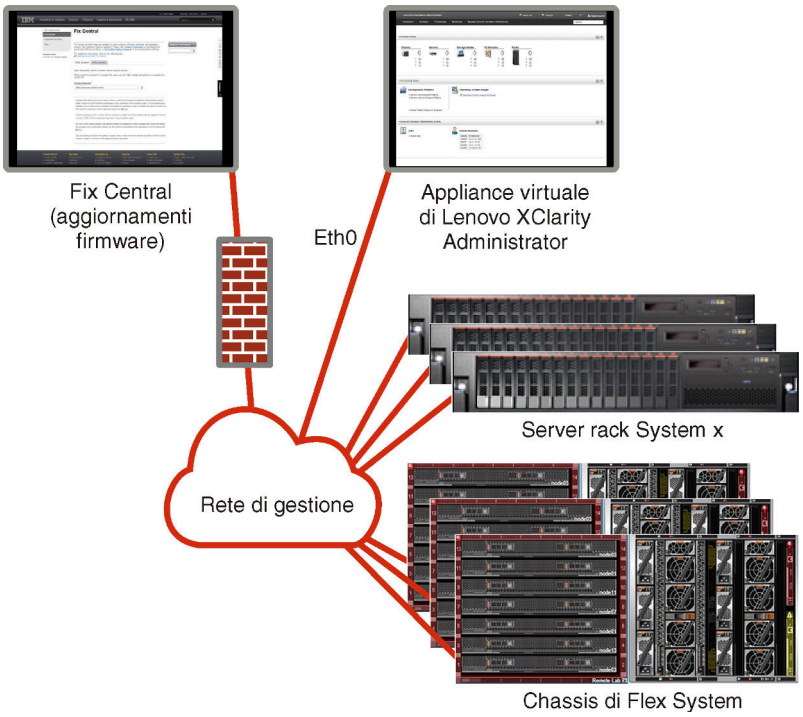


Figura 7. Implementazione di esempio di una rete di sola gestione che supporta la distribuzione del sistema operativo

Considerazioni sulla sicurezza

Piano per la sicurezza di Lenovo XClarity Administrator e di tutti i dispositivi gestiti.

Gestione dell'incapsulamento

Quando si gestiscono gli chassis e i server Lenovo in Lenovo XClarity Administrator, è possibile configurare Lenovo XClarity Administrator affinché modifichi le regole del firewall per i dispositivi in modo che le richieste in entrata vengano accettate solo da Lenovo XClarity Administrator. Questo processo è detto *incapsulamento*. É inoltre possibile abilitare o disabilitare l'incapsulamento su chassis e server già gestiti da Lenovo XClarity Administrator.

Quando abilitato sui dispositivi che supportano l'incapsulamento, Lenovo XClarity Administrator modifica la modalità di incapsulamento del dispositivo in "encapsulationLite" e le regole del firewall sul dispositivo per limitare le richieste in entrata solo a quelle provenienti da Lenovo XClarity Administrator.

Se disabilitata, la modalità di incapsulamento è impostata su "normale". Se l'incapsulamento è stato precedentemente abilitato sui dispositivi, le regole del firewall per l'incapsulamento vengono rimosse.

Attenzione: Se l'incapsulamento è abilitato e XClarity Administrator non è più disponibile prima che la gestione di un dispositivo venga annullata, è necessario eseguire la procedura per disabilitare l'incapsulamento al fine di stabilire la comunicazione con il dispositivo. Per le procedure di ripristino, vedere Ripristino della gestione dello chassis con un modulo CMM dopo un errore del server di gestione e Ripristino della gestione del server tower o rack dopo un errore del server di gestione nella documentazione online di XClarity Administrator.

Nota:

- l'incapsulamento non è supportato su switch, dispositivi di storage, chassis e server non Lenovo.
- Quando l'interfaccia di rete di gestione è configurata per utilizzare Dynamic Host Configuration Protocol (DHCP) e quando l'incapsulamento è abilitato, la gestione di un server rack può richiedere molto tempo.

Per ulteriori informazioni sull'incapsulamento, vedere Abilitazione incapsulamento nella documentazione online di XClarity Administrator.

Gestione della crittografia

La gestione crittografica è costituita da protocolli e modalità di comunicazione che regolano la modalità di gestione della comunicazione sicura tra Lenovo XClarity Administrator e i sistemi gestiti (come chassis, server e switch Flex).

Algoritmi di crittografia

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

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

- SSH-ED25519
- SSH-ED25519-CERT-V01@OPENSSH.COM
- ECDSA-SHA2-NISTP256
- ECDSA-SHA2-NISTP256-CERT-V01@OPENSSH.COM
- ECDSA-SHA2-NISTP384
- ECDSA-SHA2-NISTP384-CERT-V01@OPENSSH.COM
- ECDSA-SHA2-NISTP521
- ECDSA-SHA2-NISTP521-CERT-V01@OPENSSH.COM
- RSA-SHA2-512
- RSA-SHA2-256
- RSA-SHA2-384

Modalità crittografiche per il server di gestione

Questa impostazione determina la modalità da utilizzare per le comunicazioni sicure dal server di gestione.

- **Compatibilità**. Questo è la modalità predefinita. È compatibile con le versioni firmware precedenti, i browser e gli altri client di rete che non implementano i rigorosi standard di sicurezza richiesti per la conformità NIST SP 800-131A.
- **NIST SP 800-131A**. Questa modalità è progettata per rispettare lo standard di conformità NIST SP 800-131A. XClarity Administrator è progettato per utilizzare sempre la crittografia interna e le connessioni di rete con crittografia sicura, dove disponibile. Tuttavia, in questa modalità, le connessioni di rete che utilizzano la crittografia non approvata da NIST SP 800-131A non sono autorizzate; ad esempio, i certificati TLS (Transport Layer Security) con firma SHA-1 o hash più debole verranno respinti.

  Se si seleziona questa modalità:

  – Per tutte le porte diverse dalla porta 8443, tutte le cifrature CBC TLS e quelle che non supportano Perfect Forward Secrecy sono disabilitate.

  – Le notifiche eventi potrebbero non essere inviate correttamente ad alcune sottoscrizioni di dispositivi mobili (vedere Inoltro di eventi a dispositivi mobili nella documentazione online di XClarity Administrator). Servizi esterni, come Android e iOS, presentano certificati firmati con SHA-1. Questo algoritmo non è conforme ai requisiti più rigorosi della modalità NIST SP 800-131A. Pertanto, tutte le connessioni a questi servizi potrebbero non riuscire con un'eccezione del certificato o un errore di handshake.

  Per ulteriori informazioni sulla NIST SP 800-131A conformità, vedere Implementazione della conformità NIST 800-131A nella documentazione online di XClarity Administrator.

Per ulteriori informazioni sull'impostazione delle modalità di sicurezza sul server di gestione, vedere Impostazione della modalità crittografica e dei protocolli di comunicazione nella documentazione online di XClarity Administrator.

Modalità di sicurezza per i server gestiti

Questa impostazione determina la modalità da utilizzare per le comunicazioni sicure dai server di gestione.

- **Sicurezza della compatibilità**. Selezionare questa modalità quando i servizi e i client richiedono crittografia non conforme a CNSA/FIPS. Questa modalità supporta un'ampia gamma di algoritmi di crittografia e consente l'abilitazione di tutti i servizi.
- **NIST SP 800-131A**. Selezionare questa modalità per garantire la compatibilità con lo standard NIST SP 800-131A. Ciò include la restrizione delle chiavi RSA a 2048 bit o superiori, la restrizione degli hash utilizzati per le firme digitali a SHA-256 o più e la garanzia che vengano utilizzati solo gli algoritmi di crittografia simmetrica approvati NIST. Questa modalità richiede l'impostazione della modalità SSL/TLS sul **client del server TLS 1.2**.

  Questa modalità *non* è supportata per i server con XCC2.
- **Sicurezza standard**. Questa è la modalità di sicurezza predefinita per server con XCC2 (solo server con XCC2). Selezionare questa modalità per garantire la compatibilità con lo standard FIPS 140-3. Per il funzionamento di XCC in modalità convalidata FIPS 140-3, è possibile abilitare solo i servizi che supportano la crittografia di livello FIPS 140-3. I servizi che non supportano la crittografia di livello FIPS 140-2/140-3 sono disabilitati per impostazione predefinita, ma possono essere abilitati, se necessario. Se è abilitato un servizio che utilizza la crittografia non di livello FIPS 140-3, XCC non può funzionare in modalità convalidata FIPS 140-3. Questa modalità richiede certificati di livello FIP.
- **Sicurezza aziendale rigorosa**. Questa è la modalità più sicura (solo server con XCC2). Selezionare questa modalità per garantire la compatibilità con lo standard CNSA. Sono consentiti solo i servizi che supportano la crittografia di livello CNSA. I servizi non sicuri sono disabilitati per impostazione predefinita e non possono essere abilitati. Questa modalità richiede certificati di livello CNSA.

  XClarity Administrator utilizza le firme del certificato RSA-3072/SHA-384 per i server in modalità **Sicurezza aziendale rigorosa**.

  Importante:

  – Per utilizzare questa modalità, è necessario installare la chiave Feature On Demand di XCC2 per ogni elemento server con XCC2 selezionato.

  – In questa modalità, se XClarity Administrator utilizza un certificato autofirmato, XClarity Administrator deve utilizzare il certificato radice e il certificato server basati su RSA3072/SHA384. Se XClarity Administrator utilizza un certificato firmato esterno, XClarity Administrator deve generare una CSR basata su RSA3072/SHA384 e contattare la CA esterna per firmare un nuovo certificato server basato su RSA3072/SHA384.

  – Quando XClarity Administrator utilizza un certificato basato su RSA3072/SHA384, XClarity Administrator potrebbe scollegare i dispositivi diversi da: chassis e server Flex System (CMM), server ThinkSystem, server ThinkServer, server System x M4 e M5, switch Lenovo ThinkSystem serie DB, Lenovo RackSwitch, switch Flex System, switch Mellanox, dispositivi di storage ThinkSystem DE/DM, storage della libreria a nastro IBM e server ThinkSystem SR635/SR655 con firmware precedente alla versione 22C. Per continuare a gestire i dispositivi disconnessi, configurare un'altra istanza di XClarity Administrator con un certificato basato su RSA2048/SHA384.

Considerare le seguenti implicazioni che comporta la modifica della modalità crittografica.

- La modifica dalla modalità **Sicurezza della compatibilità** o **Sicurezza standard** a **Sicurezza aziendale rigorosa** non è supportata.
- Se si esegue l'aggiornamento dalla modalità **Sicurezza della compatibilità** alla modalità **Sicurezza standard**, se i certificati importati o le chiavi pubbliche SSH non sono conformi, verrà visualizzato un avviso ma sarà comunque possibile aggiornare alla modalità **Sicurezza standard**.
- Se si esegue il downgrade dalla modalità **Sicurezza aziendale rigorosa** alla modalità **Sicurezza della compatibilità** o **Sicurezza standard**:

  - Il server viene automaticamente riavviato affinché la modalità di sicurezza sia resa effettiva.
  - Se la chiave FoD in modalità rigorosa manca o è scaduta su XCC2 e XCC2 utilizza un certificato TLS autofirmato, XCC2 rigenera il certificato TLS autofirmato basato sull'algoritmo conforme alla modalità Rigorosa standard. XClarity Administrator mostra un errore di connessione a causa di un errore del certificato. Per risolvere l'errore di certificato non attendibile, vedere Risoluzione di un certificato server non attendibile nella documentazione online di XClarity Administrator. Se XCC2 utilizza un certificato TLS personalizzato, XCC2 consente il downgrade e avverte l'utente della necessità di importare un certificato server basato sulla crittografia della modalità **Sicurezza standard**.
- La modalità **NIST SP 800-131A** non è supportata per i server con XCC2.
- Se la modalità crittografica di XClarity Administrator è impostata su TLS v1.2 e su un server gestito che utilizza l'autenticazione gestita è impostata una modalità di sicurezza su TLS v1.2, modificando la modalità di sicurezza del server su TLS v1.3 mediante XClarity Administrator o XCC, il server risulterà definitivamente offline.
- Se la modalità crittografica di XClarity Administrator è impostata su TLS v1.2 e si tenta di gestire un server con XCC e la modalità di sicurezza impostata su TLS v1.3, non è possibile gestire il server mediante l'autenticazione gestita.

È possibile modificare i valori delle impostazioni di sicurezza per i seguenti dispositivi.
- Server Lenovo ThinkSystem con processori Intel o AMD (ad eccezione di SR635/SR655)
- Server Lenovo ThinkSystem V2
- Server Lenovo ThinkSystem V3 con processori Intel o AMD
- Server Lenovo ThinkEdge SE350/SE450
- Server Lenovo System x

Per ulteriori informazioni sull'impostazione delle modalità di sicurezza sul server gestito, vedere Configurazione delle impostazioni di sicurezza per un server nella documentazione online di XClarity Administrator.

Certificati di sicurezza

Lenovo XClarity Administrator utilizza i certificati SSL per stabilire le comunicazioni sicure e attendibile tra XClarity Administrator e i relativi dispositivi gestiti (come lo chassis e i processori di servizio dei server System x), nonché le comunicazioni con XClarity Administrator da parte degli utenti o con servizi differenti. Per impostazione predefinita, XClarity Administrator, i moduli CMM e i controller di gestione della scheda di base utilizzano i certificati generati da XClarity Administrator, autofirmati e pubblicati da un'autorità di certificazione interna.

Il certificato server autofirmato predefinito, generato in modo univoco in ogni istanza di XClarity Administrator, fornisce misure di sicurezza sufficienti per molti ambienti. È possibile delegare la gestione dei certificati a XClarity Administrator oppure avere un ruolo più attivo e personalizzare o sostituire i certificati server. XClarity Administrator 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 che può essere inviata all'autorità di certificazione preferita per firmare un certificato personalizzato che può quindi essere caricato in XClarity Administrator 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 Utilizzo dei certificati di sicurezza nella documentazione online di XClarity Administrator.

Autenticazione

Server di autenticazione supportati

Il *server di autenticazione* è un registro utente utilizzato per autenticare le credenziali utente. Lenovo XClarity Administrator supporta i seguenti tipi di server di autenticazione.

- **Server di autenticazione locale**. Per impostazione predefinita, XClarity Administrator è configurato per utilizzare il server LDAP (Lightweight Directory Access Protocol) che risiede nel server di gestione.
- **Server LDAP esterno**. Attualmente, solo Microsoft Active Directory e OpenLDAP sono supportati. Questo server deve trovarsi in un server Microsoft Windows esterno connesso alla rete di gestione. Quando viene utilizzato un server LDAP esterno, il server di autenticazione locale è disabilitato.

  Attenzione: Per configurare il metodo di collegamento Active Directory in modo da utilizzare le credenziali di login, il firmware del controller BMC (Baseboard Management Controller) di ciascun server gestito deve essere aggiornato a settembre 2016 o successivo.
- **Sistema di gestione delle identità esterno**. Attualmente è supportato solo CyberArk.

  Se gli account utente per un server ThinkSystem o ThinkAgile sono integrati in CyberArk, è possibile scegliere di utilizzare XClarity Administrator per recuperare le credenziali tramite CyberArk al fine di accedere al server durante la configurazione iniziale dei server per la gestione (con autenticazione gestita o locale). Prima che le credenziali possano essere recuperate da CyberArk, i percorsi CyberArk devono essere definiti in XClarity Administrator e l'attendibilità reciproca deve essere stabilita tra CyberArk e XClarity Administrator utilizzando l'autenticazione TLS reciproca tramite i certificati client.
- **SAML esterno provider di identità**. Attualmente, è supportato solo Microsoft Active Directory Federation Services (AD FS). Oltre all'immissione di un nome utente e una password, l'autenticazione a più fattori può essere configurata in modo da garantire un'ulteriore protezione attraverso la richiesta di un codice PIN, la lettura di una smart card e un certificato client. Quando viene utilizzato un provider di identità SAML, il server di autenticazione locale non viene disabilitato. Gli account utente locali sono richiesti per accedere direttamente a uno chassis gestito o al server (tranne se Incapsulamento non è abilitato su tale dispositivo), per l'autenticazione PowerShell e API REST, nonché per il ripristino se l'autenticazione esterna non è disponibile.

  È possibile scegliere di utilizzare sia un server LDAP esterno che un provider di identità esterno. Se entrambi sono abilitati, il server LDAP esterna viene utilizzato per accedere direttamente ai dispositivi da gestire, mentre il provider di identità viene utilizzato per accedere al server di gestione.

Per ulteriori informazioni sui server di autenticazione, vedere Gestione del server di autenticazione nella documentazione online di XClarity Administrator.

Autenticazione dispositivo

Per impostazione predefinita, i dispositivi vengono gestiti utilizzando l'autenticazione gestita di XClarity Administrator per eseguire il login ai dispositivi. Quando si gestiscono i server rack e lo chassis Lenovo, è possibile scegliere di utilizzare l'autenticazione locale o gestita per eseguire il login ai dispositivi.

- Quando l'*autenticazione locale* viene utilizzata per i server rack, lo chassis Lenovo e gli switch rack Lenovo, XClarity Administrator utilizza una credenziale memorizzata per eseguire l'autenticazione al dispositivo. La *credenziale memorizzata* può essere un account utente attivo sul dispositivo o un account utente in un server Active Directory.

  Prima di gestire il dispositivo utilizzando l'autenticazione locale è necessario creare le credenziali memorizzate in XClarity Administrator che corrispondono a un account utente attivo sul dispositivo o un account utente in un server Active Directory (vedere Gestione delle credenziali memorizzate nella documentazione online di XClarity Administrator).

  Nota:

  - I dispositivi RackSwitch supportano solo le credenziali memorizzate per l'autenticazione. Le credenziali utente di XClarity Administrator non sono supportate.
- L'*autenticazione gestita* consente di gestire e monitorare più dispositivi utilizzando le credenziali del server di autenticazione XClarity Administrator invece delle credenziali locali. Quando l'autenticazione gestita viene utilizzata per un dispositivo (diverso dai server ThinkServer e System x M4 o dagli switch), XClarity Administrator configura il dispositivo gestito e i relativi componenti installati per utilizzare il server di autenticazione XClarity Administrator per la gestione centralizzata.
  - Quando è abilitata l'autenticazione gestita, è possibile gestire i dispositivi utilizzando le credenziali memorizzate o inserite manualmente (vedere Gestione degli account utente e nella documentazione online di XClarity Administrator).

    La credenziale memorizzata viene utilizzata solo finché XClarity Administrator non configura le impostazioni LDAP sul dispositivo. Successivamente, eventuali modifiche delle credenziali memorizzate non incidono sulla gestione o sul monitoraggio di tale dispositivo.

    Nota: Quando è abilitata l'autenticazione gestita per un dispositivo, non è possibile modificare le credenziali memorizzate per tale dispositivo utilizzando XClarity Administrator.
  - Se viene utilizzato un server LDAP esterno o locale come server di autenticazione XClarity Administrator, gli account utente definiti nel server di autenticazione vengono utilizzati per eseguire il login a XClarity Administrator, CMM e controller di gestione della scheda di base nel dominio di XClarity Administrator. Gli account utente del controller di gestione e CMM locali sono disabilitati.
  - Se viene utilizzato un provider di identità SAML 2.0 come server di autenticazione XClarity Administrator, gli account SAML non saranno accessibili per i dispositivi gestiti. Tuttavia quando si utilizzano un provider di identità SAML e un server LDAP insieme, se il provider di identità utilizza gli account esistenti nel server LDAP, gli account utente LDAP possono essere utilizzati per eseguire il login ai dispositivi gestiti mentre i metodi di autenticazione più avanzati forniti da SAML 2.0 (come autenticazione a più fattori e Single Sign-On) possono essere utilizzati per eseguire il login a XClarity Administrator.
  - La funzione Single Sign-On consente a un utente già connesso a XClarity Administrator di eseguire automaticamente il login al controllo di gestione della scheda di base. L'opzione Single Sign-On è abilitata per impostazione predefinita quando un server ThinkSystem o ThinkAgile viene inserito nella gestione da XClarity Administrator (a meno che il server non sia gestito con password CyberArk). È possibile configurare l'impostazione globale per abilitare o disabilitare la funzione Single Sign-On per tutti i server ThinkSystem e ThinkAgile gestiti. L'abilitazione dell'opzione Single Sign-On per un server ThinkSystem o ThinkAgile specifico ha la precedenza sull'impostazione globale per tutti i server ThinkSystem e ThinkAgile (vedere Gestione dei server nella documentazione online di XClarity Administrator).

    Nota: Single Sign-On viene disabilitato automaticamente quando si utilizza il sistema di gestione delle identità CyberArk per l'autenticazione.
  - Quando l'autenticazione gestita è abilitata per i server ThinkSystem SR635 e SR655:
    - Il firmware del controller di gestione della scheda di base supporta fino a cinque ruoli utente LDAP. XClarity Administrator aggiunge questi ruoli utente LDAP ai server durante la gestione: **lxc-supervisor**, **lxc-sysmgr**, **lxc-admin**, **lxc-fw-admin** e **lxc-os-admin**.

      È necessario assegnare gli utenti ad almeno uno dei ruoli utente LDAP specificati per comunicare con i server ThinkSystem SR635 e SR655.
    - Il firmware del controller di gestione non supporta gli utenti LDAP con lo stesso nome utente locale del server.
  - Per i server ThinkServer e System x M4, il server di autenticazione XClarity Administrator non viene utilizzato. Di contro, viene creato un account IPMI sul dispositivo con il prefisso "LXCA_", seguito da una stringa casuale. (Gli account utente IPMI locali esistenti non vengono disabilitati). Quando si annulla la gestione di un server ThinkServer, l'account utente "LXCA_" viene disabilitato e il prefisso

"LXCA_" viene sostituito con il prefisso "DISABLED_". Per determinare se un server ThinkServer è gestito da un'altra istanza, XClarity Administrator verifica gli account IPMI con il prefisso "LXCA_". Se si sceglie di forzare la gestione di un server ThinkServer gestito, tutti gli account IPMI del dispositivo con il prefisso "LXCA_" vengono disabilitati e rinominati. Valutare la possibilità di cancellare manualmente gli account IPMI non più in uso.

Se si utilizzano credenziali inserite manualmente, XClarity Administrator crea automaticamente una credenziale memorizzata e la utilizza per gestire il dispositivo.

Nota: Quando è abilitata l'autenticazione gestita per un dispositivo, non è possibile modificare le credenziali memorizzate per tale dispositivo utilizzando XClarity Administrator.

- Ogni volta che si gestisce un dispositivo utilizzando le credenziali inserite manualmente, viene creata una nuova credenziale memorizzata per tale dispositivo, anche se è stata creata un'altra credenziale memorizzata per il dispositivo durante un processo di gestione precedente.
- Quando si annulla la gestione di un dispositivo, XClarity Administrator non elimina le credenziali memorizzate create automaticamente per tale dispositivo durante il processo di gestione.

Account utente di ripristino

Se si specifica una password di ripristino, XClarity Administrator disabilita l'account utente CMM locale o del controller di gestione e crea un nuovo account utente di ripristino (`RECOVERY_ID`) sul dispositivo per l'autenticazione futura. Se il server di gestione non funziona, è possibile utilizzare l'account `RECOVERY_ID` per eseguire il login al dispositivo e ripristinare le funzioni di gestione degli account del dispositivo, finché il nodo di gestione non viene ripristinato o sostituito.

Se si annulla la gestione di un dispositivo che dispone di un account utente `RECOVERY_ID`, tutti gli account utente locali vengono abilitati e l'account `RECOVERY_ID` viene eliminato.

- Se si modificano gli account utente locali disabilitati (ad esempio, se si modifica una password), le modifiche non hanno effetto sull'account `RECOVERY_ID`. In modalità di autenticazione gestita, l'account `RECOVERY_ID` è l'unico account utente attivato e operativo.
- Utilizzare l'account `RECOVERY_ID` solo in caso di emergenza, ad esempio, se il server di gestione non funziona o se si verifica un problema alla rete che impedisce al dispositivo di comunicare con XClarity Administrator per autenticare gli utenti.
- La password `RECOVERY_ID` viene specificata quando si rileva il dispositivo. Assicurarsi di registrare la password per gli usi successivi.

Per informazioni sul recupero della gestione di un dispositivo, vedere Ripristino della gestione dello chassis con un modulo CMM dopo un errore del server di gestione e Ripristino della gestione del server tower o rack dopo un errore del server di gestione nella documentazione online di XClarity Administrator.

Account utente e gruppi di ruoli

Gli *account utente* vengono utilizzati per accedere e gestire Lenovo XClarity Administrator e tutti gli chassis gestiti e i server. Gli account utente XClarity Administrator sono sottoposti a due processi interdipendenti: autenticazione e autorizzazione.

L'*autenticazione* è il meccanismo di sicurezza che consente di verificare le credenziali degli utenti. Il processo di autenticazione utilizza le credenziali utente memorizzate nel server di autenticazione configurato. Esso impedisce alle applicazioni dei sistemi gestiti o ai server di gestione non autorizzati di accedere alle risorse. Una volta autenticato, un utente può accedere a XClarity Administrator. Tuttavia, per accedere a una risorsa specifica o per eseguire una determinata attività, l'utente deve anche disporre dell'autorizzazione appropriata.

L'*autorizzazione* verifica le autorizzazioni dell'utente autenticato e controlla l'accesso alle risorse in base all'appartenenza degli utenti a un gruppo di ruoli. I *gruppi di ruoli* vengono utilizzati per assegnare ruoli specifici a una serie di account utente definiti e gestiti nel server di autenticazione. Ad esempio, se un utente è membro di un gruppo di ruoli con autorizzazioni di supervisore può creare, modificare ed eliminare gli account utente da XClarity Administrator. Se un utente dispone delle autorizzazioni di operatore può solo visualizzare le informazioni sull'account utente.

Per ulteriori informazioni sugli account utente e i gruppi di ruoli, vedere Gestione degli account utente nella documentazione online di XClarity Administrator.

Sicurezza degli account utente

Le impostazioni dell'account utente verificano la complessità della password, il blocco dell'account e il timeout di inattività della sessione Web. È possibile modificare i valori delle impostazioni di sicurezza dell'account.

Per ulteriori informazioni sulle impostazioni di sicurezza dell'account, vedere Modifica delle impostazioni di sicurezza dell'account utente nella documentazione online di Lenovo XClarity Administrator.

Considerazioni sulla disponibilità elevata

Per configurare l'alta disponibilità di Lenovo XClarity Administrator, utilizzare le funzioni di alta disponibilità integrate nel sistema operativo host o l'ambiente del contenitore.

Docker

È possibile utilizzare Docker Datacenter per configurare un ambiente ad alta disponibilità per i contenitori XClarity Administrator che vengono eseguiti in Docker Engine. Per ulteriori informazioni sull'alta disponibilità di Docker Datacenter, vedere Pagina Web Architettura e app ad alta disponibilità con Docker Datacenter.

Citrix

Utilizzare la funzione di disponibilità elevata fornita per l'ambiente Citrix. Per ulteriori informazioni, vedere Implementazione dell'alta disponibilità (Citrix) nella documentazione online di XClarity Administrator..

KVM (CentOS, RedHat e Ubuntu)

È possibile utilizzare OpenStack oppure, se già si dispone di un ambiente ad alta disponibilità, continuare a utilizzare i processi interni. Per ulteriori informazioni sull'alta disponibilità di OpenStack, vedere Implementazione dell'alta disponibilità (KVM) nella documentazione online di XClarity Administrator..

Microsoft Hyper-V

Utilizzare la funzione di alta disponibilità fornita per l'ambiente ESXi. Per informazioni, vedere Implementazione dell'alta disponibilità (Microsoft Hyper-V) nella documentazione online di XClarity Administrator..

Nutanix AHV

Utilizzare la funzione di alta disponibilità delle macchine virtuali fornita per l'ambiente Nutanix AHV. Per ulteriori informazioni, vedere Implementazione dell'alta disponibilità (Nutanix) nella documentazione online di XClarity Administrator..

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 seguenti componenti:

- 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 utilizzato nel cluster. Tuttavia, se tale host è spento o non utilizzabile, 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).

Per informazioni dettagliate sulla configurazione del cluster VMware High Availability, vedere Implementazione dell'alta disponibilità (VMware ESXi) nella documentazione online di XClarity Administrator..

Features on Demand

Features on Demand attiva le funzioni senza richiedere l'installazione di hardware o l'acquisto di nuove apparecchiature. L'attivazione viene eseguita acquistando e installando la chiave Features on Demand corrispondente.

Per utilizzare le operazioni di distribuzione del sistema operativo e di controllo remoto in Lenovo XClarity Administrator, è necessario abilitare il livello XClarity Controller Enterprise o l'aggiornamento avanzato MM per i server in cui queste funzionalità non sono preattivate per impostazione predefinita. Queste operazioni richiedono anche l'installazione di una chiave Features on Demand per la presenza remota sui server ThinkSystem, Converged e System x. È possibile determinare se la presenza remota è abilitata, disabilitata o non installata su un server dalla pagina Server (vedere Visualizzazione dello stato di un server gestito nella documentazione online di XClarity Administrator).

Alcune funzioni avanzate del server vengono attivate utilizzando le chiavi Features on Demand. Se è possibile configurare le impostazioni delle funzioni durante la configurazione di UEFI, è possibile modificare l'impostazione utilizzando Pattern di configurazione; tuttavia, la configurazione ottenuta non viene attivata finché non viene installata la chiave Features on Demand corrispondente.

Nota: non è possibile installare o gestire le chiavi Features on Demand da XClarity Administrator; tuttavia, è possibile visualizzare l'elenco delle chiavi Features on Demand correntemente installate sui server gestiti. Per ulteriori informazioni sulla visualizzazione delle chiavi Features on Demand installate, vedere Visualizzazione delle chiavi FoD (Feature on Demand) nella documentazione online diXClarity Administrator .

Per acquisire e installare le chiavi Features on Demand:

1. Acquistare l'aggiornamento Features on Demand utilizzando il numero parte appropriato.

   È possibile acquistare le chiavi da Portale Web Features on Demand. Una volta completato l'acquisto, verrà inviato un codice di autorizzazione via e-mail.
2. Da Portale Web Features on Demand, immettere il codice di autorizzazione ricevuto, con l'identificativo univoco di sistema del server che si intende aggiornare.
3. Scaricare la chiave di attivazione nel formato di file .KEY.
4. Caricare la chiave di attivazione nel controller di gestione del server.
5. Riavviare il server. La funzione viene attivata una volta completato il riavvio.

Per maggiori informazioni sulle chiavi Features on Demand, vedere Utilizzo di Lenovo Features on Demand.

Capitolo 3. Installazione di Lenovo XClarity Administrator

Sono disponibili diversi modi per connettere i dispositivi gestibili alla rete e per configurare l'appliance virtuale Lenovo XClarity Administrator per gestire i dispositivi. Utilizzare le informazioni in questa sezione come guida per configurare i dispositivi gestibili e installare l'appliance virtuale XClarity Administrator

In questa sezione verrà descritta la procedura per configurare varie tipologie comuni. Non verrà trattata ogni singola topologia di rete possibile.

Attenzione: Per gestire i dispositivi, XClarity Administrator deve disporre dell'accesso alla rete di gestione.

Ulteriori informazioni:

- Installazione di Lenovo XClarity Administrator in VMware vCenter
- Installazione di Lenovo XClarity Administrator in VMware vSphere
- Installazione di Lenovo XClarity Administrator in Windows Hyper-V
- Installazione di Lenovo XClarity Administrator in Red Hat KVM

Dati Single e rete di gestione

In questa topologia di rete, la rete dei dati e la rete di gestione coincidono.

Prima di iniziare

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

Accertarsi che sia installato il firmware minimo richiesto in ciascun dispositivo che si desidera gestire mediante XClarity Administrator. È possibile trovare i livelli minimi di firmware richiesti sulle Supporto XClarity Administrator - Pagina Web sulla compatibilità facendo clic sulla scheda **Compatibilità** e quindi sul collegamento per i tipi di dispositivi appropriati.

Importante: 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 viene utilizzato DHCP, verificare che le modifiche dell'indirizzo IP siano minime.

Informazioni su questa attività

Per le appliance virtuali, tutte le comunicazioni tra XClarity Administrator e la rete si verificano sull'interfaccia di rete eth0 sull'host. Per i contenitori, è possibile utilizzare un nome personalizzato. Tuttavia, questo scenario utilizza eth0.

Importante: L'implementazione di una rete di gestione e di dati condivisi può causare interruzioni del traffico, come perdita di pacchetti o problemi di connettività della rete di gestione, a seconda della configurazione di rete (ad esempio, se il traffico dei server ha priorità elevata mentre il traffico del controller di gestione ha priorità bassa). La rete di gestione utilizza il traffico UDP e TCP. Il traffico UDP può avere priorità più bassa quando il traffico di rete è elevato.

La seguente figura mostra una modalità di configurazione dell'ambiente nel caso in cui la rete di dati e la rete di gestione coincidano. I numeri nella figura corrispondono ai passaggi numerati nelle seguenti sezioni.

Nota: Questa figura non rappresenta tutte le opzioni di cablaggio che potrebbero essere necessarie per l'ambiente. La figura mostra solo i requisiti delle opzioni di cablaggio per server rack, switch rack, switch Flex e CMM in correlazione per configurare una rete singola di dati/gestione.

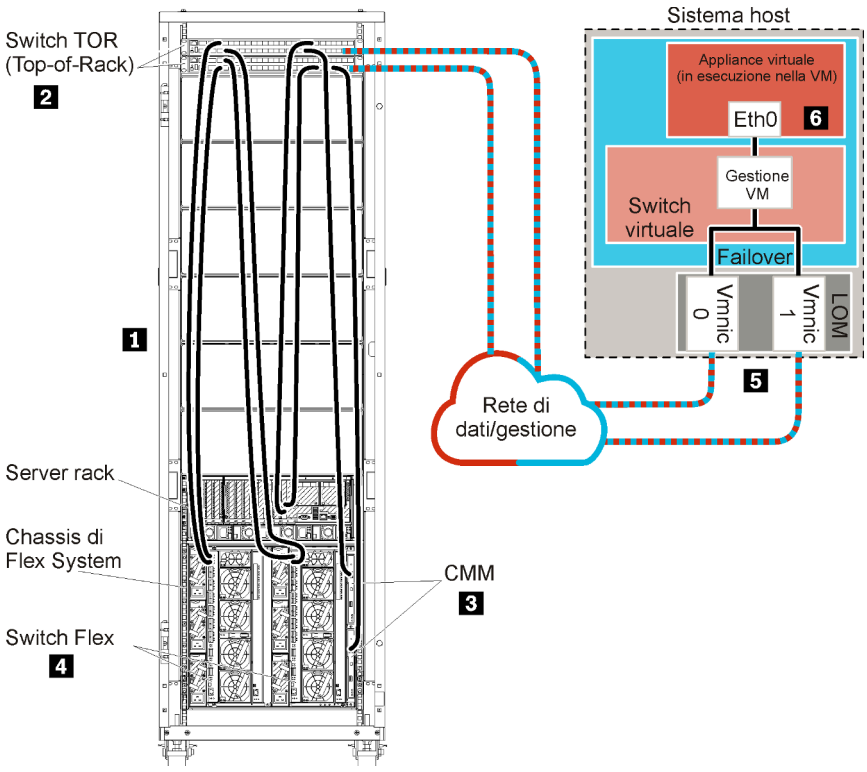


Figura 8. Esempio di topologia della rete di gestione e di dati Single per un'appliance virtuale

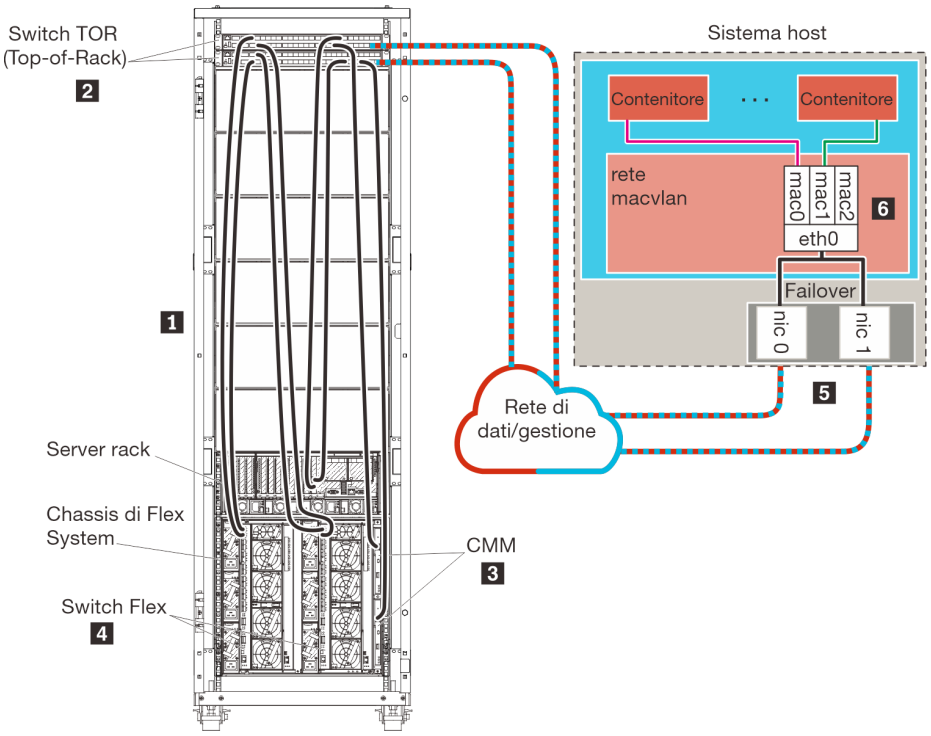


Figura 9. Esempio di topologia della rete di gestione e di dati Single per i contenitori

Importante: È possibile configurare XClarity Administrator in qualsiasi sistema che soddisfi i requisiti per XClarity Administrator, incluso un server gestito. Se si utilizza un server gestito per l'host XClarity Administrator:

- È necessario implementare una topologia di reti virtualmente separate di dati e gestione o una topologia di rete singola di dati e gestione.
- Non è possibile utilizzare XClarity Administrator per applicare aggiornamenti firmware al server gestito. Anche se il firmware viene applicato solo parzialmente con attivazione immediata, XClarity Administrator forza il riavvio del server di destinazione, determinando di conseguenza anche il riavvio di XClarity Administrator. Se gli aggiornamenti vengono applicati con attivazione posticipata, solo parte del firmware viene applicata al riavvio dell'host XClarity Administrator.
- Se si utilizza un server in uno chassis di Flex System, accertarsi che il server sia configurato per l'accensione automatica. È possibile impostare questa opzione dall'interfaccia Web CMM facendo clic su **Gestione chassis → Nodi di elaborazione**, quindi selezionando il server e **Accensione automatica** per **Modalità accensione automatica**.

Se si desidera installare XClarity Administrator per gestire lo chassis e i server rack esistenti già configurati, procedere al Passaggio 5: installare e configurare l'host.

Per ulteriori informazioni sulla pianificazione di questa topologia, incluse le informazioni sulle impostazioni di rete e sulle configurazioni Eth1 e Eth0, vedere Rete singola di dati e gestione.

Passaggio 1: cablare lo chassis, i server rack e l'host Lenovo XClarity Administrator agli switch TOR (Top-of-Rack)

Cablare lo chassis, i server rack e l'host XClarity Administrator agli switch TOR (Top-of-Rack) per consentire la comunicazione tra i dispositivi e la rete.

Procedura

Cablare ciascuno switch Flex e CMM in ogni chassis, in ogni server rack e nell'host XClarity Administrator a entrambi gli switch TOR (Top-of-Rack). È possibile scegliere qualsiasi porta negli switch TOR (Top-of-Rack).

La seguente figura rappresenta un esempio che illustra il cablaggio dallo chassis (Switch Flex e CMM), dai server rack e dall'host XClarity Administrator agli switch TOR (Top-of-Rack).

Nota: Questa figura non rappresenta tutte le opzioni di cablaggio che potrebbero essere necessarie per l'ambiente. La figura mostra solo i requisiti delle opzioni di cablaggio per server rack, switch rack, switch Flex e CMM in correlazione per configurare una rete singola di dati/gestione.

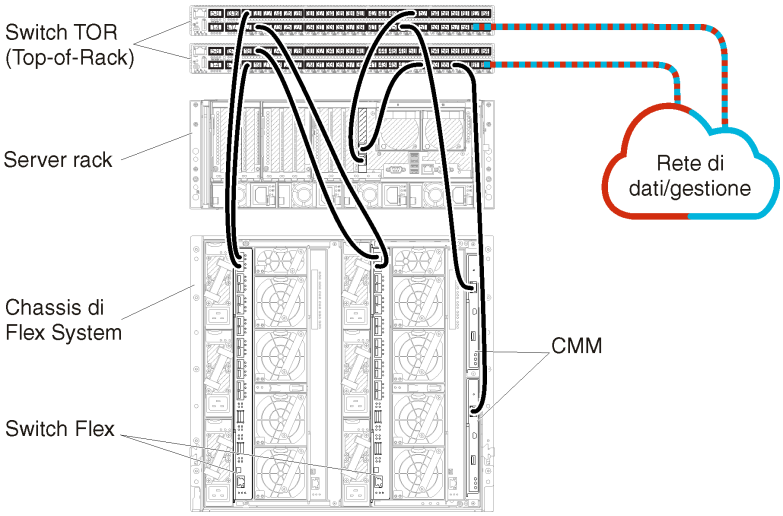


Figura 10. Esempio di cablaggio per una rete singola di dati e gestione

Passaggio 2: configurare switch TOR (Top-of-Rack)

Configurare switch TOR (Top-of-Rack).

Prima di iniziare

Oltre ai requisiti tipici di configurazione per gli switch TOR (Top-of-Rack), accertarsi che siano abilitate tutte le porte appropriate, incluse le porte esterne agli Switch Flex, ai server rack e alla rete e le porte interne al CMM, ai server rack e alla rete.

Procedura

I passaggi di configurazione possono variare a seconda del tipo di switch rack installati.

Per informazioni sulla configurazione di switch TOR (Top-of-Rack) Lenovo, vedere Switch rack nella documentazione online di System x. Se è installato un altro switch TOR (Top-of-Rack), fare riferimento alla documentazione fornita con lo switch.

Passaggio 3: configurare CMM (Chassis Management Module)

Configurare il CMM (Chassis Management Module) primario nello chassis per gestire tutti i dispositivi al suo interno.

Informazioni su questa attività

Per informazioni dettagliate sulla configurazione di un CMM, vedere Configurazione dei componenti dello chassis nella documentazione online di Flex System.

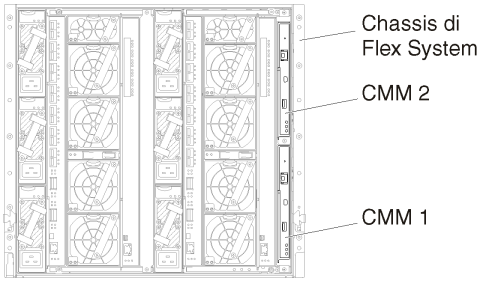
Fare inoltre riferimento ai passaggi 4.1 - 4.5 nel poster delle istruzioni fornito con lo chassis.

Procedura

Per configurare il CMM, attenersi alla procedura descritta di seguito.

Se sono installati due CMM, configurare solo il CMM *primario*, che sincronizza automaticamente la configurazione con il CMM in standby.

Passo 1. Collegare un cavo Ethernet dal CMM nel vano 1 alla workstation client per creare un collegamento diretto.



Per collegarsi al CMM per la prima volta, potrebbe essere necessario modificare le proprietà del protocollo IP nella workstation client.

Importante: Accertarsi che la sottorete della workstation client sia la stessa della sottorete del CMM. Il valore predefinito della sottorete CMM è 255.255.255.0. L'indirizzo IP scelto per la workstation client deve trovarsi nella stessa rete del CMM (ad esempio, 192.168.70.0 - 192.168.70.24).

Passo 2. Per avviare l'interfaccia di gestione CMM, aprire un browser Web nella workstation client e indirizzarla all'indirizzo IP del CMM.

Nota:

- Accertarsi di utilizzare una connessione sicura e includere **https** nell'URL (ad esempio, https://192.168.70.100). Se non si include https, verrà visualizzato un errore di pagina non trovata.
- Se si utilizza l'indirizzo IP predefinito 192.168.70.100, l'interfaccia di gestione CMM potrebbe richiedere alcuni minuti per essere disponibile. Questo ritardo si verifica a causa dei tentativi del CMM di ottenere un indirizzo DHCP per due minuti prima di eseguire il fallback all'indirizzo statico predefinito.

Passo 3. Eseguire il login all'interfaccia di gestione CMM utilizzando l'ID utente `USERID` e la password `PASSWORD` predefiniti. Dopo aver eseguito il login, sarà necessario modificare la password predefinita.

Passo 4. Completare la procedura guidata Configurazione iniziale del CMM per specificare i dettagli per l'ambiente. La procedura guidata Configurazione iniziale include le seguenti opzioni:

- Visualizzare l'inventario e lo stato dello chassis.
- Importare la configurazione da un file esistente.
- Configurare le impostazioni CMM generiche,
- Configurare la data e l'ora del CMM.

Suggerimento: quando si installa XClarity Administrator, configurare XClarity Administrator e tutti gli chassis gestiti da XClarity Administrator per l'utilizzo di un server NTP.

- Configurare le informazioni IP del CMM.
- Configurare i criteri di sicurezza del CMM.
- Configurare il DNS (Domain Name System).
- Configurare i server d'inoltro degli eventi.

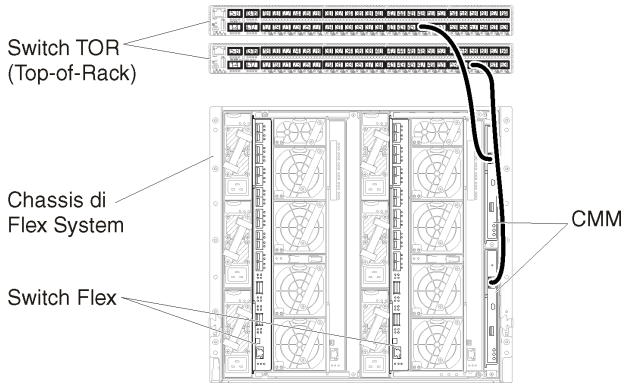
Passo 5. Dopo aver salvato le impostazioni della procedura guidata e applicato le modifiche, configurare gli indirizzi IP per tutti i componenti nello chassis.

Fare riferimento al passaggio 4.6 nel poster delle istruzioni fornito con lo chassis.

Nota: È necessario reimpostare il processore di gestione del sistema per ciascun nodo di elaborazione e riavviare gli switch Flex per visualizzare i nuovi indirizzi IP.

Passo 6. Riavviare il CMM mediante la relativa interfaccia di gestione.

Passo 7. Al riavvio del CMM, collegare un cavo dalla porta Ethernet nel CMM alla rete.



Passo 8. Eseguire il login all'interfaccia di gestione CMM mediante il nuovo indirizzo IP.

Al termine

È inoltre possibile configurare il CMM per il supporto della ridondanza. Utilizzare il sistema di guida CMM per ottenere ulteriori informazioni sui campi disponibili in ciascuna delle seguenti pagine.

- Configurare il failover per il CMM in caso si verifichi un guasto hardware nel CMM primario. Dall'interfaccia di gestione CMM, fare clic su **Gestione del modulo di gestione → Proprietà → Failover avanzato**.
- Configurare il failover come risultato di un problema di rete (Uplink). Dall'interfaccia di gestione CMM, fare clic su **Gestione del modulo di gestione → Rete**, selezionare la scheda **Ethernet** e fare clic su **Ethernet avanzata**. Come requisito minimo, verificare di selezionare **Failover in caso di perdita del collegamento fisico alla rete**.

Passaggio 4: configurare Switch Flex

Configurare Switch Flex (moduli I/O) in ogni chassis.

Prima di iniziare

Accertarsi che siano abilitate tutte le porte appropriate, incluse le porte esterne dallo switch Flex allo switch TOR (Top-of-Rack) e le porte interne al CMM.

Se gli switch Flex sono configurati per ottenere impostazioni di rete dinamiche (indirizzo IP, maschera di rete, gateway e indirizzo DNS) su DHCP, accertarsi che tali impostazioni siano coerenti (ad esempio, verificare che gli indirizzi IP si trovino nella stessa sottorete del CMM).

Importante: Per ogni chassis di Flex System, verificare che il tipo di fabric della scheda di espansione in ciascun server nello chassis sia compatibile con il tipo di fabric di tutti gli switch Flex nello stesso chassis. Se, ad esempio, in uno chassis sono installati switch Ethernet, tutti i server al suo interno devono disporre di connettività Ethernet tramite il connettore LAN su scheda madre o una scheda di espansione Ethernet. Per ulteriori informazioni sulla configurazione di switch Flex, vedere Configurazione dei moduli I/O nella documentazione online di Flex Systems.

Procedura

I passaggi di configurazione possono variare a seconda del tipo di Switch Flex installato. Per ulteriori informazioni su ogni Switch Flex supportato, vedere Switch di rete Flex System nella documentazione online di Flex Systems.

In genere, è necessario configurare gli switch Flex nei relativi vani 1 e 2.

Suggerimento: il vano 2 dello switch Flex è il terzo vano del modulo nella parte posteriore dello chassis.

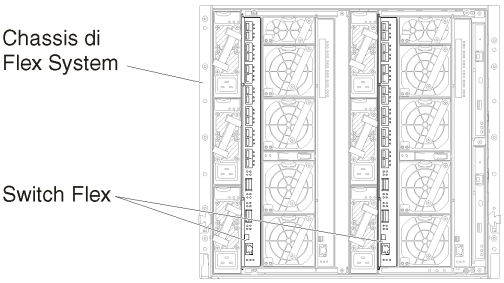


Figura 11. Posizioni degli Switch Flex in uno chassis

Passaggio 5: installare e configurare l'host

È possibile installare Docker su qualsiasi server che soddisfi i requisiti per Lenovo XClarity Administrator.

Prima di iniziare

È possibile utilizzare Docker Datacenter per configurare un ambiente ad alta disponibilità per i contenitori XClarity Administrator che vengono eseguiti in Docker Engine. Per ulteriori informazioni sull'alta disponibilità di Docker Datacenter, vedere Pagina Web Architettura e app ad alta disponibilità con Docker Datacenter.

Accertarsi che l'host soddisfi i prerequisiti definiti in Prerequisiti hardware e software.

Accertarsi che il sistema host si trovi nella stessa rete dei dispositivi che si desidera gestire.

Importante: È possibile configurare XClarity Administrator in qualsiasi sistema che soddisfi i requisiti per XClarity Administrator, incluso un server gestito. Se si utilizza un server gestito per l'host XClarity Administrator:

- È necessario implementare una topologia di reti virtualmente separate di dati e gestione o una topologia di rete singola di dati e gestione.
- Non è possibile utilizzare XClarity Administrator per applicare aggiornamenti firmware al server gestito. Anche se il firmware viene applicato solo parzialmente con attivazione immediata, XClarity Administrator forza il riavvio del server di destinazione, determinando di conseguenza anche il riavvio di XClarity Administrator. Se gli aggiornamenti vengono applicati con attivazione posticipata, solo parte del firmware viene applicata al riavvio dell'host XClarity Administrator.

- Se si utilizza un server in uno chassis di Flex System, accertarsi che il server sia configurato per l'accensione automatica. È possibile impostare questa opzione dall'interfaccia Web CMM facendo clic su **Gestione chassis → Nodi di elaborazione**, quindi selezionando il server e **Accensione automatica** per **Modalità accensione automatica**.

Procedura

Installare e configurare Docker nell'host seguendo le istruzioni fornite con la distribuzione Docker.

Passaggio 6. Installare e configurare un contenitore XClarity Administrator

Installare e configurare l'Lenovo XClarity Administrator nel contenitore sull'host Docker appena installato.

Prima di iniziare

Verificare che il sistema host soddisfi i requisiti minimi hardware e software (vedere Prerequisiti hardware e software).

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

Accertarsi che il sistema host si trovi nella stessa rete dei dispositivi che si desidera gestire.

Verificare che il sistema operativo host e XClarity Administrator utilizzino lo stesso server NTP.

XClarity Administrator consente di utilizzare un nome personalizzato per la rete di gestione di dati e hardware, oltre che per quella di distribuzione del sistema operativo (vedere Configurazioni di rete). In questo esempio nella procedura seguente viene utilizzato eth0.

Verificare che una rete macvlan sia caricata nel kernel del sistema host. Per verificare se la rete è caricata, utilizzare il comando **lsmod | grep macvlan**. Per caricare macvlan nel kernel, eseguire il comando **modprobe macvlan**.

Accertarsi di utilizzare un nome univoco e un indirizzo IP per ogni contenitore quando si eseguono più contenitori XClarity Administrator sullo stesso host.

Se si intende gestire ThinkServer e altri dispositivi legacy, accertarsi che Docker sia abilitato per supportare IPv6.

1. Modificare il file /etc/docker/daemon.json, impostare la chiave **ipv6** su true e impostare la chiave **fixed-cidr-v6** sulla sottorete IPv6. Di seguito viene riportato un file daemon di esempio.
```
{
   "ipv6": true,
   "fixed-cidr-v6": "2001:db8:1::/64",
   "experimental": true,
   "ip6tables": true
}
```
2. Ricaricare il file di configurazione Docker eseguendo il comando seguente.
```
systemctl reload docker
```

Nota: XClarity Administrator *non* viene eseguito come contenitore con privilegi.

Procedura

Per installare un contenitore XClarity Administrator utilizzando Docker Compose, completare la seguente procedura.

Passo 1. Scaricare l'immagine, il file di ambiente e il file YAML dell'appliance virtuale XClarity Administrator dalla Pagina Web di download di XClarity Administrator in una workstation client. Accedere al sito Web, quindi utilizzare la chiave di accesso fornita per scaricare l'immagine.

Passo 2. Importare l'immagine del contenitore XClarity Administrator nell'host docker, utilizzando il comando seguente.
```
docker load -i lnvgy_sw_lxca_<ver>_anyos_noarch.tar.gz
```

Passo 3. Modificare il file `docker_compose.env` e aggiornare le variabili di ambiente che seguono.

- **CONTAINER_NAME**. Nome univoco del contenitore, utilizzato per creare volumi docker per ogni istanza di XClarity Administrator (ad esempio, `CONTAINER_NAME=LXCA-203`)
- **INDIRIZZO**. Indirizzo IPv4 statico per il contenitore (ad esempio, `ADDRESS=192.0.2.0`)
- **BACKUP_MOUNT**. (Facoltativo) Percorso per la condivisione remota che può essere utilizzata per archiviare i backup di XClarity Administrator. Il percorso deve essere: `/mnt/backup_share`.
- **FIRMWARE_MOUNT**. (Facoltativo) Percorso per la condivisione remota che può essere utilizzata come repository remoto per gli aggiornamenti firmware. Il percorso deve essere: `/mnt/fw_share`.

Di seguito viene riportato un file di ambiente.
```
CONTAINER_NAME="LXCA-203"
ADDRESS="192.0.2.0"
BACKUP_MOUNT="/mnt/backup_share"
FIRMWARE_MOUNT="/mnt/fw_share"
```

Passo 4. Modificare il file `docker_compose.yml` e aggiornare le proprietà che seguono.

- Impostare la proprietà **image** con il nome del file dell'immagine di installazione utilizzato nel passaggio 2.

  Nota: È possibile modificare il nome del file di immagine (ad esempio, in "più recente") utilizzando il comando `docker tag`.
- Se si desidera utilizzare la condivisione remota come repository firmware remoto per archiviare i backup di XClarity Administrator impostare il punto di montaggio dell'host per ciascuna condivisione remota nella proprietà **volumi**.
- Impostare la proprietà **dns** sull'indirizzo IP dei server DNS.
- Il contenitore condivide il pool di risorse di memoria e processore disponibili per l'host. Facoltativamente definire i limiti sull'utilizzo delle risorse impostando le proprietà **cpus** e **memoria**.
- Impostare la proprietà **principale** sul nome dell'interfaccia di rete del sistema host da utilizzare come interfaccia principale per l'interfaccia macvlan nel contenitore. Questa interfaccia deve disporre dell'accesso diretto alla sottorete assegnata al contenitore.
- Impostare la **sottorete** e il **gateway** in base alla topologia di rete. In genere, la sottorete e il gateway sono per la rete di gestione, a cui appartiene ${ADDRESS}.
- Se si desidera supportare IPv6, impostare la proprietà **enable_ipv6** su true, impostare la proprietà **ipv6_address** sull'indirizzo IPv6 e aggiungere un'altra serie di proprietà di **sottorete** e **gateway** in base alla topologia di rete (generalmente per la rete di gestione a cui appartiene l'indirizzo IPv6).

Nota: XClarity Administrator utilizza macvlan per configurare la rete dei contenitori. Per ulteriori informazioni, consultare la sezione Utilizzo della pagina Web delle reti macvlan

Di seguito è riportato un file YML di esempio con IPv6 abilitato.

```
version: '3.8'

services:

  lxca:
    image: lenovo/lxca:4.1.0-124
    container_name: ${CONTAINER_NAME}
    tty: true
    stop_grace_period: 60s
    volumes:
      #bind mount example
      - /home/<HOST_MOUNT_POINT_FOR_BACKUP>:${BACKUP_MOUNT}
      - /home/<HOST_MOUNT_POINT_FOR_FW_SHARE>:${FIRMWARE_MOUNT}
      #docker volume mount
      - data:/opt/lenovo/lxca/data
      - postgresql:/var/lib/postgresql
      - log:/var/log
      - confluent-etc:/etc/confluent
      - confluent-log:/var/log/confluent
      - confluent:/var/lib/confluent
      - propconf:/opt/lenovo/lxca/bin/conf
      - ssh:/etc/ssh
      - xcat:/etc/xcat
    networks:
      lan:
        ipv4_address: ${ADDRESS}
        ipv6_address: "2001:8003:7d51:2003::2"
    dns:
      - 192.0.2.10
      - 192.0.2.11
    deploy:
      resources:
        limits:
          cpus: "2.0"
          memory: "8g"

volumes:
  data:
    name: ${CONTAINER_NAME}-data
  postgresql:
    name: ${CONTAINER_NAME}-postgresql
  log:
    name: ${CONTAINER_NAME}-log
  confluent-etc:
    name: ${CONTAINER_NAME}-confluent-etc
  confluent-log:
    name: ${CONTAINER_NAME}-confluent-log
  confluent:
    name: ${CONTAINER_NAME}-confluent
  propconf:
    name: ${CONTAINER_NAME}-propconf
  ssh:
    name: ${CONTAINER_NAME}-ssh
  xcat:
    name: ${CONTAINER_NAME}-xcat

networks:
  lan:
    name: lan
    driver: macvlan
    enable_ipv6: true
```

```
driver_opts:
  parent: eth0
ipam:
  config:
    - subnet: 192.0.0.0/19
      gateway: 192.0.30.1
    - subnet: "2001:8003:7d51:2000::/80"
      gateway: "2001:8003:7d51:2000::1"
```

Passo 5. Distribuire l'immagine in docker, utilizzando il comando seguente, dove <*ENV_FILENAME*> è il nome del file delle variabili d'ambiente creato nel passaggio 2.
COMPOSE_HTTP_TIMEOUT=300 `docker-compose -p ${CONTAINER_NAME} --env-file <ENV_FILENAME> up -d`

Al termine

Eseguire il login e configurare XClarity Administrator (vedere Primo accesso all'interfaccia Web di Lenovo XClarity Administrator e Configurazione di Lenovo XClarity Administrator).

Dati separati fisicamente e reti di gestione

In questa topologia, la rete dei dati e la rete di gestione sono fisicamente separate. La gestione delle comunicazioni tra Lenovo XClarity Administrator e la rete si verifica sull'interfaccia di rete Eth0 sull'host. Le comunicazioni dei dati si verificano sull'interfaccia di rete Eth1.

Prima di iniziare

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

Accertarsi che sia installato il firmware minimo richiesto in ciascun dispositivo che si desidera gestire mediante XClarity Administrator. È possibile trovare i livelli minimi di firmware richiesti sulle Supporto XClarity Administrator - Pagina Web sulla compatibilità facendo clic sulla scheda **Compatibilità** e quindi sul collegamento per i tipi di dispositivi appropriati.

Importante: 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 viene utilizzato DHCP, verificare che le modifiche dell'indirizzo IP siano minime.

Informazioni su questa attività

La seguente figura mostra una modalità di configurazione dell'ambiente in cui la rete di dati e la rete di gestione sono fisicamente diverse. I numeri nella figura corrispondono ai passaggi numerati nelle seguenti sezioni.

Nota: Questa figura non rappresenta tutte le opzioni di cablaggio che potrebbero essere necessarie per l'ambiente. La figura mostra solo i requisiti delle opzioni di cablaggio per gli switch Flex, i CMM e i server rack in correlazione per configurare reti fisicamente separate di dati e gestione.

Suggerimento: anziché configurare due switch fisici collegati a ciascuna rete per ridondanza (per un totale di quattro switch), è possibile configurare un singolo switch fisico collegato a ciascuna rete (per un totale di due switch). In tal caso, ogni switch sarebbe collegato a entrambe le reti e verrebbero implementate due VLAN, una per la rete di dati e una per la rete di gestione, per distinguere il traffico dati.

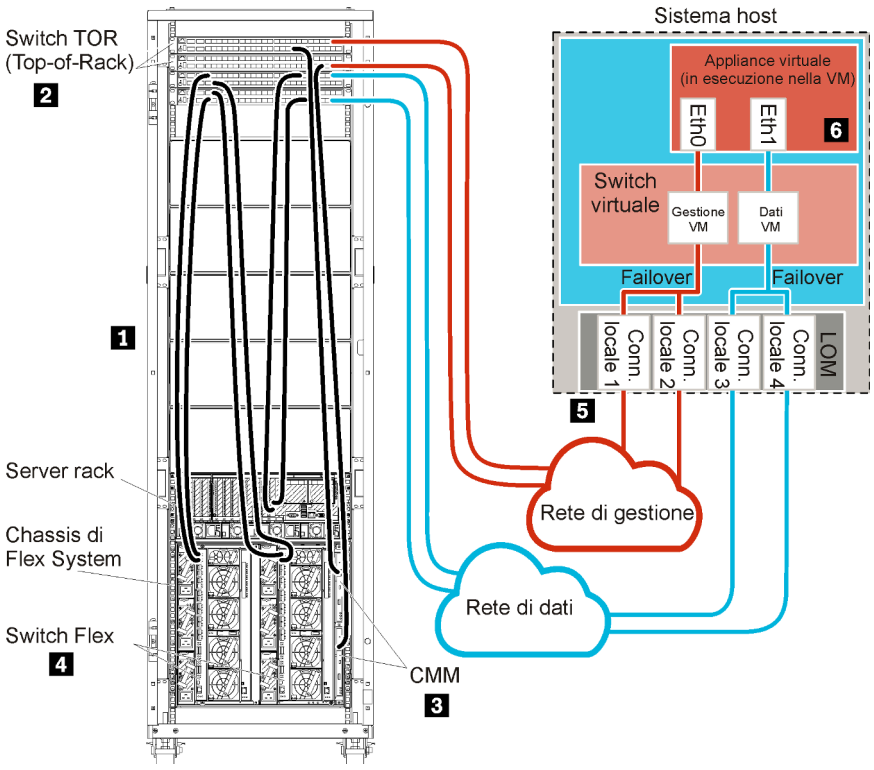


Figura 12. Esempio di topologia della rete di gestione e di dati separati fisicamente per un'appliance virtuale

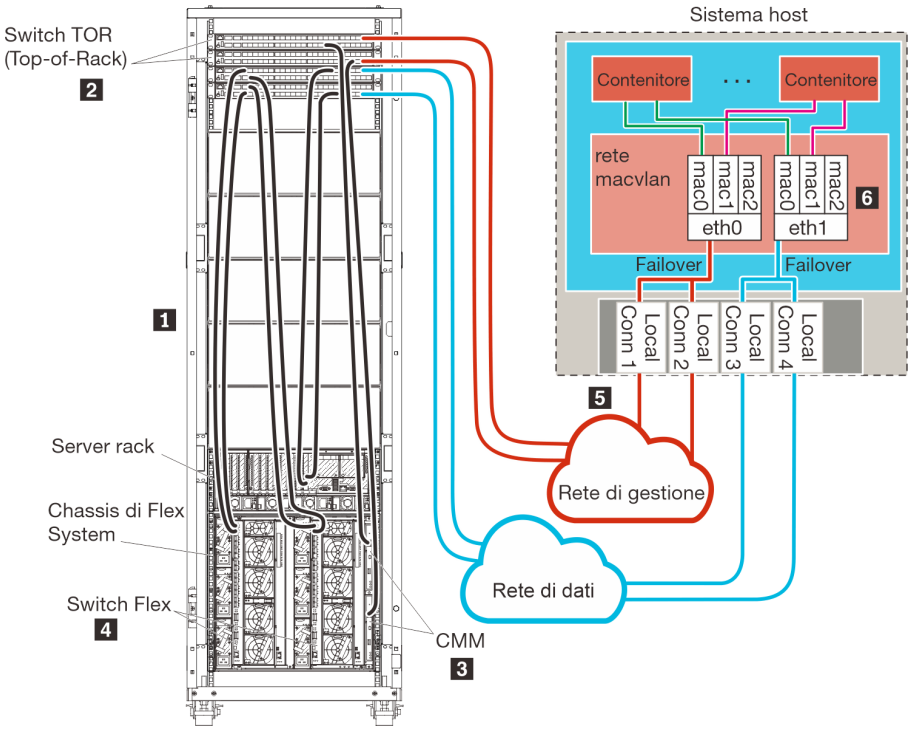


Figura 13. Esempio di topologia della rete di gestione e di dati separati fisicamente per i contenitori

Se si desidera installare XClarity Administrator per gestire lo chassis e i server rack esistenti già configurati, procedere al Passaggio 5: installare e configurare l'host.

Per ulteriori informazioni sulla pianificazione di questa topologia, incluse le informazioni sulle impostazioni di rete e sulle configurazioni Eth1 e Eth0, vedere Rete fisicamente separata di dati e gestione.

Passaggio 1: cablare lo chassis, i server rack e l'host Lenovo XClarity Administrator agli switch TOR (Top-of-Rack)

Cablare lo chassis, i server rack e l'host XClarity Administrator agli switch TOR (Top-of-Rack)per consentire la comunicazione tra i dispositivi e le reti.

Procedura

Cablare ciascuno switch Flex e CMM in ogni chassis, in ogni server rack e nell'host XClarity Administrator a entrambi gli switch TOR (Top-of-Rack). È possibile scegliere qualsiasi porta negli switch TOR (Top-of-Rack).

La seguente figura rappresenta un esempio che illustra il cablaggio dallo chassis (Switch Flex e CMM), dai server rack e dall'host XClarity Administrator agli switch TOR (Top-of-Rack).

Nota: Questa figura non rappresenta tutte le opzioni di cablaggio che potrebbero essere necessarie per l'ambiente. La figura mostra solo i requisiti delle opzioni di cablaggio per gli switch Flex, i CMM e i server rack in correlazione per configurare reti fisicamente separate di dati e gestione.

Suggerimento: anziché configurare due switch fisici collegati a ciascuna rete per ridondanza (per un totale di quattro switch), è possibile configurare un singolo switch fisico collegato a ciascuna rete (per un totale di due switch). In tal caso, ogni switch sarebbe collegato a entrambe le reti e verrebbero implementate due VLAN, una per la rete di dati e una per la rete di gestione, per distinguere il traffico dati.

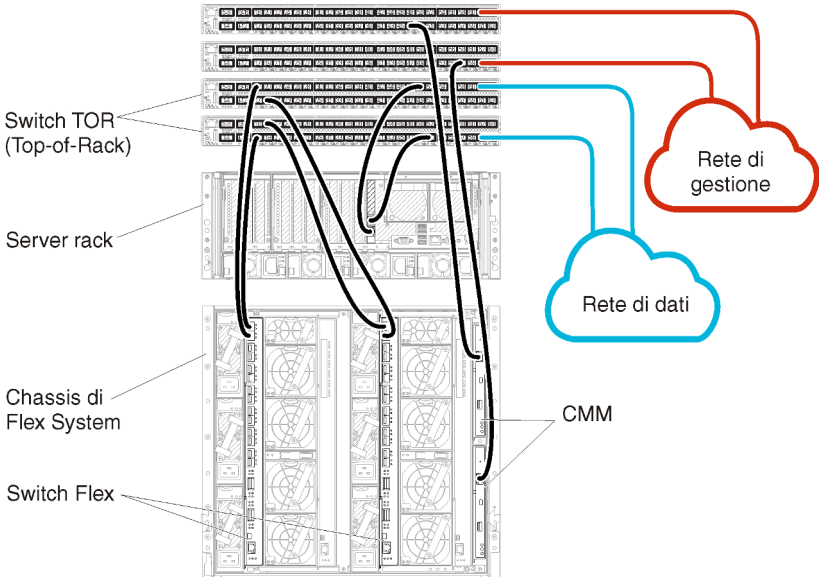


Figura 14. Esempio di cablaggio per reti fisicamente separate di dati e gestione

Passaggio 2: configurare switch TOR (Top-of-Rack)

Configurare switch TOR (Top-of-Rack).

Prima di iniziare

Oltre ai requisiti tipici di configurazione per gli switch TOR (Top-of-Rack), accertarsi che siano abilitate tutte le porte appropriate, incluse le porte esterne agli Switch Flex, ai server rack e alla rete e le porte interne al CMM, ai server rack e alla rete.

Procedura

I passaggi di configurazione possono variare a seconda del tipo di switch rack installati.

Per informazioni sulla configurazione di switch TOR (Top-of-Rack) Lenovo, vedere Switch rack nella documentazione online di System x. Se è installato un altro switch TOR (Top-of-Rack), fare riferimento alla documentazione fornita con lo switch.

Passaggio 3: configurare CMM (Chassis Management Module)

Configurare il CMM (Chassis Management Module) primario nello chassis per gestire tutti i dispositivi al suo interno.

Informazioni su questa attività

Per informazioni dettagliate sulla configurazione di un CMM, vedere Configurazione dei componenti dello chassis nella documentazione online di Flex System.

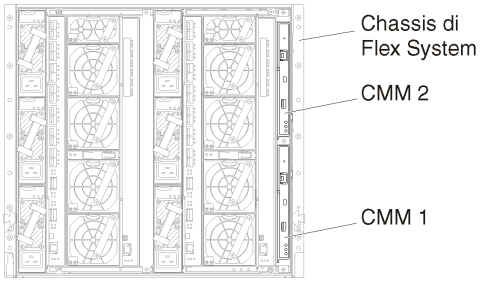
Fare inoltre riferimento ai passaggi 4.1 - 4.5 nel poster delle istruzioni fornito con lo chassis.

Procedura

Per configurare il CMM, attenersi alla procedura descritta di seguito.

Se sono installati due CMM, configurare solo il CMM *primario*, che sincronizza automaticamente la configurazione con il CMM in standby.

Passo 1. Collegare un cavo Ethernet dal CMM nel vano 1 alla workstation client per creare un collegamento diretto.



Per collegarsi al CMM per la prima volta, potrebbe essere necessario modificare le proprietà del protocollo IP nella workstation client.

Importante: Accertarsi che la sottorete della workstation client sia la stessa della sottorete del CMM. Il valore predefinito della sottorete CMM è 255.255.255.0. L'indirizzo IP scelto per la workstation client deve trovarsi nella stessa rete del CMM (ad esempio, 192.168.70.0 - 192.168.70.24).

Passo 2. Per avviare l'interfaccia di gestione CMM, aprire un browser Web nella workstation client e indirizzarla all'indirizzo IP del CMM.

Nota:

- Accertarsi di utilizzare una connessione sicura e includere **https** nell'URL (ad esempio, https://192.168.70.100). Se non si include https, verrà visualizzato un errore di pagina non trovata.
- Se si utilizza l'indirizzo IP predefinito 192.168.70.100, l'interfaccia di gestione CMM potrebbe richiedere alcuni minuti per essere disponibile. Questo ritardo si verifica a causa dei tentativi del CMM di ottenere un indirizzo DHCP per due minuti prima di eseguire il fallback all'indirizzo statico predefinito.

Passo 3. Eseguire il login all'interfaccia di gestione CMM utilizzando l'ID utente `USERID` e la password `PASSWORD` predefiniti. Dopo aver eseguito il login, sarà necessario modificare la password predefinita.

Passo 4. Completare la procedura guidata Configurazione iniziale del CMM per specificare i dettagli per l'ambiente. La procedura guidata Configurazione iniziale include le seguenti opzioni:

- Visualizzare l'inventario e lo stato dello chassis.
- Importare la configurazione da un file esistente.
- Configurare le impostazioni CMM generiche,
- Configurare la data e l'ora del CMM.

  Suggerimento: quando si installa XClarity Administrator, configurare XClarity Administrator e tutti gli chassis gestiti da XClarity Administrator per l'utilizzo di un server NTP.
- Configurare le informazioni IP del CMM.
- Configurare i criteri di sicurezza del CMM.
- Configurare il DNS (Domain Name System).
- Configurare i server d'inoltro degli eventi.

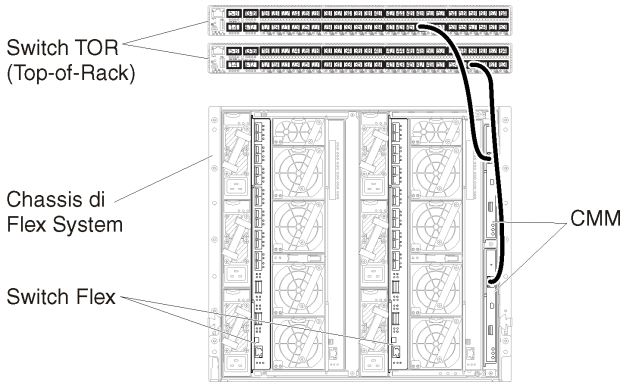
Passo 5. Dopo aver salvato le impostazioni della procedura guidata e applicato le modifiche, configurare gli indirizzi IP per tutti i componenti nello chassis.

Fare riferimento al passaggio 4.6 nel poster delle istruzioni fornito con lo chassis.

Nota: È necessario reimpostare il processore di gestione del sistema per ciascun nodo di elaborazione e riavviare gli switch Flex per visualizzare i nuovi indirizzi IP.

Passo 6. Riavviare il CMM mediante la relativa interfaccia di gestione.

Passo 7. Al riavvio del CMM, collegare un cavo dalla porta Ethernet nel CMM alla rete.



Passo 8. Eseguire il login all'interfaccia di gestione CMM mediante il nuovo indirizzo IP.

Al termine

È inoltre possibile configurare il CMM per il supporto della ridondanza. Utilizzare il sistema di guida CMM per ottenere ulteriori informazioni sui campi disponibili in ciascuna delle seguenti pagine.

- Configurare il failover per il CMM in caso si verifichi un guasto hardware nel CMM primario. Dall'interfaccia di gestione CMM, fare clic su **Gestione del modulo di gestione → Proprietà → Failover avanzato**.
- Configurare il failover come risultato di un problema di rete (Uplink). Dall'interfaccia di gestione CMM, fare clic su **Gestione del modulo di gestione → Rete**, selezionare la scheda **Ethernet** e fare clic su **Ethernet avanzata**. Come requisito minimo, verificare di selezionare **Failover in caso di perdita del collegamento fisico alla rete**.

Passaggio 4: configurare Switch Flex

Configurare gli Switch Flex in ogni chassis.

Prima di iniziare

Accertarsi che siano abilitate tutte le porte appropriate, incluse le porte esterne dallo switch Flex allo switch TOR (Top-of-Rack) e le porte interne al CMM.

Se gli switch Flex sono configurati per ottenere impostazioni di rete dinamiche (indirizzo IP, maschera di rete, gateway e indirizzo DNS) su DHCP, accertarsi che tali impostazioni siano coerenti (ad esempio, verificare che gli indirizzi IP si trovino nella stessa sottorete del CMM).

Importante: Per ogni chassis di Flex System, verificare che il tipo di fabric della scheda di espansione in ciascun server nello chassis sia compatibile con il tipo di fabric di tutti gli switch Flex nello stesso chassis. Se, ad esempio, in uno chassis sono installati switch Ethernet, tutti i server al suo interno devono disporre di connettività Ethernet tramite il connettore LAN su scheda madre o una scheda di espansione Ethernet. Per ulteriori informazioni sulla configurazione di switch Flex, vedere Configurazione dei moduli I/O nella documentazione online di Flex Systems.

Procedura

I passaggi di configurazione possono variare a seconda del tipo di Switch Flex installato. Per ulteriori informazioni su ogni Switch Flex supportato, vedere Switch di rete Flex System nella documentazione online di Flex Systems.

In genere, è necessario configurare gli switch Flex nei relativi vani 1 e 2.

Suggerimento: il vano 2 dello switch Flex è il terzo vano del modulo nella parte posteriore dello chassis.

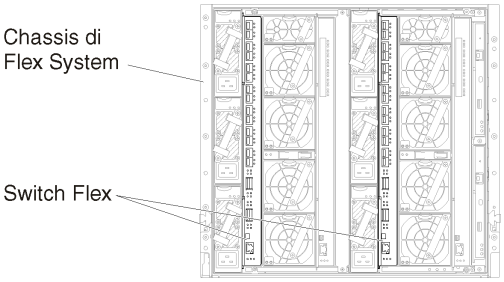


Figura 15. Posizioni degli Switch Flex in uno chassis

Passaggio 5: installare e configurare l'host

È possibile installare Docker su qualsiasi server che soddisfi i requisiti per Lenovo XClarity Administrator

Prima di iniziare

È possibile utilizzare Docker Datacenter per configurare un ambiente ad alta disponibilità per i contenitori XClarity Administrator che vengono eseguiti in Docker Engine. Per ulteriori informazioni sull'alta disponibilità di Docker Datacenter, vedere Pagina Web Architettura e app ad alta disponibilità con Docker Datacenter.

Accertarsi che l'host soddisfi i prerequisiti definiti in Prerequisiti hardware e software.

Accertarsi che il sistema host si trovi nella stessa rete dei dispositivi che si desidera gestire.

Importante: È possibile configurare XClarity Administrator in qualsiasi sistema che soddisfi i requisiti per XClarity Administrator, incluso un server gestito. Se si utilizza un server gestito per l'host XClarity Administrator:

- È necessario implementare una topologia di reti virtualmente separate di dati e gestione o una topologia di rete singola di dati e gestione.
- Non è possibile utilizzare XClarity Administrator per applicare aggiornamenti firmware al server gestito. Anche se il firmware viene applicato solo parzialmente con attivazione immediata, XClarity Administrator forza il riavvio del server di destinazione, determinando di conseguenza anche il riavvio di XClarity Administrator. Se gli aggiornamenti vengono applicati con attivazione posticipata, solo parte del firmware viene applicata al riavvio dell'host XClarity Administrator.
- Se si utilizza un server in uno chassis di Flex System, accertarsi che il server sia configurato per l'accensione automatica. È possibile impostare questa opzione dall'interfaccia Web CMM facendo clic su **Gestione chassis → Nodi di elaborazione**, quindi selezionando il server e **Accensione automatica** per **Modalità accensione automatica**.

Procedura

Installare e configurare Docker nell'host seguendo le istruzioni fornite con la distribuzione Docker.

Passaggio 6: installare e configurare XClarity Administrator

Installare e configurare l'Lenovo XClarity Administrator nel contenitore sull'host Docker appena installato.

Prima di iniziare

Verificare che il sistema host soddisfi i requisiti minimi hardware e software (vedere Prerequisiti hardware e software).

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

Accertarsi che il sistema host si trovi nella stessa rete dei dispositivi che si desidera gestire.

Verificare che il sistema operativo host e XClarity Administrator utilizzino lo stesso server NTP.

XClarity Administrator consente di utilizzare un nome personalizzato per la rete di gestione di dati e hardware, oltre che per quella di distribuzione del sistema operativo (vedere Configurazioni di rete). In questo esempio nella procedura seguente viene utilizzato eth0.

XClarity Administrator consente di utilizzare un nome personalizzato per la rete di gestione di dati e hardware, oltre che per quella di distribuzione del sistema operativo (vedere Configurazioni di rete). In questi esempi nella seguente procedura vengono utilizzati rispettivamente eth0 ed eth1

Verificare che una rete macvlan sia caricata nel kernel del sistema host. Per verificare se la rete è caricata, utilizzare il comando **lsmod | grep macvlan**. Per caricare macvlan nel kernel, eseguire il comando **modprobe macvlan**.

Accertarsi di utilizzare un nome univoco e un indirizzo IP per ogni contenitore quando si eseguono più contenitori XClarity Administrator sullo stesso host.

Se si intende gestire ThinkServer e altri dispositivi legacy, accertarsi che Docker sia abilitato per supportare IPv6.

1. Modificare il file /etc/docker/daemon.json, impostare la chiave **ipv6** su true e impostare la chiave **fixed-cidr-v6** sulla sottorete IPv6. Di seguito viene riportato un file daemon di esempio.
```
{
   "ipv6": true,
   "fixed-cidr-v6": "2001:db8:1::/64",
   "experimental": true,
   "ip6tables": true
}
```
2. Ricaricare il file di configurazione Docker eseguendo il comando seguente.
```
systemctl reload docker
```

Nota: XClarity Administrator *non* viene eseguito come contenitore con privilegi.

Procedura

Per installare un contenitore XClarity Administrator utilizzando Docker Compose, completare la seguente procedura.

Passo 1. Scaricare l'immagine, il file di ambiente e il file YAML dell'appliance virtuale XClarity Administrator dalla Pagina Web di download di XClarity Administrator in una workstation client. Accedere al sito Web, quindi utilizzare la chiave di accesso fornita per scaricare l'immagine.

Passo 2. Importare l'immagine del contenitore XClarity Administrator nell'host docker, utilizzando il comando seguente.
```
docker load -i lnvgy_sw_lxca_<ver>_anyos_noarch.tar.gz
```

Passo 3. Modificare il file `docker_compose.env` e aggiornare le variabili di ambiente che seguono.

- **CONTAINER_NAME**. Nome univoco del contenitore, utilizzato per creare volumi docker per ogni istanza di XClarity Administrator (ad esempio, `CONTAINER_NAME=LXCA-203`)
- **INDIRIZZO**. Indirizzo IPv4 statico per il contenitore (ad esempio, `ADDRESS=192.0.2.0`)
- **BACKUP_MOUNT**. (Facoltativo) Percorso per la condivisione remota che può essere utilizzata per archiviare i backup di XClarity Administrator. Il percorso deve essere: `/mnt/backup_share`.
- **FIRMWARE_MOUNT**. (Facoltativo) Percorso per la condivisione remota che può essere utilizzata come repository remoto per gli aggiornamenti firmware. Il percorso deve essere: `/mnt/fw_share`.

Di seguito viene riportato un file di ambiente.
```
CONTAINER_NAME="LXCA-203"
ADDRESS="192.0.2.0"
BACKUP_MOUNT="/mnt/backup_share"
FIRMWARE_MOUNT="/mnt/fw_share"
```

Passo 4. Modificare il file `docker_compose.yml` e aggiornare le proprietà che seguono.

- Impostare la proprietà **image** con il nome del file dell'immagine di installazione utilizzato nel passaggio 2.

  Nota: È possibile modificare il nome del file di immagine (ad esempio, in "più recente") utilizzando il comando `docker tag`.
- Se si desidera utilizzare la condivisione remota come repository firmware remoto per archiviare i backup di XClarity Administrator impostare il punto di montaggio dell'host per ciascuna condivisione remota nella proprietà **volumi**.

- Impostare la proprietà **dns** sull'indirizzo IP dei server DNS.
- Il contenitore condivide il pool di risorse di memoria e processore disponibili per l'host. Facoltativamente definire i limiti sull'utilizzo delle risorse impostando le proprietà **cpus** e **memoria**.
- Impostare la proprietà **principale** sul nome dell'interfaccia di rete del sistema host da utilizzare come interfaccia principale per l'interfaccia macvlan nel contenitore. Questa interfaccia deve disporre dell'accesso diretto alla sottorete assegnata al contenitore.
- Impostare la **sottorete** e il **gateway** in base alla topologia di rete. In genere, la sottorete e il gateway sono per la rete di gestione, a cui appartiene ${ADDRESS}.
- Se si desidera supportare IPv6, impostare la proprietà **enable_ipv6** su true, impostare la proprietà **ipv6_address** sull'indirizzo IPv6 e aggiungere un'altra serie di proprietà di **sottorete** e **gateway** in base alla topologia di rete (generalmente per la rete di gestione a cui appartiene l'indirizzo IPv6).

Di seguito è riportato un file YML di esempio con IPv6 abilitato.

```
version: '3.8'

services:

  lxca:
    image: lenovo/lxca:4.1.0-124
    container_name: ${CONTAINER_NAME}
    tty: true
    stop_grace_period: 60s
    volumes:
      #bind mount example
      - /home/<HOST_MOUNT_POINT_FOR_BACKUP>:${BACKUP_MOUNT}
      - /home/<HOST_MOUNT_POINT_FOR_FW_SHARE>:${FIRMWARE_MOUNT}
      #docker volume mount
      - data:/opt/lenovo/lxca/data
      - postgresql:/var/lib/postgresql
      - log:/var/log
      - confluent-etc:/etc/confluent
      - confluent-log:/var/log/confluent
      - confluent:/var/lib/confluent
      - propconf:/opt/lenovo/lxca/bin/conf
      - ssh:/etc/ssh
      - xcat:/etc/xcat
    networks:
      lan1:
        ipv4_address: ${ADDRESS}
        ipv6_address: "2001:8003:7d51:2000::2"
      lan2:
        ipv4_address: 192.0.1.3
        ipv6_address: "2001:8003:7d51:2003::2"
    dns:
      - 192.0.40.10
      - 192.0.50.11
    deploy:
      resources:
        limits:
          cpus: "2.0"
          memory: "8g"

volumes:
  data:
    name: ${CONTAINER_NAME}-data
```

```
  postgresql:
    name: ${CONTAINER_NAME}-postgresql
  log:
    name: ${CONTAINER_NAME}-log
  confluent-etc:
    name: ${CONTAINER_NAME}-confluent-etc
  confluent-log:
    name: ${CONTAINER_NAME}-confluent-log
  confluent:
    name: ${CONTAINER_NAME}-confluent
  propconf:
    name: ${CONTAINER_NAME}-propconf
  ssh:
    name: ${CONTAINER_NAME}-ssh
  xcat:
    name: ${CONTAINER_NAME}-xcat

networks:
  lan1:
    name: lan1
    driver: macvlan
    enable_ipv6: true
    driver_opts:
      parent: eno1
    ipam:
      config:
        - subnet: 192.0.0.0/19
          gateway: 192.0.30.1
        - subnet: "2001:8003:7d51:2000::/80"
          gateway: "2001:8003:7d51:2000::1"
  lan2:
    name: lan2
    driver: macvlan
    enable_ipv6: true
    driver_opts:
      parent: virbr0
    ipam:
      config:
        - subnet: 192.0.122.0/24
        - subnet: "2001:8003:7d51:2005::/80"
```

Passo 5. Distribuire l'immagine in docker, utilizzando il comando seguente, dove <*ENV_FILENAME*> è il nome del file delle variabili d'ambiente creato nel passaggio 2.
COMPOSE_HTTP_TIMEOUT=300 `docker-compose -p ${CONTAINER_NAME} --env-file <ENV_FILENAME> up -d`

Al termine

Eseguire il login e configurare XClarity Administrator (vedere Primo accesso all'interfaccia Web di Lenovo XClarity Administrator e Configurazione di Lenovo XClarity Administrator).

Dati separati virtualmente e topologia della rete di gestione

In questa topologia, la rete di dati e la rete di gestione sono virtualmente separate. I pacchetti dalla rete di dati e dalla rete di gestione vengono inviati sulla stessa connessione fisica. L'etichettatura VLAN viene utilizzata per tutti i pacchetti di dati della rete di gestione per separare il traffico tra le due reti.

Prima di iniziare

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

Accertarsi che sia installato il firmware minimo richiesto in ciascun dispositivo che si desidera gestire mediante XClarity Administrator. È possibile trovare i livelli minimi di firmware richiesti sulle Supporto XClarity Administrator - Pagina Web sulla compatibilità facendo clic sulla scheda **Compatibilità** e quindi sul collegamento per i tipi di dispositivi appropriati.

Accertarsi che gli ID VLAN siano configurati per le reti di dati e gestione. Facoltativamente, abilitare l'etichettatura VLAN dagli Switch Flex se la si implementa dagli Switch Flex oppure abilitarla dagli switch TOR (Top-of-Rack) se la si implementa dagli switch di questo tipo.

Accertarsi di definire le porte a cui sono connessi i CMM come appartenenti alla VLAN di gestione.

Importante: 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 viene utilizzato DHCP, verificare che le modifiche dell'indirizzo IP siano minime.

Informazioni su questa attività

La seguente figura mostra una modalità di configurazione dell'ambiente in cui la rete di gestione è separata dalla rete virtuale. I numeri nella figura corrispondono ai passaggi numerati nelle seguenti sezioni.

Nota: Questa figura non rappresenta tutte le opzioni di cablaggio che potrebbero essere necessarie per l'ambiente. La figura mostra solo i requisiti delle opzioni di cablaggio per gli switch Flex, i CMM e i server rack in correlazione per configurare reti virtualmente separate di dati e gestione.

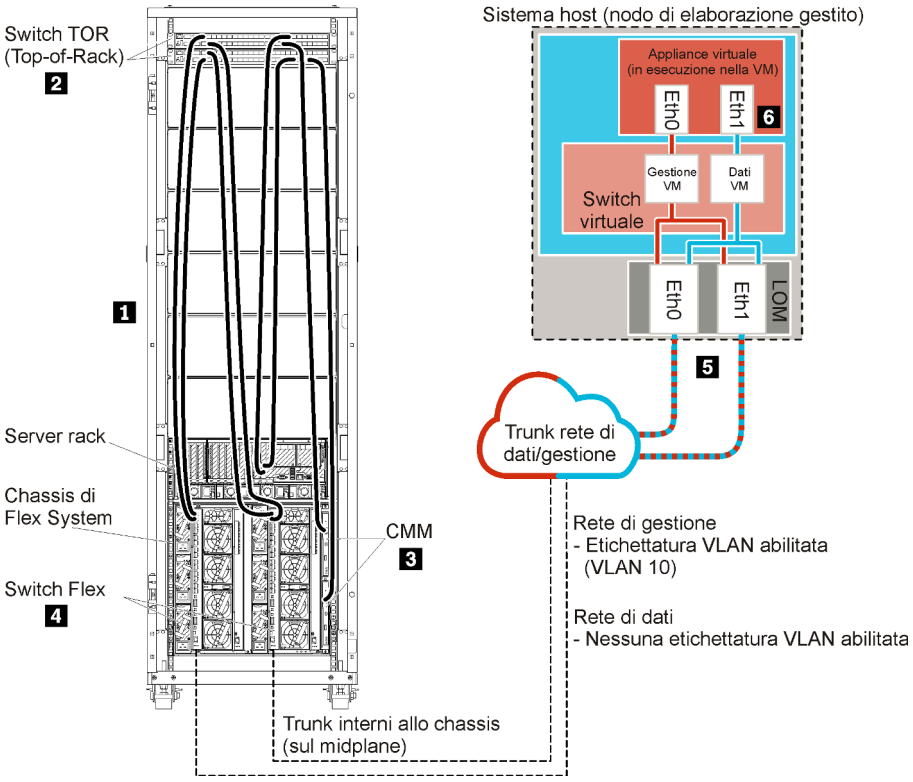


Figura 16. Esempio di topologia della rete di gestione e di dati separati virtualmente per un'appliance virtuale

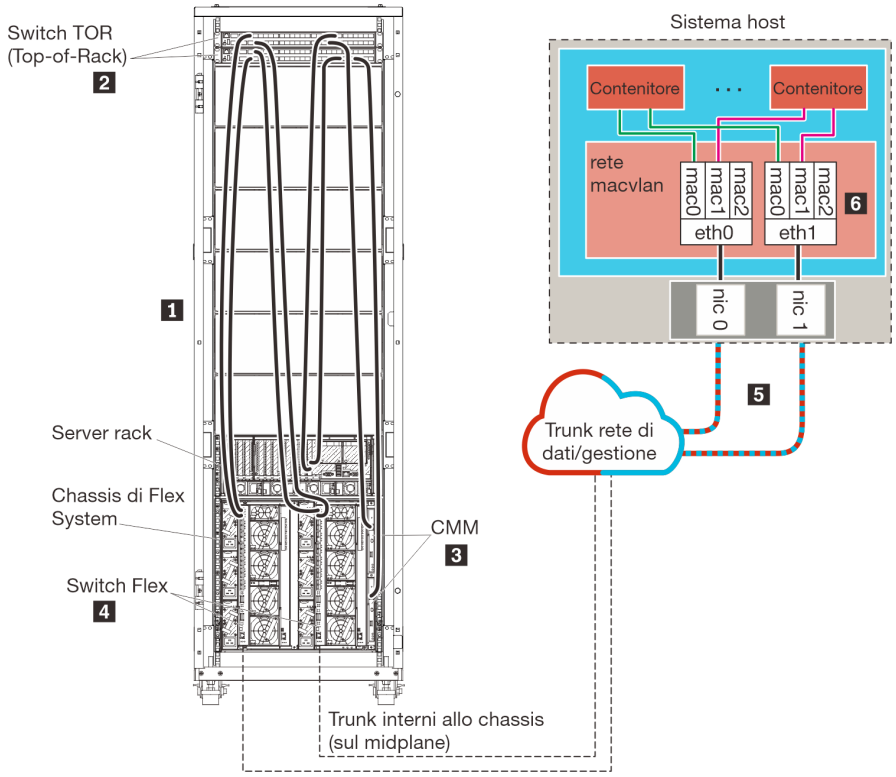


Figura 17. Esempio di topologia della rete di gestione e di dati separati virtualmente per i contenitori

In questo scenario, XClarity Administrator è installato su un server in uno chassis di Flex System gestito da XClarity Administrator.

Importante: È possibile configurare XClarity Administrator in qualsiasi sistema che soddisfi i requisiti per XClarity Administrator, incluso un server gestito. Se si utilizza un server gestito per l'host XClarity Administrator:

- È necessario implementare una topologia di reti virtualmente separate di dati e gestione o una topologia di rete singola di dati e gestione.
- Non è possibile utilizzare XClarity Administrator per applicare aggiornamenti firmware al server gestito. Anche se il firmware viene applicato solo parzialmente con attivazione immediata, XClarity Administrator forza il riavvio del server di destinazione, determinando di conseguenza anche il riavvio di XClarity Administrator. Se gli aggiornamenti vengono applicati con attivazione posticipata, solo parte del firmware viene applicata al riavvio dell'host XClarity Administrator.
- Se si utilizza un server in uno chassis di Flex System, accertarsi che il server sia configurato per l'accensione automatica. È possibile impostare questa opzione dall'interfaccia Web CMM facendo clic su **Gestione chassis → Nodi di elaborazione**, quindi selezionando il server e **Accensione automatica** per **Modalità accensione automatica**.

Sempre in questo scenario, tutti i dati vengono inviati tramite le stesse connessioni fisiche. La rete di gestione e la rete di dati vengono separate mediante l'etichettatura VLAN, in cui specifiche etichette corrispondenti alla rete di gestione vengono aggiunte ai pacchetti di dati per garantirne l'instradamento alle interfacce appropriate. Le etichette vengono rimosse dai pacchetti di dati in uscita.

È possibile abilitare l'etichettatura VLAN in uno dei seguenti dispositivi:

- **Switch TOR (Top-of-Rack)**. Le etichette VLAN corrispondenti alla rete di gestione vengono aggiunte ai pacchetti nel momento in cui accedono allo switch TOR (Top-of-Rack) e vengono passate attraverso gli

Switch Flex e ai server nello chassis di Flex System. Nell'instradamento inverso, le etichette VLAN vengono rimosse nel momento in cui vengono inviate dallo switch TOR (Top-of-Rack) ai controller di gestione.

- **Switch Flex**. Le etichette VLAN corrispondenti alla rete di gestione vengono aggiunte ai pacchetti nel momento in cui accedono agli Switch Flex e vengono passate ai server in uno chassis di Flex System. Nell'instradamento inverso, alcune etichette VLAN vengono aggiunte dai server e passate agli Switch Flex, che le rimuovono durante l'inoltro ai controller di gestione.

La decisione di implementare o meno l'etichettatura VLAN varia a seconda delle esigenze e della complessità dell'ambiente.

Se si desidera installare XClarity Administrator per gestire lo chassis e i server rack esistenti già configurati, procedere al Passaggio 5: installare e configurare l'host.

Per ulteriori informazioni sulla pianificazione di questa topologia, incluse le informazioni sulle impostazioni di rete e sulle configurazioni Eth1 e Eth0, vedere Rete virtualmente separata di dati e gestione.

Passaggio 1: cablare lo chassis e i server rack agli switch TOR (Top-of-Rack)

Cablare lo chassis e i server rack allo stesso switch TOR (Top-of-Rack) per consentire la comunicazione tra i dispositivi.

Procedura

Cablare ciascuno switch Flex e CMM in ogni chassis e in ogni server rack a entrambi gli switch TOR (Top-of-Rack). È possibile scegliere qualsiasi porta nello switch TOR (Top-of-Rack).

La seguente figura rappresenta un esempio che illustra il cablaggio dallo chassis (switch Flex e CMM) e dai server rack agli switch TOR (Top-of-Rack) quando Lenovo XClarity Administrator è installato su un server in uno chassis che verrà gestito da XClarity Administrator.

Nota: Questa figura non rappresenta tutte le opzioni di cablaggio che potrebbero essere necessarie per l'ambiente. La figura mostra solo i requisiti delle opzioni di cablaggio per gli switch Flex, i CMM e i server rack in correlazione per configurare reti virtualmente separate di dati e gestione.

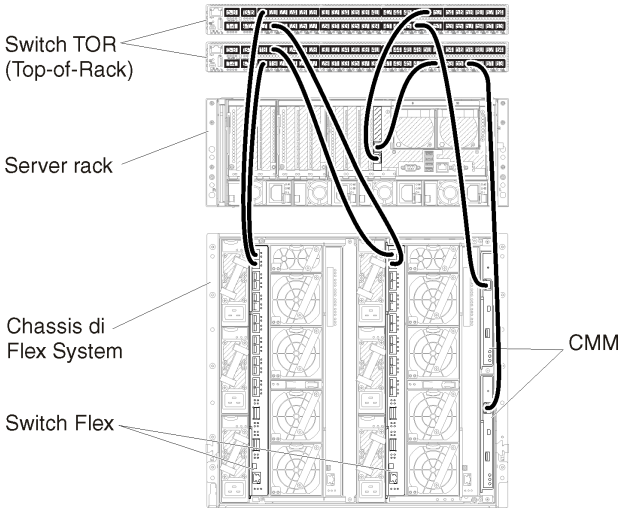


Figura 18. Esempio di cablaggio per reti virtualmente separate di dati e gestione

Passaggio 2: configurare switch TOR (Top-of-Rack)

Configurare switch TOR (Top-of-Rack).

Prima di iniziare

Oltre ai requisiti tipici di configurazione per gli switch TOR (Top-of-Rack), accertarsi che siano abilitate tutte le porte appropriate, incluse le porte esterne agli Switch Flex, ai server rack e alla rete e le porte interne al CMM, ai server rack e alla rete.

È possibile implementare l'etichettatura VLAN negli switch Flex o TOR (Top-of-Rack), a seconda delle esigenze e della complessità dell'ambiente. Se si implementa l'etichettatura dagli switch TOR (Top-of-Rack), abilitare l'etichettatura VLAN.

Accertarsi che gli ID VLAN siano configurati per le reti di gestione e dati.

Procedura

I passaggi di configurazione possono variare a seconda del tipo di switch rack installati.

La seguente figura rappresenta uno scenario di esempio che illustra l'etichettatura VLAN implementata negli switch TOR (Top-of-Rack) e abilitata nella rete di sola gestione. La VLAN di gestione è configurata come VLAN 10.

In questo scenario è necessario definire le porte a cui sono connessi i CMM come appartenenti alla VLAN di gestione.

Nota: È inoltre possibile abilitare l'etichettatura VLAN nella rete di dati per configurare una VLAN di dati.

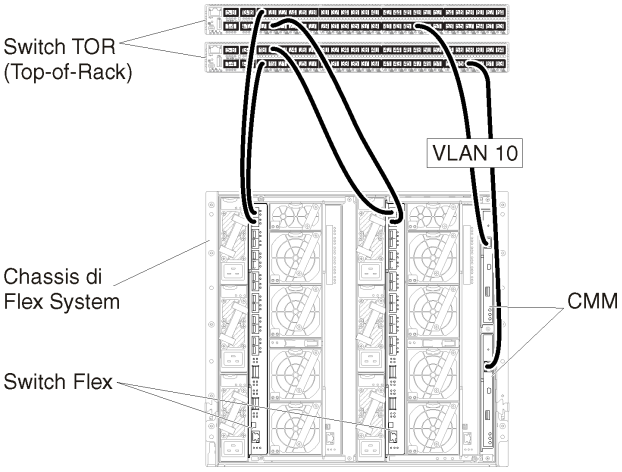


Figura 19. Configurazione di esempio per Switch Flex in reti virtualmente separate di dati e gestione (VMware ESXi) in cui l'etichettatura VLAN è abilitata nella rete di gestione

Per informazioni sulla configurazione di switch TOR (Top-of-Rack) Lenovo, vedere Switch rack nella documentazione online di System x. Se è installato un altro switch TOR (Top-of-Rack), fare riferimento alla documentazione fornita con lo switch.

Passaggio 3: configurare CMM (Chassis Management Module)

Configurare il CMM (Chassis Management Module) primario nello chassis per gestire tutti i dispositivi al suo interno.

Informazioni su questa attività

Per informazioni dettagliate sulla configurazione di un CMM, vedere Configurazione dei componenti dello chassis nella documentazione online di Flex System.

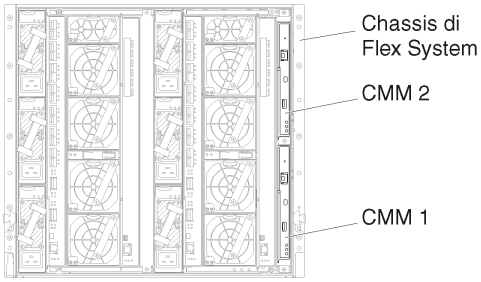
Fare inoltre riferimento ai passaggi 4.1 - 4.5 nel poster delle istruzioni fornito con lo chassis.

Procedura

Per configurare il CMM, attenersi alla procedura descritta di seguito.

Se sono installati due CMM, configurare solo il CMM *primario*, che sincronizza automaticamente la configurazione con il CMM in standby.

Passo 1. Collegare un cavo Ethernet dal CMM nel vano 1 alla workstation client per creare un collegamento diretto.



Per collegarsi al CMM per la prima volta, potrebbe essere necessario modificare le proprietà del protocollo IP nella workstation client.

Importante: Accertarsi che la sottorete della workstation client sia la stessa della sottorete del CMM. Il valore predefinito della sottorete CMM è 255.255.255.0. L'indirizzo IP scelto per la workstation client deve trovarsi nella stessa rete del CMM (ad esempio, 192.168.70.0 - 192.168.70.24).

Passo 2. Per avviare l'interfaccia di gestione CMM, aprire un browser Web nella workstation client e indirizzarla all'indirizzo IP del CMM.

Nota:

- Accertarsi di utilizzare una connessione sicura e includere **https** nell'URL (ad esempio, https://192.168.70.100). Se non si include https, verrà visualizzato un errore di pagina non trovata.
- Se si utilizza l'indirizzo IP predefinito 192.168.70.100, l'interfaccia di gestione CMM potrebbe richiedere alcuni minuti per essere disponibile. Questo ritardo si verifica a causa dei tentativi del CMM di ottenere un indirizzo DHCP per due minuti prima di eseguire il fallback all'indirizzo statico predefinito.

Passo 3. Eseguire il login all'interfaccia di gestione CMM utilizzando l'ID utente `USERID` e la password `PASSWORD` predefiniti. Dopo aver eseguito il login, sarà necessario modificare la password predefinita.

Passo 4. Completare la procedura guidata Configurazione iniziale del CMM per specificare i dettagli per l'ambiente. La procedura guidata Configurazione iniziale include le seguenti opzioni:

- Visualizzare l'inventario e lo stato dello chassis.
- Importare la configurazione da un file esistente.
- Configurare le impostazioni CMM generiche,
- Configurare la data e l'ora del CMM.

Suggerimento: quando si installa XClarity Administrator, configurare XClarity Administrator e tutti gli chassis gestiti da XClarity Administrator per l'utilizzo di un server NTP.

- Configurare le informazioni IP del CMM.
- Configurare i criteri di sicurezza del CMM.
- Configurare il DNS (Domain Name System).
- Configurare i server d'inoltro degli eventi.

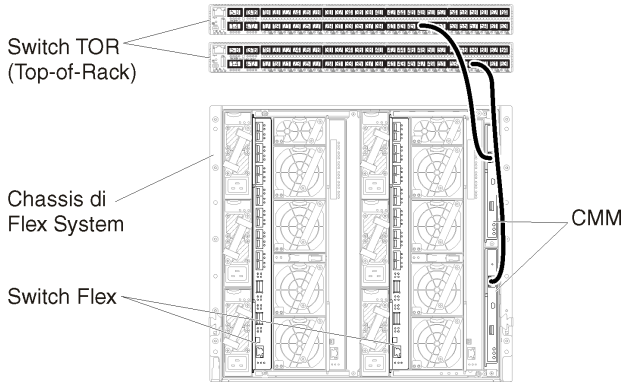
Passo 5. Dopo aver salvato le impostazioni della procedura guidata e applicato le modifiche, configurare gli indirizzi IP per tutti i componenti nello chassis.

Fare riferimento al passaggio 4.6 nel poster delle istruzioni fornito con lo chassis.

Nota: È necessario reimpostare il processore di gestione del sistema per ciascun nodo di elaborazione e riavviare gli switch Flex per visualizzare i nuovi indirizzi IP.

Passo 6. Riavviare il CMM mediante la relativa interfaccia di gestione.

Passo 7. Al riavvio del CMM, collegare un cavo dalla porta Ethernet nel CMM alla rete.



Passo 8. Eseguire il login all'interfaccia di gestione CMM mediante il nuovo indirizzo IP.

Al termine

È inoltre possibile configurare il CMM per il supporto della ridondanza. Utilizzare il sistema di guida CMM per ottenere ulteriori informazioni sui campi disponibili in ciascuna delle seguenti pagine.

- Configurare il failover per il CMM in caso si verifichi un guasto hardware nel CMM primario. Dall'interfaccia di gestione CMM, fare clic su **Gestione del modulo di gestione → Proprietà → Failover avanzato**.
- Configurare il failover come risultato di un problema di rete (Uplink). Dall'interfaccia di gestione CMM, fare clic su **Gestione del modulo di gestione → Rete**, selezionare la scheda **Ethernet** e fare clic su **Ethernet avanzata**. Come requisito minimo, verificare di selezionare **Failover in caso di perdita del collegamento fisico alla rete**.

Passaggio 4: configurare Switch Flex

Configurare gli Switch Flex in ogni chassis.

Prima di iniziare

Accertarsi che siano abilitate tutte le porte appropriate, incluse le porte esterne dallo switch Flex allo switch TOR (Top-of-Rack) e le porte interne al CMM.

È possibile implementare l'etichettatura VLAN negli switch Flex o TOR (Top-of-Rack), a seconda delle esigenze e della complessità dell'ambiente. Se si implementa l'etichettatura dagli switch Flex, abilitare l'etichettatura VLAN.

Accertarsi che gli ID VLAN siano configurati per le reti di gestione e dati.

Importante: Per ogni chassis di Flex System, verificare che il tipo di fabric della scheda di espansione in ciascun server nello chassis sia compatibile con il tipo di fabric di tutti gli switch Flex nello stesso chassis. Se, ad esempio, in uno chassis sono installati switch Ethernet, tutti i server al suo interno devono disporre di connettività Ethernet tramite il connettore LAN su scheda madre o una scheda di espansione Ethernet. Per ulteriori informazioni sulla configurazione di switch Flex, vedere Configurazione dei moduli I/O nella documentazione online di Flex Systems.

Procedura

I passaggi di configurazione possono variare a seconda del tipo di Switch Flex installato. Per ulteriori informazioni su ogni Switch Flex supportato, vedere Switch di rete Flex System nella documentazione online di Flex Systems.

La seguente figura rappresenta uno scenario di esempio che illustra l'etichettatura VLAN implementata negli switch Flex e abilitata nella rete di sola gestione. La VLAN di gestione è configurata come VLAN 10.

Nota: È possibile configurare una rete VLAN di dati abilitando l'etichettatura VLAN nell'apposita rete.

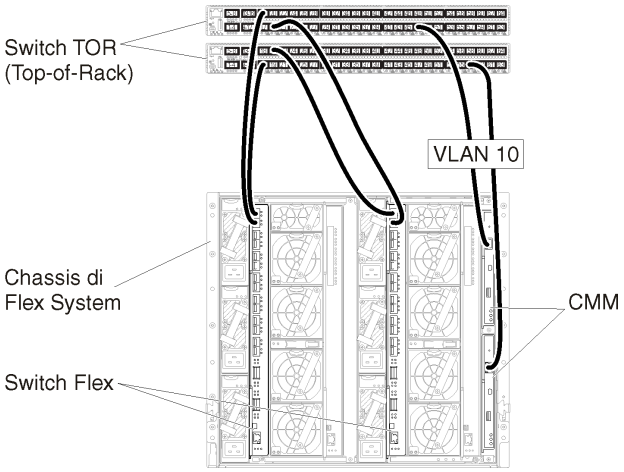


Figura 20. Configurazione di esempio per Switch Flex in reti virtualmente separate di dati e gestione (VMware ESXi) in cui l'etichettatura VLAN è abilitata nella rete di gestione

Per configurare gli switch Flex per questo scenario, attenersi alla procedura descritta di seguito.

Passo 1. Configurare lo switch Flex nel vano 1:

a. Definire la VLAN di gestione (nell'esempio è stato scelto VLAN 10) che conterrà la porta esterna in cui verrà instradato il cavo allo switch TOR (Top-of-Rack) di gestione (Ext1).

b. Definire una porta interna che dovrà far parte della rete VLAN 10 (VLAN di gestione). Verificare che il trunking VLAN sia abilitato nella porta.

Passo 2. Configurare lo switch Flex nel vano 2:

Suggerimento: il vano 2 dello switch Flex è il terzo vano del modulo sul retro dello chassis:

a. Definire la VLAN di gestione (nell'esempio è stato scelto VLAN 10) che conterrà la porta esterna in cui verrà instradato il cavo allo switch TOR (Top-of-Rack) di gestione.

b. Definire una porta interna che dovrà far parte della rete VLAN 10 (VLAN di gestione). Verificare che il trunking VLAN sia abilitato nella porta.

Passaggio 5: installare e configurare l'host

È possibile installare Docker su qualsiasi sistema che soddisfi i requisiti per Lenovo XClarity Administrator.

Prima di iniziare

È possibile utilizzare Docker Datacenter per configurare un ambiente ad alta disponibilità per i contenitori XClarity Administrator che vengono eseguiti in Docker Engine. Per ulteriori informazioni sull'alta disponibilità di Docker Datacenter, vedere Pagina Web Architettura e app ad alta disponibilità con Docker Datacenter.

Accertarsi che l'host soddisfi i prerequisiti definiti in Prerequisiti hardware e software.

Accertarsi che il sistema host si trovi nella stessa rete dei dispositivi che si desidera gestire.

Importante: È possibile configurare XClarity Administrator in qualsiasi sistema che soddisfi i requisiti per XClarity Administrator, incluso un server gestito. Se si utilizza un server gestito per l'host XClarity Administrator:

- È necessario implementare una topologia di reti virtualmente separate di dati e gestione o una topologia di rete singola di dati e gestione.
- Non è possibile utilizzare XClarity Administrator per applicare aggiornamenti firmware al server gestito. Anche se il firmware viene applicato solo parzialmente con attivazione immediata, XClarity Administrator forza il riavvio del server di destinazione, determinando di conseguenza anche il riavvio di XClarity Administrator. Se gli aggiornamenti vengono applicati con attivazione posticipata, solo parte del firmware viene applicata al riavvio dell'host XClarity Administrator.
- Se si utilizza un server in uno chassis di Flex System, accertarsi che il server sia configurato per l'accensione automatica. È possibile impostare questa opzione dall'interfaccia Web CMM facendo clic su **Gestione chassis → Nodi di elaborazione**, quindi selezionando il server e **Accensione automatica** per **Modalità accensione automatica**.

Procedura

Installare e configurare Docker nell'host seguendo le istruzioni fornite con la distribuzione Docker.

Passaggio 6: installare e configurare XClarity Administrator

Installare e configurare l'Lenovo XClarity Administrator nel contenitore sull'host Docker appena installato.

Prima di iniziare

Verificare che il sistema host soddisfi i requisiti minimi hardware e software (vedere Prerequisiti hardware e software).

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

Accertarsi che il sistema host si trovi nella stessa rete dei dispositivi che si desidera gestire.

Verificare che il sistema operativo host e XClarity Administrator utilizzino lo stesso server NTP.

XClarity Administrator consente di utilizzare un nome personalizzato per la rete di gestione di dati e hardware, oltre che per quella di distribuzione del sistema operativo (vedere Configurazioni di rete). In questo esempio nella procedura seguente viene utilizzato eth0.

XClarity Administrator consente di utilizzare un nome personalizzato per la rete di gestione di dati e hardware, oltre che per quella di distribuzione del sistema operativo (vedere Configurazioni di rete). In questi esempi nella seguente procedura vengono utilizzati rispettivamente eth0 ed eth1.

Verificare che una rete macvlan sia caricata nel kernel del sistema host. Per verificare se la rete è caricata, utilizzare il comando **lsmod | grep macvlan**. Per caricare macvlan nel kernel, eseguire il comando **modprobe macvlan**.

Accertarsi di utilizzare un nome univoco e un indirizzo IP per ogni contenitore quando si eseguono più contenitori XClarity Administrator sullo stesso host.

Se si intende gestire ThinkServer e altri dispositivi legacy, accertarsi che Docker sia abilitato per supportare IPv6.

1. Modificare il file /etc/docker/daemon.json, impostare la chiave **ipv6** su true e impostare la chiave **fixed-cidr-v6** sulla sottorete IPv6. Di seguito viene riportato un file daemon di esempio.
```
{
   "ipv6": true,
   "fixed-cidr-v6": "2001:db8:1::/64",
   "experimental": true,
   "ip6tables": true
}
```
2. Ricaricare il file di configurazione Docker eseguendo il comando seguente.
```
systemctl reload docker
```

Nota: XClarity Administrator *non* viene eseguito come contenitore con privilegi.

Procedura

Per installare un contenitore XClarity Administrator utilizzando Docker Compose, completare la seguente procedura.

Passo 1. Scaricare l'immagine, il file di ambiente e il file YAML dell'appliance virtuale XClarity Administrator dalla Pagina Web di download di XClarity Administrator in una workstation client. Accedere al sito Web, quindi utilizzare la chiave di accesso fornita per scaricare l'immagine.

Passo 2. Importare l'immagine del contenitore XClarity Administrator nell'host docker, utilizzando il comando seguente.
```
docker load -i lnvgy_sw_lxca_<ver>_anyos_noarch.tar.gz
```

Passo 3. Modificare il file `docker_compose.env` e aggiornare le variabili di ambiente che seguono.

- **CONTAINER_NAME**. Nome univoco del contenitore, utilizzato per creare volumi docker per ogni istanza di XClarity Administrator (ad esempio, `CONTAINER_NAME=LXCA-203`)
- **INDIRIZZO**. Indirizzo IPv4 statico per il contenitore (ad esempio, `ADDRESS=192.0.2.0`)
- **BACKUP_MOUNT**. (Facoltativo) Percorso per la condivisione remota che può essere utilizzata per archiviare i backup di XClarity Administrator. Il percorso deve essere: `/mnt/backup_share`.
- **FIRMWARE_MOUNT**. (Facoltativo) Percorso per la condivisione remota che può essere utilizzata come repository remoto per gli aggiornamenti firmware. Il percorso deve essere: `/mnt/fw_share`.

Di seguito viene riportato un file di ambiente.
```
CONTAINER_NAME="LXCA-203"
ADDRESS="192.0.2.0"
```

```
BACKUP_MOUNT="/mnt/backup_share"
FIRMWARE_MOUNT="/mnt/fw_share"
```

Passo 4. Modificare il file `docker_compose.yml` e aggiornare le proprietà che seguono.

- Impostare la proprietà **image** con il nome del file dell'immagine di installazione utilizzato nel passaggio 2.

  Nota: È possibile modificare il nome del file di immagine (ad esempio, in "più recente") utilizzando il comando `docker tag`.
- Se si desidera utilizzare la condivisione remota come repository firmware remoto per archiviare i backup di XClarity Administrator impostare il punto di montaggio dell'host per ciascuna condivisione remota nella proprietà **volumi**.
- Impostare la proprietà **dns** sull'indirizzo IP dei server DNS.
- Il contenitore condivide il pool di risorse di memoria e processore disponibili per l'host. Facoltativamente definire i limiti sull'utilizzo delle risorse impostando le proprietà **cpus** e **memoria**.
- Impostare la proprietà **principale** sul nome dell'interfaccia di rete del sistema host da utilizzare come interfaccia principale per l'interfaccia macvlan nel contenitore. Questa interfaccia deve disporre dell'accesso diretto alla sottorete assegnata al contenitore.
- Impostare la **sottorete** e il **gateway** in base alla topologia di rete. In genere, la sottorete e il gateway sono per la rete di gestione, a cui appartiene ${ADDRESS}.
- Se si desidera supportare IPv6, impostare la proprietà **enable_ipv6** su true, impostare la proprietà **ipv6_address** sull'indirizzo IPv6 e aggiungere un'altra serie di proprietà di **sottorete** e **gateway** in base alla topologia di rete (generalmente per la rete di gestione a cui appartiene l'indirizzo IPv6).

Di seguito è riportato un file YML di esempio con IPv6 abilitato.

```
version: '3.8'

services:

  lxca:
    image: lenovo/lxca:4.1.0-124
    container_name: ${CONTAINER_NAME}
    tty: true
    stop_grace_period: 60s
    volumes:
      #bind mount example
      - /home/<HOST_MOUNT_POINT_FOR_BACKUP>:${BACKUP_MOUNT}
      - /home/<HOST_MOUNT_POINT_FOR_FW_SHARE>:${FIRMWARE_MOUNT}
      #docker volume mount
      - data:/opt/lenovo/lxca/data
      - postgresql:/var/lib/postgresql
      - log:/var/log
      - confluent-etc:/etc/confluent
      - confluent-log:/var/log/confluent
      - confluent:/var/lib/confluent
      - propconf:/opt/lenovo/lxca/bin/conf
      - ssh:/etc/ssh
      - xcat:/etc/xcat
    networks:
      lan1:
        ipv4_address: ${ADDRESS}
        ipv6_address: "2001:8003:7d51:2000::2"
      lan2:
```

```
        ipv4_address: 192.0.1.3
        ipv6_address: "2001:8003:7d51:2003::2"
    dns:
      - 192.0.40.10
      - 192.0.50.11
    deploy:
      resources:
        limits:
          cpus: "2.0"
          memory: "8g"

volumes:
  data:
    name: ${CONTAINER_NAME}-data
  postgresql:
    name: ${CONTAINER_NAME}-postgresql
  log:
    name: ${CONTAINER_NAME}-log
  confluent-etc:
    name: ${CONTAINER_NAME}-confluent-etc
  confluent-log:
    name: ${CONTAINER_NAME}-confluent-log
  confluent:
    name: ${CONTAINER_NAME}-confluent
  propconf:
    name: ${CONTAINER_NAME}-propconf
  ssh:
    name: ${CONTAINER_NAME}-ssh
  xcat:
    name: ${CONTAINER_NAME}-xcat

networks:
  lan1:
    name: lan1
    driver: macvlan
    enable_ipv6: true
    driver_opts:
      parent: eno1
    ipam:
      config:
        - subnet: 192.0.0.0/19
          gateway: 192.0.30.1
        - subnet: "2001:8003:7d51:2000::/80"
          gateway: "2001:8003:7d51:2000::1"
  lan2:
    name: lan2
    driver: macvlan
    enable_ipv6: true
    driver_opts:
      parent: virbr0
    ipam:
      config:
        - subnet: 192.0.122.0/24
          gateway: 192.0.122.1
        - subnet: "2001:8003:7d51:2003::/80"
          gateway: "2001:8003:7d51:2003::1"
```

Passo 5. Distribuire l'immagine in docker, utilizzando il comando seguente, dove <*ENV_FILENAME*> è il nome del file delle variabili d'ambiente creato nel passaggio 2.
COMPOSE_HTTP_TIMEOUT=300 `docker-compose -p ${CONTAINER_NAME} --env-file` <*ENV_FILENAME*> `up -d`

Al termine

Eseguire il login e configurare XClarity Administrator (vedere Primo accesso all'interfaccia Web di Lenovo XClarity Administrator e Configurazione di Lenovo XClarity Administrator).

Topologia di rete di sola gestione

In questa topologia, Lenovo XClarity Administrator dispone solo della rete di gestione, non della rete di dati.

Prima di iniziare

Accertarsi che siano abilitate tutte le porte appropriate, tra cui:
- Porte che richiedono XClarity Administrator (vedere Disponibilità della porta)
- Porte esterne alla rete
- Porte interne a CMM

Accertarsi che sia installato il firmware minimo richiesto in ciascun dispositivo che si desidera gestire mediante XClarity Administrator. È possibile trovare i livelli minimi di firmware richiesti sulle Supporto XClarity Administrator - Pagina Web sulla compatibilità facendo clic sulla scheda **Compatibilità** e quindi sul collegamento per i tipi di dispositivi appropriati.

Importante: 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 viene utilizzato DHCP, verificare che le modifiche dell'indirizzo IP siano minime.

Informazioni su questa attività

La seguente figura mostra una modalità di configurazione dell'ambiente nel caso in cui Lenovo XClarity Administrator disponga della sola rete di gestione e non della rete di dati. I numeri nella figura corrispondono ai passaggi numerati nelle seguenti sezioni.

Nota: Questa figura non rappresenta tutte le opzioni di cablaggio che potrebbero essere necessarie per l'ambiente. La figura mostra solo i requisiti delle opzioni di cablaggio per gli switch Flex, i CMM e i server rack in correlazione per configurare una rete di sola gestione.

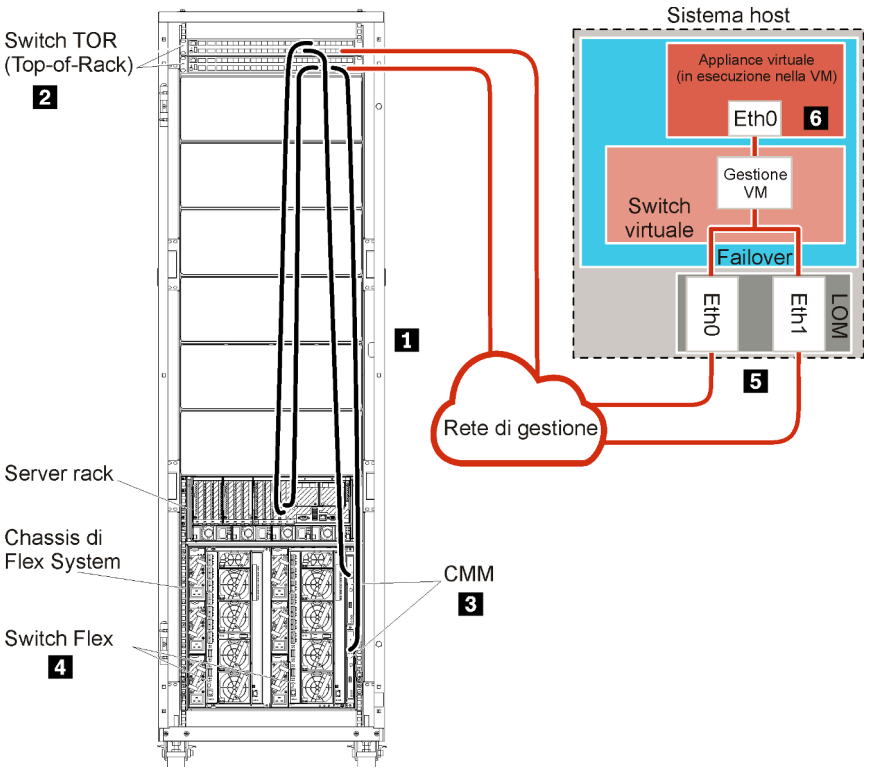


Figura 21. Esempio di topologia di rete di sola gestione per un'appliance virtuale

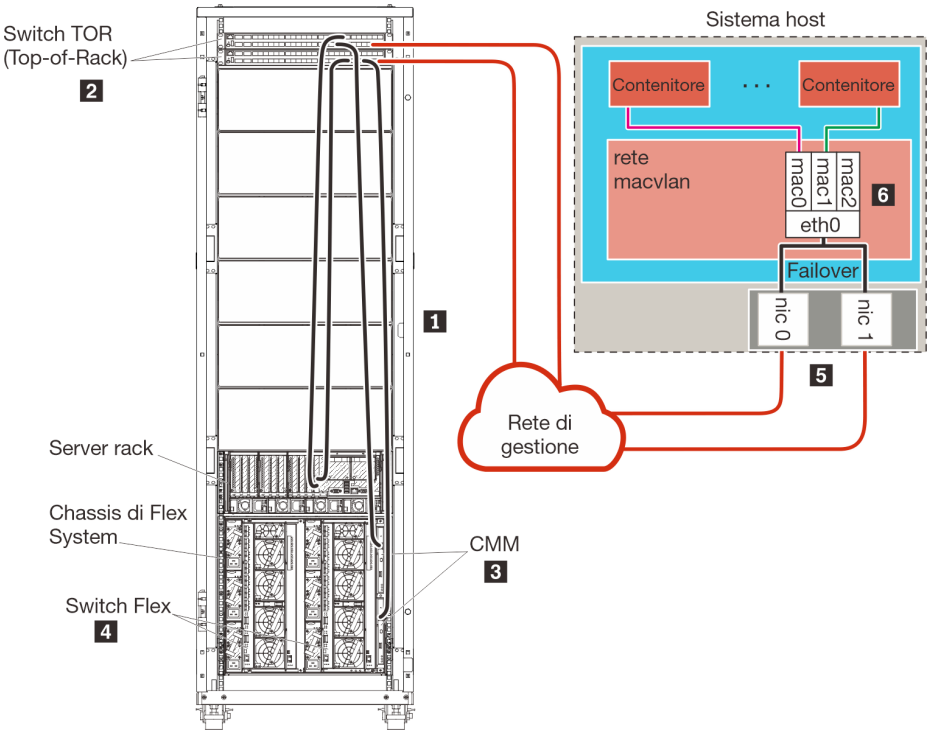


Figura 22. Esempio di topologia della rete di sola gestione per i contenitori

Se si desidera installare XClarity Administrator per gestire lo chassis e i server rack esistenti già configurati, procedere al Passaggio 5: installare e configurare l'host.

Per ulteriori informazioni sulla pianificazione di questa topologia, incluse le informazioni sulle impostazioni di rete e sulle configurazioni Eth1 e Eth0, vedere Rete di sola gestione.

Passaggio 1: cablare lo chassis, i server rack e l'host Lenovo XClarity Administrator agli switch TOR (Top-of-Rack)

Cablare lo chassis, i server rack e l'host XClarity Administrator agli switch TOR (Top-of-Rack) per consentire la comunicazione tra i dispositivi e la rete.

Procedura

Cablare ciascuno switch Flex e CMM in ogni chassis, in ogni server rack e nell'host XClarity Administrator a entrambi gli switch TOR (Top-of-Rack). È possibile scegliere qualsiasi porta negli switch TOR (Top-of-Rack).

La seguente figura rappresenta un esempio che illustra il cablaggio dallo chassis (switch Flex e CMM), dai server rack e dall'host XClarity Administrator agli switch TOR (Top-of-Rack).

Nota: Questa figura non rappresenta tutte le opzioni di cablaggio che potrebbero essere necessarie per l'ambiente. La figura mostra solo i requisiti delle opzioni di cablaggio per gli switch Flex, i CMM e i server rack in correlazione per configurare una rete di sola gestione.

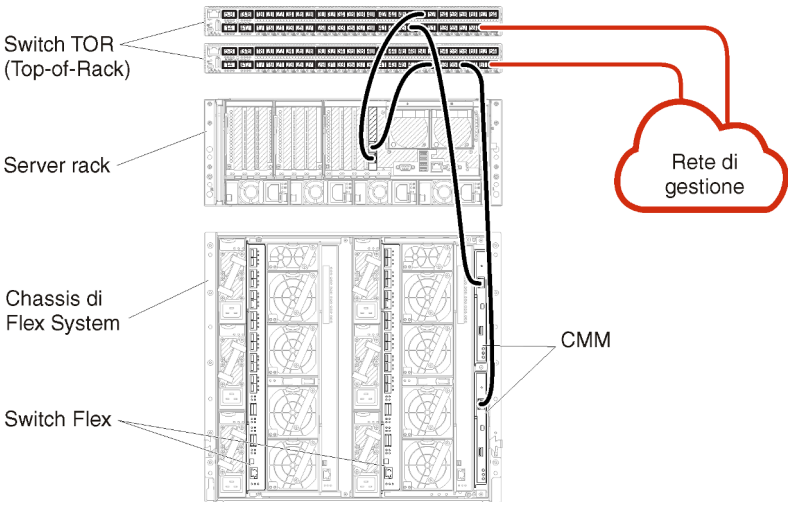


Figura 23. Esempio di cablaggio per una rete di sola gestione

Passaggio 2: configurare switch TOR (Top-of-Rack)

Configurare switch TOR (Top-of-Rack).

Prima di iniziare

Oltre ai requisiti tipici di configurazione per gli switch TOR (Top-of-Rack), accertarsi che siano abilitate tutte le porte appropriate, incluse le porte esterne agli Switch Flex, ai server rack e alla rete e le porte interne al CMM, ai server rack e alla rete.

Procedura

I passaggi di configurazione possono variare a seconda del tipo di switch rack installati.

Per informazioni sulla configurazione di switch TOR (Top-of-Rack) Lenovo, vedere Switch rack nella documentazione online di System x. Se è installato un altro switch TOR (Top-of-Rack), fare riferimento alla documentazione fornita con lo switch.

Passaggio 3: configurare CMM (Chassis Management Module)

Configurare il CMM (Chassis Management Module) primario nello chassis per gestire tutti i dispositivi al suo interno.

Informazioni su questa attività

Per informazioni dettagliate sulla configurazione di un CMM, vedere Configurazione dei componenti dello chassis nella documentazione online di Flex System.

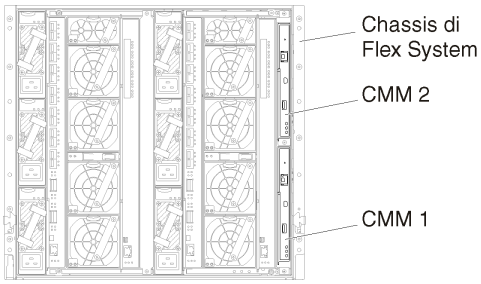
Fare inoltre riferimento ai passaggi 4.1 - 4.5 nel poster delle istruzioni fornito con lo chassis.

Procedura

Per configurare il CMM, attenersi alla procedura descritta di seguito.

Se sono installati due CMM, configurare solo il CMM *primario*, che sincronizza automaticamente la configurazione con il CMM in standby.

Passo 1. Collegare un cavo Ethernet dal CMM nel vano 1 alla workstation client per creare un collegamento diretto.



Per collegarsi al CMM per la prima volta, potrebbe essere necessario modificare le proprietà del protocollo IP nella workstation client.

Importante: Accertarsi che la sottorete della workstation client sia la stessa della sottorete del CMM. Il valore predefinito della sottorete CMM è 255.255.255.0. L'indirizzo IP scelto per la workstation client deve trovarsi nella stessa rete del CMM (ad esempio, 192.168.70.0 - 192.168.70.24).

Passo 2. Per avviare l'interfaccia di gestione CMM, aprire un browser Web nella workstation client e indirizzarla all'indirizzo IP del CMM.

Nota:

- Accertarsi di utilizzare una connessione sicura e includere **https** nell'URL (ad esempio, https://192.168.70.100). Se non si include https, verrà visualizzato un errore di pagina non trovata.
- Se si utilizza l'indirizzo IP predefinito 192.168.70.100, l'interfaccia di gestione CMM potrebbe richiedere alcuni minuti per essere disponibile. Questo ritardo si verifica a causa dei tentativi del CMM di ottenere un indirizzo DHCP per due minuti prima di eseguire il fallback all'indirizzo statico predefinito.

Passo 3. Eseguire il login all'interfaccia di gestione CMM utilizzando l'ID utente `USERID` e la password `PASSWORD` predefiniti. Dopo aver eseguito il login, sarà necessario modificare la password predefinita.

Passo 4. Completare la procedura guidata Configurazione iniziale del CMM per specificare i dettagli per l'ambiente. La procedura guidata Configurazione iniziale include le seguenti opzioni:

- Visualizzare l'inventario e lo stato dello chassis.
- Importare la configurazione da un file esistente.
- Configurare le impostazioni CMM generiche,
- Configurare la data e l'ora del CMM.

  Suggerimento: quando si installa XClarity Administrator, configurare XClarity Administrator e tutti gli chassis gestiti da XClarity Administrator per l'utilizzo di un server NTP.
- Configurare le informazioni IP del CMM.
- Configurare i criteri di sicurezza del CMM.
- Configurare il DNS (Domain Name System).
- Configurare i server d'inoltro degli eventi.

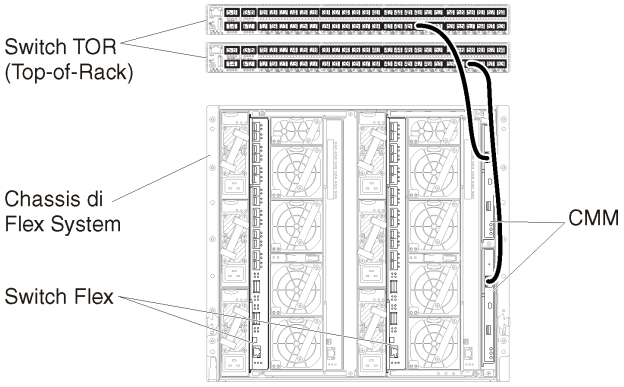
Passo 5. Dopo aver salvato le impostazioni della procedura guidata e applicato le modifiche, configurare gli indirizzi IP per tutti i componenti nello chassis.

Fare riferimento al passaggio 4.6 nel poster delle istruzioni fornito con lo chassis.

Nota: È necessario reimpostare il processore di gestione del sistema per ciascun nodo di elaborazione e riavviare gli switch Flex per visualizzare i nuovi indirizzi IP.

Passo 6. Riavviare il CMM mediante la relativa interfaccia di gestione.

Passo 7. Al riavvio del CMM, collegare un cavo dalla porta Ethernet nel CMM alla rete.



Passo 8. Eseguire il login all'interfaccia di gestione CMM mediante il nuovo indirizzo IP.

Al termine

È inoltre possibile configurare il CMM per il supporto della ridondanza. Utilizzare il sistema di guida CMM per ottenere ulteriori informazioni sui campi disponibili in ciascuna delle seguenti pagine.

- Configurare il failover per il CMM in caso si verifichi un guasto hardware nel CMM primario. Dall'interfaccia di gestione CMM, fare clic su **Gestione del modulo di gestione → Proprietà → Failover avanzato**.
- Configurare il failover come risultato di un problema di rete (Uplink). Dall'interfaccia di gestione CMM, fare clic su **Gestione del modulo di gestione → Rete**, selezionare la scheda **Ethernet** e fare clic su **Ethernet avanzata**. Come requisito minimo, verificare di selezionare **Failover in caso di perdita del collegamento fisico alla rete**.

Passaggio 4: configurare Switch Flex

Configurare gli Switch Flex in ogni chassis.

Prima di iniziare

Accertarsi che siano abilitate tutte le porte appropriate, incluse le porte esterne dallo switch Flex allo switch TOR (Top-of-Rack) e le porte interne al CMM.

Se gli switch Flex sono configurati per ottenere impostazioni di rete dinamiche (indirizzo IP, maschera di rete, gateway e indirizzo DNS) su DHCP, accertarsi che tali impostazioni siano coerenti (ad esempio, verificare che gli indirizzi IP si trovino nella stessa sottorete del CMM).

Importante: Per ogni chassis di Flex System, verificare che il tipo di fabric della scheda di espansione in ciascun server nello chassis sia compatibile con il tipo di fabric di tutti gli switch Flex nello stesso chassis. Se, ad esempio, in uno chassis sono installati switch Ethernet, tutti i server al suo interno devono disporre di connettività Ethernet tramite il connettore LAN su scheda madre o una scheda di espansione Ethernet. Per ulteriori informazioni sulla configurazione di switch Flex, vedere Configurazione dei moduli I/O nella documentazione online di Flex Systems.

Procedura

I passaggi di configurazione possono variare a seconda del tipo di Switch Flex installato. Per ulteriori informazioni su ogni Switch Flex supportato, vedere Switch di rete Flex System nella documentazione online di Flex Systems.

In genere, è necessario configurare gli switch Flex nei relativi vani 1 e 2.

Suggerimento: il vano 2 dello switch Flex è il terzo vano del modulo nella parte posteriore dello chassis.

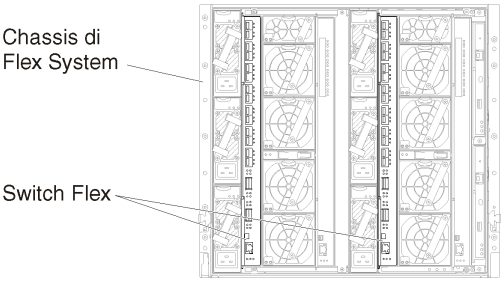


Figura 24. Posizioni degli Switch Flex in uno chassis

Passaggio 5: installare e configurare l'host

È possibile installare Docker su qualsiasi sistema che soddisfi i requisiti per Lenovo XClarity Administrator.

Prima di iniziare

È possibile utilizzare Docker Datacenter per configurare un ambiente ad alta disponibilità per i contenitori XClarity Administrator che vengono eseguiti in Docker Engine. Per ulteriori informazioni sull'alta disponibilità di Docker Datacenter, vedere Pagina Web Architettura e app ad alta disponibilità con Docker Datacenter.

Accertarsi che l'host soddisfi i prerequisiti definiti in Prerequisiti hardware e software.

Accertarsi che il sistema host si trovi nella stessa rete dei dispositivi che si desidera gestire.

Importante: È possibile configurare XClarity Administrator in qualsiasi sistema che soddisfi i requisiti per XClarity Administrator, incluso un server gestito. Se si utilizza un server gestito per l'host XClarity Administrator:

- È necessario implementare una topologia di reti virtualmente separate di dati e gestione o una topologia di rete singola di dati e gestione.
- Non è possibile utilizzare XClarity Administrator per applicare aggiornamenti firmware al server gestito. Anche se il firmware viene applicato solo parzialmente con attivazione immediata, XClarity Administrator forza il riavvio del server di destinazione, determinando di conseguenza anche il riavvio di XClarity Administrator. Se gli aggiornamenti vengono applicati con attivazione posticipata, solo parte del firmware viene applicata al riavvio dell'host XClarity Administrator.
- Se si utilizza un server in uno chassis di Flex System, accertarsi che il server sia configurato per l'accensione automatica. È possibile impostare questa opzione dall'interfaccia Web CMM facendo clic su **Gestione chassis → Nodi di elaborazione**, quindi selezionando il server e **Accensione automatica** per **Modalità accensione automatica**.

Procedura

Installare e configurare Docker nell'host seguendo le istruzioni fornite con la distribuzione Docker.

Passaggio 6: installare e configurare XClarity Administrator

Installare e configurare l'Lenovo XClarity Administrator nel contenitore sull'host Docker appena installato.

Prima di iniziare

Verificare che il sistema host soddisfi i requisiti minimi hardware e software (vedere Prerequisiti hardware e software).

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

Accertarsi che il sistema host si trovi nella stessa rete dei dispositivi che si desidera gestire.

Verificare che il sistema operativo host e XClarity Administrator utilizzino lo stesso server NTP.

XClarity Administrator consente di utilizzare un nome personalizzato per la rete di gestione di dati e hardware, oltre che per quella di distribuzione del sistema operativo (vedere Configurazioni di rete). In questo esempio nella procedura seguente viene utilizzato eth0.

XClarity Administrator consente di utilizzare un nome personalizzato per la rete di gestione di dati e hardware (vedere Configurazioni di rete). In questo esempio nella procedura seguente viene utilizzato eth0

Verificare che una rete macvlan sia caricata nel kernel del sistema host. Per verificare se la rete è caricata, utilizzare il comando **lsmod | grep macvlan**. Per caricare macvlan nel kernel, eseguire il comando **modprobe macvlan**.

Accertarsi di utilizzare un nome univoco e un indirizzo IP per ogni contenitore quando si eseguono più contenitori XClarity Administrator sullo stesso host.

Se si intende gestire ThinkServer e altri dispositivi legacy, accertarsi che Docker sia abilitato per supportare IPv6.

1. Modificare il file /etc/docker/daemon.json, impostare la chiave **ipv6** su true e impostare la chiave **fixed-cidr-v6** sulla sottorete IPv6. Di seguito viene riportato un file daemon di esempio.

```
{
   "ipv6": true,
   "fixed-cidr-v6": "2001:db8:1::/64",
   "experimental": true,
   "ip6tables": true
}
```

2. Ricaricare il file di configurazione Docker eseguendo il comando seguente.
   `systemctl reload docker`

Nota: XClarity Administrator *non* viene eseguito come contenitore con privilegi.

Procedura

Per installare un contenitore XClarity Administrator utilizzando Docker Compose, completare la seguente procedura.

Passo 1. Scaricare l'immagine, il file di ambiente e il file YAML dell'appliance virtuale XClarity Administrator dalla Pagina Web di download di XClarity Administrator in una workstation client. Accedere al sito Web, quindi utilizzare la chiave di accesso fornita per scaricare l'immagine.

Passo 2. Importare l'immagine del contenitore XClarity Administrator nell'host docker, utilizzando il comando seguente.
`docker load -i lnvgy_sw_lxca_<ver>_anyos_noarch.tar.gz`

Passo 3. Modificare il file `docker_compose.env` e aggiornare le variabili di ambiente che seguono.

- **CONTAINER_NAME**. Nome univoco del contenitore, utilizzato per creare volumi docker per ogni istanza di XClarity Administrator (ad esempio, `CONTAINER_NAME=LXCA-203`)
- **INDIRIZZO**. Indirizzo IPv4 statico per il contenitore (ad esempio, `ADDRESS=192.0.2.0`)
- **BACKUP_MOUNT**. (Facoltativo) Percorso per la condivisione remota che può essere utilizzata per archiviare i backup di XClarity Administrator. Il percorso deve essere: `/mnt/backup_share`.
- **FIRMWARE_MOUNT**. (Facoltativo) Percorso per la condivisione remota che può essere utilizzata come repository remoto per gli aggiornamenti firmware. Il percorso deve essere: `/mnt/fw_share`.

Di seguito viene riportato un file di ambiente.

```
CONTAINER_NAME="LXCA-203"
ADDRESS="192.0.2.0"
BACKUP_MOUNT="/mnt/backup_share"
FIRMWARE_MOUNT="/mnt/fw_share"
```

Passo 4. Modificare il file `docker_compose.yml` e aggiornare le proprietà che seguono.

- Impostare la proprietà **image** con il nome del file dell'immagine di installazione utilizzato nel passaggio 2.

  Nota: È possibile modificare il nome del file di immagine (ad esempio, in "più recente") utilizzando il comando `docker tag`.
- Se si desidera utilizzare la condivisione remota come repository firmware remoto per archiviare i backup di XClarity Administrator impostare il punto di montaggio dell'host per ciascuna condivisione remota nella proprietà **volumi**.
- Impostare la proprietà **dns** sull'indirizzo IP dei server DNS.
- Il contenitore condivide il pool di risorse di memoria e processore disponibili per l'host. Facoltativamente definire i limiti sull'utilizzo delle risorse impostando le proprietà **cpus** e **memoria**.

- Impostare la proprietà **principale** sul nome dell'interfaccia di rete del sistema host da utilizzare come interfaccia principale per l'interfaccia macvlan nel contenitore. Questa interfaccia deve disporre dell'accesso diretto alla sottorete assegnata al contenitore.
- Impostare la **sottorete** e il **gateway** in base alla topologia di rete. In genere, la sottorete e il gateway sono per la rete di gestione, a cui appartiene ${ADDRESS}.
- Se si desidera supportare IPv6, impostare la proprietà **enable_ipv6** su true, impostare la proprietà **ipv6_address** sull'indirizzo IPv6 e aggiungere un'altra serie di proprietà di **sottorete** e **gateway** in base alla topologia di rete (generalmente per la rete di gestione a cui appartiene l'indirizzo IPv6).

Di seguito è riportato un file YML di esempio con IPv6 abilitato.

```
version: '3.8'

services:

  lxca:
    image: lenovo/lxca:4.1.0-124
    container_name: ${CONTAINER_NAME}
    tty: true
    stop_grace_period: 60s
    volumes:
      #bind mount example
      - /home/<HOST_MOUNT_POINT_FOR_BACKUP>:${BACKUP_MOUNT}
      - /home/<HOST_MOUNT_POINT_FOR_FW_SHARE>:${FIRMWARE_MOUNT}
      #docker volume mount
      - data:/opt/lenovo/lxca/data
      - postgresql:/var/lib/postgresql
      - log:/var/log
      - confluent-etc:/etc/confluent
      - confluent-log:/var/log/confluent
      - confluent:/var/lib/confluent
      - propconf:/opt/lenovo/lxca/bin/conf
      - ssh:/etc/ssh
      - xcat:/etc/xcat
    networks:
      lan:
        ipv4_address: ${ADDRESS}
        ipv6_address: "2001:8003:7d51:2003::2"
    dns:
      - 192.0.2.10
      - 192.0.2.11
    deploy:
      resources:
        limits:
          cpus: "2.0"
          memory: "8g"

volumes:
  data:
    name: ${CONTAINER_NAME}-data
  postgresql:
    name: ${CONTAINER_NAME}-postgresql
  log:
    name: ${CONTAINER_NAME}-log
  confluent-etc:
    name: ${CONTAINER_NAME}-confluent-etc
  confluent-log:
    name: ${CONTAINER_NAME}-confluent-log
```

```
  confluent:
    name: ${CONTAINER_NAME}-confluent
  propconf:
    name: ${CONTAINER_NAME}-propconf
  ssh:
    name: ${CONTAINER_NAME}-ssh
  xcat:
    name: ${CONTAINER_NAME}-xcat

networks:
  lan:
    name: lan
    driver: macvlan
    enable_ipv6: true
    driver_opts:
      parent: eth0
    ipam:
      config:
        - subnet: 192.0.0.0/19
          gateway: 192.0.30.1
        - subnet: "2001:8003:7d51:2000::/80"
          gateway: "2001:8003:7d51:2000::1"
```

Passo 5. Distribuire l'immagine in docker, utilizzando il comando seguente, dove <*ENV_FILENAME*> è il nome del file delle variabili d'ambiente creato nel passaggio 2.

```
COMPOSE_HTTP_TIMEOUT=300 docker-compose -p ${CONTAINER_NAME} --env-file <ENV_FILENAME> up -d
```

Al termine

Eseguire il login e configurare XClarity Administrator (vedere Primo accesso all'interfaccia Web di Lenovo XClarity Administrator e Configurazione di Lenovo XClarity Administrator).

Implementazione dell'alta disponibilità

È possibile utilizzare Docker Datacenter per configurare un ambiente ad alta disponibilità per i contenitori Lenovo XClarity Administrator che vengono eseguiti in Docker Engine.

Per ulteriori informazioni sull'alta disponibilità di Docker Datacenter, vedere Pagina Web Architettura e app ad alta disponibilità con Docker Datacenter.

Capitolo 4. Configurazione di Lenovo XClarity Administrator

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

Ulteriori informazioni: XClarity Administrator: prima configurazione

Procedura

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

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

Passo 2. Leggere e accettare il contratto di licenza.

Passo 3. Creare account utente con autorità di supervisore.

Suggerimento: valutare la possibilità di creare almeno due account utente con autorità di supervisore in modo da avere un backup in caso di necessità.

Passo 4. Configurare l'accesso alla rete, inclusi gli indirizzi IP per le reti dati e di gestione.

Passo 5. Configurare la data e l'ora.

Passo 6. Configurare le impostazioni di assistenza e supporto, tra cui l'informativa sulla privacy, i dati su utilizzo e hardware, il supporto Lenovo (Call Home), la funzione Caricamento Lenovo e la garanzia del prodotto.

Passo 7. Configurare le impostazioni di sicurezza, inclusi il server di autenticazione, i gruppi di utenti, i certificati server e la modalità crittografica.

Passo 8. Gestire chassis, server, switch e dispositivi di storage.

Primo accesso all'interfaccia Web di Lenovo XClarity Administrator

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

Prima di iniziare

Accertarsi di utilizzare uno dei seguenti browser Web supportati:
- Chrome™ 48.0 o versioni successive (55.0 o versioni successive per la console remota)
- Firefox® ESR 38.6.0 o versioni successive
- Microsoft® Internet Explorer® 11
- Microsoft Edge
- Safari® 9.0.2 o versioni successive (IOS7 o versioni successive e OS X)

Nota: l'avvio delle interfacce del controller di gestione da XClarity Administrator mediante il browser Web Safari non è supportato.

Assicurarsi di eseguire il login all'interfaccia Web di XClarity Administrator da un sistema con connettività di rete al nodo di gestione di XClarity Administrator.

Procedura

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

Passo 1. Puntare il browser all'indirizzo IP di XClarity Administrator.

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

- **Per i contenitori**. Utilizzare l'indirizzo IPv4 specificato per la variabile ${ADDRESS} per accedere a XClarity Administrator utilizzando il seguente URL:
  `https://<IPv4_address>/ui/login.html`

  Ad esempio:
  `https://192.0.2.10/ui/login.html`

- **Per le appliance virtuali**. L'indirizzo IP utilizzato dipende dalla modalità di configurazione dell'ambiente.

  se le reti Eth0 e Eth1 si trovano in sottoreti diverse, e in entrambe viene usato DHCP, utilizzare l'indirizzo IP *Eth1* per accedere all'interfaccia Web ed eseguire la configurazione iniziale. Al primo avvio di XClarity Administrator sia Eth0 che Eth1 ottengono un indirizzo IP assegnato da DHCP mentre il gateway predefinito di XClarity Administrator viene impostato sul gateway assegnato da DHCP per *Eth1*.

  Utilizzo di un indirizzo IPv4 statico
  Se è stato specificato un indirizzo IPv4 in eth0_config, utilizzare tale indirizzo IPv4 per accedere a XClarity Administrator mediante il seguente URL:
  `https://<IPv4_address>/ui/login.html`

  Ad esempio:
  `https://192.0.2.10/ui/login.html`

  Utilizzo di un server DHCP nello stesso dominio di broadcast di XClarity Administrator
  Se un server DHCP è configurato nello stesso dominio di broadcast di XClarity Administrator, utilizzare l'indirizzo IPv4 visualizzato nella console della macchina virtuale di XClarity Administrator per accedere a XClarity Administrator mediante il seguente URL:
  `https://<IPv4_address>/ui/login.html`

  Ad esempio:
  `https://192.0.2.10/ui/login.html`

  Utilizzo di un server DHCP in un dominio di broadcast differente da XClarity Administrator
  Se un server DHCP *non* è configurato nello stesso dominio di broadcast, utilizzare l'indirizzo IPv6 locale rispetto al collegamento (Link-Local Address, LLA) visualizzato per eEth0, la rete di gestione, nella console della macchina virtuale di XClarity Administrator per accedere a XClarity Administrator, ad esempio:

```
------------------------------------------
Lenovo XClarity Administrator  Version x.x.x
------------------------------------------

eth0   flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500  metric 1
         inet 192.0.2.10  netmask 255.255.255.0  broadcast 192.0.2.55
         inet6 2001:db8:56ff:fe80:bea3  prefixlen 64   scopeid 0x20<link>
         ether 00:15:5d:0c:d1:92    txqueuelen 1000 (Ethernet)
         RX errors 0  dropped 0  overruns 0  frame 0

eth1   flags=4163<UP,BROADCAST,RUNNING,MULTICAST>  mtu 1500  metric 1
```

```
          inet 192.0.2.20  netmask 255.255.255.0  broadcast 192.0.2.130
          inet6 2001:db8:56ff:fe80:bea3  prefixlen 64  scopeid 0x20<link>

================================================================================
================================================================================

You have 150 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
  x. To continue without changing IP settings
  … …
```

Suggerimento: l'indirizzo IPv6 locale rispetto al collegamento (LLA) viene ricavato dall'indirizzo MAC dell'interfaccia.

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

– **Firefox:**

  Per accedere all'interfaccia Web di XClarity Administrator da un browser Firefox, eseguire il login utilizzando il seguente URL. Quando si immettono gli indirizzi IPv6, è necessario inserire le parentesi quadre.

  `https://[`*<IPv6_LLA>/ui/login.html*`]`

  Ad esempio, rispetto all'esempio precedente relativo a Eth0, immettere il seguente URL nel browser Web:

  `https://[fe80:21a:64ff:fe12:3456]/ui/login.html`

– **Internet Explorer:**

  Per accedere all'interfaccia Web di XClarity Administrator da un browser Internet Explorer, eseguire il login utilizzando il seguente URL. Quando si immettono gli indirizzi IPv6, è necessario inserire le parentesi quadre.

  `https://[`*<IPv6_LLA>*`%25`*<zone_index>*`]/ui/login.html`

  dove *<zone_index>* è l'identificativo dell'adattatore Ethernet connesso alla rete di gestione dal computer su cui si è avviato il browser Web. Se si utilizza un browser in Windows, usare il comando `ipconfig` per trovare l'indice di area, visualizzato dopo il segno di percentuale (%) nel campo **Indirizzo IPv6 locale rispetto al collegamento** per l'adattatore. Nell'esempio seguente l'indice di area è "30."

```
PS C:> ipconfig
Configurazione IP Windows

Adattatore Ethernet vEthernet (teamVirtualSwitch):

   Suffisso DNS specifico della connessione  . :
   Indirizzo IPv6 locale del collegamento . . . . . : 2001:db8:56ff:fe80:bea3%30
   Configurazione automatica dell'indirizzo IPv4. . : 192.0.2.30
   Gateway predefinito . . . . . :
```

  Se si utilizza un browser su Linux, utilizzare il comando `ifconfig` per trovare l'indice di area. Anche il nome dell'adattatore (generalmente Eth0) può essere utilizzato come indice di area.

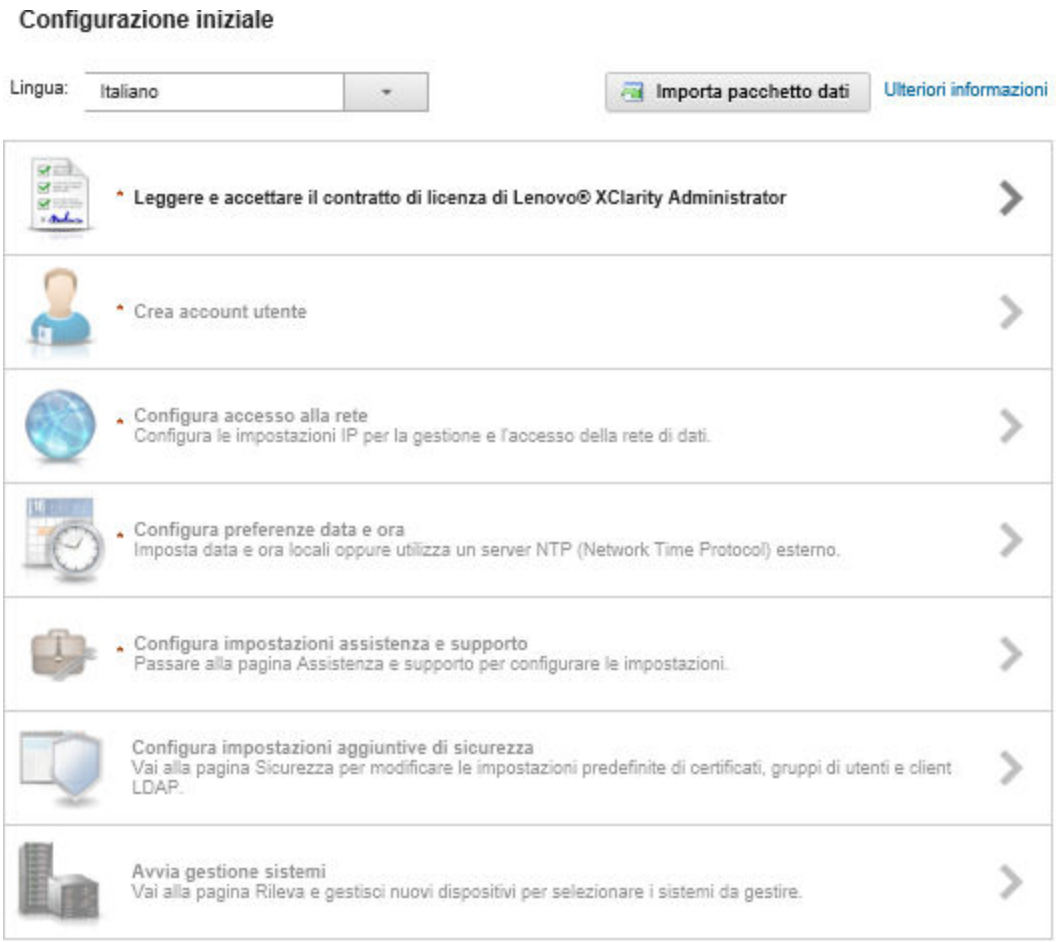
Ad esempio, rispetto agli esempi precedenti relativi a Eth0 e all'indice di area, immettere il seguente URL nel browser Web:

```
https://[2001:db8:56ff:fe80:bea3%2530]/ui/login.html
```

Passo 2. Al primo accesso a Lenovo XClarity Administrator si potrebbero ricevere avvertenze sulla sicurezza o sui certificati. È possibile ignorare tali avvertenze.

Risultati

Verrà visualizzata la pagina Configurazione iniziale.



Al termine

Completare i passaggi di configurazione iniziale per XClarity Administrator (vedere Configurazione di Lenovo XClarity Administrator).

Creazione di account utente

Gli account utente sono utilizzati per gestire l'autorizzazione e l'accesso a Lenovo XClarity Administrator e ai dispositivi gestiti con l'autenticazione gestita.

Informazioni su questa attività

Il primo account utente creato deve disporre del ruolo da supervisore e deve essere attivato (abilitato).

Come misura aggiuntiva di sicurezza, creare almeno due account utente con il ruolo **Supervisore**. Assicurarsi di registrare le password per questi account utente e memorizzarle in un'ubicazione sicura nel caso sia necessario ripristinare Lenovo XClarity Administrator.

Procedura

Per creare gli account utente, completare le seguenti operazioni.

Passo 1. Compilare le seguenti informazioni nella finestra di dialogo "Crea nuovo utente supervisore".

- Immettere un nome utente e una descrizione per l'utente stesso.
- Immettere e confermare le nuove password. Le regole per le password sono basate sulle impostazioni correnti di sicurezza dell'account.
- Selezionare uno o più gruppi di ruoli per autorizzare l'utente ad eseguire le attività appropriate.

  Per informazioni sui gruppi di ruoli e su come creare gruppi di ruoli personalizzati, vedere Creazione di un gruppo di ruoli nella documentazione online di XClarity Administrator.
- (Facoltativo) Impostare **Modifica password al primo accesso** su `Yes` se si desidera forzare l'utente a modificare la password quando esegue per la prima volta il login a XClarity Administrator.

Passo 2. Fare clic su **Crea**.

Passo 3. Fare clic sull'icona **Crea** ( ) e ripetere i passaggi precedenti per creare ulteriori utenti.

Passo 4. Fare clic su **Torna a Configurazione iniziale**.

Configurazione dell'accesso alla rete

Per configurare l'accesso alla rete, è possibile configurare fino a due interfacce di rete, il nome host per Lenovo XClarity Administrator e i server DNS da utilizzare.

Informazioni su questa attività

XClarity Administrator dispone di due interfacce di rete separate che possono essere definite in base all'ambiente, a seconda della topologia di rete implementata. Per le appliance virtuali, queste reti sono denominata eth0 ed eth1. Per i contenitori, è possibile scegliere nomi personalizzati.

- Se è presente solo un'interfaccia di rete (eth0):
  - L'interfaccia deve essere configurata per supportare il rilevamento dei dispositivi e la gestione (ad esempio, configurazione del server e aggiornamenti firmware). Deve essere in grado di comunicare con i moduli CMM e gli switch Flex di ogni chassis gestito, con il controller di gestione della scheda di base di ciascun server gestito e con ogni switch RackSwitch.
  - Se si intende acquistare gli aggiornamenti relativi a firmware e driver di dispositivo del sistema operativo mediante XClarity Administrator, almeno una delle interfacce di rete deve essere connessa a Internet, preferibilmente tramite un firewall. In caso contrario, è necessario importare gli aggiornamenti nel repository.
  - Se si desidera raccogliere i dati di servizio o utilizzare la notifica automatica dei problemi (come Call Home e Funzione Caricamento Lenovo), almeno una delle interfacce di rete deve essere collegata a Internet, preferibilmente tramite un firewall.
  - Se si intende distribuire le immagini del sistema operativo e aggiornare i driver di dispositivo del sistema operativo, l'interfaccia di rete deve disporre della connettività di rete IP all'interfaccia di rete del server utilizzata per accedere al sistema operativo host.

    Nota: Se si implementa una rete separata per la distribuzione del sistema operativo e gli aggiornamenti dei driver di dispositivo del sistema operativo, è possibile configurare la seconda interfaccia di rete per

il collegamento a questa rete invece che alla rete di dati. Tuttavia, se il sistema operativo di ciascun server non ha accesso alla rete di dati, è necessario configurare un'interfaccia aggiuntiva sui server per fornire la connettività dal sistema operativo host alla rete di dati, per la distribuzione del sistema operativo e gli aggiornamenti dei driver di dispositivo del sistema operativo

- Se sono presenti due interfacce di rete (eth0 e eth1):
  - La prima interfaccia di rete (in genere, l'interfaccia Eth0) deve essere collegata alla rete di gestione e configurata per supportare il rilevamento dei dispositivi e la gestione (come configurazione del server e aggiornamenti firmware). Deve essere in grado di comunicare con i moduli CMM e gli switch Flex di ogni chassis gestito, con il controller di gestione di ciascun server gestito e con ogni switch RackSwitch.
  - La seconda interfaccia di rete (generalmente l'interfaccia eth1) può essere configurata per comunicare con una rete di dati interna, una rete di dati pubblica o entrambe.
  - Se si intende acquistare gli aggiornamenti relativi a firmware e driver di dispositivo del sistema operativo mediante XClarity Administrator, almeno una delle interfacce di rete deve essere connessa a Internet, preferibilmente tramite un firewall. In caso contrario, è necessario importare gli aggiornamenti nel repository.
  - Se si desidera raccogliere i dati di servizio o utilizzare la notifica automatica dei problemi (come Call Home e Funzione Caricamento Lenovo), almeno una delle interfacce di rete deve essere collegata a Internet, preferibilmente tramite un firewall.
  - Se si intende distribuire le immagini del sistema operativo e aggiornare i driver di dispositivo, è possibile scegliere di utilizzare l'interfaccia eth1 o eth0. Tuttavia, l'interfaccia utilizzata deve disporre della connettività di rete IP all'interfaccia di rete del server utilizzato per accedere al sistema operativo host.

    Nota: Se si implementa una rete separata per la distribuzione del sistema operativo e gli aggiornamenti dei driver di dispositivo del sistema operativo, è possibile configurare la seconda interfaccia di rete per il collegamento a questa rete invece che alla rete di dati. Tuttavia, se il sistema operativo di ciascun server non ha accesso alla rete di dati, è necessario configurare un'interfaccia aggiuntiva sui server per fornire la connettività dal sistema operativo host alla rete di dati, per la distribuzione del sistema operativo e gli aggiornamenti dei driver di dispositivo del sistema operativo

Nella seguente tabella sono riportate le possibili configurazioni per le interfacce di rete di XClarity Administrator in base al tipo di topologia di rete implementata nell'ambiente. Utilizzare questa tabella per determinare le modalità di definizione di ciascuna interfaccia di rete.

Tabella 3. Ruolo di ciascuna interfaccia di rete basata sulla topologia di rete

Topologia di rete	Ruolo dell'interfaccia 1 (eth0)	Ruolo dell'interfaccia 2 (eth1)
Rete convergente (rete di dati e gestione con supporto per la distribuzione del sistema operativo e degli aggiornamenti dei driver di dispositivo del sistema operativo)	Rete di gestione • Rilevamento e gestione • Configurazione server • Aggiornamenti firmware • Raccolta dei dati di servizio • Notifica automatica dei problemi (ad esempio, Call Home e Funzione Aggiornamento Lenovo) • Recupero dei dati sulla garanzia • Distribuzione sistema operativo • Aggiornamenti dei driver di dispositivo del sistema operativo	Nessuna
Rete di gestione separata con supporto per la distribuzione del sistema operativo, degli aggiornamenti dei driver di dispositivo del sistema operativo e della rete di dati	Rete di gestione • Rilevamento e gestione • Configurazione server • Aggiornamenti firmware • Raccolta dei dati di servizio • Notifica automatica dei problemi (ad esempio, Call Home e Funzione Aggiornamento Lenovo) • Recupero dei dati sulla garanzia • Distribuzione sistema operativo • Aggiornamenti dei driver di dispositivo del sistema operativo	Rete di dati • Nessuna
Rete di gestione separata e rete di dati con supporto per la distribuzione del sistema operativo e degli aggiornamenti dei driver di dispositivo	Rete di gestione • Rilevamento e gestione • Configurazione server • Aggiornamenti firmware • Raccolta dei dati di servizio • Notifica automatica dei problemi (ad esempio, Call Home e Funzione Aggiornamento Lenovo) • Recupero dei dati sulla garanzia	Rete di dati • Distribuzione sistema operativo • Aggiornamenti dei driver di dispositivo del sistema operativo
Rete di gestione separata e rete di dati senza supporto per la distribuzione del sistema operativo e degli aggiornamenti dei driver di dispositivo	Rete di gestione • Rilevamento e gestione • Configurazione server • Aggiornamenti firmware • Raccolta dei dati di servizio • Notifica automatica dei problemi (ad esempio, Call Home e Funzione Aggiornamento Lenovo) • Recupero dei dati sulla garanzia	Rete di dati • Nessuna
Rete di sola gestione (la distribuzione del sistema operativo e dei driver di dispositivo del sistema operativo non è supportata)	Rete di gestione • Rilevamento e gestione • Configurazione server • Aggiornamenti firmware • Raccolta dei dati di servizio • Notifica automatica dei problemi (ad esempio, Call Home e Funzione Aggiornamento Lenovo) • Recupero dei dati sulla garanzia	Nessuna

Per ulteriori informazioni sulle interfacce di rete XClarity Administrator, vedere Considerazioni sulla rete.

Procedura

Per configurare l'accesso alla rete, attenersi alla procedura descritta di seguito.

Passo 1. Nella pagina Configurazione iniziale fare clic su **Configura accesso alla rete**. Verrà visualizzata la pagina Modifica accesso alla rete.

Passo 2. Se si intende distribuire i sistemi operativi e aggiornare i driver di dispositivo del sistema operativo mediante XClarity Administrator, scegliere l'interfaccia di rete da utilizzare per la gestione dei sistemi operativi.

- Se è definita solo un'interfaccia per XClarity Administrator, scegliere se utilizzarla solo per rilevare e gestire l'hardware oppure anche per gestire i sistemi operativi.
- Se sono definite due interfacce per XClarity Administrator (Eth0 ed Eth1), scegliere quella da utilizzare per gestire i sistemi operativi. Se si sceglie "Nessuno", *non* sarà possibile distribuire le immagini del sistema operativo o aggiornare i driver di dispositivo del sistema operativo dei server gestiti da XClarity Administrator.

Passo 3. Specificare le impostazioni IP.

a. Per la prima interfaccia, specificare l'indirizzo IPv4, l'indirizzo IPv6 o entrambi.

- **IPv4**. È necessario assegnare un indirizzo IPv4 all'interfaccia. È possibile scegliere di utilizzare un indirizzo IP assegnato staticamente oppure ottenere un indirizzo IP da un server DHCP.
- **IPv6**. Facoltativamente, è possibile assegnare un indirizzo IPv6 all'interfaccia mediante uno dei seguenti metodi di assegnazione:
  - Utilizza indirizzo IP assegnato in modo statico
  - Utilizza la configurazione dell'indirizzo senza stato (DHCPv6)
  - Utilizza configurazione automatica dell'indirizzo senza stato

  Nota: Per informazioni sulle limitazioni degli indirizzi IPv6, vedere Limitazioni della configurazione IP.

b. Se è disponibile una seconda interfaccia, specificare l'indirizzo IPv4, l'indirizzo IPv6 o entrambi.

Nota: Gli indirizzi IP assegnati a questa interfaccia devono essere in una sottorete diversa da quella degli indirizzi IP assegnati alla prima interfaccia. Se si decide di utilizzare DHCP per assegnare indirizzi IP per entrambe le interfacce (Eth0 e Eth1), il server DHCP non deve assegnare la stessa sottorete per gli indirizzi IP delle due interfacce.

- **IPv4**. È possibile scegliere di utilizzare un indirizzo IP assegnato staticamente oppure ottenere un indirizzo IP da un server DHCP.
- **IPv6**. Facoltativamente, è possibile assegnare un indirizzo IPv6 all'interfaccia mediante uno dei seguenti metodi di assegnazione:
  - Utilizza indirizzo IP assegnato in modo statico
  - Utilizza la configurazione dell'indirizzo senza stato (DHCPv6)
  - Utilizza configurazione automatica dell'indirizzo senza stato

c. Specificare il gateway predefinito.

Se si specifica un gateway predefinito, deve essere un indirizzo IP valido e utilizzare la stessa maschera di rete (la stessa sottorete) dell'indirizzo IP per una delle interfacce di rete (Eth0 o Eth1). Se si utilizza una singola interfaccia, il gateway predefinito deve essere nella stessa sottorete dell'interfaccia di rete.

Se una delle due interfaccia utilizza DHCP per ottenere l'indirizzo IP, anche il gateway predefinito utilizza DHCP. Per immettere manualmente un indirizzo gateway predefinito che sovrascriva quello ricevuto dal server DHCP, selezionare la casella di controllo **Sovrascrivi gateway**.

Suggerimenti:

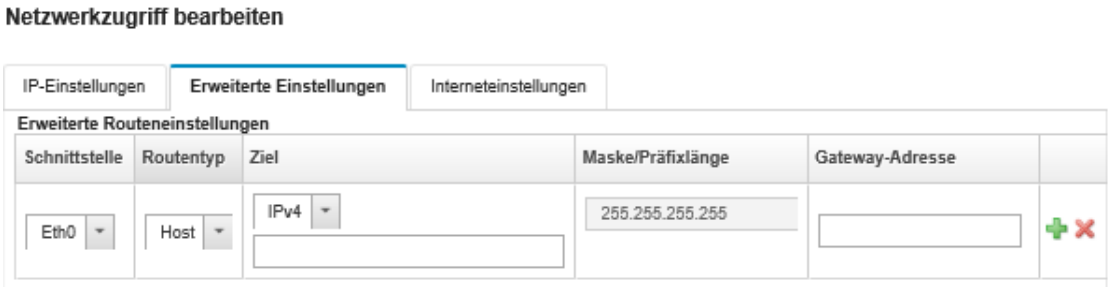
- Verificare che il gateway corrisponda a una sottorete delle interfacce di rete. Il gateway predefinito viene impostato automaticamente tramite questa interfaccia di rete.
- Per tornare a un gateway fornito da DHCP, deselezionare la casella di controllo **Sovrascrivi gateway**.

ATTENZIONE:
Se si sceglie di ignorare il gateway, immettere l'indirizzo gateway corretto. In caso contrario, questo server di gestione non sarà raggiungibile e non vi sarà alcun modo di eseguire il log in remoto per correggerlo.

d. Fare clic su **Salva impostazioni IP**.

Passo 4. **Facoltativo:** configurare le impostazioni avanzate.

a. Fare clic sulla scheda **Instradamento avanzato**.



b. Specificare una o più voci di instradamento nella tabella **Impostazioni instradamento avanzate** per l'utilizzo da parte di questa interfaccia.

Per definire una o più voci di instradamento, attenersi alla procedura descritta di seguito.

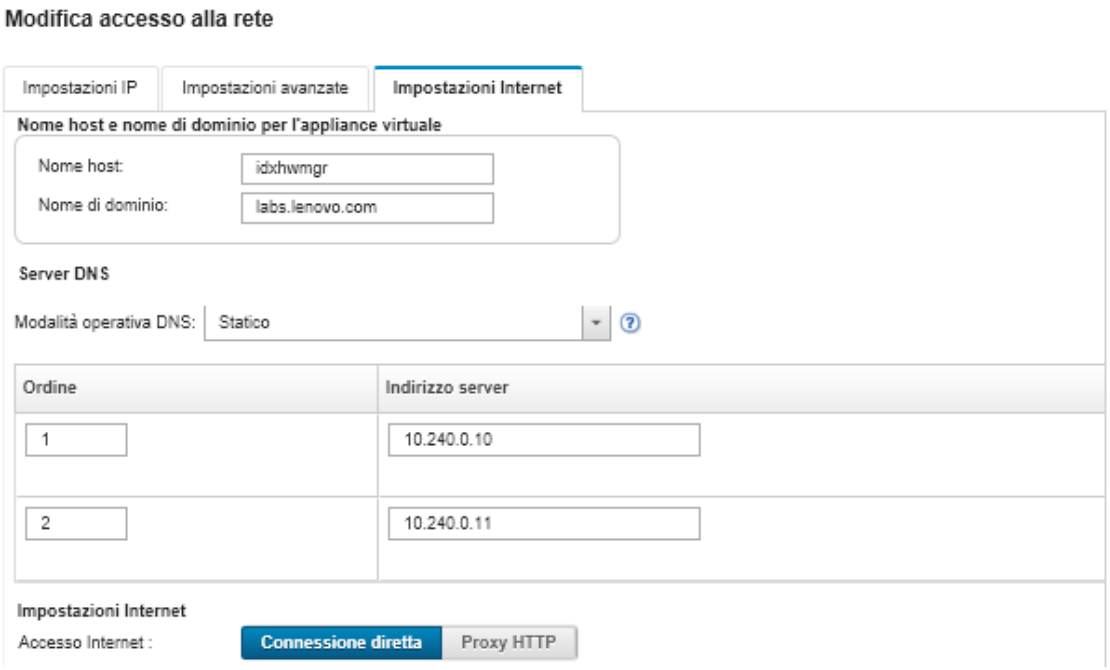
1. Scegliere l'interfaccia.

2. Specificare il tipo di instradamento, che può essere un instradamento a un altro host o a una rete.
3. Specificare l'indirizzo di rete o l'host di destinazione a cui si esegue l'indirizzamento dell'instradamento.
4. Specificare la maschera di sottorete per l'indirizzo di destinazione.
5. Specificare l'indirizzo gateway a cui verranno indirizzati i pacchetti.

c. Fare clic sulla scheda **Salva instradamento avanzato**.

Passo 5. Facoltativamente, modificare le impostazioni DNS e proxy.

a. Fare clic sulla scheda **DNS e proxy**.



b. Specificare il nome host e il nome di dominio da utilizzare per XClarity Administrator.

c. Selezionare la modalità operativa DNS. Può essere **Statica** o **DHCP**.

Attenzione: È necessario riavviare il server di gestione quando si modifica la modalità operativa DNS.

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 Administrator.

d. Specificare l'indirizzo IP di uno o più server DNS (Domain Name System) da utilizzare e l'ordine di priorità per ciascuno di essi.

e. Specificare se accedere a Internet utilizzando una connessione diretta o un proxy HTTP (se XClarity Administrator ha accesso a Internet).

Nota: Se si utilizza un proxy HTTP, verificare che siano rispettati i seguenti requisiti.
- 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.

Se si sceglie di utilizzare un proxy HTTP, compilare i campi obbligatori:

1. Specificare il nome host e la porta del server proxy.
2. Scegliere se utilizzare l'autenticazione e specificare il nome utente e la password, se necessario.
3. Specificare l'URL del test proxy.
4. Fare clic su **Test proxy** per verificare che le impostazioni proxy siano configurati e funzionino correttamente.

f. Fare clic su **Salva DNS e proxy**.

g. È possibile eseguire il push del nome FQDN (Fully-Qualified Domain Name) e delle informazioni DNS del server di gestione XClarity Administrator ai server gestiti con IMM2, XCC e XCC2, in modo che i server gestiti possano trovare il server di gestione utilizzando queste informazioni.

1. Fare clic su **Esegui push di FQDN/DNS su BMC**.
2. Scegliere come gestire le voci DNS esistenti nel controller di gestione della scheda di base.
   - Mantenere le voci DNS esistenti e aggiungere le voci DNS del server di gestione nel successivo slot disponibile.
   - Sostituire tutte le voci DNS esistenti con le voci DNS del server di gestione.
3. Digitare **SÌ** nel campo di modifica.
4. Fare clic su **Applica**.

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 Utilizzo dei processi nella documentazione online di XClarity Administrator).

È inoltre possibile rimuovere le informazioni DNS e FQDN del server di gestione dai server gestiti con IMM2, XCC e XCC2 facendo clic su **Rimuovi FQDN/DNS da BMC**. È possibile scegliere di mantenere altre voci DNS esistenti, rimuovere tutte le voci DNS oppure rimuovere solo le voci che corrispondono alle informazioni del server di gestione.

Passo 6. Fare clic su **Indietro**.

Passo 7. Fare clic su **Test della connessione** per verificare le impostazioni di rete.

Configurazione di data e ora

Sebbene sia possibile impostare manualmente la data e l'ora per Lenovo XClarity Administrator, un approccio migliore consiste nel configurare un server NTP (Network Time Protocol) utilizzabile per sincronizzare i timestamp tra XClarity Administrator e tutti i dispositivi gestiti.

Prima di iniziare

È necessario utilizzare almeno uno (e fino a quattro) server NTP (Network Time Protocol) per sincronizzare i timestamp di tutti gli eventi ricevuti dai dispositivi gestiti con XClarity Administrator.

Suggerimento: il server NTP deve essere accessibile sulla rete di gestione (in genere, l'interfaccia Eth0). Valutare la possibilità di configurare il server NTP sull'host in cui XClarity Administrator è in esecuzione.

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

Attenzione: L'appliance virtuale XClarity Administrator 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

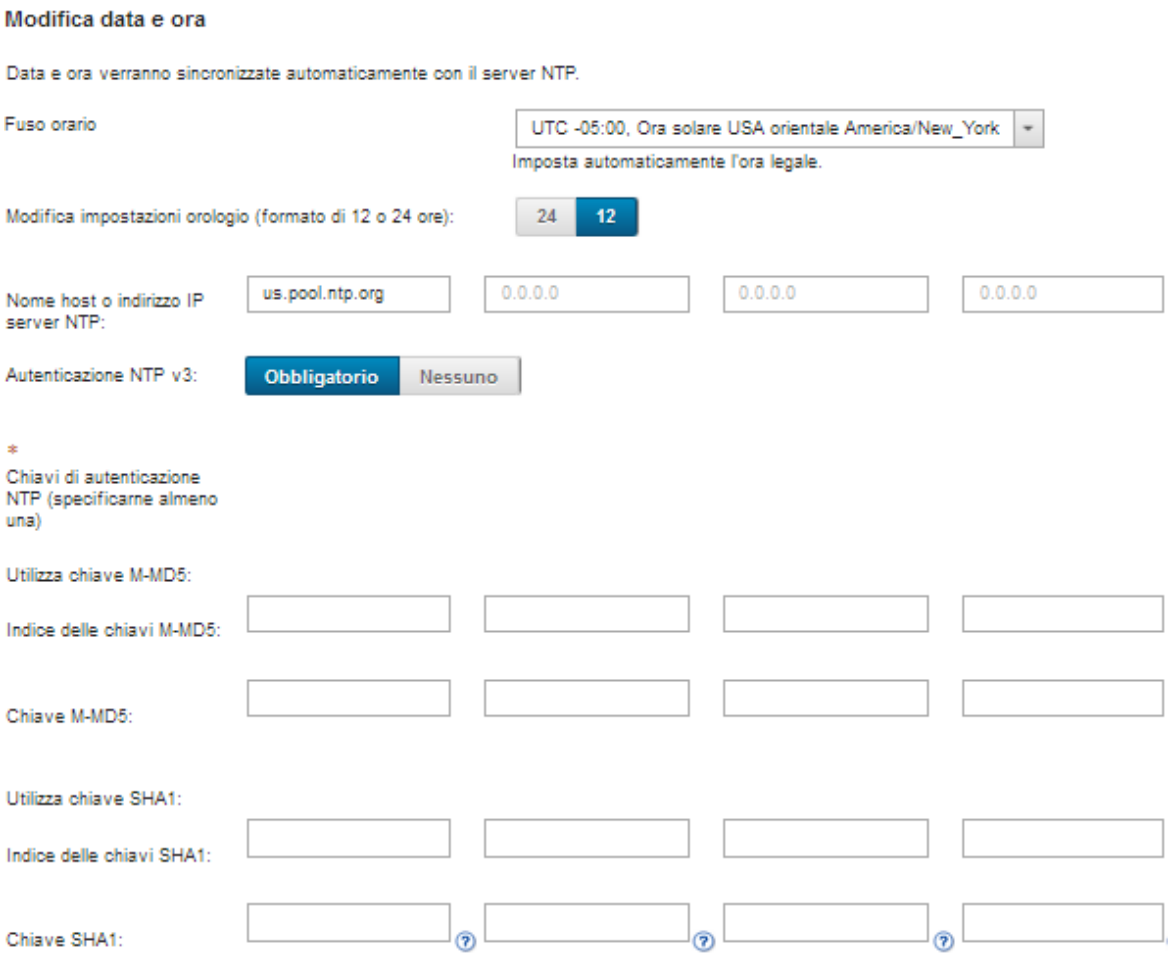
Administrator e il relativo host. In genere, l'host è configurato per sincronizzarsi con l'ora delle rispettive appliance virtuali. Se XClarity Administrator è impostato per sincronizzarsi con un'origine differente rispetto all'host, è necessario disabilitare la sincronizzazione oraria dell'host tra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

- Per ESXi, seguire le istruzioni sulla VMware - Pagina Web sulla disabilitazione della sincronizzazione dell'ora.
- Per Hyper-V di Hyper-V Manager, fare clic con il pulsante destro del mouse sulla macchina virtuale XClarity Administrator e quindi fare clic su **Impostazioni**. Nella finestra di dialogo, fare clic su **Gestione > Servizi di integrazione** nel riquadro di navigazione e quindi deselezionare **Sincronizzazione ora**.

Procedura

Per configurare un server NTP per XClarity Administrator, attenersi alla procedura descritta di seguito.

Passo 1. Nella pagina Configurazione iniziale, fare clic su **Configura preferenze data e ora**. Verrà visualizzata la pagina Modifica data e ora.



Passo 2. Compilare la finestra di dialogo Data e ora.

1. Scegliere il fuso orario in cui si trova l'host per XClarity Administrator.

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

2. Scegliere di utilizzare un formato a 12 o 24 ore.
3. Specificare il nome host o l'indirizzo IP di ciascun server NTP nella rete. È possibile definire fino a quattro server NTP.

4. Selezionare **Richiesta** per abilitare l'autenticazione NTP v3 oppure **Nessuno** per utilizzare l'autenticazione NTP v1 tra XClarity Administrator e i server NTP in rete.

   È possibile utilizzare l'autenticazione v3 se i moduli CMM di Flex System e i controller di gestione della scheda di base utilizzano firmware che richiedono l'autenticazione v3 e se l'autenticazione NTP v3 è richiesta tra XClarity Administrator e uno o più dei server NTP nella rete

5. Se si abilita l'autenticazione NTP v3, impostare la chiave di autenticazione e l'indice per ciascun server NTP applicabile. È possibile specificare una chiave M-MD5, SHA1 o entrambe. Se sono state specificate le chiavi M-MD5 e SHA1, XClarity Administrator effettua il push della chiave M-MD5 o SHA1 ai moduli CMM di Flex System e ai controller di gestione che la supportano. XClarity Administrator utilizza la chiave per eseguire l'autenticazione con il server NTP.
   - Per la chiave M-MD5, specificare una stringa ASCII che include solo lettere minuscole e maiuscole (a-z, a-Z), cifre (0-9) e i seguenti caratteri speciali @#.
   - Per la chiave SHA1, specificare una stringa ASCII di 40 caratteri, includendo esclusivamente numeri tra 0 e 9 e lettere tra a e f.
   - L'indice della chiave specificata e la chiave di autenticazione devono corrispondere all'ID della chiave e alla password impostati nel server NTP. Ad esempio, se l'indice chiave della chiave SHA1 immessa nel server NTP è 5, anche l'indice della chiave specificato della chiave SHA1 di XClarity Administrator è 5. Per informazioni sull'impostazione dell'ID della chiave e della password, vedere la documentazione del server NTP.
   - È necessario specificare la chiave per ciascun server NTP che utilizza l'autenticazione v3, anche se due o più server NTP utilizzano la stessa chiave.
   - Se si abilita l'autenticazione v3, ma non vengono fornite una chiave di autenticazione e l'indice per un server NTP, l'autenticazione v1 viene utilizzata per impostazione predefinita.
   - Se sono stati specificati più server NTP, i server NTP devono disporre tutti dell'autenticazione v3 o v1. Un insieme di server NTP con autenticazione v3 e v1 mista non è supportato.
   - Se sono stati specificati più server NTP con autenticazione v3, gli indici di chiave devono essere univoci se le chiavi non sono identiche. Ad esempio, i server NTP 1 e 2 non possono avere l'indice di chiave SHA1 del server 1, se le chiavi SHA1 del server NTP 1 e 2 sono differenti. È necessario riconfigurare uno dei server NTP per accettare la chiave con un indice di chiave differente rispetto all'altro server NTP. In caso contrario, l'ultima chiave definita associata a un indice di chiave verrà configurata per tutti i server NTP con lo stesso indice di chiave.

Passo 3. Fare clic su **Salva**.

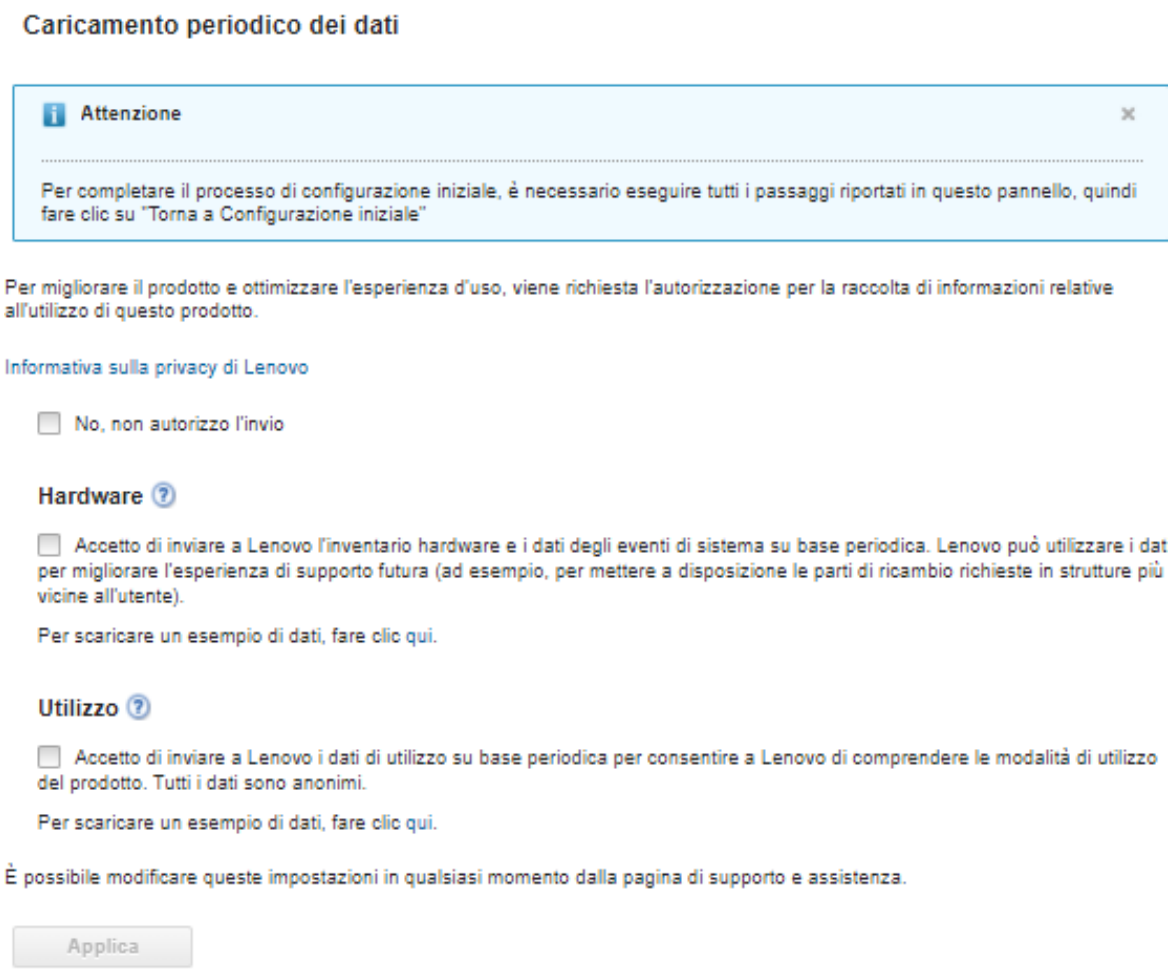
Configurazione assistenza e supporto

È possibile configurare le impostazioni di assistenza e supporto, tra cui i dati sull'utilizzo, il supporto Lenovo (Call Home), la funzione caricamento Lenovo e la garanzia del prodotto.

Procedura

Per configurare la sicurezza, attenersi alla procedura descritta di seguito.

Passo 1. Nella pagina Configurazione iniziale, fare clic su **Configura impostazioni assistenza e supporto**. Verrà visualizzata la pagina Assistenza e supporto.



Passo 2. Leggere e accettare l'Informativa sulla privacy di Lenovo.

Nota: Non è possibile raccogliere e inviare dati a Lenovo senza prima accettare l'Informativa sulla privacy di Lenovo. Se si sceglie di rifiutare l'informativa sulla privacy, è possibile rivedere e accettare l'informativa sulla privacy in un secondo momento dalla pagina **Assistenza e supporto → Configurazione Call Home**.

Passo 3. Facoltativamente, consentire a Lenovo XClarity Administrator di raccogliere informazioni su hardware e utilizzo, quindi fare clic su **Applica**.

È possibile raccogliere e inviare i seguenti tipi di dati a Lenovo.

- **Dati di utilizzo**

  Quando si accetta di inviare i dati di utilizzo a Lenovo, i seguenti dati vengono raccolti e inviati settimanalmente. Questi dati *sono anonimi*. Nessun dato privato (inclusi numeri di serie, UUID, nomi host, indirizzi IP e nomi utente) viene raccolto o inviato a Lenovo.
  - Log delle azioni eseguite
  - Elenco di eventi generati con relativa data/ora
  - Elenco di eventi di controllo generati con relativa data/ora
  - Elenco dei processi eseguiti e informazioni sull'esito positivo o negativo per ogni processo
  - Metriche di XClarity Administrator, come utilizzo della memoria, utilizzo del processore e spazio su disco
  - Dati di inventario limitati di tutti i dispositivi gestiti
- **Dati hardware**

Quando si accetta di inviare i dati hardware a Lenovo, i seguenti dati vengono raccolti e inviati periodicamente. Questi dati *non sono anonimi*. I dati hardware includono attributi, come UUID e numeri di serie. Non includono indirizzi IP o nomi host.

- **Dati hardware quotidiani**. Per ogni modifica dell'inventario vengono inclusi i seguenti dati.
  - Evento di modifica dell'inventario (FQXHMDM0001I)
  - Modifiche dei dati di inventario per il dispositivo associato a tale evento
- **Dati hardware settimanali**. I dati di inventario inclusi per tutti i dispositivi gestiti.

Quando i dati su utilizzo e hardware vengono inviati a Lenovo, viene registrato un evento nel log di controllo.

È possibile modificare questa impostazione in qualsiasi momento e scaricare l'ultimo archivio raccolto e inviato a Lenovo facendo clic sui collegamenti **Amministrazione → Assistenza e supporto**, quindi selezionando la scheda **Caricamento dati periodico**.

Passo 4. Facoltativamente, fare clic su **Configurazione Call Home** per configurare la notifica automatica dei problemi al supporto Lenovo (Call Home). Quindi, fare clic su **Applica e abilita** per creare il server d'inoltro di servizio Call Home predefinito oppure fare clic su **Applica solo** per salvare le informazioni di contatto.

Per ulteriori informazioni sull'impostazione della notifica automatica dei problemi al supporto Lenovo, vedere Configurazione di call home nella documentazione online di XClarity Administrator.

Passo 5. Facoltativamente, fare clic su **Funzione Caricamento Lenovo** per configurare la notifica automatica dei problemi per la Funzione Caricamento Lenovo. Quindi, fare clic su **Applica e abilita** per creare il server d'inoltro di servizio predefinito della Funzione Caricamento Lenovo oppure fare clic su **Applica solo** per salvare le informazioni delle impostazioni.

Per ulteriori informazioni sull'impostazione della notifica automatica dei problemi per la Funzione Caricamento Lenovo, vedere Configurazione dell'invio di notifiche automatiche dei problemi alla Funzione Caricamento Lenovo nella documentazione online di XClarity Administrator.

Passo 6. Facoltativamente, fare clic su **Garanzia** per abilitare le connessioni esterne necessarie per raccogliere le informazioni sulla garanzia per i dispositivi gestiti.

Per ulteriori informazioni sulla visualizzazione sullo stato della garanzia (incluse le estensioni della garanzia) dei dispositivi gestiti, vedere Visualizzazione delle informazioni sulla garanzia nella documentazione online di XClarity Administrator.

Passo 7. Facoltativamente, fare clic su **Servizio comunicato Lenovo** per autorizzare Lenovo a inviare comunicati di servizio a XClarity Administrator, quindi selezionare **Applica**

Per ulteriori informazioni sui tipi di comunicati di servizio inviati da Lenovo, vedere Ottenere i comunicati da Lenovo nella documentazione online di XClarity Administrator.

Passo 8. Specificare la password di ripristino del servizio che è possibile utilizzare per raccogliere e scaricare i dati di servizio e i log se XClarity Administrator non risponde e non può essere ripristinato.

Per ulteriori informazioni sulla password di ripristino del servizio, vedere Modifica della password di ripristino del servizio nella documentazione online di XClarity Administrator.

Passo 9. Fare clic su **Torna a Configurazione iniziale**.

Configurazione della protezione

È possibile configurare la sicurezza, inclusi gruppi di ruoli, server di autenticazione, impostazioni di sicurezza degli account utente, crittografia e certificati.

Procedura

Per configurare la sicurezza, attenersi alla procedura descritta di seguito.

Passo 1. Nella pagina Configurazione iniziale, fare clic su **Configura impostazioni aggiuntive di sicurezza**. Verrà visualizzata la pagina Sicurezza.

Passo 2. Creare gruppi di ruoli personalizzati per gestire l'autorizzazione e l'accesso alle risorse (vedere Creazione di un gruppo di ruoli nella documentazione online di XClarity Administrator).

Un *gruppo di ruoli* è una raccolta di uno o più ruoli che viene utilizzata per assegnare i ruoli a più utenti. I ruoli configurati per un gruppo di ruoli determinano il livello di accesso concesso a ciascun utente membro di questo gruppo di ruoli. Ogni utente XClarity Administrator deve essere membro di almeno un gruppo di ruoli.

Passo 3. Configurare il server di autenticazione (vedere Gestione del server di autenticazione nella documentazione online di XClarity Administrator).

Il *server di autenticazione* è un server Microsoft Active Directory (LDAP) utilizzato per autenticare le credenziali utente. XClarity Administrator utilizza un singolo server di autenticazione per la gestione centrale di tutti i dispositivi gestiti (ad eccezione degli switch Flex) da parte degli utenti. Quando un dispositivo è gestito da XClarity Administrator, il dispositivo gestito e i relativi componenti installati (ad eccezione degli switch Flex) vengono configurati per l'utilizzo del server di autenticazione di XClarity Administrator. Gli account utente definiti nel server di autenticazione consentono di eseguire il login a XClarity Administrator, ai CMM e al controller di gestione della scheda di base.

È possibile scegliere di utilizzare un server di autenticazione esterna invece del server di autenticazione locale sul nodo di gestione.

Passo 4. Configurare le impostazioni di sicurezza degli account utente, che controllano la complessità delle password, il blocco degli account e il timeout di inattività delle sessioni Web (vedere Modifica delle impostazioni di sicurezza dell'account utente nella documentazione online di XClarity Administrator).

Passo 5. Configurare l'impostazione crittografica che definisce le modalità e i protocolli di comunicazione che controllano la modalità di gestione delle comunicazioni sicure tra XClarity Administrator e i dispositivi gestiti (vedere Impostazione della modalità crittografica e dei protocolli di comunicazione nella documentazione online di XClarity Administrator)

Passo 6. Se si pianifica di gestire i server rack utilizzando l'autenticazione locale invece dell'autenticazione gestita di XClarity Administrator, creare uno o più credenziali memorizzate che corrispondano agli account utente attivi sul dispositivo o in Active Directory, che possono essere utilizzati per eseguire il login ai dispositivi durante il processo di gestione. Per ulteriori informazioni sulle credenziali memorizzate, vedere Gestione delle credenziali memorizzate nella documentazione online di XClarity Administrator.

Passo 7. Se si desidera utilizzare un certificato server personalizzato che include le informazioni personali oppure un certificato con firma esterna, generare e distribuire il nuovo certificato prima di iniziare a gestire i sistemi. Per informazioni sulla generazione di un certificato di sicurezza personale, vedere Utilizzo dei certificati di sicurezza nella documentazione online di XClarity Administrator.

Passo 8. Dal menu verticale nella pagina Sicurezza, fare clic su **Torna a Configurazione iniziale**.

Gestione dei dispositivi

Lenovo XClarity Administrator può gestire diversi tipi di sistemi, tra cui chassis di Flex System, server tower e rack, switch RackSwitch e dispositivi di storage. È possibile rilevare e gestire facilmente numerosi dispositivi situati nell'ambiente utilizzato, importando le informazioni sui dispositivi mediante un file di importazione di massa.

Prima di iniziare

Importante:

- È possibile gestire un massimo di 300 dispositivi contemporaneamente. Non includere non più di 300 dispositivi in un file di importazione di massa.
- Dopo aver avviato un'operazione di gestione dei dispositivi, attendere il completamento dell'intero processo di gestione prima di avviare un'altra operazione di gestione dei dispositivi.

I componenti dello chassis (CMM, nodi di elaborazione, switch e dispositivi di storage) vengono rilevati e gestiti automaticamente mentre si gestisce lo chassis che li contiene. Non è possibile rilevare e gestire componenti dello chassis separati.

Alcune porte devono essere disponibili per comunicare con i CMM nello chassis e nei controller di gestione della scheda di base nei server. Accertarsi che queste porte siano disponibili prima di gestire i sistemi. Per ulteriori informazioni sulle porte, vedere Disponibilità della porta.

Accertarsi che sia installato il firmware minimo richiesto in ciascun sistema che si desidera gestire mediante XClarity Administrator. È possibile trovare i livelli minimi di firmware richiesti sulle Supporto XClarity Administrator - Pagina Web sulla compatibilità facendo clic sulla scheda **Compatibilità** e quindi sul collegamento per i tipi di dispositivi appropriati.

Verificare che vi siano almeno tre sessioni della modalità comando TCP impostate per la comunicazione fuori banda con CMM. Per informazioni sull'impostazione del numero di sessioni, vedere Comando tcpcmdmode nella documentazione online del modulo CMM.

Implementare indirizzi IPv4 *o* IPv6 per tutti i moduli CMM e gli switch Flex gestiti da XClarity Administrator. Se si implementa IPv4 per alcuni CMM e switch Flex e IPv6 per altri, alcuni eventi potrebbero non essere ricevuti nel log di controllo (o come trap di controllo).

Verificare che sia abilitato l'inoltro SLP multicast sugli switch TOR (Top-of-Rack) e sui router del proprio ambiente. Consultare la documentazione fornita con lo switch o il router specifico per determinare se l'inoltro SLP multicast è abilitato e per reperire le procedure necessarie per abilitarlo qualora sia disabilitato.

Importante:

- A seconda della versione del firmware dello switch RackSwitch, potrebbe essere necessario abilitare manualmente l'inoltro SLP multicast e il protocollo SSH su ogni switch RackSwitch utilizzando i seguenti comandi prima che lo switch possa essere rilevato e gestito da XClarity Administrator. Per ulteriori informazioni, vedere le Switch rack nella documentazione online di System x.
- L'inoltro SLP multicast deve essere abilitato in ogni dispositivo di storage affinché possa essere rilevato da XClarity Administrator.
- Se si desidera utilizzare un certificato server personalizzato che include le informazioni personali oppure un certificato con firma esterna, generare e distribuire il nuovo certificato prima di iniziare a gestire i sistemi. Per informazioni sulla generazione di un certificato di sicurezza personale, vedere Utilizzo dei certificati di sicurezza nella documentazione online di XClarity Administrator.
- Se oltre a Lenovo XClarity Administrator si intende utilizzare un altro software di gestione per monitorare lo chassis, e tale software di gestione utilizza la comunicazione SNMPv3, è necessario prima creare un ID utente CMM locale configurato con le informazioni SNMPv3 appropriate, poi eseguire il login al CMM utilizzando tale ID utente, quindi modificare la password. Per ulteriori informazioni, vedere Considerazioni sulla gestione nella documentazione online di XClarity Administrator.
- I protocolli di rilevamento dei servizi, ad esempio SLP e SSDP, consentono di individuare automaticamente il tipo di dispositivo XClarity Administrator che sta per essere gestito e quindi di utilizzare il meccanismo appropriato per gestire il dispositivo. Alcuni tipi di dispositivo non supportano i protocolli di rilevamento dei servizi e in alcuni ambienti i protocolli di rilevamento dei servizi sono disattivati specificamente. In entrambi i casi, è necessario scegliere il tipo di dispositivo appropriato per

completare il processo di gestione. I tipi di dispositivo seguenti devono essere identificati in modo esplicito.
  - Switch Lenovo ThinkSystem serie DB
  - Switch NVIDIA Mellanox

Informazioni su questa attività

XClarity Administrator può rilevare i sistemi in un ambiente individuando i dispositivi gestibili che si trovano nella stessa sottorete IP di XClarity Administrator, utilizzando un indirizzo IP o un intervallo di indirizzi IP specificato oppure importando le informazioni da un foglio di calcolo.

Per impostazione predefinita, i dispositivi vengono gestiti utilizzando l'autenticazione gestita di XClarity Administrator per eseguire il login ai dispositivi. Quando si gestiscono i server rack e lo chassis Lenovo, è possibile scegliere di utilizzare l'autenticazione locale o gestita per eseguire il login ai dispositivi.

- Quando l'*autenticazione locale* viene utilizzata per i server rack, lo chassis Lenovo e gli switch rack Lenovo, XClarity Administrator utilizza una credenziale memorizzata per eseguire l'autenticazione al dispositivo. La *credenziale memorizzata* può essere un account utente attivo sul dispositivo o un account utente in un server Active Directory.

  Prima di gestire il dispositivo utilizzando l'autenticazione locale è necessario creare le credenziali memorizzate in XClarity Administrator che corrispondono a un account utente attivo sul dispositivo o un account utente in un server Active Directory (vedere Gestione delle credenziali memorizzate nella documentazione online di XClarity Administrator).

  Nota:

  - I dispositivi RackSwitch supportano solo le credenziali memorizzate per l'autenticazione. Le credenziali utente di XClarity Administrator non sono supportate.
- L'*autenticazione gestita* consente di gestire e monitorare più dispositivi utilizzando le credenziali del server di autenticazione XClarity Administrator invece delle credenziali locali. Quando l'autenticazione gestita viene utilizzata per un dispositivo (diverso dai server ThinkServer e System x M4 o dagli switch), XClarity Administrator configura il dispositivo gestito e i relativi componenti installati per utilizzare il server di autenticazione XClarity Administrator per la gestione centralizzata.
  - Quando è abilitata l'autenticazione gestita, è possibile gestire i dispositivi utilizzando le credenziali memorizzate o inserite manualmente (vedere Gestione degli account utente e nella documentazione online di XClarity Administrator).

    La credenziale memorizzata viene utilizzata solo finché XClarity Administrator non configura le impostazioni LDAP sul dispositivo. Successivamente, eventuali modifiche delle credenziali memorizzate non incidono sulla gestione o sul monitoraggio di tale dispositivo.

    Nota: Quando è abilitata l'autenticazione gestita per un dispositivo, non è possibile modificare le credenziali memorizzate per tale dispositivo utilizzando XClarity Administrator.
  - Se viene utilizzato un server LDAP esterno o locale come server di autenticazione XClarity Administrator, gli account utente definiti nel server di autenticazione vengono utilizzati per eseguire il login a XClarity Administrator, CMM e controller di gestione della scheda di base nel dominio di XClarity Administrator. Gli account utente del controller di gestione e CMM locali sono disabilitati.
  - Se viene utilizzato un provider di identità SAML 2.0 come server di autenticazione XClarity Administrator, gli account SAML non saranno accessibili per i dispositivi gestiti. Tuttavia quando si utilizzano un provider di identità SAML e un server LDAP insieme, se il provider di identità utilizza gli account esistenti nel server LDAP, gli account utente LDAP possono essere utilizzati per eseguire il login ai dispositivi gestiti mentre i metodi di autenticazione più avanzati forniti da SAML 2.0 (come autenticazione a più fattori e Single Sign-On) possono essere utilizzati per eseguire il login a XClarity Administrator.

- La funzione Single Sign-On consente a un utente già connesso a XClarity Administrator di eseguire automaticamente il login al controllo di gestione della scheda di base. L'opzione Single Sign-On è abilitata per impostazione predefinita quando un server ThinkSystem o ThinkAgile viene inserito nella gestione da XClarity Administrator (a meno che il server non sia gestito con password CyberArk). È possibile configurare l'impostazione globale per abilitare o disabilitare la funzione Single Sign-On per tutti i server ThinkSystem e ThinkAgile gestiti. L'abilitazione dell'opzione Single Sign-On per un server ThinkSystem o ThinkAgile specifico ha la precedenza sull'impostazione globale per tutti i server ThinkSystem e ThinkAgile (vedere Gestione dei server nella documentazione online di XClarity Administrator).

  Nota: Single Sign-On viene disabilitato automaticamente quando si utilizza il sistema di gestione delle identità CyberArk per l'autenticazione.
- Quando l'autenticazione gestita è abilitata per i server ThinkSystem SR635 e SR655:
  - Il firmware del controller di gestione della scheda di base supporta fino a cinque ruoli utente LDAP. XClarity Administrator aggiunge questi ruoli utente LDAP ai server durante la gestione: **lxc-supervisor**, **lxc-sysmgr**, **lxc-admin**, **lxc-fw-admin** e **lxc-os-admin**.

    È necessario assegnare gli utenti ad almeno uno dei ruoli utente LDAP specificati per comunicare con i server ThinkSystem SR635 e SR655.
  - Il firmware del controller di gestione non supporta gli utenti LDAP con lo stesso nome utente locale del server.
- Per i server ThinkServer e System x M4, il server di autenticazione XClarity Administrator non viene utilizzato. Di contro, viene creato un account IPMI sul dispositivo con il prefisso "LXCA_", seguito da una stringa casuale. (Gli account utente IPMI locali esistenti non vengono disabilitati). Quando si annulla la gestione di un server ThinkServer, l'account utente "LXCA_" viene disabilitato e il prefisso "LXCA_" viene sostituito con il prefisso "DISABLED_". Per determinare se un server ThinkServer è gestito da un'altra istanza, XClarity Administrator verifica gli account IPMI con il prefisso "LXCA_". Se si sceglie di forzare la gestione di un server ThinkServer gestito, tutti gli account IPMI del dispositivo con il prefisso "LXCA_" vengono disabilitati e rinominati. Valutare la possibilità di cancellare manualmente gli account IPMI non più in uso.

  Se si utilizzano credenziali inserite manualmente, XClarity Administrator crea automaticamente una credenziale memorizzata e la utilizza per gestire il dispositivo.

  Nota: Quando è abilitata l'autenticazione gestita per un dispositivo, non è possibile modificare le credenziali memorizzate per tale dispositivo utilizzando XClarity Administrator.
  - Ogni volta che si gestisce un dispositivo utilizzando le credenziali inserite manualmente, viene creata una nuova credenziale memorizzata per tale dispositivo, anche se è stata creata un'altra credenziale memorizzata per il dispositivo durante un processo di gestione precedente.
  - Quando si annulla la gestione di un dispositivo, XClarity Administrator non elimina le credenziali memorizzate create automaticamente per tale dispositivo durante il processo di gestione.

Una volta gestiti i sistemi da parte di XClarity Administrator, XClarity Administrator esegue periodicamente il polling di ciascun sistema gestito per raccogliere informazioni, quali inventario, VPD (Vital Product Data) e stato. È possibile visualizzare e monitorare ciascun sistema gestito ed eseguire azioni di gestione (ad esempio, la configurazione delle impostazioni di sistema, la distribuzione delle immagini del sistema operativo, l'accensione e lo spegnimento).

Un sistema può essere gestito da un solo XClarity Administrator per volta. La gestione da parte di più gestori non è supportata. Se un sistema è gestito da un'istanza di XClarity Administrator e si desidera gestirlo con un'altra istanza di XClarity Administrator, è in primo luogo necessario annullare la gestione del sistema nell'istanza corrente di XClarity Administrator. A questo punto sarà possibile gestire il sistema con un'altra istanza di XClarity Administrator. Per ulteriori informazioni sull'annullamento della gestione di un sistema, vedere Annullamento della gestione di uno chassis, Annullamento della gestione dei server, Annullamento della

gestione di uno switch RackSwitch e Annullamento della gestione di un sistema Lenovo Storage nella documentazione online di XClarity Administrator.

Nota: XClarity Administrator non modifica le impostazioni di sicurezza o crittografiche (la modalità crittografica e la modalità utilizzata per le comunicazioni sicure) durante il processo di gestione. Una volta gestito il sistema, sarà possibile modificare le impostazioni crittografiche (vedere Impostazione della modalità crittografica e dei protocolli di comunicazione nella documentazione online di XClarity Administrator).

Nota: XClarity Administrator può essere prepopolato con l'inventario hardware per uno chassis dimostrativo (che include CMM, nodi di elaborazione e switch) e un server rack o tower dimostrativo che simuli l'hardware reale. I dispositivi dimostrativi vengono popolati nelle pagine dell'interfaccia Web e possono essere utilizzati per dimostrare le operazioni di gestione. Tuttavia, le operazioni di gestione avranno esito negativo. Ad esempio, è possibile creare un pattern di configurazione e distribuirlo a un server dimostrativo, ma la distribuzione avrà esito negativo. È possibile rimuovere i dispositivi dimostrativi annullandone la gestione (vedere Annullamento della gestione di uno chassis e Annullamento della gestione dei server nella documentazione online di XClarity Administrator). Una volta eliminati, i dispositivi dimostrativi non possono essere gestiti di nuovo.

Procedura

Per rilevare e gestire i sistemi in XClarity Administrator mediante un file di importazione di massa, completare le seguenti operazioni.

Nota: Quando si gestiscono gli switch utilizzando l'importazione di massa, HTTPS viene abilitato sullo switch e i client NTP sullo switch vengono configurati per utilizzare le impostazioni NTP dal server di gestione. Per modificare queste impostazioni, è necessario gestire manualmente gli switch.

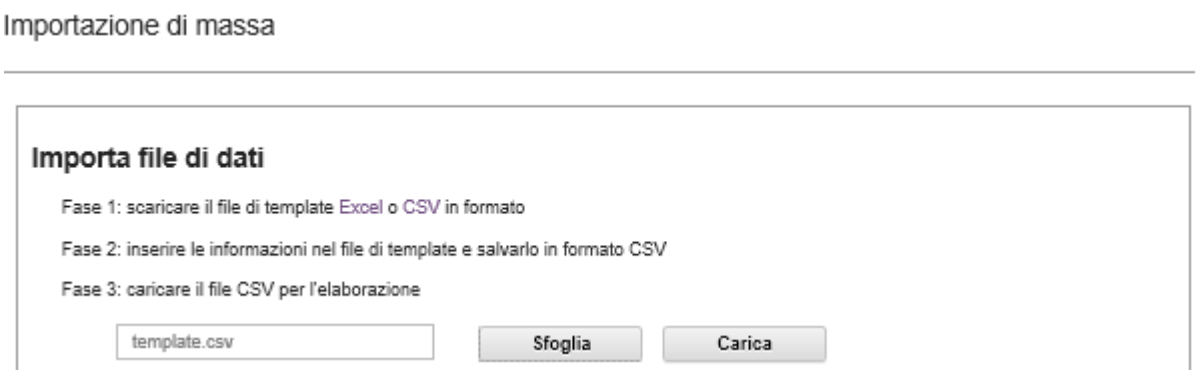
1. Dalla barra di menu di XClarity Administrator fare clic su **Hardware → Rileva e gestisci nuovi dispositivi**. Verrà visualizzata la pagina Rileva e gestisci.
2. Fare clic sulla casella di controllo **Abilita incapsulamento su tutti i prossimi dispositivi gestiti** per modificare le regole del firewall su tutti i dispositivi durante il processo di gestione affinché le richieste in entrata vengano accettate solo da XClarity Administrator.

   Nota:

   - l'incapsulamento non è supportato su switch, dispositivi di storage, chassis e server non Lenovo.
   - Quando l'interfaccia di rete di gestione è configurata per utilizzare Dynamic Host Configuration Protocol (DHCP) e quando l'incapsulamento è abilitato, la gestione di un server rack può richiedere molto tempo.

   L'incapsulamento può essere abilitato o disabilitato su dispositivi specifici dopo che sono stati gestiti.

   Attenzione: Se l'incapsulamento è abilitato e XClarity Administrator non è più disponibile prima che la gestione di un dispositivo venga annullata, è necessario eseguire la procedura per disabilitare l'incapsulamento al fine di stabilire la comunicazione con il dispositivo. Per le procedure di ripristino, vedere Ripristino della gestione dello chassis con un modulo CMM dopo un errore del server di gestione e Ripristino della gestione del server tower o rack dopo un errore del server di gestione nella documentazione online di XClarity Administrator.
3. Fare clic su **Importazione di massa**. Viene visualizzata la procedura guidata "Importazione di massa".



4. Fare clic sul collegamento **in Excel** o **in CSV** nella pagina Importa file di dati per scaricare il file di importazione di massa modello in formato Excel o CSV.

   Importante: Il file modello potrebbe cambiare a seconda della versione. Assicurarsi di utilizzare sempre il modello più recente.

5. Compilare il foglio di lavoro dati nel file modello e salvare il file in formato CSV *delimitato da virgole*.

   Suggerimento: il modello di Excel include un foglio di lavoro **Dati** e un foglio di lavoro **Leggimi**. Utilizzare il foglio di lavoro **Dati** per immettere i dati del dispositivo. Il foglio di lavoro **Leggimi** fornisce informazioni su come compilare ogni campo del foglio di lavoro **Dati** (inclusi i campi obbligatori) e diversi dati di esempio.

   Importante:

   - I dispositivi sono gestiti nell'ordine indicato nel file di importazione di massa.
   - XClarity Administrator utilizza le informazioni sull'assegnazione del rack definite nella configurazione del dispositivo, quando il dispositivo è gestito. Se si modifica l'assegnazione del rack in XClarity Administrator, XClarity Administrator aggiorna la configurazione del dispositivo. Se si aggiorna la configurazione del dispositivo dopo che il dispositivo è stato gestito, tali modifiche vengono riportate in XClarity Administrator.
   - È consigliato ma non richiesto di creare in modo esplicito un rack del foglio di calcolo, prima di assegnare il rack a un dispositivo. Se un rack non viene definito in modo esplicito e il rack non esiste già in XClarity Administrator, le informazioni sull'assegnazione del rack specificate per un dispositivo vengono utilizzate per creare il rack con un'altezza predefinita di 52U.

     Se si desidera utilizzare un'altra altezza per il rack, è necessario definire il rack in modo esplicito nel foglio di calcolo, prima di assegnarlo a un dispositivo.

   Per definire i dispositivi nel file di importazione di massa, completare le seguenti colonne.

   - (Colonne A-C) Per il rilevamento di base, è necessario specificare il tipo di dispositivo e l'indirizzo IP corrente o il numero di serie del dispositivo. Sono supportati i seguenti tipi:
     - **filler**. Segnaposti per un dispositivo non gestito. Nella vista rack questo dispositivo è mostrato come figura generica di riempimento. Vedere il foglio di lavoro **Leggimi** nel modello Excel per i tipi di elementi di riempimento aggiuntivi.
     - **flexchassis**. Chassis di Flex System 10U
     - **server**. Server rack e tower supportati da XClarity Administrator
     - **rack**. Rack 6U, 12U, 18U, 25U, 37U, 42U, 45U, 46U, 48U, 50U e 52U. Non sono supportate altre altezze di rack. 52U viene utilizzato per impostazione predefinita.
     - **storage**. Dispositivi di storage
     - **switch**. Switch RackSwitch

Nota: I dispositivi di storage, gli switch e i nodi di elaborazione Flex System vengono considerati parte del processo di rilevamento e di gestione dello chassis.

- (Colonne D - H) Se si sceglie di utilizzare le credenziali immesse manualmente invece delle credenziali memorizzate (Colonne Z) o dell'identità (Colonne AF - AJ), specificare il nome utente e la password correnti. Le credenziali immesse manualmente sono utile se le credenziali sono diverse per alcuni dispositivi. Se non sono specificate credenziali per uno o più dispositivi nel file di importazione di massa, vengono utilizzate le credenziali globali specificate nella finestra di dialogo Importazione di massa. Per ulteriori informazioni sugli utenti immessi manualmente e l'autenticazione gestita, vedere Gestione degli account utente nella documentazione online di XClarity Administrator.

  Nota:

  – Per utilizzare le credenziali immesse manualmente, è necessario selezionare l'autenticazione gestita di XClarity Administrator.

  – Alcuni campi non si applicano ad alcuni dispositivi.

  – (Per lo chassis) Se si sceglie l'autenticazione gestita (nella colonna AA o nella finestra di dialogo Importazione di massa), è possibile specificare una password `RECOVERY_ID` nella colonna G del file di importazione di massa o nella finestra di dialogo Importazione di massa. Se si sceglie l'autenticazione locale, la password di ripristino non è consentita; non specificare la password di ripristino nella colonna G del file di importazione di massa o nella finestra di dialogo "Importazione di massa".

  – (Per i server rack) Se si sceglie l'autenticazione gestita (nella colonna AA o nella finestra di dialogo "Importazione di massa"), è possibile specificare facoltativamente una password di ripristino nella colonna G del file di importazione di massa o nella finestra di dialogo "Importazione di massa". Se si sceglie l'autenticazione locale, la password di ripristino non è consentita; non specificare la password di ripristino nella colonna G del file di importazione di massa o nella finestra di dialogo "Importazione di massa".

  – (Per gli switch rack) I dispositivi RackSwitch supportano solo le credenziali memorizzate (nella colonna Z) per l'autenticazione con gli switch. Le credenziali utente manuali non sono supportate.

- (Colonne I - U) È possibile fornire informazioni aggiuntive se si desidera applicare modifiche al dispositivo dopo l'esito positivo della gestione.

  Nota: Alcuni campi non si applicano ad alcuni dispositivi. Questi campi non si applicano agli switch RackSwitch.

- (Colonne V - Z) È possibile facoltativamente fornire informazioni per la creazione e l'assegnazione di rack, come nome del rack, posizione, ambiente, unità inferiore nel rack e altezza.

  Nota:

  – Durante la creazione di un rack, è necessario specificare il nome e l'altezza del rack. Sono supportate le seguenti altezze di rack: 6U, 12U, 18U, 25U, 37U, 42U, 45U, 46U, 48U, 50U e 52U. Non sono supportate altre altezze di rack.

  – Durante la creazione di un elemento di riempimento generico, è necessario specificare il nome del rack e l'altezza dell'elemento di riempimento. Sono supportate le seguenti altezze per gli elementi di riempimento: 1U, 2U e 4U.

  – Durante la creazione di un elemento di riempimento specifico, l'altezza dell'elemento di riempimento viene ignorata. XClarity Administrator rileva l'altezza di ciascun elemento di riempimento specifico. Consultare il foglio di calcolo del modello per i tipi di elementi di riempimento e le altezze.

  – Durante l'assegnazione di un dispositivo al rack, l'altezza del dispositivo viene ignorata. L'altezza del dispositivo viene recuperata dall'inventario dei dispositivi.

- (Colonna AA) Se la gestione non è riuscita a causa di una delle seguenti condizioni di errore, ripetere questa procedura utilizzando l'opzione Forza gestione.
  - Se l'istanza XClarity Administrator di gestione è in errore e non è possibile effettuare il ripristino.

    Nota: se l'istanza di sostituzione di XClarity Administrator utilizza lo stesso indirizzo IP dell'istanza con errori di XClarity Administrator, è possibile gestire nuovamente il dispositivo utilizzando l'account e la password RECOVERY_ID (se applicabili) e l'opzione Forza gestione.
  - Se l'istanza XClarity Administrator di gestione è stata disattivata prima di avere annullato la gestione dei dispositivi.
  - Se la gestione dei dispositivi non è stata annullata correttamente.

  I dispositivi possono essere gestiti da una sola istanza di XClarity Administrator per volta. La gestione da parte di più istanze XClarity Administrator non è supportata. Se un dispositivo è gestito da un'istanza di XClarity Administrator e si desidera gestirlo con un'altra istanza di XClarity Administrator, è necessario prima annullare la gestione del dispositivo dall'istanza originale di XClarity Administrator e gestirlo quindi con la nuova istanza di XClarity Administrator.

  Importante: Se si modifica l'indirizzo IP una volta che il server sarà gestito da XClarity Administrator, XClarity Administrator riconoscerà il nuovo indirizzo IP e continuerà a gestire il server. XClarity Administrator non riconosce tuttavia la modifica dell'indirizzo IP per alcuni server. Se XClarity Administrator indica che il server è offline dopo la modifica dell'indirizzo IP, gestire nuovamente il server mediante l'opzione Forza gestione.
- (Colonna AB) Se si sceglie di utilizzare le credenziali memorizzate invece di quelle immesse manualmente (Colonne D - H) o dell'identità (Colonne AF - AJ), specificare un ID delle credenziali memorizzate. È possibile trovare l'ID delle credenziali memorizzate nella pagina "Credenziali memorizzate" facendo clic su **Amministrazione → Sicurezza** dal menu di XClarity Administrator e quindi facendo clic su **Credenziali memorizzate** nel riquadro di navigazione sinistro. Per ulteriori informazioni sulle credenziali normali e memorizzate, vedere Gestione delle credenziali memorizzate nella documentazione online di XClarity Administrator.

  Nota:
  - I dispositivi RackSwitch supportano solo le credenziali memorizzate per l'autenticazione. Le credenziali utente manuali (nella colonna D) non sono supportate.
  - Se si gestisce un dispositivo utilizzando le credenziali memorizzate e si abilita l'autenticazione gestita, non è possibile modificare tali credenziali memorizzate.
- (Colonna AC) Per i server dello chassis e del rack, se si è scelto di utilizzare l'autenticazione gestita, è possibile specificare la password RECOVERY_ID nella colonna G del file di importazione di massa o nella finestra di dialogo Importazione di massa. Se si sceglie l'autenticazione locale, la password di ripristino non è consentita; non specificare la password di ripristino nella colonna G del file di importazione di massa o nella finestra di dialogo "Importazione di massa".
- (Colonna AD) Per i server rack, è possibile scegliere facoltativamente di utilizzare l'autenticazione locale invece dell'autenticazione gestita di XClarity Administrator, specificando FALSE in questa colonna. Per ulteriori informazioni sull'autenticazione gestita e locale, vedere Gestione del server di autenticazione nella documentazione online di XClarity Administrator.
- (Colonna AE) È possibile scegliere di specificare un elenco dei gruppi di ruoli autorizzati a visualizzare e gestire il dispositivo. È possibile specificare solo i gruppi di ruoli a cui appartiene l'utente corrente.

  Nota: Se si aggiungono i dispositivi in uno chassis gestito, i nuovi dispositivi apparterranno agli stessi gruppi di ruoli dello chassis.
- (Colonna AF - AJ) Se si sceglie di utilizzare un sistema di gestione delle identità invece di credenziali immesse manualmente (Colonne D - H) o credenziali memorizzate (Colonne AB), specificare

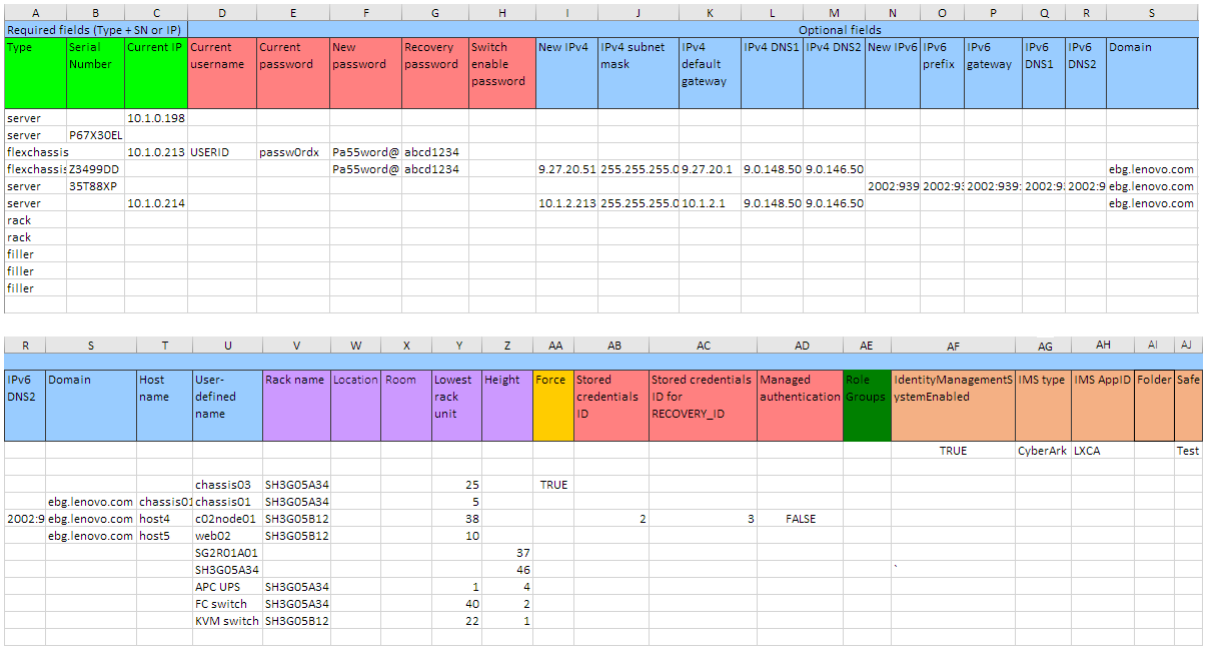
l'indirizzo IP o il nome host del server gestito, il nome utente e, facoltativamente, l'ID applicazione, la cassaforte e la cartella.

Se viene specificato l'ID applicazione, è necessario specificare anche la cartella e la sicurezza, se applicabile.

Se non viene specificato l'ID dell'applicazione, XClarity Administrator utilizza i percorsi definiti al momento della configurazione di CyberArk per identificare gli account in CyberArk.

Nota: Sono supportati solo i server ThinkSystem o ThinkAgile. Il sistema di gestione delle identità deve essere configurato in XClarity Administrator, e Lenovo XClarity Controller per i server ThinkSystem o ThinkAgile gestiti deve essere integrato con CyberArk.

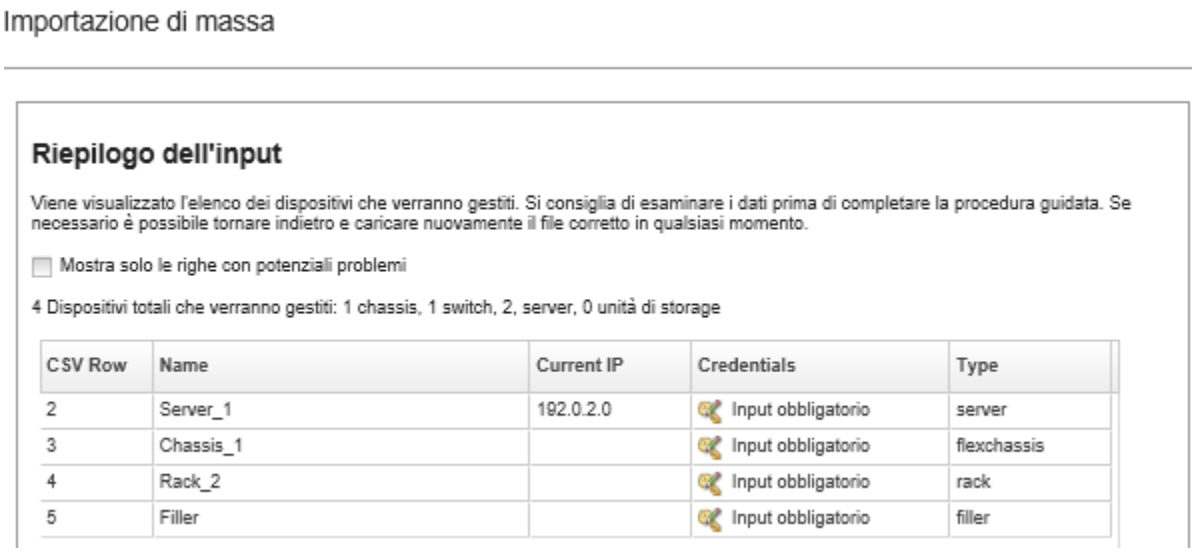
La figura seguente mostra un file di importazione di massa di esempio:



A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
Required fields (Type + SN or IP)			Optional fields															
Type	Serial Number	Current IP	Current username	Current password	New password	Recovery password	Switch enable password	New IPv4	IPv4 subnet mask	IPv4 default gateway	IPv4 DNS1	IPv4 DNS2	New IPv6	IPv6 prefix	IPv6 gateway	IPv6 DNS1	IPv6 DNS2	Domain
server		10.1.0.198																
server	P67X30EL																	
flexchassis		10.1.0.213	USERID	passw0rdx	Pa55word@	abcd1234												
flexchassis	Z3499DD				Pa55word@	abcd1234		9.27.20.51	255.255.255.0	9.27.20.1	9.0.148.50	9.0.146.50						ebg.lenovo.com
server	35T88XP												2002:939	2002:9	2002:939:	2002:9	2002:9	ebg.lenovo.com
server		10.1.0.214						10.1.2.213	255.255.255.0	10.1.2.1	9.0.148.50	9.0.146.50						ebg.lenovo.com
rack																		
rack																		
filler																		
filler																		
filler																		

R	S	T	U	V	W	X	Y	Z	AA	AB	AC	AD	AE	AF	AG	AH	AI	AJ
IPv6 DNS2	Domain	Host name	User-defined name	Rack name	Location	Room	Lowest rack unit	Height	Force	Stored credentials ID	Stored credentials ID for RECOVERY_ID	Managed authentication	Role Groups	IdentityManagementSystemEnabled	IMS type	IMS AppID	Folder	Safe
														TRUE	CyberArk	LXCA		Test
			chassis03	SH3G05A34			25		TRUE									
	ebg.lenovo.com	chassis01	chassis01	SH3G05A34			5											
2002:9	ebg.lenovo.com	host4	c02node01	SH3G05B12			38			2	3	FALSE						
	ebg.lenovo.com	host5	web02	SH3G05B12			10											
			SG2R01A01					37										
			SH3G05A34					46										
			APC UPS	SH3G05A34			1	4										
			FC switch	SH3G05A34			40	2										
			KVM switch	SH3G05B12			22	1										

6. Dalla procedura guidata Importazione di massa immettere il nome del file CSV da caricare per l'elaborazione. È possibile fare clic su **Sfoglia** per trovare il file.
7. Fare clic su **Carica** per caricare e convalidare il file.
8. Fare clic su **Avanti** per visualizzare la pagina "Riepilogo immissioni" con un elenco dei dispositivi da gestire.



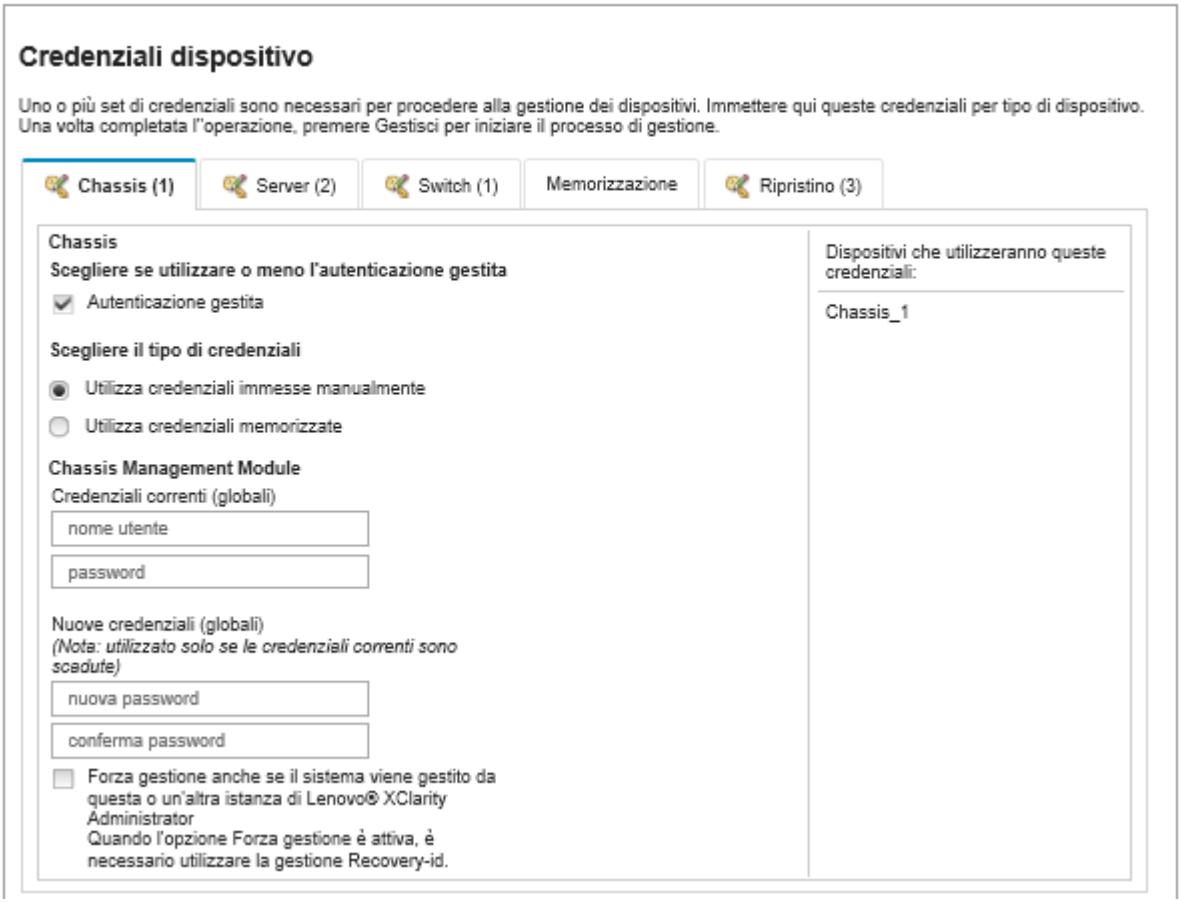
9. Esaminare il riepilogo dei dispositivi che si desidera gestire.

   Selezionare **Mostra solo le righe con problemi potenziali** per visualizzare le righe con dati incompleti. Risolvere eventuali problemi nel file di importazione di massa e quindi fare clic su **Indietro** per caricare il file CSV corretto.

   Nota:

   - Se i dati richiesti non vengono forniti nel file di importazione di massa, i dispositivi associati non vengono gestiti.
   - Nella pagina Riepilogo immissioni vengono contrassegnate le righe che non dispongono di informazioni sulle credenziali. Se non sono specificate le credenziali nel file di importazione di massa, vengono utilizzate le credenziali globali specificate nella procedura guidata Importazione di massa.

10. Fare clic su **Avanti** per visualizzare la pagina "Credenziali dispositivi".



11. **Facoltativo:** fare clic su ciascuna scheda e specificare le impostazioni globali e le credenziali da utilizzare per tutti i dispositivi di un tipo specifico. I dispositivi che utilizzeranno le impostazioni globali e le credenziali sono elencati sul lato destro di ciascuna scheda.

    Se si sceglie di utilizzare le credenziali globali, le credenziali per uno specifico tipo di dispositivo devono essere le stesse per tutti i dispositivi dello stesso tipo che non dispongono delle credenziali immesse nel file di importazione di massa. Ad esempio, le credenziali di CMM devono essere le stesse per tutti gli chassis e le credenziali di gestione dello storage devono essere le stesse per tutti i dispositivi di storage. Se le credenziali non sono le stesse, è necessario immettere le credenziali nel file di importazione di massa.

    - **Chassis**. Specificare la modalità di autenticazione e il tipo di credenziali. Specificare le credenziali correnti per eseguire il login a tutti gli chassis definiti nel file di importazione di massa. Specificare la nuova password da utilizzare se le credenziali correnti del modulo CMM sono scadute.

      Se si forza la gestione di uno chassis, specificare l'account RECOVERY_ID e la password per le credenziali del dispositivo.
    - **Server**. Specificare la modalità di autenticazione e il tipo di credenziali. Specificare le credenziali correnti per eseguire il login a tutti i server rack e tower definiti nel file di importazione di massa. Specificare la nuova password da utilizzare se le credenziali correnti del controller di gestione della scheda di base sono scadute.

      Se si forza la gestione di un server, specificare l'account RECOVERY_ID e la password per le credenziali del dispositivo.

- **Switch**. Specificare le credenziali memorizzate per eseguire il login a tutti gli switch RackSwitch definiti nel file di importazione di massa. Se impostata, specificare inoltre la password "enable" utilizzata per accedere alla modalità di esecuzione con privilegi nello switch.
- **Storage**. Specificare le credenziali correnti per eseguire il login a tutti i dispositivi di storage definiti nel file di importazione di massa.
- **Ripristino**. Specificare la password di ripristino per eseguire il login a tutti i server e gli chassis definiti nel file di importazione di massa.

  È possibile scegliere di utilizzare un account utente locale o le credenziali di ripristino memorizzate. In entrambi i casi, il nome utente è sempre `RECOVERY_ID`.

  Quando viene specificata una password, l'account `RECOVERY_ID` viene creato sul dispositivo e tutti gli account utente locali vengono disabilitati.

  – Per lo chassis, è richiesta la password di ripristino.
  – Per i server, la password di ripristino è facoltativa se si sceglie di utilizzare l'autenticazione gestita e non è consentita se si sceglie di utilizzare l'autenticazione locale.
  – Verificare che la password rispetti i criteri di sicurezza e delle password per il dispositivo. I criteri di sicurezza e delle password possono variare.
  – Assicurarsi di registrare la password di ripristino per gli usi futuri.
  – L'account di ripristino non è supportato per i server ThinkServer e System x M4.

Le informazioni specificate nel file di importazione di massa sovrascrivono le informazioni simili specificate nella pagina "Credenziali dispositivi".

È possibile scegliere facoltativamente di forzare la gestione di ogni tipo di dispositivo se:

- I dispositivi sono attualmente gestiti da un altro sistema, come un'altra istanza di XClarity Administrator o IBM Flex System Manager
- XClarity Administrator è stato disattivato senza avere annullato la gestione dei dispositivi
- Non è stato eseguito correttamente l'annullamento della gestione dei dispositivi e la sottoscrizione CIM non è stata cancellata

Nota: se è gestito da un'altra istanza di XClarity Administrator, il dispositivo sarà gestito dall'istanza originale per un periodo di tempo successivo alla gestione forzata. È possibile non gestire il dispositivo per rimuoverlo dall'istanza originale di XClarity Administrator.

12. Fare clic su **Gestisci**. Viene visualizzata la pagina "Risultati monitoraggio" con informazioni sullo stato della gestione di ciascun dispositivo nel file di importazione di massa.

    Viene creato un processo per il processo di gestione. Se si chiude la procedura guidata di importazione di massa, il processo di gestione continua in background. È possibile monitorare lo stato del processo di gestione dal log dei processi. Per ulteriori informazioni sul log processi, vedere Monitoraggio dei processi nella documentazione online di XClarity Administrator.

    Se XClarity Administrator non è in grado di eseguire il login a un dispositivo utilizzando le credenziali specificate nel file di importazione di massa o le credenziali globali specificate nella finestra di dialogo, la gestione di tale dispositivo non riesce e XClarity Administrator passa al dispositivo successivo nel file di importazione di massa.

    Nota: Se la gestione non è riuscita a causa di una delle seguenti condizioni di errore, ripetere questa procedura utilizzando l'opzione **Forza gestione**.

    - Se l'istanza XClarity Administrator di gestione è in errore e non è possibile effettuare il ripristino.

Nota: se l'istanza di sostituzione XClarity Administrator utilizza lo stesso indirizzo IP del XClarity Administrator malfunzionante, è possibile gestire nuovamente il dispositivo utilizzando l'account e la password RECOVERY_ID (se applicabile) e l'opzione **Forza gestione**.

- Se l'istanza XClarity Administrator di gestione è stata disattivata prima di avere annullato la gestione dei dispositivi.
- Se la gestione dei dispositivi non è stata annullata correttamente.

Attenzione: I dispositivi possono essere gestiti da una sola istanza di XClarity Administrator per volta. La gestione da parte di più istanze XClarity Administrator non è supportata. Se un dispositivo è gestito da un'istanza di XClarity Administrator e si desidera gestirlo con un'altra istanza di XClarity Administrator, è necessario prima annullare la gestione del dispositivo dall'istanza originale di XClarity Administrator e quindi gestirlo con la nuova istanza di XClarity Administrator.

13. Se il file di importazione di massa include un nuovo chassis, convalidare e modificare le impostazioni di rete di gestione per l'intero chassis (inclusi nodi di elaborazione e switch Flex) e per configurare le informazioni del nodo di elaborazione, lo storage locale, gli adattatori I/O, le destinazioni avvio e le impostazioni del firmware creando e distribuendo pattern server. Per ulteriori informazioni, vedere Modifica delle impostazioni IP di gestione per uno chassis e Configurazione dei server mediante XClarity Administrator nella documentazione online di XClarity Administrator.

Al termine

Una volta gestiti i sistemi, sarà possibile procedere come segue:

- Rilevare e gestire sistemi aggiuntivi (vedere Gestione dello chassis, Gestione dei rack, Gestione dei server, Gestione di dispositivi di storage e Gestione degli switch nella documentazione online di Lenovo XClarity Administrator).
- Per configurare le informazioni di sistema, lo storage locale, gli adattatori I/O, le impostazioni di avvio le impostazioni del firmware, creare e distribuire pattern server (vedere Configurazione dei server mediante XClarity Administrator nella documentazione online di Lenovo XClarity Administrator).
- Distribuire le immagini del sistema operativo nei server in cui non ne è installato uno (vedere Distribuzione di un'immagine del sistema operativo nella documentazione online di XClarity Administrator).
- Aggiornare il firmware sui dispositivi non conformi ai criteri correnti (vedere Aggiornamento del firmware sui dispositivi gestiti nella documentazione online di XClarity Administrator).
- Aggiungere i sistemi appena gestiti al rack appropriato per riflettere l'ambiente fisico (vedere Gestione dei rack nella documentazione online di XClarity Administrator).
- Monitorare lo stato e i dettagli dell'hardware (vedere Visualizzazione dello stato di un server gestito nella documentazione online di XClarity Administrator).
- Monitorare eventi e avvisi (vedere Utilizzo degli eventi e Gestione degli avvisi nella documentazione online di XClarity Administrator).
- Disabilitare o abilitare la funzione Single Sign-On per i server ThinkSystem e ThinkAgile gestiti.
  - Per tutti i server ThinkSystem e ThinkAgile gestiti (globalmente), fare clic su **Amministrazione → Sicurezza** sulla barra dei menu di XClarity Administrator, fare clic su **Sessioni attive**, quindi abilitare o disabilitare **Single Sign-On**.
  - Per un server ThinkSystem o ThinkAgile specifico, fare clic su **Hardware → Server** sulla barra dei menu di XClarity Administrator, quindi su **Tutte le azioni → Sicurezza → Abilita Single Sign-On** o **Tutte le azioni → Sicurezza → Disabilita Single Sign-On**.

Nota: La funzione Single Sign-On consente a un utente già connesso a XClarity Administrator di eseguire automaticamente il login al controllo di gestione della scheda di base. L'opzione Single Sign-On è abilitata per impostazione predefinita quando un server ThinkSystem o ThinkAgile viene inserito nella gestione da XClarity Administrator (a meno che il server non sia gestito con password CyberArk). È possibile

configurare l'impostazione globale per abilitare o disabilitare la funzione Single Sign-On per tutti i server ThinkSystem e ThinkAgile gestiti. L'abilitazione dell'opzione Single Sign-On per un server ThinkSystem o ThinkAgile specifico ha la precedenza sull'impostazione globale per tutti i server ThinkSystem e ThinkAgile.

Capitolo 5. Registrazione di XClarity Administrator

Registrando l'istanza di Lenovo XClarity Administrator è possibile utilizzare le funzioni base senza ricevere avvisi ricorrenti relativi alla scadenza della versione di prova e alle licenze non conformi. Una volta completata la registrazione, l'avviso sulla licenza non conforme non viene più visualizzato. Tuttavia, tutte le funzioni che richiedono una licenza sono disabilitate fino all'acquisto e all'installazione delle licenze, in base al numero di dispositivi gestiti.

Informazioni su questa attività

La registrazione dell'istanza di XClarity Administrator non richiede la condivisione delle informazioni di contatto. Lenovo non condivide le informazioni fornite con altre entità esterne.

Se sono state installate licenze per funzioni avanzate, non è necessario registrare l'istanza di XClarity Administrator. Per ulteriori informazioni sulle licenze e sulle funzioni avanzate, vedere Installazione della licenza di abilitazione di tutte le funzionalità.

Procedura

Per registrare XClarity Administrator, completare i seguenti passaggi.

- Se XClarity Administrator è collegato a Internet
  1. Dalla barra dei menu di Lenovo XClarity Administrator, fare clic su **Amministrazione → Registrazione** per visualizzare la pagina Registrazione.
  2. Fare clic su **Registrati** per registrare una nuova istanza di XClarity Administrator.
  3. Immettere il nome dell'azienda, il numero di dispositivi che XClarity Administrator deve gestire e il paese in cui si trova XClarity Administrator.
  4. Fare clic su **Invia**.
- Se XClarity Administrator non è collegato a Internet
  1. Registrare XClarity Administrator.
     a. In un browser Web, aprire la Portale Web per la registrazione di Lenovo XClarity.
     b. Immettere il nome dell'azienda, il numero di dispositivi che XClarity Administrator deve gestire e il paese in cui si trova XClarity Administrator.
     c. Fare clic su **Invia** per ricevere un token di registrazione.
  2. Dalla barra dei menu di Lenovo XClarity Administrator, fare clic su **Amministrazione → Registrazione** per visualizzare la pagina Registrazione.
  3. Fare clic sull'icona **Importa** per importare il token di registrazione.
  4. Compilare il token di registrazione ricevuto nel passaggio 1.
  5. Fare clic su **Invia**.

Capitolo 6. Installazione della licenza di abilitazione di tutte le funzionalità

Dopo la scadenza di 90 giorni della versione di prova, è necessario acquistare e installare le licenze per Lenovo XClarity Pro per tutti i dispositivi gestiti che supportano funzioni avanzate per continuare a utilizzare le funzioni di configurazione dei dispositivi e di distribuzione del sistema operativo in Lenovo XClarity Administrator. È necessario disporre di licenze per Lenovo XClarity Pro per *tutti* i dispositivi gestiti per ottenere assistenza e supporto per XClarity Administrator.

Ulteriori informazioni:  XClarity Administrator: installazione della licenza

Prima di iniziare

Prendere visione delle considerazioni sulla licenza che seguono.

- Una licenza *non è* legata a un dispositivo specifico.
- 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 Administrator XClarity Administrator.
  - Server ThinkServer
  - Server System x M4
  - Server System x X5
  - Server System x3850 X6 e x3950 X6 (3837)
  - Dispositivi di storage
  - Switch

Per installare le licenze è necessario disporre dei privilegi **lxc-supervisor** o **lxc-security-admin**.

Informazioni su questa attività

XClarity Administrator supporta la seguente licenza.

- **Lenovo XClarity Pro**. Ogni licenza fornisce i diritti che seguono per un singolo dispositivo.
  - Assistenza e supporto per Lenovo XClarity Integrator
  - Assistenza e supporto per XClarity Administrator
  - Funzioni avanzate in XClarity Administrator:
    - Configurazione dei server mediante i pattern di configurazione
    - Distribuzione dei sistemi operativi
    - Segnalazione dei problemi di XClarity Administrator mediante Call Home (Call Home per avvisi hardware non è interessato).

Il periodo di attivazione per la licenza inizia quando la licenza viene acquistata e il codice di autorizzazione viene creato.

La conformità della licenza viene determinata in base al numero di dispositivi gestiti che supportano le funzioni avanzate. Il numero di dispositivi gestiti non deve superare il numero totale di licenze in tutte le chiavi di licenza attive. Se XClarity Administrator non è conforme alle licenze installate (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. Ogni volta che XClarity Administrator non è conforme, il periodo di tolleranza viene reimpostato su 90 giorni. Se il periodo di tolleranza (inclusa la versione di prova gratuita) termina prima che le licenze siano conformi, le funzioni avanzate sono disabilitate per tutti i dispositivi.

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

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 Administrator, la licenza di prova o il periodo di tolleranza viene reimpostato su 90 giorni.

Nota:

- Le funzioni di configurazione del server e di distribuzione del sistema operativo vengono disabilitate alla scadenza del periodo di tolleranza.
- Call Home per i problemi di XClarity Administrator (funzione Call Home software) è disabilitata quando le licenze non sono conformi. Non è previsto un periodo di tolleranza per questa funzione. Tuttavia, la funzione Call Home per gli avvisi hardware non è interessata.

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

È possibile determinare lo stato delle licenze, incluso il numero di giorni rimasti per la licenza di prova, facendo clic sul menu azioni utente (

) sulla barra del titolo XClarity Administrator, quindi selezionando **Informazioni su**.

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.

Installazione delle licenze di abilitazione di tutte le funzionalità mediante l'interfaccia Web di XClarity Administrator

Se XClarity Administrator ha accesso a Internet, è possibile utilizzare l'interfaccia Web di XClarity Administrator per riscattare e recuperare le licenze per l'autorizzazione e quindi importarle e installarle.

Prima di iniziare

Contattare il responsabile o il business partner Lenovo autorizzato per acquistare le licenze Lenovo XClarity Pro in base alle funzioni che si desidera abilitare e 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*. Il codice di autorizzazione è una stringa alfanumerica di 22 caratteri, che è necessario utilizzare per installare le licenze. Se non si riceve l'e-mail e le licenze sono state acquistate tramite un business partner, contattare il business partner per richiedere il codice di autorizzazione.

È inoltre possibile recuperare i codici di autorizzazione da Portale Web Features on Demand facendo clic su **Recupera codice di autorizzazione**.

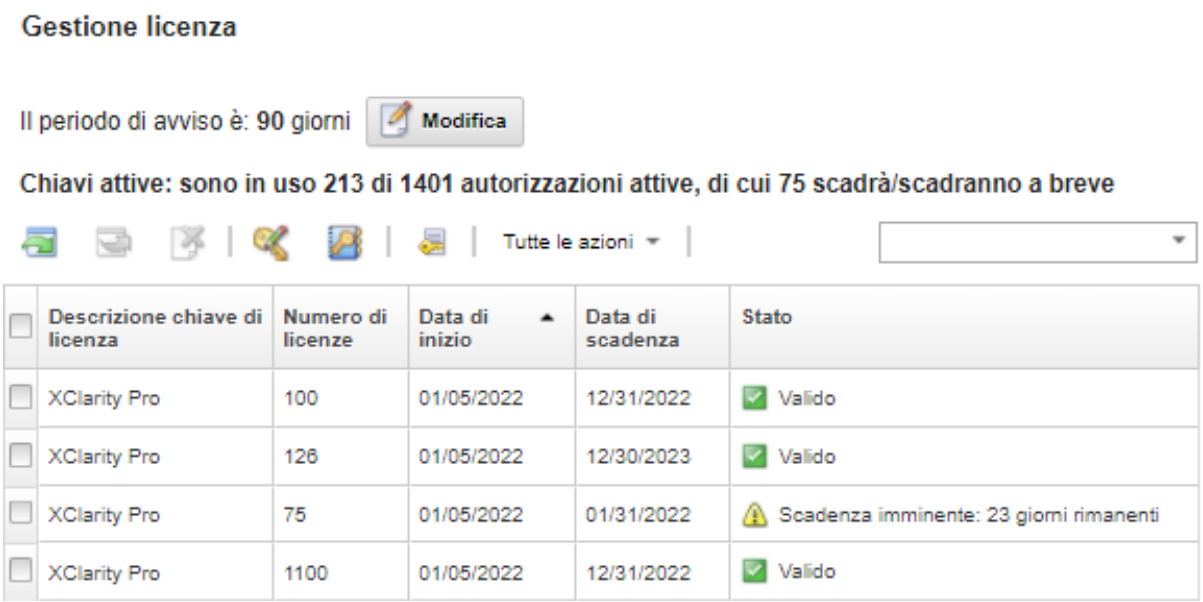
Procedura

Per installare le licenze Lenovo XClarity Pro nel server di gestione, completare una delle seguenti procedure.

- **Riscattare e installare tutte o un sottoinsieme di licenze rimanenti da un singolo codice di autorizzazione**

  È possibile eliminare tutte o un sottoinsieme di licenze disponibili per un singolo codice di autorizzazione per creare una chiave di attivazione della licenza, un file che contiene tutte le informazioni sulla licenza riscattata. È quindi possibile installare le licenze riscattate utilizzando il file della chiave di attivazione della licenza.

  1. Dalla barra dei menu di XClarity Administrator, fare clic su **Amministrazione → Licenze** per visualizzare la pagina Gestione licenza.



2. Fare clic sull'icona **Richiedi chiave di attivazione** () per visualizzare la finestra di dialogo Richiedi chiave di attivazione.
3. Fare clic su **Codice di autorizzazione singolo**.
4. Immettere il codice di autorizzazione di 22 caratteri e fare clic su **Cerca** per recuperare le informazioni sulle licenze acquistate per il codice di autorizzazione specificato dal sito Web Features on Demand.

   Se il codice di autorizzazione ricevuto non viene accettato, contattare il supporto Lenovo.
5. Immettere il numero cliente Lenovo di 10 cifre 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 nel codice di autorizzazione, inserire il numero corrispondente nel campo **Licenze disponibili**.

   Se si riscatta un sottoinsieme di licenze disponibili, è possibile riscattare le licenze rimanenti in un secondo momento, utilizzando lo stesso codice di autorizzazione.

   Suggerimento: ogni XClarity Administrator supporta fino a 1.000 dispositivi gestiti. Una singola chiave di attivazione della licenza che viene installata in un'istanza di XClarity Administrator può quindi disporre di massimo 1.000 licenze.
7. Riesaminare le informazioni di contatto e apportare eventuali modifiche, se necessario.
8. Fare clic su **Invia richiesta** per riscattare le licenze e creare la chiave di attivazione della licenza.
9. Selezionare la chiave di attivazione della licenza che contiene le licenze da installare.
10. Fare clic su **Installa** per installare le licenze nel server di gestione.
11. Fare clic su **Chiudi**.

- **Non riscattare e installare tutte le licenze restanti da più codici di autorizzazione**

  È possibile riscattare tutte le licenze restanti per più codici di autorizzazione. Viene creata una chiave di attivazione della licenza per ogni codice di autorizzazione. È quindi possibile installare le licenze riscattate utilizzando le chiavi di attivazione della licenza. I codici di autorizzazione devono essere forniti in un file in formato CSV, utilizzando il modello fornito.
  1. Dalla barra dei menu di XClarity Administrator, fare clic su **Amministrazione → Licenze** per visualizzare la pagina Gestione licenza.
  2. Fare clic sull'icona **Richiedi chiave di attivazione** () per visualizzare la finestra di dialogo Richiedi chiave di attivazione.
  3. Fare clic su **Codici di autorizzazione multipli**.
  4. Fare clic su **Scarica modello** per aprire un file Excel. Aggiungere ogni codice di autorizzazione al file e salvare il file in formato CSV nel sistema locale.
  5. Fare clic su **Sfoglia** per individuare e selezionare il file CSV del codice di autorizzazione, quindi fare clic su **Cerca** per recuperare le informazioni sul codice di autorizzazione dal sito Web del supporto Lenovo.
  6. Esaminare le informazioni sulla licenza acquistata e le chiavi di attivazione disponibili associate a ciascun codice di autorizzazione.
  7. Immettere il numero cliente Lenovo di 10 cifre nel campo **Numero cliente Lenovo**.
  8. Riesaminare le informazioni di contatto e apportare eventuali modifiche, se necessario. Quindi, fare clic su **Continua**.
  9. Selezionare **Sì, desidero riscattare tutti i codici di autorizzazione validi**, quindi fare clic su **Invia richiesta** per generare le chiavi di attivazione della licenza.
  10. Selezionare le chiavi di attivazione della licenza che si desidera installare.

11. Fare clic su **Installa** per installare le chiavi di attivazione della licenza nel server di gestione.
12. Fare clic su **Chiudi**.

- **Recupero e installazione di licenze non riscattate**

  È possibile scaricare le chiavi di attivazione della licenza nel sistema locale da un'istanza XClarity Administrator che ha accesso a Portale Web Features on Demand, e quindi importare e installare le chiavi di attivazione della licenza in un'altra istanza di XClarity Administrator. Questa operazione è utile quando si desidera installare le licenze in un'istanza di XClarity Administrator che non dispone di accesso Internet o quando XClarity Administrator è stato reinstallato ed è necessario ripristinare le licenze installate.

  1. Dalla barra dei menu di XClarity Administrator, fare clic su **Amministrazione → Licenze** per visualizzare la pagina Gestione licenza.
  2. Fare clic sull'icona **Recupera cronologia** ( ) per visualizzare la finestra di dialogo Recupera cronologia.
  3. Immettere il numero cliente Lenovo o il codice di autorizzazione di 22 caratteri.
  4. Fare clic su **Cerca** per recuperare le informazioni sulle licenze disponibili e non riscattate.

     Se il codice di autorizzazione ricevuto non viene accettato, contattare il supporto Lenovo.
  5. Selezionare i file delle chiavi di licenza che si desidera installare.
  6. Fare clic su **Installa** per installare le chiavi di attivazione della licenza in XClarity Administrator.
  7. Fare clic su **Chiudi**.

- **Importare e installare le licenze non installate in un'altra istanza di XClarity Administrator**

  Se si riscattano licenze utilizzando un'istanza di XClarity Administrator e si desidera installarle in un'altra istanza di XClarity Administrator o si verifica una condizione di errore che richiede il ripristino delle licenze installate, è possibile importare il file della chiave di licenza dal sistema locale in un'altra istanza di XClarity Administrator.

  1. Da un'istanza XClarity Administrator che ha accesso al Portale Web Features on Demand, recuperare le chiavi di attivazione della licenza da Portale Web Features on Demand e quindi salvarle come file sul sistema locale.
     a. Dalla barra dei menu di XClarity Administrator, fare clic su **Amministrazione → Licenze** per visualizzare la pagina Gestione licenza.
     b. Fare clic sull'icona **Recupera cronologia** ( ) per visualizzare la finestra di dialogo Recupera cronologia.
     c. Immettere il codice di autorizzazione di 22 caratteri.
     d. Fare clic su **Cerca** per recuperare le informazioni sulle licenze disponibili e riscattate per il codice di autorizzazione.

        Se il codice di autorizzazione ricevuto non viene accettato, contattare il supporto Lenovo.
     e. Selezionare i file delle chiavi di attivazione della licenza che si desidera installare.
     f. Fare clic su **Scarica** per salvare i file delle chiavi di licenza nel sistema locale.
  2. Dall'istanza di XClarity Administrator in cui si desidera installare le chiavi di attivazione della licenza:
     a. Dalla barra dei menu di XClarity Administrator, fare clic su **Amministrazione → Licenze** per visualizzare la pagina Gestione licenza.
     b. Fare clic sull'icona **Importa e applica** ( ) per importare e installare le licenze.
     c. Fare clic su **Sfoglia** per selezionare le chiavi di attivazione della licenza che si desidera installare.

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

d. Fare clic su **Accetta licenza** per importare e applicare le licenze.

   Al termine dell'installazione, le chiavi di attivazione della licenza vengono elencate nella tabella con il numero di licenze installate e il periodo di attivazione (data di inizio e di scadenza).

Al termine

Dalla pagina Licenze è possibile completare le seguenti azioni.

- Scaricare una o più chiavi di attivazione di una licenza specifica nel sistema locale facendo clic sull'icona **Esporta** ( ).

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

- Eliminare una chiave di attivazione di una licenza specifica facendo clic sull'icona **Elimina** ( ).
- Configurare il periodo di avviso della licenza facendo clic sul pulsante **Modifica** nella parte superiore della pagina. Il periodo di avviso della licenza rappresenta il numero di giorni restanti prima della scadenza delle licenze, quando viene attivato un avviso di XClarity Administrator.

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.

Installazione di licenze di abilitazione di tutte le funzionalità mediante il portale Web Features on Demand

Se XClarity Administrator *non* ha accesso a Internet, è possibile riscattare e recuperare le licenze per i codici di autorizzazione esistenti utilizzando il Portale Web Features on Demand da un altro sistema con accesso di rete a XClarity Administrator. È quindi possibile utilizzare l'interfaccia Web di XClarity Administrator per importare e installare le licenze non riscattate.

Procedura

Per installare le licenze Lenovo XClarity Pro nel server di gestione, completare la seguente procedura.

Passo 1. Acquistare una licenza Lenovo XClarity Pro per ogni dispositivo gestito.

Contattare il responsabile o il business partner Lenovo autorizzato per acquistare le licenze Lenovo XClarity Pro in base alle funzioni che si desidera abilitare e 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*. Il codice di autorizzazione è una stringa alfanumerica di 22 caratteri, che è necessario utilizzare per installare le licenze. Se non si riceve l'e-mail e le licenze sono state acquistate tramite un business partner, contattare il business partner per richiedere il codice di autorizzazione.

È inoltre possibile recuperare i codici di autorizzazione da Portale Web Features on Demand facendo clic su **Recupera codice di autorizzazione**.

Passo 2. Riscattare tutte le licenze o un sottoinsieme di licenze utilizzando il codice di autorizzazione. Quando le licenze vengono riscattate, viene generato un file della chiave di attivazione della licenza.

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 questo codice di autorizzazione, 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 della licenza utilizzando lo stesso codice di autorizzazione.

   Suggerimento: ogni XClarity Administrator supporta fino a 1.000 dispositivi gestiti. Una singola chiave di attivazione della licenza che viene installata in un'istanza di XClarity Administrator può quindi disporre di massimo 1.000 licenze.
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 della licenza.
8. Facoltativamente, specificare i destinatari aggiuntivi cui inviare le chiavi di attivazione della licenza.
9. Fare clic su **Invia** per inviare le chiavi di attivazione della licenza.

   La persona assegnata all'ordine di acquisto e i destinatari aggiuntivi riceveranno un'e-mail con la chiave di attivazione della licenza. La chiave è un file in formato .KEY.

   Nota: È inoltre possibile scaricare le chiavi di attivazione della licenza (singolarmente o in batch) da Portale Web Features on Demand facendo clic su **Recupera cronologia** e utilizzando il numero cliente Lenovo per individuare le chiavi di attivazione della licenza. Quindi è possibile scaricare tutte le chiavi o un sottoinsieme di chiavi. 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. Importare e installare le licenze in XClarity Administrator.

1. Dalla barra dei menu di XClarity Administrator, fare clic su **Amministrazione → Licenze** per visualizzare la pagina Gestione licenza.
2. Fare clic sull'icona **Importa e applica** () per installare le licenze.
3. Fare clic su **Sfoglia** per selezionare il file della chiave di attivazione della licenza per le licenze che si desidera installare.

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

4. Fare clic su **Accetta licenza** per importare e applicare le licenze.

   Al termine dell'installazione, la chiave di attivazione della licenza viene elencata nella tabella con il numero di licenze installate e il periodo di attivazione (data di inizio e di scadenza).

Al termine

Dalla pagina Licenze è possibile completare le seguenti azioni.

- Scaricare una o più chiavi di attivazione di una licenza specifica nel sistema locale facendo clic sull'icona **Esporta** ( ).

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

- Eliminare una chiave di attivazione di una licenza specifica facendo clic sull'icona **Elimina** ( ).
- Configurare il periodo di avviso della licenza facendo clic sul pulsante **Modifica** nella parte superiore della pagina. Il periodo di avviso della licenza rappresenta il numero di giorni restanti prima della scadenza delle licenze, quando viene attivato un avviso di XClarity Administrator.

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 7. Aggiornamento di XClarity Administrator come

Quando Lenovo XClarity Administrator viene eseguito come contenitore, utilizzare questa procedura di aggiornamento per installare il software più recente come nuovo contenitore e collegare i volumi del contenitore originale al nuovo contenitore.

Prima di iniziare

È possibile aggiornare XClarity Administrator v4.0 o versioni successive solo da un'istanza XClarity Administrator v3.0 o successiva. Se si utilizza una versione precedente alla 3.0, è necessario eseguire l'aggiornamento alla versione 3.0 o successive, prima di eseguire l'aggiornamento a XClarity Administrator v4.0.

Per gestire istanze v4.0 o successive XClarity Administrator mediante Lenovo XClarity Orchestrator, è necessario XClarity Orchestrator v2.0 o versioni successive. Se si sta aggiornando XClarity Administrator alla versione 4.0 o successive, verificare che la versione di XClarity Orchestrator sia già la 2.0 o successive.

Informazioni su questa attività

Il file `docker-compose.yml` utilizza le seguenti variabili di ambiente, impostate durante l'installazione del contenitore *originale*. Queste variabili di ambiente vengono utilizzate anche dal nuovo contenitore.

- **CONTAINER_NAME**. Nome univoco del contenitore, utilizzato per creare volumi docker per ciascuna istanza XClarity Administrator (ad esempio, `CONTAINER_NAME=LXCA-203`)

  XClarity Administrator utilizza il nome del contenitore per creare i volumi per il contenitore. Se si utilizza lo stesso nome del contenitore per il nuovo contenitore, la nuova istanza XClarity Administrator utilizzerà gli stessi volumi e avrà quindi avrà accesso agli stessi dati e impostazioni di sistema dell'istanza XClarity Administrator originale (contenitore).

  Se si modifica il nome del contenitore vengono creati nuovi volumi per il contenitore e la nuova istanza XClarity Administrator non avrà accesso agli stessi dati e impostazioni di sistema dell'istanza XClarity Administrator originale (contenitore). Se è necessario modificare il nome del contenitore o l'indirizzo IP, eseguire il backup dei dati e delle impostazioni di sistema per l'istanza XClarity Administrator originale, prima di installare il nuovo contenitore. Utilizzare quindi questo backup per ripristinare i dati di sistema e le impostazioni nel nuovo contenitore.
- **INDIRIZZO**. Indirizzo IPv4 statico o IPv6 per il contenitore (ad esempio, `ADDRESS=192.0.2.0`)

  La modifica dell'indirizzo IP di XClarity Administrator dopo la gestione dei dispositivi potrebbe determinare l'attivazione dello stato offline dei dispositivi in XClarity Administrator. Verificare che tutti i dispositivi risultino non gestiti prima di modificare l'indirizzo IP.
- **BACKUP_MOUNT** e **FIRMWARE_MOUNT** (facoltativo). Percorsi per le condivisioni remote che possono essere utilizzati per memorizzare i backup di XClarity Administrator o come repository remoto per gli aggiornamenti firmware. I percorsi devono essere rispettivamente: `/mnt/backup_share` e `/mnt/fw_share`.

Nota: XClarity Administrator *non* viene eseguito come contenitore con privilegi.

Procedura

Per importare un contenitore XClarity Administrator, completare la seguente procedura.

Passo 1. Scaricare l'immagine del contenitore XClarity Administrator dalla Pagina Web di download di XClarity Administrator in una workstation client. Accedere al sito Web, quindi utilizzare la chiave di accesso fornita per scaricare l'immagine.

Passo 2. Importare l'immagine del contenitore XClarity Administrator nell'host docker, utilizzando il comando seguente.

```
docker load -i lnvgy_sw_lxca_1l0-3.5.0_anyos_noarch
```

Passo 3. Modificare lo stesso file `docker-compose.yml` utilizzato per il contenitore originale. Aggiornare la proprietà dell'immagine nella parte superiore del file in modo che punti alla nuova immagine del docker del passaggio 2. È possibile modificare l'etichetta dell'immagine utilizzando il comando `docker tag`.

Di seguito viene mostrato un file yml di esempio, con IPv6 abilitato.

```
version: '3.8'

services:

  lxca:
    image: lenovo/lxca:4.1.0-124
    container_name: ${CONTAINER_NAME}
    tty: true
    stop_grace_period: 60s
    volumes:
      #bind mount example
      - /home/<HOST_MOUNT_POINT_FOR_BACKUP>:${BACKUP_MOUNT}
      - /home/<HOST_MOUNT_POINT_FOR_FW_SHARE>:${FIRMWARE_MOUNT}
      #docker volume mount
      - data:/opt/lenovo/lxca/data
      - postgresql:/var/lib/postgresql
      - log:/var/log
      - confluent-etc:/etc/confluent
      - confluent-log:/var/log/confluent
      - confluent:/var/lib/confluent
      - propconf:/opt/lenovo/lxca/bin/conf
      - ssh:/etc/ssh
      - xcat:/etc/xcat
    networks:
      lan:
        ipv4_address: ${ADDRESS}
        ipv6_address: "2001:8003:7d51:2003::2"
    dns:
      - 192.0.2.10
      - 192.0.2.11
    deploy:
      resources:
        limits:
          cpus: "2.0"
          memory: "8g"

volumes:
  data:
    name: ${CONTAINER_NAME}-data
  postgresql:
    name: ${CONTAINER_NAME}-postgresql
  log:
    name: ${CONTAINER_NAME}-log
  confluent-etc:
    name: ${CONTAINER_NAME}-confluent-etc
  confluent-log:
    name: ${CONTAINER_NAME}-confluent-log
  confluent:
    name: ${CONTAINER_NAME}-confluent
  propconf:
```

```
    name: ${CONTAINER_NAME}-propconf
  ssh:
    name: ${CONTAINER_NAME}-ssh
  xcat:
    name: ${CONTAINER_NAME}-xcat

networks:
  lan:
    name: lan
    driver: macvlan
    enable_ipv6: true
    driver_opts:
      parent: eth0
    ipam:
      config:
        - subnet: 192.0.0.0/19
          gateway: 192.0.30.1
        - subnet: "2001:8003:7d51:2000::/80"
          gateway: "2001:8003:7d51:2000::1"
```

Passo 4. Arrestare il contenitore *originale* utilizzando il comando seguente.

```
docker-compose -p ${CONTAINER_NAME} down
```

Passo 5. Distribuire la *nuova* immagine nel docker utilizzando il comando seguente, dove <*ENV_FILENAME*> è il nome del file delle variabili di ambiente.

```
COMPOSE_HTTP_TIMEOUT=300 docker-compose -p ${CONTAINER_NAME} --env-file <ENV_FILENAME> up -d
```

Capitolo 8. Disinstallazione di XClarity Administrator

Completare la seguente procedura per disinstallare un'appliance virtuale o un contenitore di Lenovo XClarity Administrator.

Procedura

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

Passo 1. Annullare la gestione di tutti i dispositivi attualmente gestiti da XClarity Administrator (vedere Gestione dello chassis, Gestione dei server e Gestione degli switch nella documentazione online di XClarity Administrator).

Passo 2. Disinstallare XClarity Administrator, a seconda del sistema operativo:

- **Docker-compose**Eseguire il seguente comando per interrompere il contenitore e rimuovere le reti e i volumi.
  ```
  docker-compose down -v
  ```
- **CentOS, Red Hat, Rocky e Ubuntu**
  1. Connettersi all'host mediante Virtual Machine Manager.
  2. Fare clic con il pulsante destro del mouse sulla macchina virtuale e scegliere **Arresta → Forza spegnimento**.
  3. Fare nuovamente clic con il pulsante destro del mouse sulla macchina virtuale e scegliere **Elimina**. Verrà visualizzata la finestra di dialogo Conferma eliminazione.
  4. Selezionare tutte le caselle di controllo e fare clic su **Elimina**.
- **ESXi**
  1. Connettersi all'host tramite VMware vSphere Client.
  2. Fare clic con il pulsante destro del mouse sulla macchina virtuale e scegliere **Alimentazione → Spegni**.
  3. Fare nuovamente clic con il pulsante destro del mouse sulla macchina virtuale e scegliere **Elimina dal disco**.
- **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 e scegliere **Arresta**.
  4. Fare nuovamente clic con il pulsante destro del mouse sulla macchina virtuale e scegliere **Elimina**.