



Guida per l'utente di Lenovo XClarity Orchestrator



Versione 2.1

Nota

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

Seconda edizione (Luglio 2024)

© Copyright Lenovo 2020, 2024.

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

Contenuto

Contenuto	i
----------------------------	----------

Riepilogo delle modificheiii
--------------------------------------------	-------------

Capitolo 1. Panoramica di Lenovo XClarity Orchestrator **1**

Login a XClarity Orchestrator	3
Suggerimenti e tecniche dell'interfaccia utente.	7

Capitolo 2. Amministrazione di XClarity Orchestrator **11**

Connessione degli strumenti di gestione delle risorse	11
Rilevamento e gestione dei dispositivi	15
Considerazioni sulla gestione dei dispositivi	16
Configurazione delle impostazioni di rilevamento globali	20
Gestione dei server	21
Gestione dei dispositivi client ThinkEdge	26
Gestione di dispositivi di storage	30
Gestione dello chassis	33
annullamento della gestione dei dispositivi	37
Utilizzo di VMware Tools	37
Configurazione delle impostazioni di rete	37
Configurazione di data e ora	40
Utilizzo dei certificati di sicurezza	42
Aggiunta di un certificato attendibile per i servizi esterni	43
Aggiunta di un certificato attendibile per i servizi interni	44
Installazione di un certificato del server XClarity Orchestrator con firma esterna, attendibile	45
Rigenerazione del certificato del XClarity Orchestrator server con firma interna.	47
Importazione del certificato server in un browser Web	49
Gestione autenticazione	50
Configurazione di un server di autenticazione LDAP esterno	50
Gestione di utenti e sessioni utente	54
Creazione degli utenti.	54
Creazione di gruppi di utenti	56
Modifica dei dettagli per l'account utente	58
Modifica dei dettagli per un altro utente.	59
Configurazione delle impostazioni di sicurezza utente	60
Monitoraggio delle sessioni utente attive	66
Controllo dell'accesso alle funzioni	66

Assegnazione dei ruoli agli utenti	68
Controllo dell'accesso alle risorse.	68
Abilitazione dell'accesso basato sulle risorse.	69
Creazione degli elenchi di controllo degli accessi	70
Gestione dello spazio su disco	72
Riavvio di XClarity Orchestrator.	72
Backup e ripristino dei dati del server Orchestrator	74
Backup e ripristino dei dati del server Orchestrator su un host VMware ESXi	75
Backup e ripristino dei dati del server Orchestrator su un host Microsoft Hyper-V	76

Capitolo 3. Monitoraggio di risorse e attività **79**

Visualizzazione del riepilogo dell'ambiente in uso.	79
Visualizzazione dello stato e dei dettagli degli strumenti di gestione delle risorse.	82
Visualizzazione dello stato dei dispositivi	83
Visualizzazione dei dettagli dei dispositivi.	87
Visualizzazione dello stato e dei dettagli delle risorse dell'infrastruttura	89
Monitoraggio dei processi.	91
Monitoraggio degli avvisi attivi	93
Monitoraggio degli eventi	95
Esclusione di avvisi ed eventi	96
Inoltro di dati di eventi, inventario e metrica	97
Creazione di filtri di inoltro dei dati.	99
Inoltro di eventi a SAP Data Intelligence	102
Inoltro di eventi a un servizio Web REST	104
Inoltro di eventi a un servizio e-mail tramite SMTP	106
Inoltro di inventario ed eventi a Splunk	111
Inoltro di eventi a un syslog	112
Inoltro dei dati di metrica a Lenovo TruScale Infrastructure Services	115
Inoltro di report	117
Creazione di configurazioni di destinazione del server d'inoltro	118
Inoltro di report tramite e-mail	119

Capitolo 4. Gestione delle risorse. **123**

Creazione dei gruppi di risorse	123
Gestione dei dispositivi offline	126
Esecuzione di azioni di alimentazione sui server gestiti.	126

Apertura di una sessione di controllo remoto per server gestiti	128
Apertura di una sessione di controllo remoto per i server ThinkSystem o ThinkAgile	128
Apertura di una sessione di controllo remoto per i server ThinkServer	129
Apertura di una sessione di controllo remoto per i server System x	130

Capitolo 5. Provisioning delle risorse137

Provisioning delle configurazioni dei server	137
Considerazioni sulla configurazione dei server	139
Apprendere un pattern di configurazione server da un server esistente	140
Assegnazione e distribuzione di un pattern di configurazione server	143
Gestione della conformità della configurazione server	146
Provisioning dei sistemi operativi	147
Considerazioni sulla distribuzione del sistema operativo	149
Sistemi operativi supportati	152
Profili immagine del sistema operativo	153
Disponibilità della porta per i sistemi operativi distribuiti.	156
Importazione delle immagini del sistema operativo	157
Configurazione dei profili del sistema operativo	159
Distribuzione di un'immagine del sistema operativo	161
Provisioning degli aggiornamenti alle risorse gestite	164
Considerazioni sulla distribuzione degli aggiornamenti	166
Download e importazione degli aggiornamenti	167
Creazione e assegnazione di criteri di conformità degli aggiornamenti	172
Applicazione e attivazione degli aggiornamenti agli strumenti di gestione delle risorse	176

Applicazione e attivazione degli aggiornamenti ai server gestiti	178
----------------------------------------------------------------------------	-----

Capitolo 6. Analisi delle tendenze e previsione dei problemi183

Creazione di report di analisi personalizzati	183
Creazione di regole per avvisi di analisi personalizzati	183
Creazione di report personalizzati (query)	186
Analisi dei tempi di avvio dei dispositivi	189
Analisi dei problemi di connettività	189
Analisi delle correzioni di sicurezza	190
Analisi dell'integrità dell'unità	190
Analisi del firmware	191
Analisi degli eventi persi	192
Analisi e previsione della capacità degli strumenti di gestione delle risorse.	192
Analisi e previsione delle tendenze di utilizzo	193
Analisi delle metriche di prestazioni e utilizzo	193
Analisi degli eventi ripetuti	195
Analisi dei tentativi di accesso non autorizzato.	196
Analisi dell'integrità del dispositivo	196
Analisi dell'integrità delle risorse dell'infrastruttura	198
Analisi di avvisi attivi	199

Capitolo 7. Utilizzo di assistenza e supporto201

Invio di dati periodici a Lenovo	201
Raccolta dei dati di servizio per XClarity Orchestrator	202
Raccolta dei dati di servizio per dispositivi	204
Importazione dei dati di servizio per i dispositivi	206
Creazione e assegnazione di contatti per assistenza e supporto	207
Apertura automatica dei ticket di assistenza mediante Call Home	208
Apertura manuale di un ticket di assistenza nel centro di supporto Lenovo	212
Visualizzazione di ticket di assistenza e stato	214
Visualizzazione delle informazioni sulla garanzia.	217

Riepilogo delle modifiche

Le versioni successive del software di gestione Lenovo XClarity Orchestrator supportano nuovi miglioramenti software e correzioni.

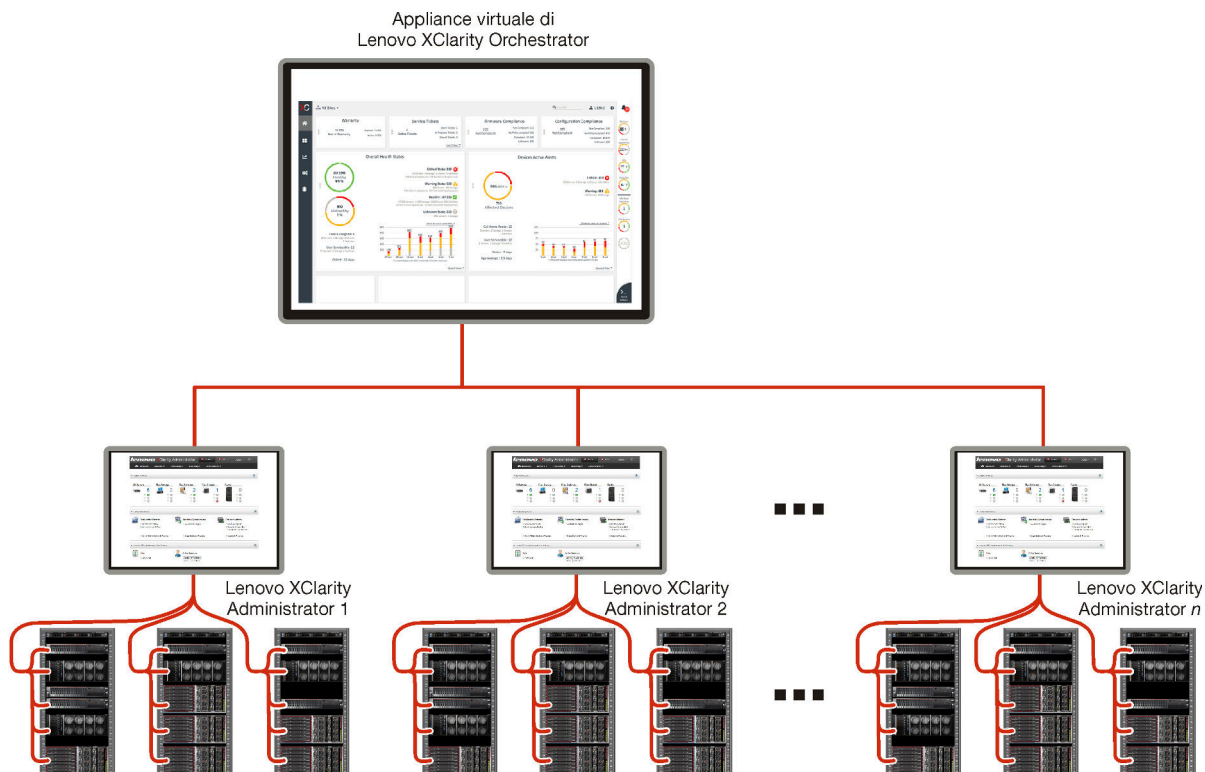
Per informazioni sulle correzioni, fare riferimento al file di cronologia modifiche (*.chg) fornito nel pacchetto di aggiornamento.

Questa versione supporta i seguenti miglioramenti del software di gestione. Per informazioni sulle modifiche delle versioni precedenti, vedere [Novità](#) nella documentazione online di XClarity Orchestrator.

Funzione	Descrizione
Amministrazione	È possibile riavviare il server Orchestrator dall'interfaccia utente (vedere Riavvio di XClarity Orchestrator).
Gestione delle risorse	Lenovo XClarity Management Hub 2.0 è un nuovo strumento di gestione dei dispositivi leggero, che è possibile utilizzare per gestire i server Lenovo ThinkSystem e ThinkEdge SE (vedere Connessione degli strumenti di gestione delle risorse). È possibile gestire un numero elevato di server utilizzando l'opzione di gestione di massa (vedere Gestione dei server). È possibile gestire i server utilizzando nomi di dominio completi (vedere Gestione dei server).
Monitoraggio di risorse e attività	I dati di inventario della memoria vengono ora visualizzati in un formato tabulare (vedere Visualizzazione dei dettagli dei dispositivi). È possibile visualizzare un elenco di tutti i processi pianificati (vedere Monitoraggio dei processi).
Provisioning delle risorse	È possibile pianificare l'esecuzione di un aggiornamento firmware in una data e un'ora specifiche (vedere Applicazione e attivazione degli aggiornamenti ai server gestiti).

Capitolo 1. Panoramica di Lenovo XClarity Orchestrator

Lenovo XClarity Orchestrator fornisce il monitoraggio centralizzato, la gestione, il provisioning e l'analisi per ambienti con numerosi dispositivi. Utilizza gli strumenti di gestione delle risorse esistenti (come Lenovo XClarity Administrator e Schneider Electric EcoStruxure IT Expert) su più siti per visualizzare l'integrità globale, raccogliere i riepiloghi di inventario e integrità dei dispositivi, eseguire il drill-down dettagliato dei dispositivi e visualizzare i log eventi e di controllo e applicare gli aggiornamenti alle risorse gestite.



Ulteriori informazioni:

- [Panoramica di XClarity Orchestrator](#)
- [Funzionalità di gestione](#)

Gestione e monitoraggio centralizzati delle risorse

XClarity Orchestrator fornisce un'unica interfaccia per monitorare e gestire gli strumenti di gestione delle risorse e i dispositivi gestiti tramite questi strumenti di gestione delle risorse.

- Viste di riepilogo dell'integrità delle risorse gestite, inclusi gli strumenti di gestione delle risorse, i dispositivi e le risorse dell'infrastruttura (ad esempio, PSU e UPS)
- Riepilogo e viste dettagliate dell'integrità dei componenti, dell'inventario delle risorse, dello stato della garanzia e avvisi per i dispositivi su più siti
- Aggregazione di avvisi ed eventi critici, creazione di avvisi personalizzati e inoltro di eventi ad applicazioni esterne
- Controllo del ciclo di vita per i dispositivi gestiti (incluse le operazioni di alimentazione)
- Avvio nel contesto dell'interfaccia utente per gli strumenti di gestione delle risorse e i dispositivi gestiti dalle pagine di riepilogo dei dispositivi

Provisioning degli aggiornamenti

È possibile utilizzare XClarity Orchestrator per gestire i livelli software correnti sulle risorse gestite. È possibile utilizzare il catalogo degli aggiornamenti per conoscere i livelli software disponibili, utilizzare i criteri di conformità degli aggiornamenti per identificare quali risorse devono essere aggiornate in base ai criteri personalizzati e quindi distribuire gli aggiornamenti a queste risorse. XClarity Orchestrator assicura il provisioning del software sulle risorse di destinazione nell'ordine corretto.

XClarity Orchestrator supporta le seguenti operazioni di provisioning.

- Distribuzione degli aggiornamenti agli strumenti di gestione delle risorse di Lenovo XClarity Administrator.
- Distribuzione degli aggiornamenti firmware ai dispositivi gestiti da XClarity Administrator.

Per ulteriori informazioni sugli aggiornamenti di provisioning, vedere [Provisioning degli aggiornamenti alle risorse gestite](#).

Provisioning della configurazione dei server

È possibile eseguire rapidamente il provisioning dei server gestiti utilizzando una configurazione coerente. Le impostazioni di configurazione (tra cui le impostazioni del controller di gestione della scheda di base e UEFI) vengono salvate come pattern che è possibile applicare a più server.

XClarity Orchestrator non distribuisce direttamente i pattern di configurazione ai server gestiti. Invia invece una richiesta al gestore delle risorse applicabile per avviare un processo per eseguire la distribuzione e quindi tenere traccia dell'avanzamento della richiesta.

Per ulteriori informazioni sul provisioning delle configurazioni dei server, vedere [Provisioning delle configurazioni dei server](#).

Provisioning dei sistemi operativi

È possibile utilizzare XClarity Orchestrator per distribuire le immagini del sistema operativo su più server.

XClarity Orchestrator non distribuisce direttamente il sistema operativo ai server gestiti. Invia invece una richiesta allo strumento di gestione delle risorse applicabile di XClarity Administrator per avviare un processo per eseguire l'aggiornamento, quindi tiene traccia dell'avanzamento della richiesta.

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

Per ulteriori informazioni sul provisioning delle configurazioni dei server, vedere [Provisioning dei sistemi operativi](#).

Apprendimento automatico della business intelligence e analisi predittiva

XClarity Orchestrator può connettersi a servizi di terze parti (come Splunk) per l'apprendimento automatico della business intelligence e l'analisi predittiva per:

- Raccogliere e visualizzare i dati di tendenza (come utilizzo del processore e della memoria, consumo energetico, temperatura, accesso non autorizzato, eventi ripetuti e persi e tempo medio tra i processi, come gli aggiornamenti firmware e i riavvii del sistema)
- Utilizzare dati di metrica per prevedere gli errori (ad esempio, eventi ripetuti e rapporti sull'integrità)
- Creare report di analisi personalizzati in base ai dati esistenti, inclusi avvisi, eventi, inventario dei dispositivi e metriche dei dispositivi.
- Definire regole di avviso personalizzate che, se abilitate, generano avvisi in caso di condizioni specifiche nell'ambiente.

Ulteriori informazioni:  [Funzionalità di analisi e predittive](#)

Per ulteriori informazioni sull'analisi predittiva, vedere [Analisi delle tendenze e previsione dei problemi](#).

Assistenza e supporto

XClarity Orchestrator può essere configurato in modo da raccogliere e inviare file di diagnostica automaticamente al supporto Lenovo mediante Call Home quando si verificano determinati eventi che richiedono assistenza nelle risorse gestite. È inoltre possibile raccogliere manualmente i file di diagnostica, aprire un record del problema e inviare i file di diagnostica al centro di supporto Lenovo.

Per maggiori informazioni su servizio e supporto, vedere [Utilizzo di assistenza e supporto](#).

Documentazione

La documentazione online viene regolarmente aggiornata in inglese. Per le informazioni e le procedure più recenti, vedere [Documentazione online di XClarity Orchestrator](#).

La documentazione online è disponibile nelle seguenti lingue.

- Inglese (en)
- Cinese semplificato (zh-CN)
- Cinese tradizionale (zh-TW)
- Francese (fr)
- Tedesco (de)
- Italiano (it)
- Giapponese (ja)
- Coreano (ko)
- Portoghese brasiliano (pt-BR)
- Russo (ru)
- Spagnolo (es)
- Tailandese (th)

È possibile modificare la lingua della documentazione online nei modi che seguono.

- Aggiungere `<language_code>` dopo `https://pubs.lenovo.com/lxco/`, ad esempio, per visualizzare la documentazione online in cinese semplificato.
`https://pubs.lenovo.com/lxco/zh-CN/lxco_overview`

Login a XClarity Orchestrator

Eseguire il login a un'interfaccia Web di Lenovo XClarity Orchestrator da un sistema con connettività di rete all'appliance virtuale XClarity Orchestrator.

Prima di iniziare

Accertarsi di utilizzare uno dei seguenti browser Web supportati. Per ulteriori informazioni, vedere [Hardware e software supportati](#) nella documentazione online di XClarity Orchestrator..

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

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

Quando si utilizza un account utente LDAP, è possibile accedere utilizzando il nome utente o `username@domain` (ad esempio `user1@company.com`).

XClarity Orchestrator disconnette automaticamente le sessioni utente che sono state inattive per una certa quantità di tempo e le sessioni utente aperte per un certo periodo di tempo, indipendentemente dall'attività. I seguenti valori predefiniti vengono impostati da XClarity Orchestrator.

- Se non è stato fatto clic o non è stato inserito testo nell'interfaccia utente per **30 minuti**, la sessione utente viene limitata alle operazioni di sola lettura. Se si tenta di modificare i dati, la sessione utente verrà automaticamente scollegata.
- Se non sono stati visualizzati attivamente i dati per **1440 minuti** (24 ore), la sessione utente verrà automaticamente scollegata.
- Dopo **24 ore** le sessioni utente vengono automaticamente scollegate, indipendentemente dall'attività dell'utente.

Procedura

Per eseguire il login all'interfaccia Web di XClarity Orchestrator, completare le seguenti operazioni.

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

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

Ad esempio:

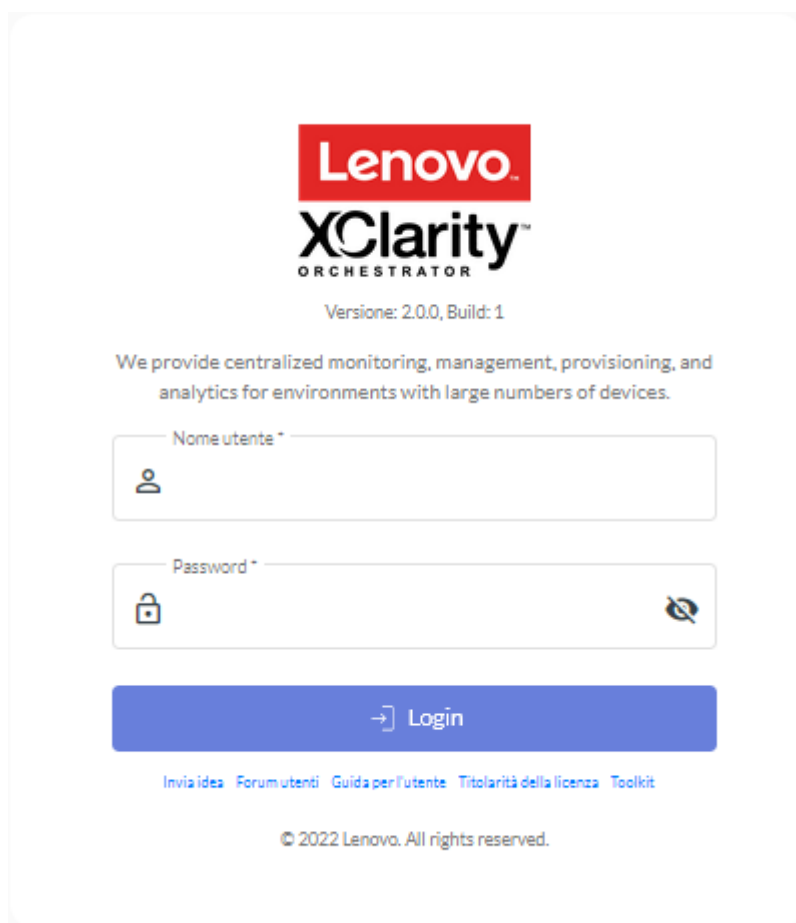
`https://192.0.2.10/#/login.html`

- **Utilizzo di un server DHCP nello stesso dominio di broadcast di XClarity Orchestrator** Se un server DHCP è configurato nello stesso dominio di broadcast di XClarity Orchestrator, utilizzare l'indirizzo IPv4 visualizzato nella console dell'appliance virtuale di XClarity Orchestrator per accedere all'interfaccia Web mediante l'URL che segue.
`https://{IPv4_address}#/login.html`

Ad esempio:

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

Viene visualizzata la pagina di login iniziale.



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

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

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

3. Immettere un ID utente e una password validi e fare clic su **Login**. La prima volta che si utilizzerà un account utente specifico per il login a XClarity Orchestrator, verrà richiesto di cambiare la password. Per impostazione predefinita, le password devono contenere da **8 a 256** caratteri e devono soddisfare i criteri che seguono.


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

- Deve contenere almeno un carattere alfabetico e non deve avere più di due caratteri sequenziali, tra cui sequenze di caratteri alfabetici, cifre e tasti della tastiera QWERTY (ad esempio, "abc", "123" e "asd" non sono consentiti)

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

Al termine

Verrà visualizzato il dashboard di XClarity Orchestrator con un riepilogo dell'integrità delle risorse e delle attività dell'ambiente in uso.

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

- Modificare la password dell'utente corrente facendo clic su **Modifica password**.
- È possibile effettuare il logout dalla sessione corrente facendo clic su **Disconnetti**. Viene visualizzata la pagina di login di XClarity Orchestrator.

Dalla pagina di login, è possibile fare clic sul collegamento **Autorizzazione licenza** per aprire il [Portale Web Features on Demand](#), dove è possibile trovare e gestire tutte le licenze dei prodotti Lenovo.

- Inviare idee per XClarity Orchestrator sul [Sito Web di Lenovo XClarity Ideation](#) oppure facendo clic su **Invia idea**.
- Porre domande e individuare risposte sul [Sito Web del forum della community dedicata a Lenovo XClarity](#) facendo clic su **Forum utenti**.
- Scaricare il toolkit PowerShell (LXTOOLSTool) di XClarity Orchestrator facendo clic su **Toolkit**. Il toolkit LXCOPSTool fornisce una libreria di cmdlet per l'automatizzazione del provisioning e la gestione delle risorse da una sessione di Microsoft PowerShell.
- È possibile consultare le informazioni su come utilizzare XClarity Orchestrator nel sistema di guida integrato, facendo clic su **Guida**.

La documentazione online viene regolarmente aggiornata in inglese. Per le informazioni e le procedure più recenti, vedere [Documentazione online di XClarity Orchestrator](#).

- È possibile visualizzare le informazioni sulla versione di XClarity Orchestrator facendo clic su **Informazioni su**.

Dalla finestra di dialogo Informazioni su è possibile trovare i collegamenti per visualizzare il **Accordo di licenza dell'utente finale**, le **Licenze open source** e l'**Informativa sulla privacy di Lenovo**.

- È possibile modificare la lingua dell'interfaccia utente facendo clic su **Modifica lingua**. Sono supportate le seguenti lingue.
 - Inglese (en)
 - Cinese semplificato (zh-CN)
 - Cinese tradizionale (zh-TW)
 - Francese (fr)
 - Tedesco (de)
 - Italiano (it)
 - Giapponese (ja)
 - Coreano (ko)
 - Portoghese brasiliano (pt-BR)
 - Russo (ru)

- Spagnolo (es)
- Tailandese (th)


Suggerimenti e tecniche dell'interfaccia utente

Tenere presente questi suggerimenti e queste tecniche durante l'utilizzo delle interfacce utente di Lenovo XClarity Orchestrator e Lenovo XClarity Management Hub.

Importazione di file

È possibile importare i file trascinandoli e rilasciandoli nella finestra di dialogo Importa.

Quando si importa un file, nell'angolo inferiore destro dell'interfaccia utente viene visualizzato un popup espandibile con le informazioni sull'avanzamento e lo stato di ciascun processo di importazione. Le icone sul popup consentono di identificare rapidamente lo stato del processo per ogni importazione. Al termine dell'importazione viene avviato un processo per convalidare il file. Se si verifica un errore durante il processo di importazione, nella finestra di dialogo a comparsa viene elencato un messaggio di errore che consente di risolvere rapidamente il problema.

Quando il popup è compresso, è possibile fare clic e tenere premuta l'icona **Trascina**  per spostare il modulo in una posizione differente.

Fare clic su **Cancella tutto** per cancellare l'elenco dei processi di importazione completati. Se tutti i processi di importazione sono stati completati, il popup è nascosto.



Immissione del testo negli appositi campi

I caratteri che possono essere immessi in alcuni campi di testo sono limitati. Nel seguente elenco vengono descritti i caratteri consentiti.

- **Nomi.** Include tutte le lettere e i caratteri numerici nelle lingue supportate e i caratteri speciali @ - _ + / [] . , : e lo spazio.
- **Descrizioni.** Include tutte le lettere e i caratteri numerici nelle lingue supportate e i caratteri speciali @ - _ % & * + = / () { } [] . , : e lo spazio.
- **Password.** Per gli account utente locali, le password possono essere formate da **8-256** caratteri per impostazione predefinita, sebbene siano consigliati 16 o più caratteri. Non sono presenti restrizioni per le password. Tuttavia, le password richiedono determinati tipi di caratteri e limitano alcune sequenze per la sicurezza.
 - Deve contenere almeno un carattere alfabetico e non deve avere più di due caratteri sequenziali, tra cui sequenze di caratteri alfabetici, cifre e tasti della tastiera QWERTY (ad esempio, "abc", "123" e "asd" non sono consentiti)
 - Deve contenere almeno un numero
 - Deve contenere almeno due dei caratteri che seguono:
 - Caratteri alfabetici maiuscoli (A - Z)
 - Caratteri alfabetici minuscoli (a - z)
 - Caratteri speciali ; @ _ ! ' \$ & +Gli spazi non sono consentiti.
 - Non deve essere una ripetizione o l'inversione del nome utente.
 - Non deve contenere consecutivamente più di due degli stessi caratteri (ad esempio, "aaa", "111" e "...") non sono ammessi).

Espansione e compressione del riquadro di navigazione

Il riquadro di navigazione è compresso per impostazione predefinita e visualizza solo le icone che rappresentano voci di menu specifiche. È possibile fare clic su un'icona per espandere temporaneamente il riquadro di navigazione e il menu di tale icona. Quando si allontana il cursore dal riquadro di navigazione, il riquadro viene compresso in modo da visualizzare solo le icone.

Per mantenere il riquadro di navigazione espanso in modo permanente, fare clic sull'icona **Espandi** (). È quindi possibile comprimere il riquadro di spostamento facendo clic sull'icona **Comprimi** ().

Ambito dell'interfaccia utente

Per impostazione predefinita, in XClarity Orchestrator vengono visualizzati i dati di *tutte le risorse*. È possibile limitare l'ambito dei dati visualizzati nella sessione utente corrente alle sole risorse che si trovano in gruppi e strumenti di gestione delle risorse specifici utilizzando il menu a discesa **Ambito corrente** nella parte superiore della pagina. Nel menu a discesa è possibile visualizzare l'elenco degli strumenti di gestione delle risorse e dei gruppi nell'ambito corrente in **Elenco ambito personale**, fare clic su **Modifica ambito** per visualizzare una finestra di dialogo in cui è possibile creare un ambito personalizzato con più strumenti di gestione delle risorse e gruppi oppure selezionare **Tutte le risorse** per modificare l'ambito e visualizzare tutte le risorse.

L'ambito selezionato è persistente solo all'interno della sessione utente corrente. È possibile aprire più sessioni utente, ciascuna con viste diverse di dashboard, risorse, eventi e dati degli avvisi.

Nota: Gli strumenti di gestione delle risorse di VMware vRealize Operations Manager non sono inclusi nell'elenco degli strumenti di gestione delle risorse in quanto non gestiscono i dispositivi in XClarity Orchestrator.

Visualizzazione di una quantità maggiore o minore di dati per pagina

Cambiare il numero di righe che vengono elencate in una tabella per pagina utilizzando l'elenco a discesa **Righe per pagina** nella parte inferiore di ciascuna tabella. È possibile visualizzare 10, 15, 25 o 50 righe.

Ricerca di dati in elenchi di grandi dimensioni

Sono disponibili diversi modi per visualizzare un sottoinsieme di un elenco di grandi dimensioni in base a criteri specifici.

- Ordinare le righe della tabella facendo clic sull'intestazione di colonna.
- È possibile limitare l'ambito dei dati visualizzati nella sessione utente corrente alle sole risorse che si trovano in un gruppo o strumento di gestione delle risorse specifico utilizzando il menu a discesa **Ambito corrente** nella parte superiore della pagina (vedere "Ambito dell'interfaccia utente" sopra).
- Creare dinamicamente un sottoinsieme di elenchi, in base ai dati rilevati in colonne specifiche utilizzando i campi di immissione **Filtri**. È possibile filtrare le colonne mostrate e nascoste. È inoltre possibile salvare le query del filtro che si desidera utilizzare regolarmente.
- Perfezionare ulteriormente il sottoinsieme immettendo del testo (ad esempio, un nome o un indirizzo IP) nel campo **Cerca** per individuare i dati presenti in qualsiasi colonna disponibile.

Suggerimento: separare più ricerche con una virgola. Ad esempio, "180,190" consente di visualizzare tutte le righe che contengono 180 o 190 in una delle colonne disponibili.

- Fare clic sulla casella di controllo nell'intestazione della tabella per selezionare o deselezionare tutti gli elementi elencati nella tabella.

Visualizzazione dei dati delle tabelle

Aggiornare le tabelle di dati facendo clic sull'icona **Aggiorna** ().

Espandere o comprimere ogni riga per visualizzare o nascondere i dettagli secondari delle tabelle con righe espandibili (ad esempio, sulle schede Processi e Gestione repository). È inoltre possibile fare clic sull'icona **Comprimi tutto** (☰) per nascondere i dettagli secondari di tutte le righe.

Se le dimensioni delle colonne impediscono la visualizzazione di alcune informazioni nella cella della tabella (indicata dai puntini di sospensione), è possibile visualizzare le informazioni complete in un popup passando il mouse sulla cella.

Esportazione dei dati delle tabelle

Esportare i dati nella tabella corrente nel sistema locale facendo clic sull'icona **Esporta dati** (↗). È possibile scegliere di esportare tutte le pagine, la pagina corrente o le righe selezionate, scegliere il formato di file (XLSX, CSV o JSON) e specificare se includere tutte le colonne o solo le colonne visibili. Per il formato CSV, è anche possibile scegliere come separare i dati (utilizzando un punto e virgola, una scheda o una barra verticale).

Suggerimento: per il formato JSON, i timestamp nei dati esportati riflettono il fuso orario impostato per XClarity Orchestrator, non il sistema locale. Per i formati CSV e XLSX, i timestamp vengono convertiti nel fuso orario dell'utente, visualizzato nell'interfaccia Web.

Quando si esportano i dati, nell'angolo inferiore destro dell'interfaccia utente viene visualizzato un popup espandibile con le informazioni sull'avanzamento e lo stato. Le icone sul popup consentono di identificare rapidamente lo stato del processo per ogni esportazione. Se si verifica un errore durante il processo di esportazione, nella finestra di dialogo a comparsa viene elencato un messaggio di errore che consente di risolvere rapidamente il problema.

Quando il popup è compresso, è possibile fare clic e tenere premuta l'icona **Trascina** (☰) per spostare il modulo in una posizione differente.

Fare clic su **Cancella tutto** per cancellare l'elenco dei processi di esportazione completati. Se tutti i processi di esportazione sono stati completati, il popup è nascosto.

Configurazione delle colonne delle tabelle

Configurare le tabelle per visualizzare le informazioni più importanti per l'utente.

- Scegliere le colonne da visualizzare o nascondere facendo clic su **Tutte le azioni → Attiva/Disattiva colonne**.
- Riordinare le colonne trascinando le relative intestazioni nella posizione preferita.

Modifica della lingua dell'interfaccia utente

È possibile cambiare la lingua dell'interfaccia utente dopo aver effettuato il login iniziale.


Dopo il login è possibile modificare la lingua facendo clic sul menu **Account utente** (👤), quindi su **Modifica lingua**.

Nota: Il sistema di guida viene visualizzato nella stessa lingua selezionata per l'interfaccia utente.

Richiesta di supporto

Sono disponibili diversi modi per ottenere assistenza con l'interfaccia utente.

- Posizionare il cursore su un'icona **Guida** (?) su alcune pagine per visualizzare un popup con dettagli aggiuntivi su un campo specifico.
- Fare clic sul collegamento **Ulteriori informazioni** su alcune pagine per aprire il sistema di guida e ottenere ulteriori informazioni nel contesto.

- Ottenere informazioni su come eseguire azioni specifiche tramite l'interfaccia utente facendo clic sul menu **Account utente** () , quindi su **Guida**. La documentazione online viene regolarmente aggiornata in inglese. Per le informazioni e le procedure più recenti, vedere [Documentazione online di XClarity Orchestrator](#).

Capitolo 2. Amministrazione di XClarity Orchestrator

Sono disponibili diverse attività di amministrazione, come la configurazione delle impostazioni di sistema, ad esempio data e ora e accesso alla rete, la connessione degli strumenti di gestione delle risorse, la gestione dei server di autenticazione e dell'accesso utente e la gestione dei certificati di sicurezza.

Connessione degli strumenti di gestione delle risorse

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

Prima di iniziare

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

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

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

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

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

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

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

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

Informazioni su questa attività

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

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

Importante: Il processo di registrazione XClarity Management Hub 2.0 è diverso da quello di un altro strumento di gestione delle risorse. Per istruzioni dettagliate, vedere [Collegamento di XClarity Management Hub 2.0 a XClarity Orchestrator](#) nella documentazione online di XClarity Orchestrator..

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

Importante: Il processo di registrazione XClarity Management Hub è diverso da quello di un altro strumento di gestione delle risorse. Per istruzioni dettagliate, vedere [Collegamento di XClarity Management Hub a XClarity Orchestrator](#) nella documentazione online di XClarity Orchestrator..

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

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

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

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

Procedura

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

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

<input type="checkbox"/>	Strumento di gestione	Stato di integrità	Tipo	Versione	Build	Connesso	Dati di analisi	Gruppi
<input type="checkbox"/>	XClarity...	🟢 No...	XClarity...	2.0.0	279	Non dispor	Non dispor	Non dispor
<input type="checkbox"/>	host-10-...	🟢 No...	XClarity...	3.6.0	108	16/02/23	<input checked="" type="checkbox"/> ⓘ	Non dispor

0 selezionato / 2 Totale Righe per pagina: 10

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

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

- **XClarity Management Hub 2.0 o XClarity Management Hub**
 1. Immettere la chiave di registrazione generata dall'istanza dell'hub di gestione e fare clic su **Connetti**. Per ottenere il token di richiesta della registrazione, eseguire l'accesso al portale dell'hub di gestione, fare clic su **Registrazione** e selezionare **Crea chiave di registrazione**.
 2. Copiare la chiave di registrazione generata da XClarity Orchestrator.
 3. Dal portale dell'hub di gestione, fare clic su **Registrazione** e selezionare **Installa chiave di registrazione**, incollare il token di registrazione di XClarity Orchestrator e fare clic su **Connetti**.
- **XClarity Administrator**
 - Specificare il nome di dominio completo o l'indirizzo IP (IPv4 o IPv6). L'utilizzo del nome host senza il nome di dominio non è supportato.
 - Facoltativamente è possibile modificare la porta dello strumento di gestione delle risorse. Il valore predefinito è 443.
 - Specificare l'account utente e la password da utilizzare per eseguire il login a strumento di gestione delle risorse.
 - È possibile abilitare **Raccolta dei dati di analisi unità**. Se abilitata, i dati di analisi dell'unità vengono raccolti quotidianamente per i dispositivi ThinkSystem e ThinkAgile e utilizzati per l'analisi predittiva. La raccolta dei dati di analisi dell'unità è supportata solo per gli strumenti di gestione delle risorse XClarity Administrator v3.3.0 e successive.

Attenzione: La raccolta dei dati potrebbe incidere sulle prestazioni del sistema.
- **Esperto EcoStruxure IT**. Specificare il nome, la chiave token e l'URL da utilizzare per la connessione.
- **vRealize Operations Manager**

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

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

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

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

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

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

Al termine

Nella scheda Strumenti di gestione delle risorse è possibile effettuare le operazioni che seguono.

- Visualizzare lo stato di connessione per lo strumento di gestione delle risorse nella colonna **Stato di integrità**.
- Modificare le credenziali e le proprietà per uno strumento di gestione delle risorse selezionato, facendo clic sull'icona **Modifica** (✎).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).
- Abilitare o disabilitare la raccolta dei dati di analisi dell'unità di uno strumento di gestione delle risorse di XClarity Administrator selezionato facendo clic sull'icona **Modifica** (✎).

Nota: L'interruttore **Raccolta dei dati di analisi unità** è disabilitato in caso di problemi di connettività o credenziali di XClarity Administrator (vedere [Perdita improvvisa di connettività a uno strumento di gestione delle risorse](#) nella documentazione online di XClarity Orchestrator).

- Scollegare e rimuovere uno strumento di gestione delle risorse selezionato, facendo clic sull'icona **Elimina** (🗑️).

Nota: Se XClarity Orchestrator non riesce a connettersi allo strumento di gestione delle risorse (ad esempio, se le credenziali sono scadute o se sono presenti problemi di rete), selezionare **Forza disconnessione**.

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).

Una volta rimosso lo strumento di gestione delle risorse, verranno rimossi anche tutti i dispositivi gestiti dallo strumento di gestione delle risorse rimosso, che includono inventario dei dispositivi, log, dati di metrica e report di analisi.

- Risolvere i problemi di connessione di uno strumento di gestione delle risorse (vedere [Impossibile connettere uno strumento di gestione delle risorse](#) nella documentazione online di XClarity Orchestrator).

Rilevamento e gestione dei dispositivi

È possibile rilevare e gestire i dispositivi mediante Lenovo XClarity Orchestrator e assegnare la gestione di questi dispositivi a uno strumento di gestione delle risorse specifico.

Prima di iniziare

Per eseguire questa attività è necessario essere membri di un gruppo di utenti a cui è assegnato il ruolo predefinito di **Supervisore** o **Amministratore della sicurezza**.

Informazioni su questa attività

XClarity Orchestrator monitora e gestisce i dispositivi tramite gli strumenti di gestione delle risorse. Quando si collega uno strumento di gestione delle risorse, XClarity Orchestrator gestisce tutti i dispositivi controllati da questo strumento di gestione delle risorse.

È inoltre possibile gestire i dispositivi mediante XClarity Orchestrator. XClarity Orchestrator elenca i dispositivi già rilevati (ma non gestiti) dagli strumenti di gestione delle risorse. Quando si gestiscono i dispositivi rilevati da XClarity Orchestrator, i dispositivi vengono gestiti dallo strumento di gestione delle risorse che lo ha rilevato. Quando si rilevano e gestiscono manualmente i dispositivi utilizzando indirizzi IP, nomi host o sottoreti, è necessario scegliere lo strumento di gestione delle risorse da utilizzare per gestire i dispositivi. XClarity Management Hub può essere utilizzato per gestire i dispositivi client ThinkEdge. XClarity Management Hub 2.0 può essere utilizzato per gestire i dispositivi ThinkServer. Lenovo XClarity Administrator può essere utilizzato per gestire server, storage, switch e chassis.

Nota:

- Se si tenta di gestire un dispositivo tramite XClarity Management Hub 2.0 e questo dispositivo è già gestito mediante un altro XClarity Management Hub 2.0, XClarity Orchestrator rimuove l'account utente di gestione e le sottoscrizioni dal dispositivo senza la precedente conferma di gestione e quindi gestisce nuovamente il dispositivo tramite il nuovo hub di gestione. Al termine di questo processo, il dispositivo è offline ma ancora gestito dall'hub di gestione precedente, al quale non invia più dati. Tenere presente che è necessario annullare manualmente la gestione dei dispositivi dal primo hub di gestione mediante il portale connesso.
- Se si tenta di gestire un dispositivo mediante XClarity Management Hub 2.0 e questo dispositivo è già gestito tramite un altro XClarity Administrator, XClarity Orchestrator rimuove l'account utente di gestione, le sottoscrizioni e le informazioni LDAP e SSO registrate per XCC da XClarity Administrator dal dispositivo senza la conferma di XClarity Administrator e quindi gestisce nuovamente il dispositivo tramite il nuovo XClarity Management Hub 2.0. Al termine di questo processo, il dispositivo è offline ma ancora gestito dall'hub XClarity Administrator, al quale non invia più dati. Tenere presente che è necessario annullare manualmente la gestione dei dispositivi da XClarity Administrator mediante il portale connesso.

I seguenti dispositivi possono essere rilevati automaticamente dagli strumenti di gestione delle risorse mediante un protocollo di rilevamento dei servizi.

- Server e appliance ThinkSystem e ThinkAgile
- Server ThinkEdge SE
- Chassis di Flex System e dispositivi ThinkSystem e Flex System in uno chassis di Flex System
- Server tower e rack ThinkServer
- Server e appliance System x, Converged HX e NeXtScale
- Dispositivi di storage

I seguenti dispositivi *non possono* essere rilevati automaticamente dagli strumenti di gestione delle risorse mediante un protocollo di rilevamento dei servizi. È necessario installare l'agente UDC su questi dispositivi prima che possano essere rilevati e gestiti in modo sicuro.

- Client ThinkCentre
- Client ThinkEdge

Attualmente non è possibile gestire gli switch in XClarity Orchestrator. Inoltre non è possibile annullare la gestione degli switch Flex System in XClarity Orchestrator.

Considerazioni sulla gestione dei dispositivi

Prima di tentare di rilevare e gestire i dispositivi mediante XClarity Orchestrator, esaminare le seguenti considerazioni.

- [Considerazioni generali](#)
- [Considerazioni sui server](#)
- [Considerazioni sullo storage](#)
- [Considerazioni sugli switch](#)
- [Considerazioni sugli chassis](#)
- [Considerazioni su più strumenti di gestione](#)

Considerazioni generali

Verificare che XClarity Orchestrator supporti i dispositivi da gestire.

Accertarsi che sia installato il firmware minimo richiesto in ciascun sistema che si desidera gestire.

Alcune porte devono essere disponibili per la comunicazione con i dispositivi. Accertarsi che tutte le porte necessarie siano disponibili prima di gestire i server.

XClarity Orchestrator consente di rilevare automaticamente i dispositivi nell'ambiente utilizzato, analizzando i dispositivi gestibili che si trovano nella stessa sottorete IP di XClarity Orchestrator mediante un protocollo di rilevamento dei servizi. Per rilevare i dispositivi presenti in altre sottoreti, è possibile specificare manualmente gli indirizzi IP, i nomi host, l'intervallo di indirizzi IP o le sottoreti.

Una volta che i dispositivi sono gestiti da XClarity Orchestrator, XClarity Orchestrator esegue periodicamente il polling di ciascun dispositivo di storage gestito per raccogliere informazioni, quali inventario, VPD (Vital Product Data) e stato.

Se XClarity Orchestrator perde la comunicazione con un dispositivo (ad esempio, a causa di un'interruzione dell'alimentazione, di un errore di rete o se lo switch è offline) durante la raccolta dell'inventario nel processo di gestione, la gestione viene completata correttamente. Alcune informazioni di inventario potrebbero tuttavia essere incomplete. Attendere che il dispositivo torni online e che XClarity Orchestrator esegua il polling del dispositivo per l'inventario oppure raccogliere manualmente l'inventario sul dispositivo dall'interfaccia Web dello strumento di gestione delle risorse, selezionando il dispositivo e facendo clic su **Tutte le azioni** → **Inventario** → **Aggiorna inventario**.

I dispositivi possono essere gestiti da un solo strumento di gestione delle risorse per volta (XClarity Orchestrator, XClarity Management Hub 2.0, XClarity Management Hub o XClarity Administrator). Se un dispositivo è gestito da uno strumento di gestione delle risorse e si desidera gestirlo utilizzandone un altro, è necessario prima annullare la gestione del dispositivo dallo strumento di gestione delle risorse originale.

Se si modifica l'indirizzo IP di un dispositivo dopo che tale dispositivo è stato gestito da XClarity Orchestrator, questo riconosce il nuovo indirizzo IP e continua a gestire il server. Tuttavia, XClarity Orchestrator non riconosce la modifica dell'indirizzo IP per alcuni server. Se XClarity Orchestrator indica che il server è offline dopo la modifica dell'indirizzo IP, gestire nuovamente il server mediante l'opzione **Forza gestione**.

Se si rimuovono, sostituiscono o configurano gli adattatori di un dispositivo, riavviare il dispositivo almeno una volta per aggiornare le informazioni dell'inventario.

Per individuare un dispositivo situato su una sottorete *differente* dello strumento di gestione delle risorse, assicurarsi che una delle seguenti condizioni venga soddisfatta:

- Verificare che sia abilitato l'inoltro SLP multicast sugli switch rack e sui router dell'ambiente in uso. 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.
- Se SLP è disabilitato sul dispositivo o sulla rete, in alternativa è possibile utilizzare il metodo di rilevamento DNS, aggiungendo manualmente un record di servizio (record SRV) al server DNS (Domain Name Server).

Ad esempio:

```
lxco.company.com service = 0 0 443 server1.company.com
```

Abilitare quindi il rilevamento DNS sulla console di gestione della scheda di base dall'interfaccia Web di gestione, facendo clic su **Configurazione BMC → Rete** e selezionando la scheda **DNS**.

Considerazioni sull'incapsulamento

È possibile scegliere di abilitare l'incapsulamento sullo chassis e sui server durante il processo di gestione dei dispositivi. Quando l'impostazione globale di incapsulamento è abilitata e il dispositivo supporta l'incapsulamento, lo strumento di gestione delle risorse comunica con il dispositivo durante il processo di gestione per modificare la modalità di incapsulamento del dispositivo e impostarla su **encapsulationLite** e per modificare le regole del firewall sul dispositivo per limitare le richieste in entrata solo a quelle provenienti dallo strumento di gestione delle risorse.

Nota: Quando l'interfaccia di rete di gestione è configurata per utilizzare Dynamic Host Configuration Protocol (DHCP) ed è abilitato l'incapsulamento, la gestione dei dispositivi può richiedere molto tempo.

L'impostazione globale di incapsulamento è disabilitata per impostazione predefinita. Se disabilitata, la modalità di incapsulamento del dispositivo è impostata su **normale** e le regole del firewall non vengono modificate durante il processo di gestione del dispositivo.

Attenzione: Se la modalità di incapsulamento è **encapsulationLite** sui dispositivi gestiti, le seguenti situazioni potrebbero causare problemi di comunicazione e autenticazione tra lo strumento di gestione delle risorse e i dispositivi gestiti, rendendo irraggiungibili i dispositivi gestiti. Poiché i dispositivi sono configurati per ignorare le richieste TCP di altre origini, non è possibile accedere a tali dispositivi mediante un'interfaccia di rete. Nella maggior parte dei casi, questi dispositivi non rispondono a richieste ping, SSH o TELNET.

- Modifiche di rete sull'hypervisor in cui è in esecuzione lo strumento di gestione delle risorse
- VLAN (Virtual Local Area Network) o modifiche dei tag VLAN
- Modifiche permanenti agli indirizzi IP del dispositivo quando è abilitato l'incapsulamento
- Annullamento forzato della gestione di un dispositivo quando è abilitato l'incapsulamento
- Perdita della macchina virtuale dello strumento di gestione delle risorse
- Interruzione della comunicazione TCP tra la macchina virtuale e i dispositivi gestiti
- Altri problemi di rete che impediscono allo strumento di gestione delle risorse di comunicare direttamente con i dispositivi gestiti quando è abilitata la modalità di incapsulamento

Se si verifica un problema permanente, effettuare una delle seguenti operazioni per ripristinare l'accesso ai dispositivi precedentemente gestiti. Per ulteriori informazioni, vedere [Gestione dell'incapsulamento](#), [Ripristino della gestione con un modulo CMM dopo un errore del server di gestione](#) e [Ripristino della gestione con un modulo CMM dopo un errore del server di gestione](#) nella documentazione online di XClarity Administrator.

- Per ripristinare l'accesso a un IMM gestito in cui è attiva la modalità di incapsulamento, le impostazioni predefinite devono essere caricate dalla console locale tramite l'interfaccia utente grafica UEFI.
- Utilizzare il bridge da USB a Ethernet per accedere in-band al controller di gestione ed eseguire il seguente comando:
encaps lite -off

- Per ripristinare l'accesso a un CMM gestito in cui è attiva la modalità di incapsulamento, le impostazioni predefinite devono essere caricate utilizzando il pulsante di reimpostazione posteriore oppure eseguendo il seguente comando se è ancora possibile raggiungere la console:
`accesscontrol -off -T mm[p]`

Considerazioni sui server

Accertarsi che nel dispositivo sia abilitato il protocollo CIM over HTTPS. Eseguire il login all'interfaccia Web di gestione per il server utilizzando l'account utente `RECOVERY_ID`. Fare clic su **Configurazione BMC** → **Sicurezza** e quindi selezionare la scheda **CIM su HTTPS** e verificare che l'opzione **Abilita CIM su HTTPS** sia selezionata.

Quando si eseguono azioni di gestione su un server, accertarsi che quest'ultimo sia spento oppure acceso con avvio alla configurazione BIOS/UEFI o con un sistema operativo in esecuzione (vedere [Esecuzione di azioni di alimentazione sui server gestiti](#)). Se acceso senza un sistema operativo, il server verrà costantemente reimpostato dal controller di gestione nel tentativo di rilevare un sistema operativo.

Accertarsi che tutte le impostazioni `UEFI_Ethernet_*` e `UEFI_Slot_*` siano abilitate in Impostazioni uEFI nel server. Per verificare le impostazioni, riavviare il server e una volta visualizzato il prompt `<F1> Setup`, premere **F1** per avviare Setup Utility. Selezionare **Impostazioni di sistema** → **Dispositivi e porte di I/O** → **Abilita/Disabilita supporto ROM opzione adattatore**, quindi individuare la sezione **Abilita/Disabilita ROM opzionali UEFI** per verificare che le impostazioni siano abilitate. Se supportata, è inoltre possibile utilizzare la funzione Console remota nell'interfaccia del controller di gestione della scheda di base per esaminare e modificare le impostazioni in remoto.

Se il certificato del server del dispositivo è firmato da un'autorità di certificazione esterna, accertarsi che il certificato e gli eventuali certificati intermedi vengano importati nell'archivio attendibile di XClarity Orchestrator (vedere [Installazione di un certificato del server XClarity Orchestrator con firma esterna, attendibile](#)).

Dispositivi client ThinkEdge

I dispositivi client ThinkEdge non dispongono di controller di gestione della scheda di base e quindi non sono rilevabili mediante protocolli di rilevamento dei servizi. È necessario installare un agente UDC sui dispositivi client ThinkEdge prima di poterli rilevare e gestire in modo sicuro dallo strumento di gestione delle risorse di Lenovo XClarity Management Hub assegnato. Per ulteriori informazioni, vedere [Gestione dei dispositivi client ThinkEdge](#).

Server ThinkSystem SR635 e SR655

Verificare che sia installato un sistema operativo e che il server sia stato avviato sul sistema operativo, sul supporto avviabile montato oppure sulla shell EFI almeno una volta, in modo che XClarity Orchestrator possa raccogliere l'inventario per questi server.

Accertarsi che l'opzione IPMI su LAN sia abilitata. L'opzione IPMI su LAN è disabilitata per impostazione predefinita su questi server e deve essere abilitata manualmente prima di poter gestire i server. Per abilitare IPMI su LAN dall'interfaccia Web di ThinkSystem System Manager, fare clic su **Impostazioni** → **Configurazione IPMI**. Per rendere effettiva la modifica potrebbe essere necessario riavviare il server.

Server ThinkServer

Il nome host del server deve essere configurato mediante un nome host o un indirizzo IP valido per rilevare automaticamente questi server.

La configurazione di rete deve consentire il traffico SLP tra XClarity Orchestrator e il server.

È necessario il protocollo SLP unicast.

Per rilevare automaticamente i server ThinkServer è richiesto il protocollo SLP multicast. È inoltre necessario abilitare il protocollo SLP in ThinkServer System Manager (TSM).

Se i server ThinkServer si trovano su una rete diversa da XClarity Orchestrator, accertarsi che la rete sia configurata per consentire il protocollo UDP in ingresso attraverso la porta 162, in modo che XClarity Orchestrator possa ricevere eventi per tali dispositivi.

Server System x3950 X6

Questi server devono essere gestiti come due enclosure 4U, ciascuno con il proprio controller di gestione della scheda di base.

Per maggiori informazioni sulla gestione dei server, vedere [Gestione dei server](#) e [Gestione dei dispositivi client ThinkEdge](#).

Considerazioni sullo storage

Prima di rilevare e gestire i dispositivi di storage rack, verificare che i seguenti requisiti siano stati soddisfatti (diverso da ThinkSystem serie DE).

- La configurazione di rete deve consentire il traffico SLP tra lo strumento di gestione delle risorse e il dispositivo di storage rack.
- È necessario il protocollo SLP unicast.
- Affinché XClarity Orchestrator rilevi automaticamente i dispositivi Lenovo Storage, è richiesto il protocollo SLP multicast. Il protocollo SLP deve inoltre essere abilitato sul dispositivo di storage rack.

Per ulteriori informazioni sulla gestione dei dispositivi di storage, vedere [Gestione di dispositivi di storage](#).

Considerazioni sugli switch

La gestione degli switch rack mediante XClarity Orchestrator al momento non è supportata.

Considerazioni sugli chassis

Quando si gestisce uno chassis, vengono gestiti anche tutti i dispositivi nello chassis. Non è possibile rilevare e gestire i componenti nello chassis indipendenti dallo chassis.

Verificare che l'impostazione Numero di sessioni attive simultanee per gli utenti LDAP nel modulo CMM sia configurata su 0 (zero) per lo chassis. È possibile verificare questa impostazione dall'interfaccia Web del modulo CMM facendo clic su **Configurazione BMC → Account utente, Impostazioni di login globali** e quindi selezionando la scheda **Generale**.

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](#).

Considerare la possibilità di implementare indirizzi IPv4 o IPv6 per tutti i moduli CMM e gli switch Flex System gestiti da XClarity Orchestrator. 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).

Per individuare uno chassis situato su una sottorete *differente* dello strumento di gestione delle risorse, assicurarsi che una delle seguenti condizioni venga soddisfatta:

- Verificare che sia abilitato l'inoltro SLP multicast sugli switch rack e sui router dell'ambiente in uso. 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.
- Se SLP è disabilitato sul dispositivo o sulla rete, in alternativa è possibile utilizzare il metodo di rilevamento DNS, aggiungendo manualmente un record di servizio (record SRV) al server DNS (Domain Name Server).
Ad esempio:

```
lxco.company.com service = 0 0 443 cmm1.company.com
```

Abilitare quindi il rilevamento DNS sulla console di gestione della scheda di base dall'interfaccia Web di gestione, facendo clic su **Configurazione BMC → Rete** e selezionando la scheda **DNS**.

Per ulteriori informazioni sulla gestione degli chassis, vedere [Gestione dello chassis](#).

Considerazioni su più strumenti di gestione

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 Orchestrator.

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 del controller di gestione della scheda di base. 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 **Configurazione BMC → Account utente**.
 - b. Fare clic sulla scheda **Account**.
 - c. Fare clic sulle impostazioni **Login globale**.
 - 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.

Configurazione delle impostazioni di rilevamento globali

Scegliere le impostazioni preferite da utilizzare per il rilevamento dei dispositivi.

Procedura

Passo 1. Dalla barra dei menu di XClarity Orchestrator, fare clic su **Risorse** (⚙️) → **Nuovi dispositivi** per visualizzare la scheda Rileva e gestisci nuovi dispositivi.

Passo 2. Fare clic su ⚙️ **Configurazione** per visualizzare la finestra di dialogo Impostazioni rilevamento.

Passo 3. Selezionare le impostazioni di rilevamento preferite.

- **Rilevamento SLP** Indica se rilevare automaticamente i dispositivi utilizzando il protocollo SLP (Service Location Protocol).

Se abilitato, XClarity Orchestrator tenta di rilevare nuovi dispositivi ogni 15 minuti e a ogni login utente.

Nota: L'impostazione di rilevamento SLP scelta in XClarity Orchestrator sovrascrive qualsiasi impostazione di rilevamento SLP selezionata per le istanze Lenovo XClarity Administrator gestite da XClarity Orchestrator. Se l'impostazione di rilevamento SLP viene modificata in Lenovo XClarity Administrator, verrà sincronizzata con XClarity Orchestrator.

- **Incapsulamento su tutti i prossimi dispositivi gestiti** Indica se l'incapsulamento è abilitato durante la gestione del dispositivo.

L'incapsulamento è disabilitato per impostazione predefinita. Se disabilitata, la modalità di incapsulamento del dispositivo è impostata su **normale** e le regole del firewall non vengono modificate nell'ambito del processo di gestione.

Quando l'incapsulamento è abilitato e un dispositivo supporta l'incapsulamento, XClarity Orchestrator comunica con il dispositivo (tramite lo strumento di gestione delle risorse) durante il processo di gestione per la modifica della modalità di incapsulamento del dispositivo su **encapsulationLite** e delle regole del firewall sul dispositivo per limitare le richieste in entrata solo a quelle provenienti dallo strumento di gestione delle risorse scelto per gestire il dispositivo.

Attenzione: Se l'incapsulamento è abilitato e lo strumento di gestione delle risorse selezionato per gestire il dispositivo 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 tale dispositivo.

- **Richiesta di registrazione abilitata** Indica se gli strumenti di gestione delle risorse (Lenovo XClarity Administrator e Lenovo XClarity Management Hub) accettano le richieste di rilevamento da un controller di gestione della scheda di base, quando il controller di gestione utilizza DNS per individuare le istanze dello strumento di gestione delle risorse. Se abilitato, il controller di gestione può eseguire la registrazione con lo strumento di gestione delle risorse come dispositivo rilevato.
- **Pulizia dispositivi offline.** Indica se annullare automaticamente la gestione dei dispositivi offline per almeno il periodo di tempo specificato dalla voce **Timeout dispositivi offline**. Se abilitato, XClarity Orchestrator verifica i dispositivi offline ogni ora e ogni volta che un utente esegue l'accesso al portale.
- **Timeout dispositivi offline** Quantità di tempo, espressa in ore, che i dispositivi devono essere offline prima che vengano non gestiti automaticamente. Questo valore può essere compreso tra **1-24** ore. Il valore predefinito è **24** ore.

Passo 4. Fare clic su **Salva**.

Gestione dei server

È possibile utilizzare Lenovo XClarity Orchestrator per gestire diversi tipi di server.

Prima di iniziare

Per eseguire questa attività è necessario essere membri di un gruppo di utenti a cui è assegnato il ruolo predefinito di **Supervisore** o **Amministratore della sicurezza**.

Prima di gestire un dispositivo, osservare le relative considerazioni sulla gestione (vedere [Considerazioni sulla gestione dei dispositivi](#)).

Prima di gestire un dispositivo, esaminare le impostazioni globali di rilevamento (vedere [Configurazione delle impostazioni di rilevamento globali](#)).

Per rilevare e gestire i dispositivi Edge che non rispondono al protocollo di rilevamento dei servizi, vedere [Gestione dei dispositivi client ThinkEdge](#).

L'opzione di gestione di massa è disponibile solo per i server. Non sono supportati altri tipi di dispositivi.

Informazioni su questa attività

XClarity Orchestrator monitora e gestisce i dispositivi tramite gli strumenti di gestione delle risorse. Quando si collega uno strumento di gestione delle risorse, XClarity Orchestrator gestisce tutti i dispositivi controllati da questo strumento di gestione delle risorse.

È inoltre possibile gestire i dispositivi mediante XClarity Orchestrator. XClarity Orchestrator elenca i dispositivi già rilevati (ma non gestiti) dagli strumenti di gestione delle risorse. Quando si gestiscono i dispositivi rilevati da XClarity Orchestrator, i dispositivi vengono gestiti dallo strumento di gestione delle risorse che lo ha rilevato. Quando si rilevano e gestiscono manualmente i dispositivi utilizzando indirizzi IP, nomi host o sottoreti, è necessario scegliere lo strumento di gestione delle risorse da utilizzare per gestire i dispositivi. XClarity Management Hub può essere utilizzato per gestire i dispositivi client ThinkEdge. XClarity Management Hub 2.0 può essere utilizzato per gestire i dispositivi ThinkServer. Lenovo XClarity Administrator può essere utilizzato per gestire server, storage, switch e chassis.

Nota:

- Se si tenta di gestire un dispositivo tramite XClarity Management Hub 2.0 e questo dispositivo è già gestito mediante un altro XClarity Management Hub 2.0, XClarity Orchestrator rimuove l'account utente di gestione e le sottoscrizioni dal dispositivo senza la precedente conferma di gestione e quindi gestisce nuovamente il dispositivo tramite il nuovo hub di gestione. Al termine di questo processo, il dispositivo è offline ma ancora gestito dall'hub di gestione precedente, al quale non invia più dati. Tenere presente che è necessario annullare manualmente la gestione dei dispositivi dal primo hub di gestione mediante il portale connesso.
- Se si tenta di gestire un dispositivo mediante XClarity Management Hub 2.0 e questo dispositivo è già gestito tramite un altro XClarity Administrator, XClarity Orchestrator rimuove l'account utente di gestione, le sottoscrizioni e le informazioni LDAP e SSO registrate per XCC da XClarity Administrator dal dispositivo senza la conferma di XClarity Administrator e quindi gestisce nuovamente il dispositivo tramite il nuovo XClarity Management Hub 2.0. Al termine di questo processo, il dispositivo è offline ma ancora gestito dall'hub XClarity Administrator, al quale non invia più dati. Tenere presente che è necessario annullare manualmente la gestione dei dispositivi da XClarity Administrator mediante il portale connesso.

I seguenti dispositivi possono essere rilevati automaticamente dagli strumenti di gestione delle risorse mediante un protocollo di rilevamento dei servizi.

- Server e appliance ThinkSystem e ThinkAgile
- Server ThinkEdge SE
- Chassis di Flex System e dispositivi ThinkSystem e Flex System in uno chassis di Flex System
- Server tower e rack ThinkServer
- Server e appliance System x, Converged HX e NeXtScale
- Dispositivi di storage

Procedura

Per gestire i server, completare una delle seguenti procedure.

- [Rilevare manualmente i server](#)
- [Gestire i server rilevati](#)
- [Gestire un numero elevato di server](#)

Rilevare manualmente i server

Per rilevare e gestire manualmente server specifici che non si trovano nella stessa sottorete del server Orchestrator, completare le seguenti operazioni.

1. Dalla barra dei menu di XClarity Orchestrator, fare clic su **Risorse** (🔍) → **Nuovi dispositivi** per visualizzare la scheda Rileva e gestisci nuovi dispositivi.
2. Fare clic su **Immissione manuale** per visualizzare la finestra di dialogo Rileva nuovi dispositivi.
3. Selezionare **Dispositivi che rispondono al protocollo di rilevamento del servizio** e fare clic su **Avanti**.
4. Selezionare **Manuale** e fare clic su **Avanti**.
5. Scegliere la modalità di rilevamento dei dispositivi e specificare i valori appropriati.
 - **Indirizzi IP/Nomi host.** Immettere l'indirizzo IP IPV4 o IPv6 o il nome di dominio completo per ciascun dispositivo da gestire (ad esempio, 192.0.2.0 o d1.acme.com).
 - **Intervalli IP.** Immettere gli indirizzi IP iniziale e finale per la serie di dispositivi che si desidera gestire.
 - **Sottoreti.** Immettere l'indirizzo IP e la maschera per la sottorete. XClarity Orchestrator esegue la scansione della sottorete per ricercare i dispositivi gestibili.
6. Selezionare lo strumento di gestione delle risorse che si desidera utilizzare per gestire i dispositivi.
7. Fare clic su **Rileva dispositivi**. Una volta completato il processo di rilevamento, i dispositivi rilevati verranno elencati nella tabella Nuovi dispositivi.

Gestire i server rilevati

Per gestire i dispositivi già rilevati, completare le seguenti operazioni.

1. Dalla barra dei menu di XClarity Orchestrator, fare clic su **Risorse** (🔍) → **Nuovi dispositivi** per visualizzare la scheda Rileva e gestisci nuovi dispositivi.

Rileva e gestisci nuovi dispositivi

Fare clic su **Configurazione** per definire le impostazioni di rilevamento globali.
 Fare clic su **Credenziali UDS Portal** per impostare le credenziali UDS Portal necessarie per scaricare i pacchetti di provisioning UDC per dispositivi che non rispondono a un protocollo di rilevamento dei servizi.
 Se il seguente elenco non contiene il dispositivo previsto, utilizzare l'opzione **Immissione manuale** per rilevare il dispositivo. Per ulteriori informazioni sui motivi per cui un dispositivo non viene rilevato automaticamente, consultare il seguente argomento della guida: [Impossibile rilevare un dispositivo](#).

🔍 Immissione manuale ⚙️ Configurazione 🔒 Credenziali portale UDS

Nuovi dispositivi

🔄 ⏩ 📄 Tutte le azioni ▼ Filtri ▼ 🔍 Cerca ✕

<input type="checkbox"/>	Dispositivo rilevato	Indirizzi IP	Numero di serie	Tipo/modello	Tipo	Rilevato da
<input type="checkbox"/>	G8052-1	10.241.5.1, 10.:	Y010CM345...	7309/HC1 (...)	Switch	10.241.5.134
<input type="checkbox"/>	G8052-2	10.241.5.254, 1	Y010CM35C...	7309/HC1 (...)	Switch	10.241.5.134
<input type="checkbox"/>	Shanghai-SD...	10.241.5.42, 10	1234567890	7D75/CTO1...	Server	10.241.5.134

0 selezionato / 3 Totale Righe per pagina: 10 ▼

2. Fare clic su **Tutte le azioni** → **Aggiorna** per rilevare tutti i dispositivi gestibili nel dominio di XClarity Orchestrator. Il rilevamento potrebbe richiedere diversi minuti.
3. Selezionare uno o più server che si desidera gestire.

4. Fare clic sull'icona **Gestisci dispositivi selezionati** (⊕) per visualizzare la finestra di dialogo Gestisci dispositivi rilevati.
5. Controllare l'elenco dei dispositivi selezionati da gestire e fare clic su **Avanti**.
6. Specificare il nome utente e la password per l'autenticazione con il server.

Suggerimento: considerare la possibilità di utilizzare un account supervisore o amministratore per gestire il dispositivo. Se si usa un account con autorizzazione di livello inferiore, la gestione potrebbe avere esito negativo o positivo, ma con alcune caratteristiche che potrebbero non funzionare correttamente.

7. **Facoltativo:** selezionare **Crea un account di ripristino e disabilita tutti gli utenti locali**, quindi specificare la password di ripristino. Se l'opzione è disabilitata, per l'autenticazione vengono utilizzati gli account utente locali.

Se l'opzione è abilitata, lo strumento di gestione delle risorse assegnato crea un account utente di autenticazione gestita e un account di ripristino (RECOVERY_ID) sul server e tutti gli altri account utente locali vengono disabilitati. L'account utente di autenticazione gestita viene utilizzato da XClarity Orchestrator e dallo strumento di gestione delle risorse per l'autenticazione. Se si verifica un problema con XClarity Orchestrator o con lo strumento di gestione delle risorse e il sistema smette di funzionare per qualche motivo, *non* è possibile eseguire il login al controller di gestione della scheda di base utilizzando i normali account utente. È comunque possibile eseguire il login utilizzando l'account RECOVERY_ID.

Importante: Assicurarsi di registrare la password di ripristino per gli usi futuri.

Nota: L'account di ripristino non è supportato per i server ThinkServer e System x M4.

8. **Facoltativo:** abilitare l'opzione **Imposta la nuova password se le credenziali sono scadute**, quindi specificare la nuova password del server. Se la password del server corrente è scaduta, il rilevamento avrà esito negativo finché la password non verrà modificata. Se viene specificata una nuova password, le credenziali vengono modificate e il processo di gestione può continuare. La password viene modificata solo se la password corrente è scaduta.
9. Selezionare **Gestisci**. Viene creato un processo per completare il processo di gestione in background. È possibile monitorare lo stato del processo di gestione dalla finestra di dialogo o dal log dei processi facendo clic su **Monitoraggio** (📄) → **Processi** (vedere [Monitoraggio dei processi](#)).

Se la gestione non è riuscita a causa di una delle seguenti condizioni di errore, ripetere questa procedura utilizzando l'opzione Forza gestione.

- Lo strumento di gestione delle risorse non funziona correttamente e non può essere ripristinato.

Nota: Se l'istanza dello strumento di gestione delle risorse di sostituzione utilizza lo stesso indirizzo IP dello strumento di gestione delle risorse malfunzionante, è possibile gestire nuovamente il dispositivo utilizzando l'account e la password RECOVERY_ID (se applicabili) e l'opzione **Forza gestione**.

- Lo strumento di gestione delle risorse è stato disattivato prima di annullare la gestione dei dispositivi.
- La gestione dei dispositivi non è stata annullata correttamente.
- XClarity Orchestrator visualizza un dispositivo gestito come offline, dopo che l'indirizzo IP del dispositivo è stato modificato.

Gestire un numero elevato di server

Per gestire un numero elevato di server, completare le seguenti operazioni.

1. Dalla barra dei menu di XClarity Orchestrator, fare clic su **Risorse** (📄) → **Nuovi dispositivi** per visualizzare la scheda Rileva e gestisci nuovi dispositivi.
2. Fare clic sul pulsante **Gestione di massa** per visualizzare la finestra di dialogo Gestione di massa.

3. Selezionare lo strumento di gestione delle risorse che si desidera utilizzare per gestire i dispositivi.
4. Immettere l'indirizzo IP o il nome di dominio completo per ciascun server da gestire, separati da una virgola (ad esempio 192.0.2.0, d1.acme.com).

Importante:

- Tutti i server specificati devono utilizzare le stesse credenziali.
 - Gli FQDN possono contenere solo caratteri alfanumerici, punti e trattini.
5. Fare clic su **Avanti**.
 6. Specificare il nome utente e la password per l'autenticazione con il server.

Suggerimento: considerare la possibilità di utilizzare un account supervisore o amministratore per gestire il dispositivo. Se si usa un account con autorizzazione di livello inferiore, la gestione potrebbe avere esito negativo o positivo, ma con alcune caratteristiche che potrebbero non funzionare correttamente.

7. **Facoltativo:** selezionare **Crea un account di ripristino e disabilita tutti gli utenti locali**, quindi specificare la password di ripristino. Se l'opzione è disabilitata, per l'autenticazione vengono utilizzati gli account utente locali.

Se l'opzione è abilitata, lo strumento di gestione delle risorse assegnato crea un account utente di autenticazione gestita e un account di ripristino (RECOVERY_ID) sul server e tutti gli altri account utente locali vengono disabilitati. L'account utente di autenticazione gestita viene utilizzato da XClarity Orchestrator e dallo strumento di gestione delle risorse per l'autenticazione. Se si verifica un problema con XClarity Orchestrator o con lo strumento di gestione delle risorse e il sistema smette di funzionare per qualche motivo, *non* è possibile eseguire il login al controller di gestione della scheda di base utilizzando i normali account utente. È comunque possibile eseguire il login utilizzando l'account RECOVERY_ID.

Importante: Assicurarsi di registrare la password di ripristino per gli usi futuri.

Nota: L'account di ripristino non è supportato per i server ThinkServer e System x M4.

8. **Facoltativo:** abilitare l'opzione **Imposta la nuova password se le credenziali sono scadute**, quindi specificare la nuova password del server. Se la password del server corrente è scaduta, il rilevamento avrà esito negativo finché la password non verrà modificata. Se viene specificata una nuova password, le credenziali vengono modificate e il processo di gestione può continuare. La password viene modificata solo se la password corrente è scaduta.
9. Selezionare **Gestisci**. Viene creato un processo per completare il processo di gestione in background. È possibile monitorare lo stato del processo di gestione dalla finestra di dialogo o dal log dei processi facendo clic su **Monitoraggio** (📄) → **Processi** (vedere [Monitoraggio dei processi](#)).

Se la gestione non è riuscita a causa di una delle seguenti condizioni di errore, ripetere questa procedura utilizzando l'opzione Forza gestione.

- Lo strumento di gestione delle risorse non funziona correttamente e non può essere ripristinato.

Nota: Se l'istanza dello strumento di gestione delle risorse di sostituzione utilizza lo stesso indirizzo IP dello strumento di gestione delle risorse malfunzionante, è possibile gestire nuovamente il dispositivo utilizzando l'account e la password RECOVERY_ID (se applicabili) e l'opzione **Forza gestione**.

- Lo strumento di gestione delle risorse è stato disattivato prima di annullare la gestione dei dispositivi.
- La gestione dei dispositivi non è stata annullata correttamente.
- XClarity Orchestrator visualizza un dispositivo gestito come offline, dopo che l'indirizzo IP del dispositivo è stato modificato.

Al termine

È possibile effettuare le seguenti azioni sul dispositivo gestito.

- Monitorare lo stato del dispositivo e i dettagli (vedere [Visualizzazione dello stato dei dispositivi](#) e [Visualizzazione dei dettagli dei dispositivi](#)).
- Annullare la gestione e rimuovere un dispositivo selezionato facendo clic su **Risorse** (⚙️) e quindi selezionando il tipo di dispositivo nel riquadro di navigazione sinistro per visualizzare una scheda con una vista tabulare di tutti i dispositivi gestiti di questo tipo. Selezionare quindi i dispositivi per i quali si desidera annullare la gestione e fare clic sull'icona **Non gestire** (🗑️).

Nota:

- È possibile annullare la gestione di un massimo di **50** dispositivi alla volta.
- Verificare che non vi siano processi attivi in esecuzione sul dispositivo.
- Se XClarity Orchestrator non riesce a connettersi allo strumento di gestione delle risorse (ad esempio, se le credenziali sono scadute o se sono presenti problemi di rete), selezionare **Forza annullamento gestione anche se il dispositivo non è raggiungibile**.
- Per impostazione predefinita, la gestione dei dispositivi gestiti da XClarity Administrator che sono offline da almeno 24 ore viene annullata automaticamente (vedere [Configurazione delle impostazioni di rilevamento globali](#)).
- Per la maggior parte dei dispositivi, lo strumento di gestione delle risorse mantiene determinate informazioni sul dispositivo dopo l'annullamento della gestione. Quando i dispositivi non sono gestiti:
 - L'account utente di gestione e le sottoscrizioni di eventi e metriche vengono rimossi dal dispositivo.
 - Per i dispositivi gestiti da XClarity Administrator, se Call Home è attualmente abilitato su XClarity Administrator, Call Home è disabilitato sul dispositivo.
 - Per i dispositivi gestiti da XClarity Administrator, se l'incapsulamento è abilitato sul dispositivo, le regole del firewall del dispositivo vengono modificate con le impostazioni precedenti alla gestione del dispositivo.
 - Le informazioni sensibili, l'inventario, gli eventi e gli avvisi generati dal dispositivo vengono rimossi dall'hub di gestione.
 - Gli eventi e gli avvisi generati dall'hub di gestione per il dispositivo vengono mantenuti sull'hub di gestione.

Gestione dei dispositivi client ThinkEdge

I dispositivi client ThinkEdge non dispongono di controller di gestione della scheda di base e quindi non sono rilevabili mediante protocolli di rilevamento dei servizi. È necessario installare un agente UDC (Universal Device Client) sui dispositivi client ThinkEdge prima di poterli rilevare e gestire in modo sicuro mediante lo strumento di gestione delle risorse di Lenovo XClarity Management Hub assegnato. Solo gli strumenti di gestione delle risorse di Lenovo XClarity Management Hub possono rilevare e gestire questi dispositivi.

Prima di iniziare

Prima di gestire un dispositivo, osservare le relative considerazioni sulla gestione (vedere [Considerazioni sulla gestione dei dispositivi](#)).

Verificare che almeno uno strumento di gestione delle risorse di Lenovo XClarity Management Hub sia connesso a XClarity Orchestrator (vedere [Connessione degli strumenti di gestione delle risorse](#)).

Per eseguire questa attività è necessario essere membri di un gruppo di utenti a cui è assegnato il ruolo predefinito di **Supervisore** o **Amministratore della sicurezza**.

Verificare che le credenziali UDS Portal siano configurate con l'ID e il segreto client. Le credenziali vengono utilizzate per firmare i criteri usati nel pacchetto di provisioning client. UDS Portal è la fonte attendibile per la firma di questi criteri affinché l'agente UDC funzioni correttamente. Per configurare le credenziali, fare clic su

Risorse (🔍) → **Nuovi dispositivi** dalla barra dei menu, selezionare **Credenziali UDS Portal**, quindi immettere l'ID e il segreto client. È necessario richiedere l'ID e il segreto client a Lenovo. A tal fine inviare un messaggio e-mail all'indirizzo uedmcredreq@lenovo.com, usando "Credenziali UDS Portal" nella descrizione dell'e-mail, e includere il nome dell'azienda, le informazioni di contatto (indirizzo e-mail o numero di telefono) e il numero cliente Lenovo a 10 cifre.

Verificare che un agente UDC *non sia* attualmente installato sul dispositivo client ThinkEdge. Se è installato un agente UDC, è necessario disinstallarlo eseguendo i seguenti comandi. È necessario disporre dei privilegi elevati per installare l'agente UDC.

- **Linux**

```
sudo apt purge udc-release
```

- **Windows**

```
PUSHD %windir%\System32\drivers\Lenovo\udc\Data\InfBackup\.\UDCInfInstaller.exe -uninstall
```

```
POPD
```

Accertarsi che il server DNS sia configurato per includere i seguenti domini, dove *{hub-domain}* è il nome di dominio completo dello strumento di gestione delle risorse di XClarity Management Hub che si desidera utilizzare per gestire i dispositivi client ThinkEdge.

- *api.{hub-domain}*
- *api-mtls.{hub-domain}*
- *auth.{hub-domain}*
- *mqtt.{hub-domain}*
- *mqtt-mtls.{hub-domain}*
- *s3.{hub-domain}*
- *s3console.{hub-domain}*

Informazioni su questa attività

XClarity Orchestrator monitora e gestisce i dispositivi tramite gli strumenti di gestione delle risorse. Quando si collega uno strumento di gestione delle risorse, XClarity Orchestrator gestisce tutti i dispositivi controllati da questo strumento di gestione delle risorse.

È inoltre possibile gestire i dispositivi mediante XClarity Orchestrator. XClarity Orchestrator elenca i dispositivi già rilevati (ma non gestiti) dagli strumenti di gestione delle risorse. Quando si gestiscono i dispositivi rilevati da XClarity Orchestrator, i dispositivi vengono gestiti dallo strumento di gestione delle risorse che lo ha rilevato. Quando si rilevano e gestiscono manualmente i dispositivi utilizzando indirizzi IP, nomi host o sottoreti, è necessario scegliere lo strumento di gestione delle risorse da utilizzare per gestire i dispositivi. XClarity Management Hub può essere utilizzato per gestire i dispositivi client ThinkEdge. XClarity Management Hub 2.0 può essere utilizzato per gestire i dispositivi ThinkServer. Lenovo XClarity Administrator può essere utilizzato per gestire server, storage, switch e chassis.

L'elenco completo dei dispositivi client ThinkEdge supportati è disponibile sul [Sito Web del supporto per Lenovo XClarity](#). A tal fine fare clic sulla scheda **Compatibilità** e quindi sul collegamento per i tipi di dispositivi appropriati.

Nota: I server ThinkEdge (come SE350, SE360 e SE450) dispongono di un controller di gestione della scheda di base e possono essere rilevati mediante un protocollo di rilevamento del servizio. Per gestire questi dispositivi, vedere [Gestione dei server](#).

Procedura

Per rilevare e gestire i dispositivi client ThinkEdge, completare le seguenti operazioni.

1. Installare l'agente UDC in ogni dispositivo client ThinkEdge.

- a. Dalla barra dei menu di XClarity Orchestrator, fare clic su **Risorse** (🔧) → **Nuovi dispositivi** per visualizzare la scheda Rileva e gestisci nuovi dispositivi.
 - b. Fare clic su **Immissione manuale** per visualizzare la finestra di dialogo Rileva nuovi dispositivi.
 - c. Selezionare **Dispositivi che non rispondono al protocollo di rilevamento del servizio** e fare clic su **Avanti**.
 - d. Selezionare l'indirizzo IP dello strumento di gestione delle risorse di XClarity Management Hub che si desidera utilizzare per gestire i dispositivi client ThinkEdge. È possibile selezionare solo gli strumenti di gestione delle risorse di XClarity Management Hub con stato integro.
 - e. Selezionare il tipo di sistema operativo installato sul server.
 - **Linux ARM**
 - **Linux x86**
 - **Windows**
 - f. Selezionare il numero di giorni prima che il programma di installazione dell'agente UDC diventi inutilizzabile dopo il download. Il valore predefinito è **30** giorni.
 - g. Selezionare il numero di volte che si prevede di installare l'agente UDC su un server. Questo è in genere il numero di dispositivi su cui è necessario installare l'agente UDC. È possibile specificare fino a **1.000.000** utilizzi; il valore predefinito è **10** utilizzi.
 - h. Fare clic su **Scarica agente UDC** per scaricare il programma di installazione dell'agente UDC nel sistema locale. Viene creato un processo per completare l'operazione di download in background. Per monitorare lo stato del processo di download nella finestra di dialogo o nel log dei processi, fare clic su **Monitoraggio** (📄) → **Processi** (vedere [Monitoraggio dei processi](#)).
 - i. Fare clic su **Chiudi** per chiudere la finestra di dialogo.
 - j. Copiare il programma di installazione dell'agente UDC in ogni dispositivo client ThinkEdge appropriato, decomprimere il pacchetto e installare l'agente UDC su questi dispositivi utilizzando il comando seguente. È necessario disporre dei privilegi di **amministratore** per installare l'agente.
 - **Linux** `install.sh`
 - **Windows** `setup.cmd`
 Una volta installato correttamente l'agente UDC in ogni dispositivo client ThinkEdge, i dispositivi possono essere rilevati automaticamente dallo strumento di gestione delle risorse di XClarity Management Hub selezionato.
2. Gestire i dispositivi client ThinkEdge.
 - a. Dalla barra dei menu di XClarity Orchestrator, fare clic su **Risorse** (🔧) → **Nuovi dispositivi** per visualizzare la scheda Rileva e gestisci nuovi dispositivi.




Nota: La visualizzazione degli indirizzi IP nella tabella potrebbe richiedere del tempo.

Rileva e gestisci nuovi dispositivi




Fare clic su **Configurazione** per definire le impostazioni di rilevamento globali.

Fare clic su **Credenziali UDS Portal** per impostare le credenziali UDS Portal necessarie per scaricare i pacchetti di provisioning UDC per dispositivi che non rispondono a un protocollo di rilevamento dei servizi.

Se il seguente elenco non contiene il dispositivo previsto, utilizzare l'opzione **Immissione manuale** per rilevare il dispositivo. Per ulteriori informazioni sui motivi per cui un dispositivo non viene rilevato automaticamente, consultare il seguente argomento della guida: [Impossibile rilevare un dispositivo](#).

 Immissione manuale
  Configurazione
  Credenziali portale UDS

Nuovi dispositivi




 Tutte le azioni ▼ Filtri ▼ Cerca

<input type="checkbox"/>	Dispositivo rilevato	Indirizzi IP	Numero di serie	Tipo/modello	Tipo	Rilevato da
<input type="checkbox"/>	G8052-1	10.241.5.1, 10:	Y010CM345...	7309/HC1 (...)	Switch	10.241.5.134
<input type="checkbox"/>	G8052-2	10.241.5.254, 1	Y010CM35C...	7309/HC1 (...)	Switch	10.241.5.134
<input type="checkbox"/>	Shanghai-SD...	10.241.5.42, 1C	1234567890	7D75/CTO1...	Server	10.241.5.134

0 selezionato / 3 Totale Righe per pagina: 10 ▼

- b. Fare clic su **Tutte le azioni** → **Aggiorna** per rilevare tutti i dispositivi gestibili nel dominio di XClarity Orchestrator. Il rilevamento potrebbe richiedere diversi minuti.
- c. Selezionare uno o più dispositivi client ThinkEdge che si desidera gestire.
- d. Fare clic sull'icona **Gestisci** (+) per visualizzare la finestra di dialogo Gestisci dispositivi.
- e. Controllare l'elenco dei dispositivi selezionati da gestire.
- f. Selezionare **Gestisci**. Viene creato un processo per completare il processo di gestione in background. È possibile monitorare lo stato del processo di gestione dalla finestra di dialogo o dal log dei processi facendo clic su **Monitoraggio** (📧) → **Processi** (vedere [Monitoraggio dei processi](#)).

Se la gestione non è riuscita a causa di una delle seguenti condizioni di errore, ripetere questa procedura utilizzando l'opzione Forza gestione.

- Lo strumento di gestione delle risorse non funziona correttamente e non può essere ripristinato.

Nota: Se l'istanza dello strumento di gestione delle risorse di sostituzione utilizza lo stesso indirizzo IP dello strumento di gestione delle risorse malfunzionante, è possibile gestire nuovamente il dispositivo utilizzando l'account e la password RECOVERY_ID (se applicabili) e l'opzione **Forza gestione**.

- Lo strumento di gestione delle risorse è stato disattivato prima di annullare la gestione dei dispositivi.
- La gestione dei dispositivi non è stata annullata correttamente.
- XClarity Orchestrator visualizza un dispositivo gestito come offline, dopo che l'indirizzo IP del dispositivo è stato modificato.

Al termine

È possibile effettuare le seguenti azioni sul dispositivo gestito.

- Monitorare lo stato del dispositivo e i dettagli (vedere [Visualizzazione dello stato dei dispositivi](#) e [Visualizzazione dei dettagli dei dispositivi](#)).
- Annullare la gestione e rimuovere un dispositivo selezionato facendo clic su **Risorse** (⚙️) e quindi selezionando il tipo di dispositivo nel riquadro di navigazione sinistro per visualizzare una scheda con una vista tabulare di tutti i dispositivi gestiti di questo tipo. Selezionare quindi i dispositivi per i quali si desidera annullare la gestione e fare clic sull'icona **Non gestire** (🗑️).

Nota:

- È possibile annullare la gestione di un massimo di **50** dispositivi alla volta.
- Verificare che non vi siano processi attivi in esecuzione sul dispositivo.
- Se XClarity Orchestrator non riesce a connettersi allo strumento di gestione delle risorse (ad esempio, se le credenziali sono scadute o se sono presenti problemi di rete), selezionare **Forza annullamento gestione anche se il dispositivo non è raggiungibile**.
- Per impostazione predefinita, la gestione dei dispositivi gestiti da XClarity Administrator che sono offline da almeno 24 ore viene annullata automaticamente (vedere [Configurazione delle impostazioni di rilevamento globali](#)).
- Per la maggior parte dei dispositivi, lo strumento di gestione delle risorse mantiene determinate informazioni sul dispositivo dopo l'annullamento della gestione. Quando i dispositivi non sono gestiti:
 - L'account utente di gestione e le sottoscrizioni di eventi e metriche vengono rimossi dal dispositivo.
 - Per i dispositivi gestiti da XClarity Administrator, se Call Home è attualmente abilitato su XClarity Administrator, Call Home è disabilitato sul dispositivo.
 - Per i dispositivi gestiti da XClarity Administrator, se l'incapsulamento è abilitato sul dispositivo, le regole del firewall del dispositivo vengono modificate con le impostazioni precedenti alla gestione del dispositivo.
 - Le informazioni sensibili, l'inventario, gli eventi e gli avvisi generati dal dispositivo vengono rimossi dall'hub di gestione.
 - Gli eventi e gli avvisi generati dall'hub di gestione per il dispositivo vengono mantenuti sull'hub di gestione.

Gestione di dispositivi di storage

Lenovo XClarity Orchestrator consente di gestire diversi tipi di appliance di storage, dispositivi e librerie nastro Lenovo.

Prima di iniziare

Per eseguire questa attività è necessario essere membri di un gruppo di utenti a cui è assegnato il ruolo predefinito di **Supervisore** o **Amministratore della sicurezza**.

Prima di gestire un dispositivo, osservare le relative considerazioni sulla gestione (vedere [Considerazioni sulla gestione dei dispositivi](#)).

Per rilevare e gestire i dispositivi Edge che non rispondono al protocollo di rilevamento dei servizi, vedere [Gestione dei dispositivi client ThinkEdge](#).

L'opzione di gestione di massa è disponibile solo per i server. Non sono supportati altri tipi di dispositivi.

Informazioni su questa attività

XClarity Orchestrator monitora e gestisce i dispositivi tramite gli strumenti di gestione delle risorse. Quando si collega uno strumento di gestione delle risorse, XClarity Orchestrator gestisce tutti i dispositivi controllati da questo strumento di gestione delle risorse.

È inoltre possibile gestire i dispositivi mediante XClarity Orchestrator. XClarity Orchestrator elenca i dispositivi già rilevati (ma non gestiti) dagli strumenti di gestione delle risorse. Quando si gestiscono i dispositivi rilevati da XClarity Orchestrator, i dispositivi vengono gestiti dallo strumento di gestione delle risorse che lo ha rilevato. Quando si rilevano e gestiscono manualmente i dispositivi utilizzando indirizzi IP, nomi host o sottoreti, è necessario scegliere lo strumento di gestione delle risorse da utilizzare per gestire i dispositivi. XClarity Management Hub può essere utilizzato per gestire i dispositivi client ThinkEdge. XClarity Management Hub 2.0 può essere utilizzato per gestire i dispositivi ThinkServer. Lenovo XClarity Administrator può essere utilizzato per gestire server, storage, switch e chassis.

Procedura

Per gestire i dispositivi di storage, completare una delle seguenti procedure.

- [Rilevare manualmente i dispositivi di storage](#)
- [Gestire i dispositivi di storage rilevati](#)

Rilevare manualmente i dispositivi di storage

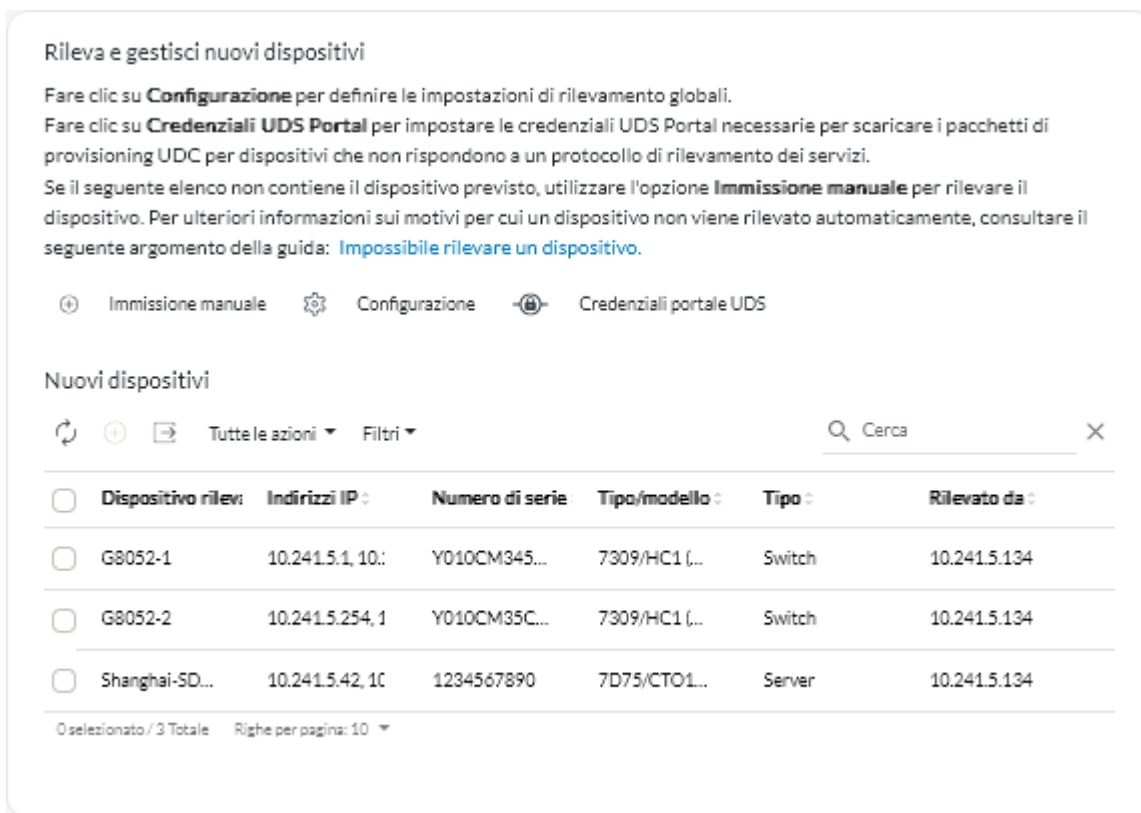
Per rilevare e quindi gestire manualmente dispositivi di storage specifici che non si trovano nella stessa sottorete del server Orchestrator, completare le seguenti operazioni.

1. Dalla barra dei menu di XClarity Orchestrator, fare clic su **Risorse** (🔍) → **Nuovi dispositivi** per visualizzare la scheda Rileva e gestisci nuovi dispositivi.
2. Fare clic su **Immissione manuale** per visualizzare la finestra di dialogo Rileva nuovi dispositivi.
3. Selezionare **Dispositivi che rispondono al protocollo di rilevamento del servizio** e fare clic su **Avanti**.
4. Selezionare **Manuale** e fare clic su **Avanti**.
5. Scegliere la modalità di rilevamento dei dispositivi e specificare i valori appropriati.
 - **Indirizzi IP/Nomi host**. Immettere l'indirizzo IP IPV4 o IPV6 o il nome di dominio completo per ciascun dispositivo da gestire (ad esempio, 192.0.2.0 o d1.acme.com).
 - **Intervalli IP**. Immettere gli indirizzi IP iniziale e finale per la serie di dispositivi che si desidera gestire.
 - **Sottoreti**. Immettere l'indirizzo IP e la maschera per la sottorete. XClarity Orchestrator esegue la scansione della sottorete per ricercare i dispositivi gestibili.
6. Selezionare lo strumento di gestione delle risorse che si desidera utilizzare per gestire i dispositivi.
7. Fare clic su **Rileva dispositivi**. Una volta completato il processo di rilevamento, i dispositivi rilevati verranno elencati nella tabella Nuovi dispositivi.

Gestire i dispositivi di storage rilevati

Per gestire i dispositivi già rilevati, completare le seguenti operazioni.

1. Dalla barra dei menu di XClarity Orchestrator, fare clic su **Risorse** (🔍) → **Nuovi dispositivi** per visualizzare la scheda Rileva e gestisci nuovi dispositivi.



- Fare clic su **Tutte le azioni** → **Aggiorna** per rilevare tutti i dispositivi gestibili nel dominio di XClarity Orchestrator. Il rilevamento potrebbe richiedere diversi minuti.
- Selezionare uno o più dispositivi di storage che si desidera gestire.
- Fare clic sull'icona **Gestisci dispositivi selezionati** (+) per visualizzare la finestra di dialogo Gestisci dispositivi rilevati.
- Controllare l'elenco dei dispositivi selezionati da gestire e fare clic su **Avanti**.
- Specificare il nome utente e la password per l'autenticazione con il server.

Suggerimento: considerare la possibilità di utilizzare un account supervisore o amministratore per gestire il dispositivo. Se si usa un account con autorizzazione di livello inferiore, la gestione potrebbe avere esito negativo o positivo, ma con alcune caratteristiche che potrebbero non funzionare correttamente.

- Selezionare **Gestisci**. Viene creato un processo per completare il processo di gestione in background. È possibile monitorare lo stato del processo di gestione dalla finestra di dialogo o dal log dei processi facendo clic su **Monitoraggio** (📄) → **Processi** (vedere [Monitoraggio dei processi](#)).

Se la gestione non è riuscita a causa di una delle seguenti condizioni di errore, ripetere questa procedura utilizzando l'opzione Forza gestione.

- Lo strumento di gestione delle risorse non funziona correttamente e non può essere ripristinato.

Nota: Se l'istanza dello strumento di gestione delle risorse di sostituzione utilizza lo stesso indirizzo IP dello strumento di gestione delle risorse malfunzionante, è possibile gestire nuovamente il dispositivo utilizzando l'account e la password RECOVERY_ID (se applicabili) e l'opzione **Forza gestione**.

- Lo strumento di gestione delle risorse è stato disattivato prima di annullare la gestione dei dispositivi.
- La gestione dei dispositivi non è stata annullata correttamente.

- XClarity Orchestrator visualizza un dispositivo gestito come offline, dopo che l'indirizzo IP del dispositivo è stato modificato.

Al termine

È possibile effettuare le seguenti azioni sul dispositivo gestito.

- Monitorare lo stato del dispositivo e i dettagli (vedere [Visualizzazione dello stato dei dispositivi](#) e [Visualizzazione dei dettagli dei dispositivi](#)).
- Annullare la gestione e rimuovere un dispositivo selezionato facendo clic su **Risorse** (⚙️) e quindi selezionando il tipo di dispositivo nel riquadro di navigazione sinistro per visualizzare una scheda con una vista tabulare di tutti i dispositivi gestiti di questo tipo. Selezionare quindi i dispositivi per i quali si desidera annullare la gestione e fare clic sull'icona **Non gestire** (🗑️).

Nota:

- È possibile annullare la gestione di un massimo di **50** dispositivi alla volta.
- Verificare che non vi siano processi attivi in esecuzione sul dispositivo.
- Se XClarity Orchestrator non riesce a connettersi allo strumento di gestione delle risorse (ad esempio, se le credenziali sono scadute o se sono presenti problemi di rete), selezionare **Forza annullamento gestione anche se il dispositivo non è raggiungibile**.
- Per impostazione predefinita, la gestione dei dispositivi gestiti da XClarity Administrator che sono offline da almeno 24 ore viene annullata automaticamente (vedere [Configurazione delle impostazioni di rilevamento globali](#)).
- Per la maggior parte dei dispositivi, lo strumento di gestione delle risorse mantiene determinate informazioni sul dispositivo dopo l'annullamento della gestione. Quando i dispositivi non sono gestiti:
 - L'account utente di gestione e le sottoscrizioni di eventi e metriche vengono rimossi dal dispositivo.
 - Per i dispositivi gestiti da XClarity Administrator, se Call Home è attualmente abilitato su XClarity Administrator, Call Home è disabilitato sul dispositivo.
 - Per i dispositivi gestiti da XClarity Administrator, se l'incapsulamento è abilitato sul dispositivo, le regole del firewall del dispositivo vengono modificate con le impostazioni precedenti alla gestione del dispositivo.
 - Le informazioni sensibili, l'inventario, gli eventi e gli avvisi generati dal dispositivo vengono rimossi dall'hub di gestione.
 - Gli eventi e gli avvisi generati dall'hub di gestione per il dispositivo vengono mantenuti sull'hub di gestione.

Gestione dello chassis

Lenovo XClarity Orchestrator consente di gestire diversi tipi di chassis e di componenti di chassis.

Prima di iniziare

Per eseguire questa attività è necessario essere membri di un gruppo di utenti a cui è assegnato il ruolo predefinito di **Supervisore** o **Amministratore della sicurezza**.

Prima di gestire un dispositivo, osservare le relative considerazioni sulla gestione (vedere [Considerazioni sulla gestione dei dispositivi](#)).

Per rilevare e gestire i dispositivi Edge che non rispondono al protocollo di rilevamento dei servizi, vedere [Gestione dei dispositivi client ThinkEdge](#).

L'opzione di gestione di massa è disponibile solo per i server. Non sono supportati altri tipi di dispositivi.

Informazioni su questa attività

XClarity Orchestrator monitora e gestisce i dispositivi tramite gli strumenti di gestione delle risorse. Quando si collega uno strumento di gestione delle risorse, XClarity Orchestrator gestisce tutti i dispositivi controllati da questo strumento di gestione delle risorse.

È inoltre possibile gestire i dispositivi mediante XClarity Orchestrator. XClarity Orchestrator elenca i dispositivi già rilevati (ma non gestiti) dagli strumenti di gestione delle risorse. Quando si gestiscono i dispositivi rilevati da XClarity Orchestrator, i dispositivi vengono gestiti dallo strumento di gestione delle risorse che lo ha rilevato. Quando si rilevano e gestiscono manualmente i dispositivi utilizzando indirizzi IP, nomi host o sottoreti, è necessario scegliere lo strumento di gestione delle risorse da utilizzare per gestire i dispositivi. XClarity Management Hub può essere utilizzato per gestire i dispositivi client ThinkEdge. XClarity Management Hub 2.0 può essere utilizzato per gestire i dispositivi ThinkServer. Lenovo XClarity Administrator può essere utilizzato per gestire server, storage, switch e chassis.

Procedura

Per gestire lo chassis, completare una delle seguenti procedure.

- [Rilevare manualmente lo chassis](#)
- [Gestire lo chassis rilevato](#)

Rilevare manualmente lo chassis

Per rilevare e quindi gestire manualmente lo chassis specifico che non si trova nella stessa sottorete del server Orchestrator, completare le seguenti operazioni.

1. Dalla barra dei menu di XClarity Orchestrator, fare clic su **Risorse** (🔍) → **Nuovi dispositivi** per visualizzare la scheda Rileva e gestisci nuovi dispositivi.
2. Fare clic su **Immissione manuale** per visualizzare la finestra di dialogo Rileva nuovi dispositivi.
3. Selezionare **Dispositivi che rispondono al protocollo di rilevamento del servizio** e fare clic su **Avanti**.
4. Selezionare **Manuale** e fare clic su **Avanti**.
5. Scegliere la modalità di rilevamento dei dispositivi e specificare i valori appropriati.
 - **Indirizzi IP/Nomi host.** Immettere l'indirizzo IP IPV4 o IPv6 o il nome di dominio completo per ciascun dispositivo da gestire (ad esempio, 192.0.2.0 o d1.acme.com).
 - **Intervalli IP.** Immettere gli indirizzi IP iniziale e finale per la serie di dispositivi che si desidera gestire.
 - **Sottoreti.** Immettere l'indirizzo IP e la maschera per la sottorete. XClarity Orchestrator esegue la scansione della sottorete per ricercare i dispositivi gestibili.
6. Selezionare lo strumento di gestione delle risorse che si desidera utilizzare per gestire i dispositivi.
7. Fare clic su **Rileva dispositivi**. Una volta completato il processo di rilevamento, i dispositivi rilevati verranno elencati nella tabella Nuovi dispositivi.

Gestire lo chassis rilevato

Per gestire i dispositivi già rilevati, completare le seguenti operazioni.




1. Dalla barra dei menu di XClarity Orchestrator, fare clic su **Risorse** (🔍) → **Nuovi dispositivi** per visualizzare la scheda Rileva e gestisci nuovi dispositivi.

Rileva e gestisci nuovi dispositivi




Fare clic su **Configurazione** per definire le impostazioni di rilevamento globali.

Fare clic su **Credenziali UDS Portal** per impostare le credenziali UDS Portal necessarie per scaricare i pacchetti di provisioning UDC per dispositivi che non rispondono a un protocollo di rilevamento dei servizi.

Se il seguente elenco non contiene il dispositivo previsto, utilizzare l'opzione **Immissione manuale** per rilevare il dispositivo. Per ulteriori informazioni sui motivi per cui un dispositivo non viene rilevato automaticamente, consultare il seguente argomento della guida: [Impossibile rilevare un dispositivo](#).

 Immissione manuale
  Configurazione
  Credenziali portale UDS

Nuovi dispositivi




 Tutte le azioni ▼ Filtri ▼ Cerca

<input type="checkbox"/>	Dispositivo rilevato	Indirizzi IP	Numero di serie	Tipo/modello	Tipo	Rilevato da
<input type="checkbox"/>	G8052-1	10.241.5.1, 10.241.5.134	Y010CM345...	7309/HC1 (...)	Switch	10.241.5.134
<input type="checkbox"/>	G8052-2	10.241.5.254, 10.241.5.134	Y010CM35C...	7309/HC1 (...)	Switch	10.241.5.134
<input type="checkbox"/>	Shanghai-SD...	10.241.5.42, 10.241.5.134	1234567890	7D75/CTO1...	Server	10.241.5.134

0 selezionato / 3 Totale Righe per pagina: 10 ▼

- Fare clic su **Tutte le azioni** → **Aggiorna** per rilevare tutti i dispositivi gestibili nel dominio di XClarity Orchestrator. Il rilevamento potrebbe richiedere diversi minuti.
- Selezionare uno o più chassis che si desidera gestire.
- Fare clic sull'icona **Gestisci dispositivi selezionati** (+) per visualizzare la finestra di dialogo Gestisci dispositivi rilevati.
- Controllare l'elenco dei dispositivi selezionati da gestire e fare clic su **Avanti**.
- Specificare il nome utente e la password per l'autenticazione con il server.


Suggerimento: considerare la possibilità di utilizzare un account supervisore o amministratore per gestire il dispositivo. Se si usa un account con autorizzazione di livello inferiore, la gestione potrebbe avere esito negativo o positivo, ma con alcune caratteristiche che potrebbero non funzionare correttamente.

- Facoltativo:** selezionare **Crea un account di ripristino e disabilita tutti gli utenti locali**, quindi specificare la password di ripristino. Se l'opzione è disabilitata, per l'autenticazione vengono utilizzati gli account utente locali.

Se l'opzione è abilitata, lo strumento di gestione delle risorse assegnato crea un account utente di autenticazione gestita e un account di ripristino (RECOVERY_ID) sul server e tutti gli altri account utente locali vengono disabilitati. L'account utente di autenticazione gestita viene utilizzato da XClarity Orchestrator e dallo strumento di gestione delle risorse per l'autenticazione. Se si verifica un problema con XClarity Orchestrator o con lo strumento di gestione delle risorse e il sistema smette di funzionare per qualche motivo, *non* è possibile eseguire il login al controller di gestione della scheda di base utilizzando i normali account utente. È comunque possibile eseguire il login utilizzando l'account RECOVERY_ID.

Importante: Assicurarsi di registrare la password di ripristino per gli usi futuri.

Nota: L'account di ripristino non è supportato per i server ThinkServer e System x M4.

8. **Facoltativo:** abilitare l'opzione **Imposta la nuova password se le credenziali sono scadute**, quindi specificare la nuova password del server. Se la password del server corrente è scaduta, il rilevamento avrà esito negativo finché la password non verrà modificata. Se viene specificata una nuova password, le credenziali vengono modificate e il processo di gestione può continuare. La password viene modificata solo se la password corrente è scaduta.
9. Selezionare **Gestisci**. Viene creato un processo per completare il processo di gestione in background. È possibile monitorare lo stato del processo di gestione dalla finestra di dialogo o dal log dei processi facendo clic su **Monitoraggio**  → **Processi** (vedere [Monitoraggio dei processi](#)).

Se la gestione non è riuscita a causa di una delle seguenti condizioni di errore, ripetere questa procedura utilizzando l'opzione Forza gestione.



- Lo strumento di gestione delle risorse non funziona correttamente e non può essere ripristinato.

Nota: Se l'istanza dello strumento di gestione delle risorse di sostituzione utilizza lo stesso indirizzo IP dello strumento di gestione delle risorse malfunzionante, è possibile gestire nuovamente il dispositivo utilizzando l'account e la password `RECOVERY_ID` (se applicabili) e l'opzione **Forza gestione**.

- Lo strumento di gestione delle risorse è stato disattivato prima di annullare la gestione dei dispositivi.
- La gestione dei dispositivi non è stata annullata correttamente.
- XClarity Orchestrator visualizza un dispositivo gestito come offline, dopo che l'indirizzo IP del dispositivo è stato modificato.

Al termine

È possibile effettuare le seguenti azioni sul dispositivo gestito.

- Monitorare lo stato del dispositivo e i dettagli (vedere [Visualizzazione dello stato dei dispositivi](#) e [Visualizzazione dei dettagli dei dispositivi](#)).
- Annullare la gestione e rimuovere un dispositivo selezionato facendo clic su **Risorse**  e quindi selezionando il tipo di dispositivo nel riquadro di navigazione sinistro per visualizzare una scheda con una vista tabulare di tutti i dispositivi gestiti di questo tipo. Selezionare quindi i dispositivi per i quali si desidera annullare la gestione e fare clic sull'icona **Non gestire** .

Nota:

- È possibile annullare la gestione di un massimo di **50** dispositivi alla volta.
- Verificare che non vi siano processi attivi in esecuzione sul dispositivo.
- Se XClarity Orchestrator non riesce a connettersi allo strumento di gestione delle risorse (ad esempio, se le credenziali sono scadute o se sono presenti problemi di rete), selezionare **Forza annullamento gestione anche se il dispositivo non è raggiungibile**.
- Per impostazione predefinita, la gestione dei dispositivi gestiti da XClarity Administrator che sono offline da almeno 24 ore viene annullata automaticamente (vedere [Configurazione delle impostazioni di rilevamento globali](#)).
- Per la maggior parte dei dispositivi, lo strumento di gestione delle risorse mantiene determinate informazioni sul dispositivo dopo l'annullamento della gestione. Quando i dispositivi non sono gestiti:
 - L'account utente di gestione e le sottoscrizioni di eventi e metriche vengono rimossi dal dispositivo.
 - Per i dispositivi gestiti da XClarity Administrator, se Call Home è attualmente abilitato su XClarity Administrator, Call Home è disabilitato sul dispositivo.
 - Per i dispositivi gestiti da XClarity Administrator, se l'incapsulamento è abilitato sul dispositivo, le regole del firewall del dispositivo vengono modificate con le impostazioni precedenti alla gestione del dispositivo.
 - Le informazioni sensibili, l'inventario, gli eventi e gli avvisi generati dal dispositivo vengono rimossi dall'hub di gestione.

- Gli eventi e gli avvisi generati dall'hub di gestione per il dispositivo vengono mantenuti sull'hub di gestione.

annullamento della gestione dei dispositivi

È possibile utilizzare Lenovo XClarity Orchestrator per rimuovere i dispositivi dalla gestione da parte dei rispettivi strumenti di gestione delle risorse. Questo processo è denominato *annullamento della gestione*.

Prima di iniziare

Per eseguire questa attività è necessario essere membri di un gruppo di utenti a cui è assegnato il ruolo predefinito di **Supervisore** o **Amministratore della sicurezza**.

Verificare che non vi siano processi attivi in esecuzione sul dispositivo.

Informazioni su questa attività

Per impostazione predefinita, XClarity Orchestrator annulla automaticamente la gestione dei dispositivi offline da almeno 24 ore (vedere [Configurazione delle impostazioni di rilevamento globali](#)).

Per la maggior parte dei dispositivi, XClarity Orchestrator e lo strumento di gestione delle risorse mantengono determinate informazioni sul dispositivo dopo l'annullamento della gestione. Queste informazioni verranno riapplicate quando lo stesso dispositivo verrà gestito nuovamente.

Procedura

Per annullare la gestione dei dispositivi, completare le seguenti operazioni.

- Passo 1. Sulla barra dei menu di XClarity Orchestrator fare clic su **Risorse** (🔍), quindi sul tipo di dispositivo per visualizzare una scheda con una vista tabulare di tutti i dispositivi gestiti simili.
- Passo 2. Selezionare uno o più dispositivi per i quali si desidera annullare la gestione.
- Passo 3. Fare clic sull'icona **Non gestire** (🛑) per visualizzare la finestra di dialogo di annullamento della gestione.
- Passo 4. Selezionare **Forza annullamento gestione anche se il dispositivo non è raggiungibile**.
- Passo 5. Fare clic su **Non gestire**.

La finestra di dialogo Non gestire mostra l'avanzamento di ogni operazione nel processo di annullamento della gestione.

Utilizzo di VMware Tools

Il pacchetto VMware Tools viene installato nel sistema operativo guest della macchina virtuale, quando si installa Lenovo XClarity Orchestrator in ambienti basati su VMware ESXi. Questo pacchetto fornisce una serie di strumenti VMware che supportano il backup e la migrazione ottimizzati delle appliance virtuali, preservando lo stato e la continuità delle applicazioni.

Per ulteriori informazioni sull'utilizzo di VMware Tools, vedere [Utilizzo di VMware Tools Configuration Utility nel sito Web del centro documentazione di VMware vSphere](#).

Configurazione delle impostazioni di rete

È possibile configurare una singola interfaccia di rete (mediante le impostazioni IPv4 e IPv6), le impostazioni di routing di Internet e le impostazioni proxy.

Prima di iniziare

Ulteriori informazioni:  [Come configurare le reti e i server NTP](#)

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


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

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

Attenzione:

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

Procedura

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

- **Configurare le impostazioni IP** È possibile scegliere di utilizzare le impostazioni di rete IPv4 e IPv6 delle schede Configurazione IPv4 e Configurazione IPv6. Abilitare e modificare le impostazioni di configurazione IP applicabili, quindi fare clic su **Applica**.
 - **Impostazioni IPv4.** È possibile configurare il metodo di assegnazione IP, l'indirizzo IPv4, la maschera di rete e il gateway predefinito. Per il metodo di assegnazione IP, è possibile scegliere di utilizzare un indirizzo IP assegnato staticamente oppure di ottenere un indirizzo IP da un server DHCP. Quando si utilizza un indirizzo IP statico, è necessario fornire un indirizzo IP, una maschera di rete e un gateway predefinito. Il gateway predefinito deve essere un indirizzo IP valido e deve trovarsi nella stessa sottorete dell'interfaccia di rete.

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

Configurazione IPv4

Abilitato

Metodo <input type="text" value="Ottieni indirizzo IP da ..."/>	Maschera di rete IPv4 <input type="text" value="255.255.224.0"/>
Intervallo IPv4 <input type="text" value="10.243.14.36"/>	Gateway predefinito IPv4 <input type="text" value="10.243.0.1"/>

Configurazione IPv6

Abilitato

Metodo <input type="text" value="Utilizza configurazio..."/>	Lunghezza del prefisso IPv6 <input type="text" value="64"/>
Indirizzo IPv6 <input type="text" value="fd55:faaf:e1ab:2021:20c:2'"/>	Gateway predefinito IPv6 <input type="text" value="fe80::5:73ff:fea0:2c"/>

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

Attualmente, solo gli indirizzi IPv4 sono supportati.

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

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

Nota:

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

Configurazione DNS

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

Tipo di indirizzi DNS preferiti IPv4 IPv6

Abilitato

Primo indirizzo DNS
10.240.0.10

Metodo
Utilizza il nome di d... ▼

Secondo indirizzo DNS
10.240.0.11

Nome di dominio

Nome Host
lxco

Applica Reimposta

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

Nota:

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

Configurazione proxy

Disabilitato

Nome host server proxy

Nome utente

Porta server proxy

Password

Applica Reimposta

Configurazione di data e ora

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

Prima di iniziare

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

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

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

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

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

Procedura

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

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

The screenshot shows the 'Data e ora' configuration page in XClarity Orchestrator. At the top, it states 'Data e ora verranno sincronizzate automaticamente con il server NTP'. Below this, the current settings are displayed: 'Data' is 04/10/22, 'Tempo' is 18:50:59, and 'Fuso orario' is UTC -00:00, Coordinated Universal Time Universal. A light blue notification bar indicates that the page will be updated automatically after changes. There are two input fields: 'Fuso orario' with a dropdown menu currently showing 'UTC -00:00, Coordinated Universal Time Universal', and 'Server NTP' with a text input field containing 'Server NTP 1 Indirizzo FQDN o IP'. Below these fields is a button with a plus icon and the text 'Aggiungi nuovo server NTP'. At the bottom left, there is an 'Applica' button.

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

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

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

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

Utilizzo dei certificati di sicurezza

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

Prima di iniziare

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

Informazioni su questa attività

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

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

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

XClarity Orchestrator funge da client durante la comunicazione con gli strumenti di gestione delle risorse e i servizi esterni. In questo caso lo strumento di gestione delle risorse o il servizio esterno sottopone il relativo certificato server a XClarity Orchestrator per la verifica. XClarity Orchestrator gestisce un elenco di certificati ritenuti attendibili. Se il *certificato attendibile* fornito dallo strumento di gestione delle risorse o dal servizio esterno non è nell'elenco, XClarity Orchestrator si disconnette dal dispositivo gestito o dal servizio esterno per evitare lo scambio di eventuali informazioni di sicurezza riservate con un'origine non attendibile.

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

- **Certificato server.** Durante l'avvio iniziale vengono generati una chiave univoca e un certificato autofirmato. Entrambi vengono utilizzati come autorità di certificazione radice predefinita, gestibile dalla pagina Autorità di certificazione tra le impostazioni di sicurezza di XClarity Orchestrator. Non è necessario rigenerare questo certificato radice, a meno che la chiave non sia stata compromessa o la politica della

propria organizzazione non preveda la sostituzione periodica di tutti i certificati (vedere [Rigenerazione del certificato del XClarity Orchestrator server con firma interna](#)). Durante la configurazione iniziale viene generata una chiave separata e un certificato server viene creato e sottoscritto dall'autorità di certificazione interna. Questo certificato viene utilizzato come certificato server predefinito di XClarity Orchestrator. Esso si rigenera automaticamente ogni volta che XClarity Orchestrator rileva che i rispettivi indirizzi di rete (indirizzi DNS o IP) sono stati modificati per garantire che il certificato contenga gli indirizzi corretti per il server. Può essere personalizzato e generato su richiesta (vedere [Rigenerazione del certificato del XClarity Orchestrator server con firma interna](#)).

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

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

La seguente categoria (archivi attendibili) di certificati viene utilizzata dai client di XClarity Orchestrator.

- **Certificati attendibili** Questo archivio attendibile gestisce i certificati utilizzati per stabilire una connessione sicura alle risorse locali quando XClarity Orchestrator viene utilizzato come client. Esempi di risorse locali sono gli strumenti di gestione delle risorse gestiti, il software locale per l'inoltro di eventi, ecc.
- **Certificati servizi esterni.** Questo archivio attendibile gestisce i certificati utilizzati per stabilire una connessione sicura con servizi esterni quando XClarity Orchestrator viene utilizzato come client. Esempi di servizi esterni sono i servizi online del supporto Lenovo, utilizzati per recuperare le informazioni sulla garanzia o creare ticket di assistenza, e il software esterno (come Splunk) ai quali possono essere inoltrati gli eventi. Contiene certificati attendibili preconfigurati, provenienti da autorità di certificazione radice di determinati fornitori da autorità di certificazione comunemente attendibili e note in tutto il mondo (come Digicert e Globalsign). Quando si configura XClarity Orchestrator per utilizzare una funzione che richiede una connessione a un altro servizio esterno, fare riferimento alla documentazione per determinare se è necessario aggiungere manualmente un certificato a questo archivio attendibile.

Nota: i certificati in questo archivio attendibile non sono attendibili quando si stabiliscono connessioni per altri servizi (come LDAP) a meno che anche questi non vengano aggiunti all'archivio attendibile principale dei certificati attendibili. La rimozione di certificati da questo archivio attendibile impedisce il corretto funzionamento di questi servizi.

Aggiunta di un certificato attendibile per i servizi esterni

Questi certificati vengono utilizzati per stabilire relazioni attendibili con i servizi esterni. Ad esempio, i certificati di questo archivio attendibile vengono utilizzati per il recupero delle informazioni sulla garanzia da Lenovo, la creazione di ticket, l'inoltro di eventi a un'applicazione esterna (come Splunk) e l'uso di server LDAP esterni.

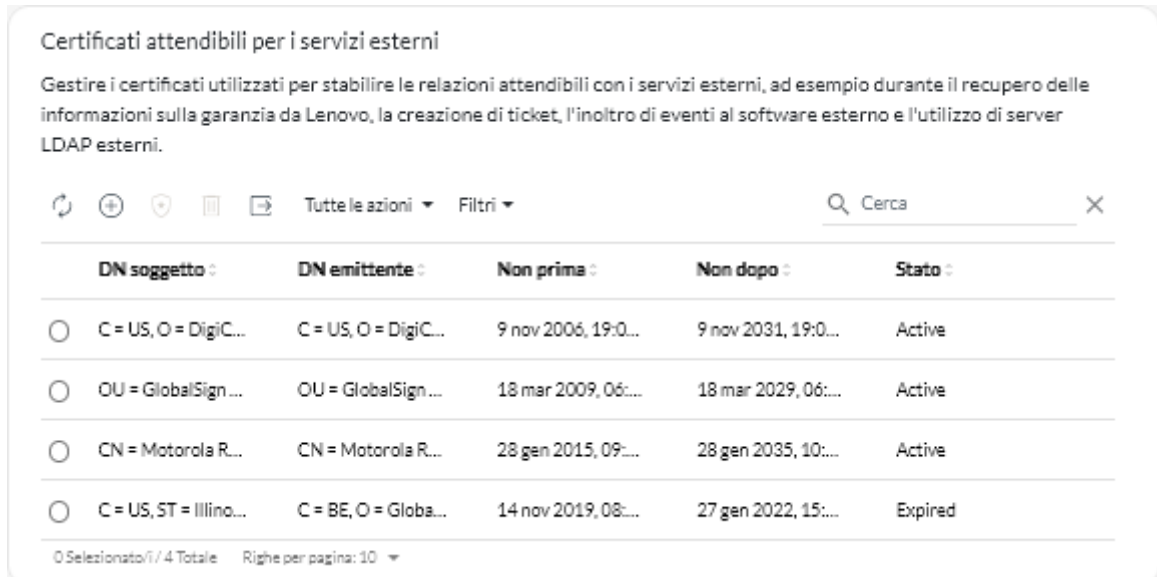
Prima di iniziare

I certificati presenti in questo archivio attendibile non sono attendibili quando si stabiliscono connessioni per altri servizi, a meno che anche questi non vengano aggiunti all'archivio attendibile principale dei certificati attendibili. La rimozione di certificati da questo archivio attendibile impedisce il corretto funzionamento di questi servizi.

Procedura

Per aggiungere un certificato attendibile, completare le seguenti operazioni.

Passo 1. Sulla barra dei menu di XClarity Orchestrator fare clic su **Amministrazione** (⚙️) → **Sicurezza**, quindi su **Certificati servizi esterni** nel riquadro di navigazione sinistro per visualizzare la scheda Certificati attendibili per i servizi esterni.



Certificati attendibili per i servizi esterni

Gestire i certificati utilizzati per stabilire le relazioni attendibili con i servizi esterni, ad esempio durante il recupero delle informazioni sulla garanzia da Lenovo, la creazione di ticket, l'inoltro di eventi al software esterno e l'utilizzo di server LDAP esterni.

Tutte le azioni ▾ Filtri ▾

	DN soggetto :	DN emittente :	Non prima :	Non dopo :	Stato :
<input type="radio"/>	C = US, O = DigiC...	C = US, O = DigiC...	9 nov 2006, 19:0...	9 nov 2031, 19:0...	Active
<input type="radio"/>	OU = GlobalSign...	OU = GlobalSign...	18 mar 2009, 06:...	18 mar 2029, 06:...	Active
<input type="radio"/>	CN = Motorola R...	CN = Motorola R...	28 gen 2015, 09:...	28 gen 2035, 10:...	Active
<input type="radio"/>	C = US, ST = Illino...	C = BE, O = Globa...	14 nov 2019, 08:...	27 gen 2022, 15:...	Expired

0 Selezionato/i / 4 Totale Righe per pagina: 10 ▾

Passo 2. Fare clic sull'icona **Aggiungi** (+) per aggiungere un certificato. Viene visualizzata la finestra di dialogo Aggiungi certificato.

Passo 3. Copiare e incollare i dati del certificato in formato PEM.

Passo 4. Fare clic su **Aggiungi**.

Al termine

È possibile effettuare le operazioni che seguono nella scheda Certificati attendibili per i servizi esterni.

- Visualizzare i dettagli di un certificato attendibile selezionato, facendo clic sull'icona **Visualizza** (*).
- Salvare un certificato attendibile selezionato nel sistema locale facendo clic sull'icona **Visualizza** (*), quindi su **Salva come PEM**.
- Eliminare un certificato attendibile selezionato facendo clic sull'icona **Elimina** (☒).

Aggiunta di un certificato attendibile per i servizi interni

Questi certificati vengono utilizzati per stabilire le relazioni di attendibilità con le risorse locali quando Lenovo XClarity Orchestrator funge da client per tali risorse, ad esempio gli strumenti di gestione delle risorse, inoltrando eventi al software locale e al server LDAP incorporato. Inoltre, il certificato CA interno e il certificato CA di un certificato del server con firma esterna personalizzato, se installato, sono presenti in questo archivio attendibile per supportare la comunicazione interna di XClarity Orchestrator.


Procedura

Per aggiungere un certificato attendibile, completare le seguenti operazioni.

Passo 1. Sulla barra dei menu di XClarity Orchestrator fare clic su **Amministrazione** (⚙️) → **Sicurezza**, quindi su **Certificati attendibili** nel riquadro di navigazione sinistro per visualizzare la scheda Certificato attendibile.

Certificati attendibili

Gestire i certificati utilizzati per stabilire le relazioni attendibili con le risorse locali, quando XClarity Orchestrator viene utilizzato come client per queste risorse, quali gli strumenti di gestione delle risorse (XClarity Administrator), l'inoltro di eventi al software locale e il server LDAP.






 Tutte le azioni ▾ Filtri ▾ Cerca X

	DN soggetto :	DN emittente :	Non prima :	Non dopo :	Stato :
<input type="radio"/>	C = US, ST = Nort...	C = US, ST = Nort...	31 dic 1969, 19:0...	31 dic 2069, 18:5...	Active
<input type="radio"/>	C = US, ST = NC, L...	C = US, ST = NC, L...	3 ott 2022, 11:14...	3 ott 2023, 11:14...	Active

0 Selezionato/i / 2 Totale Righe per pagina: 10 ▾

Passo 2. Fare clic sull'icona **Aggiungi** (+) per aggiungere un certificato. Viene visualizzata la finestra di dialogo **Aggiungi certificato**.

Passo 3. Copiare e incollare i dati del certificato in formato PEM.

Passo 4. Fare clic su **Aggiungi**.

Al termine

Nella scheda **Certificato attendibile** è possibile effettuare le operazioni che seguono.

- Visualizzare i dettagli di un certificato attendibile selezionato, facendo clic sull'icona **Visualizza** (*).
- Salvare un certificato attendibile selezionato nel sistema locale facendo clic sull'icona **Visualizza** (*), quindi su **Salva come PEM**.
- Eliminare un certificato attendibile selezionato facendo clic sull'icona **Elimina** (III).

Installazione di un certificato del server XClarity Orchestrator con firma esterna, attendibile

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

Informazioni su questa attività

Si consiglia di utilizzare sempre certificati con firma v3.

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

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

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

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

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

Procedura

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

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

1. Sulla barra dei menu di XClarity Orchestrator fare clic su **Amministrazione** (⚙️) → **Sicurezza** e selezionare **Certificato server** nel riquadro di navigazione sinistro per visualizzare la scheda Genera CSR (Certificate Signing Request).

Genera CSR (Certificate Signing Request)

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

Paese/Area geografica*
UNITED STATES

Organizzazione*
Lenovo

Stato/Provincia*
NC

Unità organizzativa*
DCG

Città*
Raleigh

Nome comune*
Generated by Lenovo Management Ecosystem

Nomi alternativi oggetto ?

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

Genera file CSR Importa certificato

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

- (Facoltativo) Nomi alternativi dell'oggetto che vengono aggiunti all'estensione "subjectAltName" X.509 quando viene generata una richiesta CSR. Per impostazione predefinita, XClarity Orchestrator definisce automaticamente i nomi alternativi dell'oggetto per la richiesta CSR in base all'indirizzo IP e al nome host rilevati dalle interfacce di rete del sistema operativo guest di XClarity Orchestrator. Questi valori dei nomi alternativi dell'oggetto possono essere personalizzati, eliminati o incrementati. Tuttavia, i nomi alternativi dell'oggetto devono disporre del nome FQDN (Fully-Qualified Domain Name) o dell'indirizzo IP del server e il nome dell'oggetto deve essere impostato sul nome FQDN.

Il nome specificato deve essere valido per il tipo selezionato.

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

Nota: Tutti i nomi alternativi dell'oggetto elencati nella tabella vengono convalidati, salvati e aggiunti alla richiesta CSR solo dopo che la richiesta è stata generata nel passaggio successivo.

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

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

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

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

Rigenerazione del certificato del XClarity Orchestrator server con firma interna

È possibile generare un nuovo certificato del server per sostituire il certificato corrente del server Lenovo XClarity Orchestrator con firma interna o per reintegrare un certificato generato da XClarity Orchestrator qualora XClarity Orchestrator utilizzi un certificato del server con firma esterna personalizzato. Il nuovo certificato del server con firma interna viene utilizzato da XClarity Orchestrator per l'accesso HTTPS.


Informazioni su questa attività

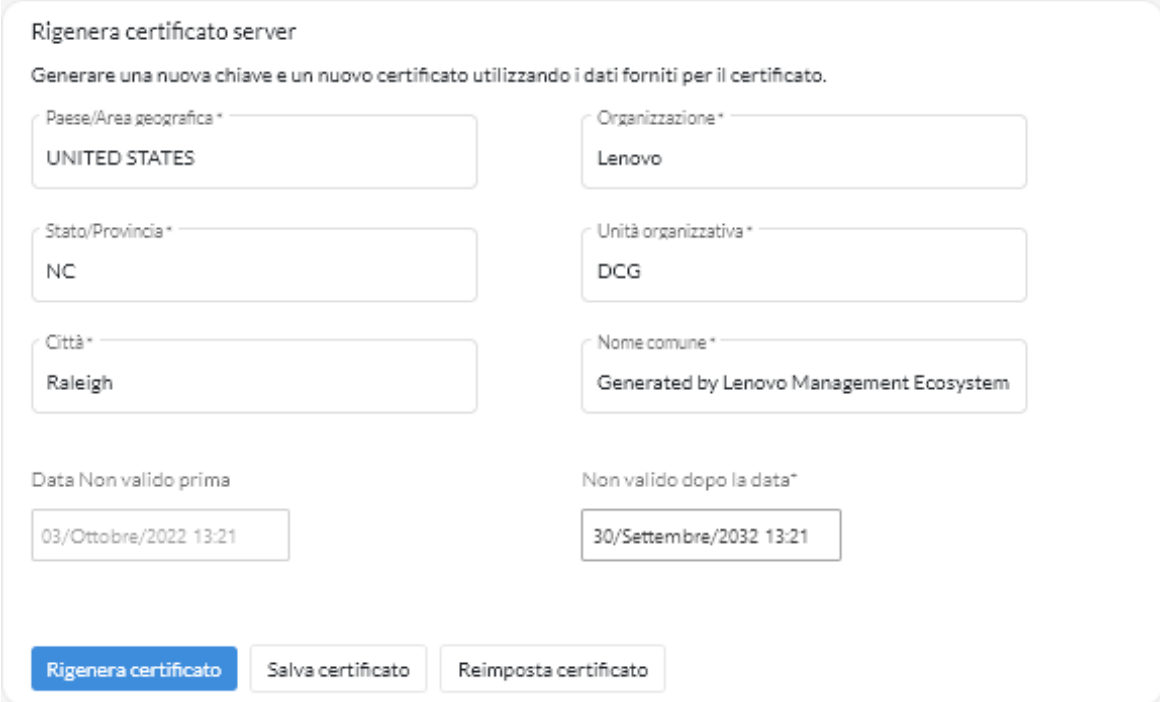
Il certificato corrente del server, sia esso con firma interna o esterna, rimarrà in uso finché non verrà rigenerato e firmato un nuovo certificato del server.

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

Procedura

Per generare un certificato del server XClarity Orchestrator con firma interna, effettuare le operazioni che seguono.

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



Rigenera certificato server

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

Paese/Area geografica *	Organizzazione *
UNITED STATES	Lenovo
Stato/Provincia *	Unità organizzativa *
NC	DCG
Città *	Nome comune *
Raleigh	Generated by Lenovo Management Ecosystem
Data Non valido prima	Non valido dopo la data *
03/Ottobre/2022 13:21	30/Settembre/2032 13:21

Rigenera certificato Salva certificato Reimposta certificato

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

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

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

Passo 3. Fare clic su **Rigenera certificato** per rigenerare il certificato con firma interna, quindi su **Rigenera certificato** per confermare.

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

Al termine

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

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

Importazione del certificato server in un browser Web

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

Procedura

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

• Chrome

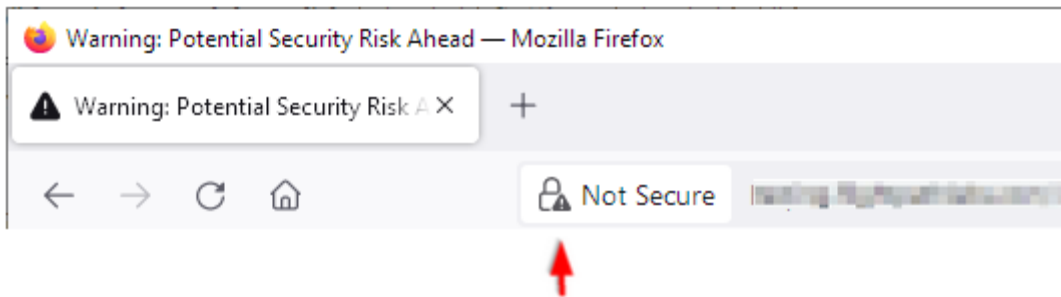
1. Esportare il certificato del server XClarity Orchestrator.
 - a. Fare clic sull'icona di avvertenza "Non sicuro" nella barra degli indirizzi superiore, ad esempio:



- b. Fare clic su **Certificato (non valido)** per visualizzare la finestra di dialogo Certificato.
 - c. Fare clic sulla scheda **Dettagli**.
 - d. Fare clic su **Copia su file** per visualizzare la finestra Esportazione guidata certificati.
 - e. Selezionare **Standard sintassi del messaggio crittografato** e fare clic su **Avanti**.
 - f. Specificare il nome e la posizione del file del certificato, quindi selezionare **Fine** per esportare il certificato.
 - g. Fare clic su **OK** per chiudere la finestra di dialogo Certificato.
2. Importare il certificato del server XClarity Orchestrator nell'elenco dei certificati radice attendibili dell'autorità per il browser in uso.
 - a. Dal browser Chrome, fare clic sui tre punti nell'angolo superiore destro della finestra, quindi selezionare **Impostazioni**.
 - b. Scorrere fino alla sezione **Privacy e sicurezza** e fare clic su **Gestisci certificati** per visualizzare la finestra Certificati.
 - c. Fare clic su **Importa** e selezionare il file del certificato esportato in precedenza, quindi fare clic su **Avanti**.
 - d. Fare clic su **Sfoggia** accanto ad **Archivio certificati** e selezionare **Autorità di certificazione radice attendibile**. Quindi fare clic su **OK**.
 - e. Fare clic su **Fine**.
 - f. Chiudere e riaprire il browser Chrome, quindi aprire XClarity Orchestrator.

- **Firefox**

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



- b. Espandere Connessione non sicura e fare clic su Ulteriori informazioni per visualizzare una finestra di dialogo.
 - c. Fare clic su **Mostra certificati**.
 - d. Scorrere verso il basso fino alla sezione Download e fare clic sul collegamento **PEM (cert)**.
 - e. Selezionare **Salva file** e fare clic su **OK**.
2. Importare il certificato del server XClarity Orchestrator nell'elenco dei certificati radice attendibili dell'autorità per il browser in uso.
 - a. Aprire il browser e fare clic su **Strumenti → Opzioni → Avanzate**.
 - b. Fare clic sulla scheda **Certificati**.
 - c. Fare clic su **Mostra certificati**.
 - d. Fare clic su **Importa** e accedere alla posizione in cui è stato scaricato il certificato.
 - e. Selezionare il certificato e fare clic su **Apri**.

Gestione autenticazione

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

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

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

Configurazione di un server di autenticazione LDAP esterno

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

Prima di iniziare

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

Solo Microsoft Active Directory è supportato come server LDAP esterno.

XClarity Orchestrator non clona automaticamente i gruppi di utenti definiti nel server LDAP esterno; tuttavia, è possibile clonare manualmente il gruppo di utenti LDAP (vedere [Creazione di gruppi di utenti](#)).

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

Informazioni su questa attività


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

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

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

Procedura

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

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

Client LDAP ↻

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

Informazioni sul server

636

🗑️ ⊕ ↑ ↓

Active Directory
 LDAP personalizzato

LDAP su SSL

Configurazione

Credenziali di associazione ⓘ

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

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

Recupera

Reimposta
Applica modifiche

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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


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

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

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

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

Al termine

È possibile rimuovere una configurazione del server LDAP facendo clic sull'icona **Elimina**  accanto alla configurazione. Quando si elimina una configurazione del server LDAP, se non sono disponibili altre configurazioni del server LDAP nello stesso dominio, vengono rimossi anche gli utenti clone e i gruppi di utenti clone del dominio.

Gestione di utenti e sessioni utente

Gli *account utente* vengono utilizzati per eseguire il login e gestire Lenovo XClarity Orchestrator.

Creazione degli utenti

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

Informazioni su questa attività

La prima volta che eseguono il login, gli utenti di un server LDAP esterno vengono automaticamente clonati nel server di autenticazione locale con il nome *{username}@{domain}*. Questo account utente clonato può essere utilizzato solo per autorizzare l'accesso alle risorse. Per questi utenti, l'autenticazione viene eseguita sempre mediante il server di autenticazione LDAP e le modifiche all'account utente (tranne per descrizione e ruoli) devono essere apportate tramite LDAP.

XClarity Orchestrator controlla l'accesso alle funzioni (azioni) utilizzando i ruoli. È possibile assegnare un ruolo differente agli utenti locali e clonati aggiungendo gli utenti a uno o più gruppi di utenti associati ai ruoli desiderati. Per impostazione predefinita, tutti gli utenti sono membri del gruppo di utenti **OperatorGroup** (vedere [Creazione di gruppi di utenti](#)).

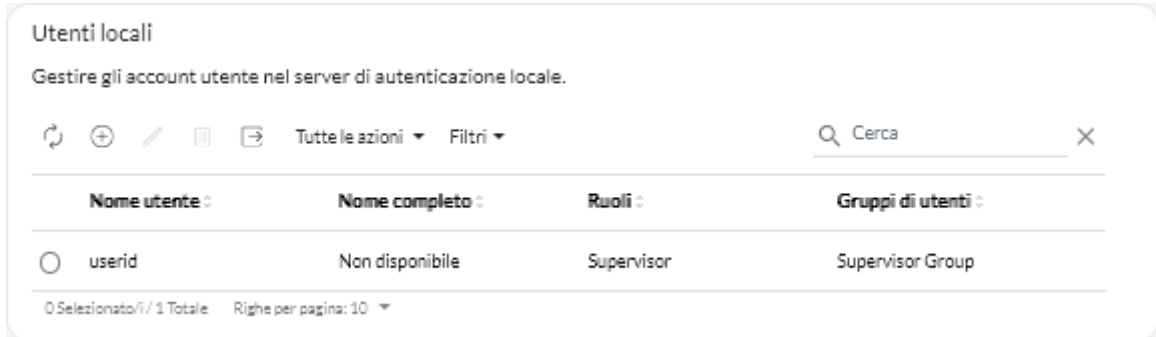
Almeno un utente deve essere membro di un gruppo di utenti *locale* a cui è assegnato il ruolo predefinito di **Supervisore** (vedere [Controllo dell'accesso alle funzioni](#)).

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

Procedura

Per creare un utente locale, effettuare le seguenti operazioni.

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



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

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

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

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

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

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

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

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

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

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

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

L'account utente viene aggiunto alla tabella.

Al termine

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

- Visualizzare le proprietà di un utente facendo clic sulla relativa riga nella tabella per aprire la finestra di dialogo Dettagli utente.
- Modificare le proprietà di un utente selezionato, come password e gruppi di utenti, facendo clic sull'icona **Modifica** (✎).
- Eliminare un utente selezionato facendo clic sull'icona **Elimina** (🗑️). Non è possibile eliminare il gruppo di utenti LDAP esistente dagli utenti LDAP.
- Esportare i dettagli utente, ad esempio nome utente, nome e cognome, facendo clic sull'icona **Esporta** (📤).

Creazione di gruppi di utenti

I gruppi di utenti vengono utilizzati per autorizzare l'accesso alle risorse.

Prima di iniziare

Ulteriori informazioni:  [Come creare un gruppo di utenti](#)

È possibile creare manualmente i gruppi di utenti nel repository locale. I gruppi di utenti locali contengono utenti locali e clonati.

È possibile clonare qualsiasi gruppo di utenti definito in un server LDAP esterno. Il gruppo di utenti LDAP clonato è denominato `{domain}\{groupName}` nel repository locale. Questo gruppo di utenti clonato può essere utilizzato solo per autorizzare l'accesso alle risorse. Le modifiche apportate al nome del gruppo, alla descrizione e all'appartenenza devono essere eseguite tramite LDAP.

Prima che un utente LDAP esterno possa accedere a XClarity Orchestrator, l'utente deve essere un membro diretto di un gruppo di utenti LDAP clonato in XClarity Orchestrator.

Se la configurazione del server LDAP è impostata per utilizzare le credenziali di login e si è eseguito il login a XClarity Orchestrator con un ID utente locale per XClarity Orchestrator, verrà chiesto di fornire credenziali utente LDAP quando si clona un gruppo di utenti LDAP. In tutti gli altri casi, le credenziali non sono richieste.

Informazioni su questa attività

XClarity Orchestrator fornisce i seguenti gruppi predefiniti di utenti, uno per ogni ruolo predefinito. Per maggiori informazioni sui ruoli, vedere [Controllo dell'accesso alle funzioni](#).

- **Gruppo supervisore.** Gli utenti in questo gruppo di utenti vengono assegnati al ruolo di **Supervisore**.
- **Gruppo amministratori hardware.** Gli utenti in questo gruppo di utenti vengono assegnati al ruolo di **Amministratore hardware**.
- **Gruppo amministratori della sicurezza.** Gli utenti in questo gruppo di utenti vengono assegnati al ruolo di **Amministratore della sicurezza**.
- **Gruppo reporter.** Gli utenti in questo gruppo di utenti vengono assegnati al ruolo di **Reporter**.
- **Gruppo amministratori degli aggiornamenti.** Gli utenti in questo gruppo di utenti vengono assegnati al ruolo di **Amministratore degli aggiornamenti**.
- **Gruppo operatore.** Gli utenti in questo gruppo di utenti vengono assegnati al ruolo di **Operatore**.
- **Gruppo legacy operatore.** Gli utenti in questo gruppo di utenti vengono assegnati al ruolo di **Legacy operatore**. Tenere presente che questo gruppo di utenti verrà deprecato in una versione successiva.

Almeno un utente deve essere membro di un gruppo di utenti *locale* a cui è assegnato il ruolo predefinito di **Supervisore** (vedere [Controllo dell'accesso alle funzioni](#)).

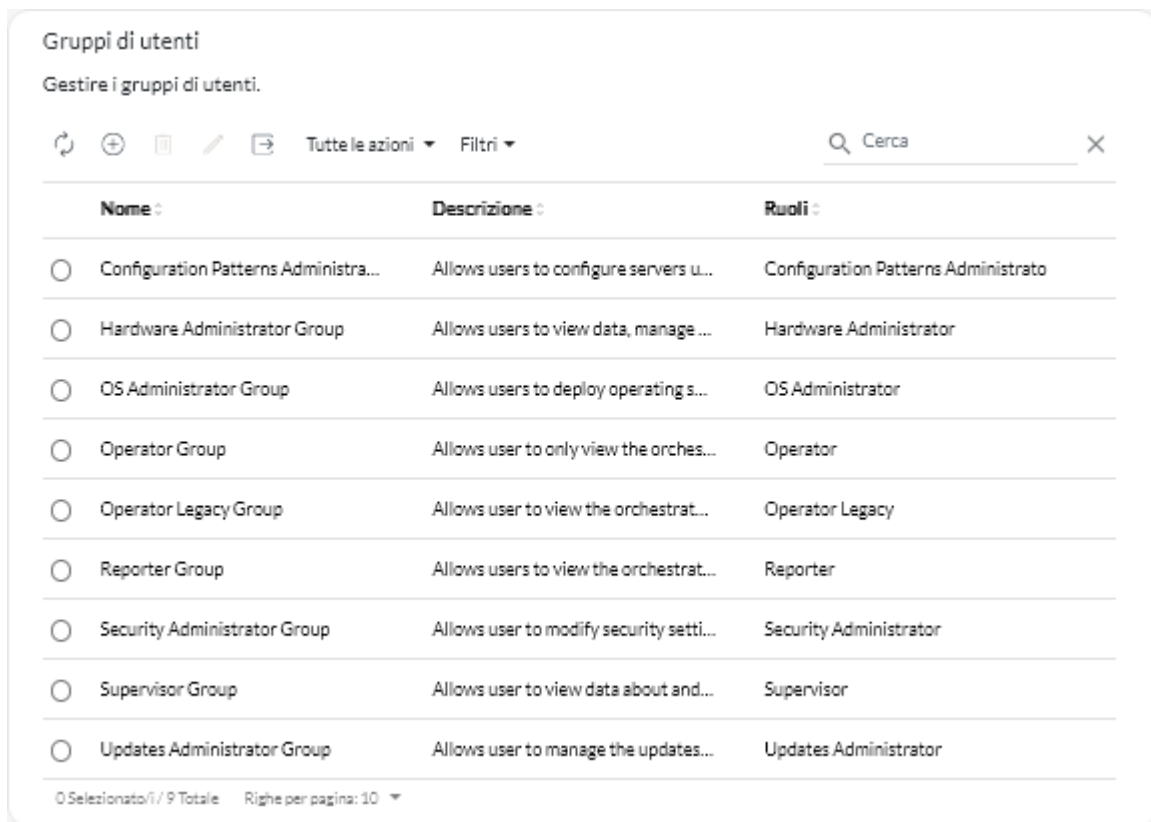
Prima che un utente LDAP esterno possa accedere a XClarity Orchestrator, l'utente deve essere un membro diretto di un gruppo di utenti LDAP clonato in XClarity Orchestrator. XClarity Orchestrator non riconosce gli utenti membri di gruppi di utenti nidificati nel gruppo di utenti LDAP clonato, definito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

Procedura

Per creare un gruppo di utenti, effettuare le seguenti operazioni.

- **Creare un gruppo di utenti locali**

1. Sulla barra dei menu di XClarity Orchestrator fare clic su **Amministrazione** (⚙️) → **Sicurezza** e selezionare **Gruppi di utenti** nel riquadro di navigazione sinistro per visualizzare la scheda Gruppi di utenti.



2. Fare clic sull'icona **Crea** (+) per visualizzare la finestra di dialogo Crea gruppo.
3. Selezionare **Gruppo utenti locali** come tipo di gruppo.
4. Specificare il nome e la descrizione facoltativa per questo gruppo di utenti.
5. Fare clic sulla scheda **Utenti disponibili** e selezionare gli utenti che si desidera includere in questo gruppo di utenti.
6. Fare clic sulla scheda **Ruoli** e selezionare i ruoli che si desidera assegnare in questo gruppo di utenti. Se non viene selezionato alcun ruolo, per impostazione predefinita, viene assegnato il ruolo **Operatore**.
7. Fare clic su **Crea**.

- **Clonare un gruppo di utenti da un server LDAP esterno**

1. Dalla barra dei menu di XClarity Orchestrator, fare clic su **Amministrazione** (⚙️) → **Sicurezza**, quindi selezionare **Gruppi di utenti** nel riquadro di navigazione sinistro per visualizzare la scheda Gruppi di utenti.
2. Fare clic sull'icona **Crea** (+) per visualizzare la finestra di dialogo Crea gruppo.
3. Selezionare **Gruppo di utenti LDAP** come tipo di gruppo.
4. Facoltativamente specificare una descrizione per il gruppo.
5. Selezionare la configurazione LDAP per il server LDAP esterno che contiene il gruppo di utenti che si desidera aggiungere.

Suggerimento: Iniziare a digitare per trovare tutti i nomi del gruppo che contengono la parola chiave specificata

6. Se il server LDAP esterno viene configurato utilizzando credenziali di login, specificare il nome utente e la password per eseguire il login al server LDAP esterno.
7. Specificare una stringa di ricerca (con almeno tre caratteri) nel campo **Gruppo di ricerca** e fare clic su **Cerca** per individuare i gruppi di utenti nel server LDAP esterno corrispondenti alla stringa di ricerca. Selezionare quindi il gruppo che si desidera aggiungere.
8. Fare clic sulla scheda **Ruoli** e selezionare i ruoli che si desidera assegnare in questo gruppo di utenti. Se non viene selezionato alcun ruolo, per impostazione predefinita, viene assegnato il ruolo **Operatore**.
9. Fare clic su **Crea**.

Al termine

Nella scheda Gruppi di utenti è possibile effettuare le operazioni che seguono.

- Modificare le proprietà, l'appartenenza locale e i ruoli di un gruppo di utenti selezionato facendo clic sull'icona **Modifica** (✎).
- Quando si aggiunge o si rimuove un utente da un gruppo, l'utente viene automaticamente disconnesso se i ruoli (autorizzazioni) vengono modificati dopo la nuova assegnazione dei gruppi. Quando accede nuovamente, l'utente può eseguire le azioni in base ai ruoli aggregati dei gruppi di utenti assegnati.
- Ogni utente deve essere membro di almeno un gruppo di utenti. Se si imposta questo attributo su un array vuoto o nullo, **OperatorGroup** viene assegnato per impostazione predefinita.
- Per i gruppi di utenti predefiniti è possibile modificare solo l'appartenenza del gruppo.
- Per il gruppo di utenti LDAP è possibile modificare solo la descrizione e i ruoli. Utilizzare il server LDAP esterno per modificare altre proprietà e appartenenza.
- Eliminare un gruppo di utenti selezionato facendo clic sull'icona **Elimina** (🗑️).

Nota: Non è possibile eliminare i gruppi di utenti predefiniti.

- Visualizzare i membri di un gruppo di utenti facendo clic sul nome del gruppo per visualizzare la finestra di dialogo Visualizza gruppo, quindi sulla scheda **Riepilogo membri**.

Modifica dei dettagli per l'account utente


È possibile modificare la password, il nome completo, l'e-mail e il numero di telefono per l'account utente.

Informazioni su questa attività

Per impostazione predefinita, le password utente scadono dopo **0** giorni.

Procedura

Per modificare la password e altri attributi, completare le seguenti operazioni.

Passo 1. Sulla barra del titolo di XClarity Orchestrator fare clic sul menu **Account utente**  nell'angolo superiore destro, quindi su **Modifica password**. Viene visualizzata la finestra di dialogo Modifica password.

Passo 2. Immettere la password corrente.

Passo 3. Immettere e confermare le nuove password. Per impostazione predefinita, le password devono contenere da **8** a **256** caratteri e devono soddisfare i criteri che seguono.

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

Passo 4. Modificare il nome completo, l'indirizzo e-mail e il numero di telefono, se necessario.

Passo 5. Fare clic su **Modifica**.

Modifica dei dettagli per un altro utente

Gli utenti supervisore possono modificare i dettagli, come la password per un altro utente.


Informazioni su questa attività

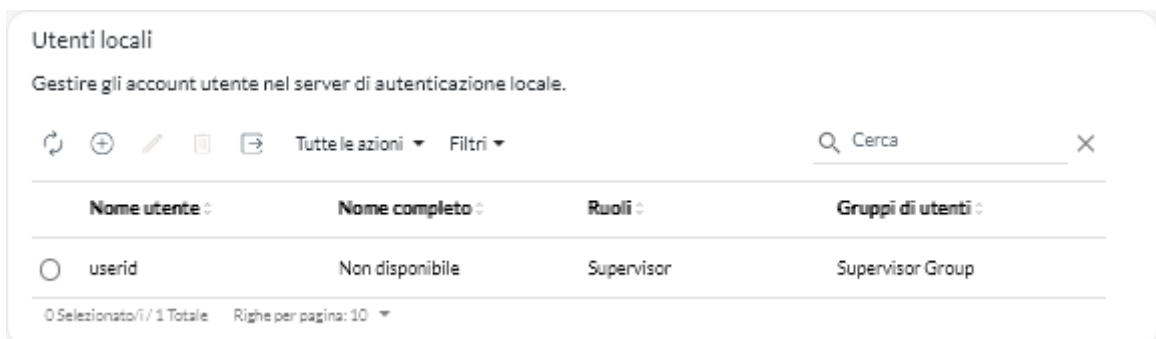
Per impostazione predefinita, le password utente scadono dopo **0** giorni.

È possibile configurare la data di scadenza della password e anche le regole di complessità della password (vedere [Configurazione delle impostazioni di sicurezza utente](#)).

Procedura


Per creare un utente locale, effettuare le seguenti operazioni.

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



Nome utente	Nome completo	Ruoli	Gruppi di utenti
userid	Non disponibile	Supervisor	Supervisor Group

Passo 2. Selezionare l'account utente.

Passo 3. Fare clic sull'icona **Modifica** () per modificare le proprietà dell'utente. Viene visualizzata la finestra di dialogo Modifica utente.

Passo 4. Immettere e confermare le nuove password. Per impostazione predefinita, le password devono contenere da **8 a 256** caratteri e devono soddisfare i criteri che seguono.

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

Passo 5. Fare clic su **Modifica**.


Configurazione delle impostazioni di sicurezza utente

Le impostazioni di sicurezza dell'account utente configurano le impostazioni di password, login e sessione utente per gli utenti locali.

Ulteriori informazioni:  [Come configurare le impostazioni di sicurezza utente](#)

Procedura

Per configurare le impostazioni di sicurezza per gli utenti locali, completare le seguenti operazioni.

Passo 1. Sulla barra dei menu di XClarity Orchestrator fare clic su **Amministrazione** () → **Sicurezza**, quindi su **Impostazioni di sicurezza dell'account** nel riquadro di navigazione sinistro per visualizzare la scheda Impostazioni di sicurezza dell'account.

Passo 2. Configurare le seguenti impostazioni di sicurezza.

Impostazioni di sicurezza	Descrizione	Valori consentiti	Valori predefiniti
Periodo di scadenza password	L'intervallo di tempo (espresso in giorni) durante il quale un utente può utilizzare una password prima che sia tenuto a modificarla. Valori più piccoli riducono il periodo di tempo in cui gli utenti malintenzionati possono tentare di indovinare le password. Se impostata su 0, le password non scadranno.	0 – 365	0
Periodo di avviso scadenza password	L'intervallo di tempo (espresso in giorni) precedente alla data di scadenza della password durante il quale gli utenti ricevono avvisi relativi a un'imminente scadenza della password. Se il valore è impostato su 0, gli utenti non riceveranno avvisi.	0 – 30	0
Ciclo minimo di riutilizzo password	Il numero minimo di volte che è necessario specificare una password univoca durante la modifica della password, prima che l'utente possa iniziare a utilizzare nuovamente le password. Se il valore è impostato su 0, gli utenti possono riutilizzare le password immediatamente.	0 – 10	5
Intervallo minimo di modifica password	L'intervallo di tempo minimo (espresso in ore) che deve trascorrere prima che un utente possa modificare nuovamente una password già modificata in precedenza. Il valore specificato per questa impostazione non può superare il valore specificato per l'impostazione Periodo di scadenza password . Se impostato su 0, gli utenti possono modificare le password immediatamente.	0 – 240	1
Numero massimo di errori di login	Il numero massimo di volte che un utente può tentare di accedere con una password non corretta prima che l'account utente venga bloccato. Nota: I tentativi di login consecutivi con gli stessi nome utente e password vengono considerati come un singolo login non riuscito. Se impostata su 0, gli account non vengono bloccati.	0 – 10	5

Impostazioni di sicurezza	Descrizione	Valori consentiti	Valori predefiniti
Reimpostazione del contatore di login non riuscita	<p>L'intervallo di tempo trascorso dall'ultimo tentativo di login non riuscito prima che il contatore Numero massimo di errori di login venga reimpostato su 0.</p> <p>Se impostato su 0, il contatore non verrà mai reimpostato. Ad esempio, se il numero massimo di errori di login è 2 e, dopo aver fallito una prima volta, si fallisce una seconda volta 24 ore più tardi, il sistema registra i due tentativi di login falliti e l'account viene bloccato.</p> <p>Nota: questa impostazione viene applicata solo quando l'impostazione Numero massimo di errori di login è impostata su 1 o su un valore superiore.</p>	0 – 60	15
Periodo di blocco in seguito al numero massimo di errori di login	<p>L'intervallo minimo di tempo (espresso in minuti) trascorso il quale un utente bloccato può provare nuovamente a eseguire il login. Un account utente bloccato non può essere utilizzato per accedere a XClarity Orchestrator, anche se viene immessa una password valida.</p> <p>Se impostati su 0, gli account utente non vengono mai bloccati.</p> <p>Nota: questa impostazione viene applicata solo quando l'impostazione Numero massimo di errori di login è impostata su 1 o su un valore superiore.</p>	0 – 2880	60

Impostazioni di sicurezza	Descrizione	Valori consentiti	Valori predefiniti
Timeout sessione di inattività Web	<p>Il periodo di tempo, in minuti, in cui una sessione utente stabilita con il server Orchestrator può restare inattiva, prima che la sessione utente scada e che l'utente venga disconnesso automaticamente. Questo timeout si applica a tutte le azioni (ad esempio, l'apertura di una pagina, l'aggiornamento della pagina corrente o la modifica dei dati). Questo è il timeout principale per la sessione utente.</p> <p>Quando una sessione è attiva, questo timer viene reimpostato ogni volta che l'utente esegue qualsiasi azione. Una volta superato il valore di timeout, viene visualizzata la pagina di login al successivo tentativo dell'utente di eseguire un'azione.</p> <p>Se il valore è impostato su 0, questo timeout è disabilitato.</p> <p>Nota: La modifica di questa impostazione ha effetto immediato su tutte le sessioni utente, indipendentemente dal tipo di autenticazione. Le sessioni esistenti che sono state inattive per un periodo di tempo superiore al nuovo valore di timeout scadono.</p>	0, 60 – 1440	1440
Timeout di inattività Web per le operazioni complete	<p>Il periodo di tempo, in minuti, in cui una sessione utente stabilita con il server Orchestrator può essere inattiva, prima che le azioni che modificano i dati (ad esempio creazione, aggiornamento o eliminazione di una risorsa) vengano disabilitate. Si tratta di un timeout secondario facoltativo ed è inferiore al valore primario Timeout sessione di inattività Web.</p> <p>Quando una sessione è attiva, questo timer viene reimpostato ogni volta che l'utente esegue qualsiasi azione. Se questo valore di timeout viene superato ma il valore primario Timeout sessione di inattività Web non viene superato, l'utente è limitato ad azioni di sola lettura (ad esempio, apertura o aggiornamento di una pagina) finché non viene superato il valore Timeout sessione di inattività Web. Tuttavia se l'utente tenta di eseguire un'azione che modifica i dati, la sessione utente scade e viene visualizzata la pagina di login.</p> <p>Se il valore è impostato su 0, questo timeout è disabilitato.</p> <p>Nota: La modifica di questa impostazione ha effetto immediato su tutte le sessioni</p>	0, 15 – 60	30

Impostazioni di sicurezza	Descrizione	Valori consentiti	Valori predefiniti
	utente, indipendentemente dal tipo di autenticazione. Le sessioni esistenti che sono state inattive per un periodo di tempo superiore al nuovo valore di timeout scadono.		
Tempo di scadenza obbligatorio di una sessione Web	Il periodo di tempo, in ore, in cui una sessione utente stabilita con il server Orchestrator può restare aperta prima che l'utente venga disconnesso automaticamente, a prescindere dall'attività. Nota: La modifica di questa impostazione ha effetto immediato su tutte le sessioni utente, indipendentemente dal tipo di autenticazione. Le sessioni esistenti che sono state inattive per un periodo di tempo superiore al nuovo valore di timeout scadono.	24 – 240	24
Lunghezza minima password	Il numero minimo di caratteri che possono essere utilizzati per specificare una password valida.	8 – 256	256
Lunghezza massima password	Il numero massimo di caratteri che è possibile utilizzare per specificare una password valida.	8 – 128	128
Numero massimo di sessioni attive per un utente specifico	Il numero massimo di sessioni attive per un utente specifico consentito in un determinato momento. Quando viene raggiunto il numero massimo, la sessione attiva meno recente per un utente (in base al timestamp di creazione) viene eliminata prima di creare una nuova sessione per l'utente. Se il valore è impostato su 0, il numero di sessioni attive consentito per un utente specifico è illimitato. Nota: riguarda solo le sessioni utente avviate dopo avere modificato l'impostazione.	0 – 20	20

Impostazioni di sicurezza	Descrizione	Valori consentiti	Valori predefiniti
Numero di regole di complessità che devono essere seguite durante la creazione di una nuova password.	<p>Numero di regole di complessità che devono essere seguite durante la creazione di una nuova password.</p> <p>Le regole vengono applicate a partire dalla regola 1 e fino al numero di regole specificato. Ad esempio, se la complessità della password è impostata su 4, è necessario seguire le regole 1, 2, 3 e 4. Se la complessità della password è impostata su 2, è necessario seguire le regole 1 e 2.</p> <p>XClarity Orchestrator supporta le seguenti regole di complessità della password.</p> <ul style="list-style-type: none"> • Deve contenere almeno un carattere alfabetico e non deve avere più di due caratteri sequenziali, tra cui sequenze di caratteri alfabetici, cifre e tasti della tastiera QWERTY (ad esempio, "abc", "123" e "asd" non sono consentiti) • Deve contenere almeno un numero • Deve contenere almeno due dei caratteri che seguono: <ul style="list-style-type: none"> – Caratteri alfabetici maiuscoli (A - Z) – Caratteri alfabetici minuscoli (a - z) – Caratteri speciali ; @ _ ! ' \$ & + Gli spazi non sono consentiti. • Non deve essere una ripetizione o l'inversione del nome utente. • Non deve contenere consecutivamente più di due degli stessi caratteri (ad esempio, "aaa", "111" e "...") non sono ammessi). <p>Se impostate su 0, le password non sono necessarie per conformarsi alle regole di complessità.</p>	0 – 5	4
Forza utente a modificare la password al primo accesso	Indica se un utente deve modificare la password quando esegue per la prima volta il login a XClarity Orchestrator	Sì o No	Sì

Passo 3. Fare clic su **Applica**.

Una volta applicate le modifiche, le nuove impostazioni hanno effetto immediato. I criteri di modifica delle password vengono applicati al successivo login o alla successiva modifica della password da parte dell'utente.

Al termine

Nella scheda Impostazioni di sicurezza dell'account è possibile effettuare l'operazione che segue.

- Per ripristinare i valori predefiniti di queste impostazioni, fare clic su **Ripristina valori predefiniti**.

Monitoraggio delle sessioni utente attive

È possibile determinare chi ha effettuato il login all'interfaccia Web di XClarity Orchestrator.

Prima di iniziare

Per impostazione predefinita, le sessioni utente inattive per più di 24 ore vengono automaticamente disconnesse. È possibile configurare il timeout della sessione di inattività Web (vedere [Configurazione delle impostazioni di sicurezza utente](#)).

Procedura

Per visualizzare un elenco di tutte le sessioni utente attive (inclusa quella corrente), fare clic su **Amministrazione** (🔧) → **Sicurezza** sulla barra dei menu di XClarity Orchestrator, quindi su **Sessioni attive** nel riquadro di navigazione per visualizzare la scheda Sessioni attive.

Nome utente	Indirizzo IP	Ultimo accesso
userid	Non disponibile	04/10/22, 03:36
userid	Non disponibile	04/10/22, 13:32

Al termine

Nella scheda Sessioni attive è possibile effettuare l'operazione che segue.

- Per disconnettere una sessione utente selezionata, fare clic sull'icona **Elimina** (🗑️).

Nota: Non è possibile disconnettere la sessione corrente.

Controllo dell'accesso alle funzioni

Lenovo XClarity Orchestrator utilizza *ruoli* e *gruppi di utenti* per determinare le funzioni (azioni) che un utente può eseguire.

Informazioni su questa attività

Un *ruolo* è una serie di funzioni. Quando un ruolo è assegnato a un gruppo di utenti, tutti gli utenti del gruppo possono eseguire le funzioni incluse in questo ruolo.

XClarity Orchestrator fornisce i seguenti ruoli predefiniti.

- **Supervisore.** Consente agli utenti di visualizzare i dati e di eseguire tutte le azioni disponibili sul server Orchestrator e su tutte le risorse gestite (strumenti di gestione delle risorse e dispositivi). Gli utenti assegnati a questo ruolo hanno sempre accesso a tutte le risorse (dispositivi e strumenti di gestione delle risorse) e a tutte le funzioni. Non è possibile limitare l'accesso a risorse o funzioni per questo ruolo.

È necessario disporre dei privilegi di supervisore per eseguire le azioni seguenti.

- Riavviare il server Orchestrator
- Eseguire attività di manutenzione, come installazione delle licenze e aggiornamento a una versione più recente
- Connettere e disconnettere gli strumenti di gestione delle risorse
- Modificare le impostazioni di sistema, come preferenze di rete, data e ora
- Accettare l'invio di dati periodici a Lenovo

Deve essere presente almeno un utente con privilegi di supervisore.

Importante: Quando si aggiorna da XClarity Orchestrator v1.0 a una versione successiva, tutti gli utenti creati in XClarity Orchestrator v1.0 vengono forniti dei privilegi di supervisore per impostazione predefinita. Un utente supervisore può rimuovere i privilegi di supervisore per gli utenti che non devono disporre di questi privilegi.

- **Amministratore hardware.** Consente agli utenti di visualizzare i dati, di gestire e distribuire pattern di configurazione, di gestire e distribuire i sistemi operativi utilizzando i profili del sistema operativo, di visualizzare e personalizzare le informazioni personali e di eseguire azioni sulle risorse accessibili. Questo ruolo impedisce agli utenti di aggiornare software o firmware sulle risorse gestite e di gestire i gruppi di risorse.
- **Amministratore di configurazione server.** Consente agli utenti di configurare i server tramite i pattern di configurazione, di visualizzare le analisi predefinite e di visualizzare i dati per le risorse accessibili. Questo ruolo impedisce agli utenti di accedere in remoto ai dispositivi e di accendere e spegnere i dispositivi.
- **Amministratore sistema operativo.** Consente agli utenti di distribuire i sistemi operativi mediante i profili del sistema operativo, di visualizzare le analisi predefinite e di visualizzare i dati per le risorse accessibili. Questo ruolo impedisce agli utenti di accedere in remoto ai dispositivi e di accendere e spegnere i dispositivi.
- **Amministratore degli aggiornamenti.** Consente agli utenti di aggiornare il firmware sui dispositivi e il software degli strumenti di gestione delle risorse, di visualizzare i dati per le risorse accessibili e di visualizzare le informazioni personali predefinite.
- **Amministratore della sicurezza.** Consente agli utenti di modificare le impostazioni di sicurezza e di eseguire le azioni correlate alla sicurezza sul server Orchestrator, di visualizzare i dati per tutte le risorse gestite, di gestire il gruppo di risorse e di visualizzare le analisi predefinite. Gli utenti assegnati a questo ruolo hanno sempre accesso a tutte le risorse (dispositivi e strumenti di gestione delle risorse). Non è possibile limitare l'accesso alle risorse per questo ruolo.
- **Reporter.** Consente agli utenti di visualizzare la configurazione del server Orchestrator, di visualizzare i dati relativi alle risorse accessibili, di creare query per generare report personalizzati e di creare server d'invio dei dati per pianificare e inviare i report via e-mail. Questo ruolo impedisce agli utenti di eseguire il provisioning delle risorse e di accendere e spegnere i dispositivi.
- **Operatore.** Consente agli utenti di visualizzare la configurazione del server Orchestrator e i dati per le risorse accessibili. Questo ruolo impedisce agli utenti di eseguire azioni o di modificare le impostazioni delle configurazioni sul server Orchestrator e le risorse gestite, di creare e visualizzare report di analisi e di creare avvisi personalizzati.
- **Legacy operatore.** Consente agli utenti di visualizzare i dati e di eseguire determinate azioni sulle risorse accessibili, come la gestione dell'inventario, degli avvisi e dei ticket di servizio. Questo ruolo impedisce agli utenti di aggiornare il software o il firmware delle risorse gestite, di creare gruppi di risorse, di creare e visualizzare report di analisi e di creare avvisi personalizzati.

Attenzione: Quando si esegue l'aggiornamento da XClarity Orchestrator v1.2 a una versione successiva, agli utenti con ruolo **Operatore** viene automaticamente assegnato il ruolo **Legacy operatore**. Gli utenti vengono inoltre aggiunti al gruppo di utenti **OperatorLegacyGroup**. Il ruolo **Legacy operatore** e il gruppo di utenti **OperatorLegacyGroup** verranno deprecati in una versione successiva.

Se un utente non è autorizzato a eseguire azioni specifiche, le voci di menu, le icone della barra degli strumenti e i pulsanti utilizzati per eseguire queste azioni saranno disabilitati (evidenziati in grigio).

Nota: La visualizzazione dei dati relativi alle risorse non è limitata in base ai ruoli. Tutti gli utenti possono visualizzare i dati relativi alle risorse (ad esempio inventario, avvisi, processi e ticket di assistenza) delle risorse a cui possono accedere.

Procedura

Per visualizzare le informazioni sui ruoli predefiniti, fare clic su **Amministrazione** (🔗) → **Sicurezza** dalla barra dei menu di XClarity Orchestrator, quindi selezionare **Ruoli** nel riquadro di navigazione sinistro.

Fare clic sulla riga di un qualsiasi ruolo per visualizzare la finestra di dialogo Ruoli con informazioni sulle proprietà del ruolo, l'elenco delle funzioni nel ruolo e un elenco di gruppi di utenti a cui è assegnato il ruolo.

Assegnazione dei ruoli agli utenti

Lenovo XClarity Orchestrator utilizza *ruoli* e *gruppi di utenti* per determinare le funzioni (azioni) che un utente può eseguire.

Prima di iniziare

Quando i ruoli vengono modificati per un utente che attualmente ha eseguito il login a una sessione attiva, la sessione dell'utente viene terminata automaticamente e l'utente viene disconnesso dall'interfaccia utente. Quando l'utente accede nuovamente può eseguire le funzioni in base alle nuove assegnazioni del ruolo.

Informazioni su questa attività

Quando si assegnano più ruoli a un gruppo di utenti, le funzioni in ciascun ruolo vengono aggregate.

Tutti gli utenti membri di un gruppo di utenti possono eseguire le funzioni incluse nei ruoli assegnati a questo gruppo di utenti.

È possibile modificare i ruoli di un utente:

- Aggiungendo o rimuovendo l'utente da un gruppo di utenti
- Aggiungendo o rimuovendo i ruoli da un gruppo di utenti di cui l'utente è membro
- Eliminando un gruppo di utenti di cui l'utente è membro

Nota:

- Quando gli utenti LDAP vengono aggiunti o rimossi dai gruppi di utenti LDAP sul server LDAP, le modifiche delle associazioni tra l'utente LDAP e il gruppo di utenti LDAP vengono automaticamente aggiornate in XClarity Orchestrator in base ai gruppi di utenti LDAP clonati esistenti.
- Quando i ruoli assegnati a un gruppo di utenti cambiano, l'utente deve eseguire nuovamente il login per rendere effettive le modifiche dei ruoli.

Controllo dell'accesso alle risorse

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

Informazioni su questa attività

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

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

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

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

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

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

Procedura

Completare le seguenti operazioni per controllare l'accesso alle risorse.

Passo 1. Creare un gruppo di utenti che può accedere alle risorse.

Passo 2. Creare uno o più gruppi di risorse per cui si desidera controllare l'accesso.

Passo 3. Creare un elenco di controllo degli accessi che contenga il gruppo di utenti e uno o più gruppi di risorse.

Passo 4. Abilitare il controllo accessi basato sulle risorse.

Abilitazione dell'accesso basato sulle risorse

Se si desidera limitare le risorse a cui gli utenti possono accedere, abilitare l'accesso basato sulle risorse.

Informazioni su questa attività


Gli utenti che sono membri di un gruppo a cui è assegnato il ruolo predefinito di **Supervisore** hanno sempre accesso a tutte le risorse. Non è possibile limitare l'accesso alla risorsa per gli utenti supervisore.

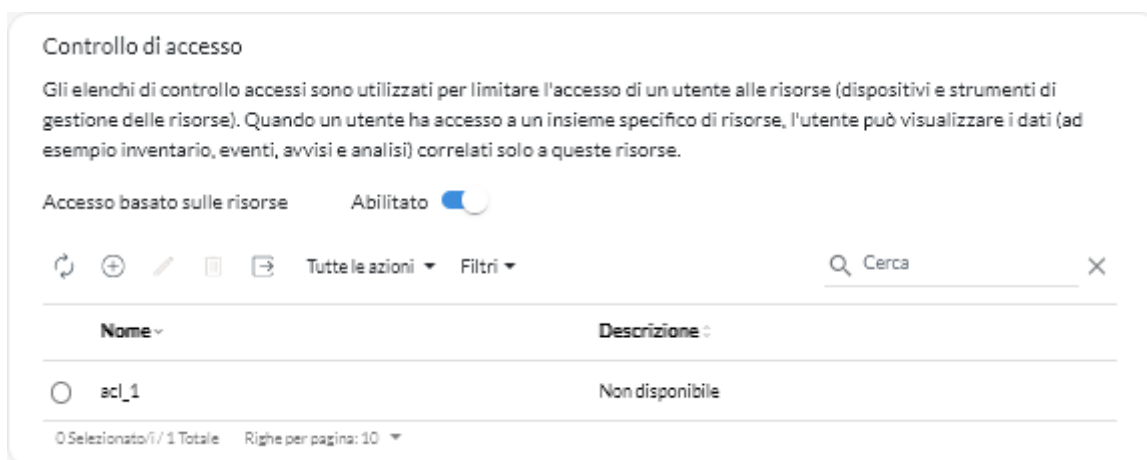
Quando è abilitato l'accesso basato sulle risorse, gli utenti che *non sono* membri di un gruppo a cui è assegnato il ruolo predefinito di **Supervisore** non hanno accesso ad alcuna risorsa (dispositivi e strumenti di gestione delle risorse) per impostazione predefinita. È necessario aggiungere gli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

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

Procedura

Completare le seguenti operazioni per abilitare i controlli degli accessi basati sulle risorse.

Passo 1. Dalla barra dei menu di XClarity Orchestrator fare clic su **Amministrazione**  → **Sicurezza**, quindi su **Controlli degli accessi** nel riquadro di navigazione sinistro per visualizzare la scheda Controlli degli accessi.



Passo 2. Fare clic sull'interruttore **Accesso basato sulle risorse** per abilitare il controllo degli accessi alle risorse mediante gli elenchi di controllo degli accessi.

Creazione degli elenchi di controllo degli accessi

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

Prima di iniziare

Ulteriori informazioni:  [Come creare gli elenchi di controllo degli accessi](#)

Accertarsi di aver definito i gruppi di utenti che si desidera associare all'elenco di controllo degli accessi (vedere [Creazione di gruppi di utenti](#)).

Accertarsi di aver definito tutti i gruppi di risorse che si desidera associare a questo elenco di controllo degli accessi (vedere [Creazione dei gruppi di risorse](#)).

Informazioni su questa attività

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

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

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


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

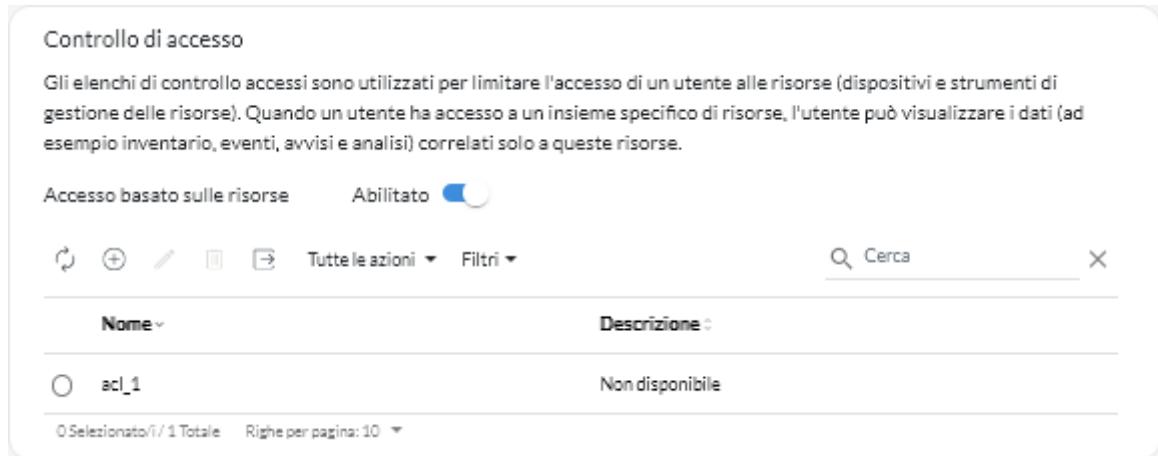
- I *gruppi di risorse* identificano le risorse (dispositivi, strumenti di gestione delle risorse e XClarity Orchestrator) a cui è possibile accedere. L'elenco di controllo degli accessi deve contenere almeno un gruppo di risorse.


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

Procedura

Completare le seguenti operazioni per creare un elenco di controllo degli accessi.

Passo 1. Dalla barra dei menu di XClarity Orchestrator fare clic su **Amministrazione**  → **Sicurezza**, quindi su **Controlli degli accessi** nel riquadro di navigazione sinistro per visualizzare la scheda Controlli degli accessi.



Passo 2. Fare clic sull'icona **Aggiungi**  per aggiungere un elenco di controllo degli accessi. Viene visualizzata la finestra di dialogo Crea controllo accessi.

Passo 3. Specificare il nome e la descrizione facoltativa dell'elenco di controllo degli accessi.

Passo 4. Fare clic su **Gruppo di utenti** e selezionare il gruppo di utenti che si desidera includere in questo elenco di controllo degli accessi.



Passo 5. Fare clic su **Gruppi di risorse** e selezionare i gruppi di risorse che si desidera includere in questo elenco di controllo degli accessi.

Passo 6. Fare clic su **Crea**.

L'elenco di controllo degli accessi viene aggiunto alla tabella.

Al termine

Da questa pagina, è possibile eseguire le seguenti azioni.

- Visualizzare il gruppo di utenti e i gruppi di risorse in un elenco di controllo degli accessi specifico, facendo clic in un punto qualsiasi nella riga dell'elenco di controllo degli accessi.
- Modificare le proprietà e l'appartenenza di un elenco di controllo degli accessi selezionato facendo clic sull'icona **Modifica** .
- Eliminare un elenco di controllo degli accessi selezionato facendo clic sull'icona **Elimina** .
- Se un utente non può accedere ai dati per una risorsa specifica o può accedere ai dati per una risorsa specifica a cui non dovrebbe essere possibile accedere, identificare gli elenchi di controllo degli accessi associati all'utente e quindi visualizzare l'appartenenza di ciascun gruppo di risorse associato anche a questi elenchi di controllo degli accessi. Verificare che la risorsa in questione sia o non sia inclusa in questi gruppi di risorse.

Gestione dello spazio su disco

È possibile gestire la quantità di spazio su disco utilizzato da Lenovo XClarity Orchestrator eliminando le risorse che non sono più necessarie.

Informazioni su questa attività

Procedura

Completare una o più delle seguenti procedure per eliminare i file non necessari.

File di dati di servizio del dispositivo

1. Sulla barra dei menu di Lenovo XClarity Orchestrator fare clic su **Amministrazione** (🔧) → **Assistenza e supporto** e selezionare la scheda **Dati di servizio** per visualizzare la scheda Dati di servizio dispositivo.
2. Selezionare uno o più file di dati di servizio da eliminare e fare clic sull'icona **Elimina** (🗑️).

Immagini del sistema operativo

1. Sulla barra dei menu di Lenovo XClarity Orchestrator fare clic su **Amministrazione** (🔧) → **Distribuzione sistema operativo** e selezionare **Gestione sistema operativo** per visualizzare la scheda Immagini sistema operativo.
2. Selezionare una o più immagini del sistema operativo da eliminare e fare clic sull'icona **Elimina** (🗑️).

Aggiornamento dei file payload

Verificare che gli aggiornamenti non vengano utilizzati nei criteri di conformità degli aggiornamenti. È possibile rimuovere un aggiornamento da un criterio dalla scheda Applica e attiva (vedere [Creazione e assegnazione di criteri di conformità degli aggiornamenti](#)).

1. Dalla barra dei menu di XClarity Orchestrator, fare clic su **Provisioning** (🔧) → **Aggiornamenti**, quindi selezionare la scheda **Gestione repository** per visualizzare la scheda Gestione repository.
2. Selezionare uno o più file o pacchetti di aggiornamento da eliminare.
3. Fare clic sull'icona **Elimina solo file payload** (🗑️) per eliminare solo il file immagine (payload) per ogni aggiornamento selezionato. Le informazioni sull'aggiornamento (il file di metadati XML) restano nel repository e lo stato del download viene modificato in "Non scaricato".

Aggiornamenti di XClarity Orchestrator

È possibile eliminare gli aggiornamenti del server Orchestrator con stato Scaricato. La colonna **Stato applicato** nella tabella indica lo stato dell'aggiornamento.

1. Dalla barra dei menu di XClarity Orchestrator, fare clic su **Manutenzione** (🔧), quindi selezionare la scheda **Aggiornamento del server Orchestrator** per visualizzare la scheda Aggiornamento del server Orchestrator.
2. Selezionare uno o più aggiornamenti da eliminare e fare clic sull'icona **Elimina** (🗑️). La colonna **Stato acquisito** degli aggiornamenti eliminati viene modificata in "Non scaricato".

Riavvio di XClarity Orchestrator

In alcuni casi, potrebbe essere necessario riavviare Lenovo XClarity Orchestrator, ad esempio quando si rigenera o si carica un certificato server. È possibile riavviare Lenovo XClarity Orchestrator dall'interfaccia Web.

Prima di iniziare

È necessario disporre dell'autorità **Supervisore** per riavviare XClarity Orchestrator.

Valutare la possibilità di eseguire il backup del server Orchestrator prima di riavviare il sistema (vedere [Backup e ripristino dei dati del server Orchestrator](#)).

Verificare che non ci siano processi in esecuzione. I processi in esecuzione verranno annullati durante il riavvio. Per visualizzare il log processi, vedere [Monitoraggio dei processi](#).

Durante l'operazione di riavvio, i processi vengono arrestati, tutti gli utenti vengono disconnessi e la connettività al server Orchestrator viene persa. Attendere almeno 15 minuti (a seconda del numero di dispositivi gestiti) per il riavvio del server Orchestrator, prima di eseguire nuovamente l'accesso ([Login a XClarity Orchestrator](#)).

Una volta riavviato, XClarity Orchestrator raccoglie nuovamente l'inventario per ogni dispositivo gestito. Attendere circa 30-45 minuti, a seconda del numero di dispositivi gestiti, prima di provare ad eseguire gli aggiornamenti firmware, le distribuzioni dei pattern di configurazione o le distribuzioni del sistema operativo.

Procedura

Per riavviare XClarity Orchestrator completare una delle seguenti procedure.

Dall'interfaccia utente

1. Dalla barra dei menu di XClarity Orchestrator, fare clic su **Manutenzione → Riavvio appliance**.
2. Fare clic su **Riavvia**.
3. Fare clic su **Sì**.
4. Aggiornare il browser.

Dall'hypervisor

Microsoft Hyper-V

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

VMware ESXi

1. Connettersi all'host tramite VMware vSphere Client.
2. Fare clic con il pulsante destro del mouse sulla macchina virtuale e scegliere **Alimentazione → Reimposta**.
3. Selezionare la scheda **Console**.

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

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

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

=====

You have 118 seconds to change IP settings. Enter one of the following:

1. To set a static IP address for Lenovo XClarity virtual appliance eth0 port
 2. To use a DHCP address for Lenovo XClarity virtual appliance eth0 port
 3. To select subnet for Lenovo XClarity virtual appliance internal network
 - x. To continue without changing IP settings
-

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

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

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

Backup e ripristino dei dati del server Orchestrator

Lenovo XClarity Orchestrator non include funzioni di backup e ripristino integrate. Utilizzare le funzioni di backup disponibili a seconda del sistema operativo host virtuale in cui è installato XClarity Orchestrator.

Informazioni su questa attività

Eseguire sempre il backup di XClarity Orchestrator dopo aver eseguito la configurazione iniziale e dopo aver apportato modifiche significative alla configurazione, incluse le situazioni seguenti:

- Prima di aggiornare XClarity Orchestrator
- Dopo avere apportato eventuali modifiche alla rete
- Dopo avere aggiunto utenti al server di autenticazione locale di XClarity Orchestrator
- Dopo avere gestito nuovi strumenti di gestione delle risorse

Se sono già state implementate procedure di backup e ripristino per gli host virtuali, assicurarsi che tali procedure includano XClarity Orchestrator.

Importante:

- Assicurarsi che tutti i processi in esecuzione siano stati completati e che XClarity Orchestrator sia stato arrestato prima di avviare la creazione di un backup.
- Assicurarsi di eseguire backup regolari di XClarity Orchestrator. Se il sistema operativo host si arresta in modo imprevisto, non è possibile eseguire l'autenticazione con XClarity Orchestrator dopo che tale sistema operativo host sarà stato riavviato. Per risolvere questo problema, ripristinare XClarity Orchestrator dall'ultimo backup.

Backup e ripristino dei dati del server Orchestrator su un host VMware ESXi

Talvolta potrebbe essere necessario ripristinare i dati del server Orchestrator da un backup. Sono disponibili varie opzioni per eseguire e ripristinare un backup di un'appliance virtuale XClarity Orchestrator in esecuzione su un host VMware ESXi. Il processo specifico da utilizzare per eseguire un ripristino da un backup si basa generalmente sul processo utilizzato per creare il backup. In questa sezione viene descritto come eseguire e ripristinare un backup mediante VMware vSphere Client.

Informazioni su questa attività

Se VMware vCenter Server è installato, è possibile utilizzare la funzione di backup inclusa con VMware vCenter per eseguire il backup di XClarity Orchestrator.

Se VMware vCenter Server non è installato, è possibile utilizzare VMware vSphere Client per creare un backup della macchina virtuale copiando i file dalla cartella XClarity Orchestrator a un'altra cartella nello stesso archivio dati. È inoltre possibile copiare i file in un archivio dati differente o perfino in un altro host per un'ulteriore protezione del backup.

Nota: VMware vCenter Server non è richiesto per eseguire un backup con questa procedura.

Procedura

- **Backup di XClarity Orchestrator** Per creare un backup di XClarity Orchestrator mediante VMware vSphere Client, effettuare le operazioni che seguono.

1. Chiudere XClarity Orchestrator.
2. Avviare VMware vSphere Client e collegarsi all'host ESXi su cui si trova XClarity Orchestrator.
3. Creare una nuova cartella nello stesso archivio dati utilizzato da XClarity Orchestrator.
 - a. Selezionare l'host ESXi nella struttura di navigazione e fare clic sulla scheda **Configura** nella finestra a destra.
 - b. Fare clic su **Hardware** → **Storage**.
 - c. Fare clic con il pulsante destro del mouse sull'archivio dati di XClarity Orchestrator e scegliere **Sfogliare archivio dati**.
 - d. Selezionare la cartella radice, quindi creare una nuova cartella in cui conservare una copia dei file di XClarity Orchestrator.
4. Fare clic sulla cartella XClarity Orchestrator.
5. Selezionare tutti i file nella cartella e copiare i file nella cartella di backup appena creata.
6. Riavviare XClarity Orchestrator.

- **Ripristino di XClarity Orchestrator** Per ripristinare XClarity Orchestrator utilizzando il backup creato durante la procedura precedente, effettuare le operazioni che seguono.

1. Avviare VMware vSphere Client e collegarsi all'host ESXi su cui è installato XClarity Orchestrator.
2. Fare clic con il pulsante destro del mouse su XClarity Orchestrator nella struttura di navigazione a sinistra e quindi selezionare **Alimentazione** → **Spegni**.
3. Fare nuovamente clic con il pulsante destro del mouse su XClarity Orchestrator nella struttura di navigazione a sinistra e scegliere **Rimuovi dall'inventario**.
4. Eliminare i file dalla cartella XClarity Orchestrator nell'archivio dati utilizzato da XClarity Orchestrator.
 - a. Selezionare l'host ESXi nella struttura di navigazione e quindi fare clic sulla scheda **Configura** nella finestra a destra.
 - b. Fare clic su **Hardware** → **Storage**.

- c. Fare clic con il pulsante destro del mouse sull'archivio dati di XClarity Orchestrator e scegliere **Sfoggia archivio dati**.
 - d. Selezionare la cartella XClarity Orchestrator.
 - e. Selezionare tutti i file nella cartella, fare clic con il pulsante destro del mouse sui file e scegliere **Elimina elementi selezionati**.
5. Selezionare la cartella in cui sono archiviati i file di backup.
 6. Selezionare tutti i file nella cartella e copiarli nella cartella XClarity Orchestrator.
 7. Nella cartella XClarity Orchestrator fare clic con il pulsante destro del mouse sul file VMX e scegliere **Aggiungi all'inventario**.
 8. Completare la procedura guidata per aggiungere dati di XClarity Orchestrator.
 9. Riavviare XClarity Orchestrator da VMware vSphere Client.
 10. Quando viene richiesto di scegliere se la macchina virtuale è stata spostata o copiata, selezionare **spostata**.

Importante: Se si seleziona **copiata**, alla macchina virtuale viene assegnato un UUID differente da quello della macchina virtuale originale. Questo fa sì che la macchina virtuale funzioni come una nuova istanza e, pertanto, non sia in grado di vedere i dispositivi precedentemente gestiti.

Backup e ripristino dei dati del server Orchestrator su un host Microsoft Hyper-V

Talvolta potrebbe essere necessario ripristinare i dati del server Lenovo XClarity Orchestrator Orchestrator da un backup. Sono disponibili varie opzioni per eseguire e ripristinare un backup di un'appliance virtuale XClarity Orchestrator in esecuzione su un host Microsoft Hyper-V. Il processo specifico da utilizzare per eseguire un ripristino da un backup si basa generalmente sul processo utilizzato per creare il backup. In questa sezione viene descritto come eseguire e ripristinare un backup mediante Windows Server Backup.

Prima di iniziare

Verificare che Windows Server Backup sia configurato correttamente effettuando le operazioni che seguono.

1. Avviare Windows Server Manager.
2. Fare clic su **Gestisci → Aggiungi ruoli e funzioni**.
3. Spostarsi all'interno della procedura guidata fino alla pagina **Seleziona funzioni**.
4. Selezionare la casella di controllo **Windows Server Backup**.
5. Completare la procedura guidata.

Procedura

- **Backup di XClarity Orchestrator** Per creare un backup di XClarity Orchestrator mediante Windows Server Backup, effettuare le operazioni che seguono.
 1. Avviare Windows Server Backup e visualizzare **Backup locale**.
 2. Nel riquadro Azione fare clic su **Backup unico** per avviare la relativa procedura guidata.
 3. Nella pagina Opzioni di backup fare clic su **Opzioni differenti**, quindi su **Avanti**.
 4. Nella pagina Seleziona configurazione di backup fare clic su **Personalizzato**, quindi su **Avanti**.
 5. Nella pagina Seleziona elementi per il backup fare clic su **Aggiungi elementi** per visualizzare la finestra Seleziona elementi.
 6. Espandere l'elemento Hyper-V, fare clic sulla macchina virtuale XClarity Orchestrator, quindi su **OK**.
 7. Fare clic su **Avanti** per continuare.
 8. Nella pagina Specifica tipo di destinazione scegliere il tipo di storage per il backup (un'unità locale o una cartella condivisa remota) e fare clic su **Avanti**.

9. Nella pagina Seleziona destinazione backup o Specifica cartella remota specificare il percorso in cui si desidera archiviare il backup, quindi fare clic su **Avanti**.
 10. Fare clic su **Backup** per avviare il processo di backup.
- **Ripristino di XClarity Orchestrator** Per ripristinare XClarity Orchestrator utilizzando il backup creato durante la procedura precedente, effettuare le operazioni che seguono.
 1. Avviare Windows Server Backup e visualizzare **Backup locale**.
 2. Nel riquadro Azione fare clic su **Ripristina** per avviare la relativa procedura guidata.
 3. Nella pagina Introduzione specificare il percorso in cui è archiviato il backup e fare clic su **Avanti**.
 4. Nella pagina Seleziona data del backup scegliere il backup che si desidera ripristinare e fare clic su **Avanti**.
 5. Nella pagina Seleziona tipo di ripristino selezionare **Opzione Hyper-V** e fare clic su **Avanti**.
 6. Nella pagina Seleziona elementi da ripristinare espandere Hyper-V e selezionare la macchina virtuale XClarity Orchestrator. Quindi, fare clic su **Avanti**.
 7. Nella pagina Specifica opzioni di ripristino scegliere di ripristinare il percorso originale della macchina virtuale e fare clic su **Avanti**.
 8. Nella pagina Conferma fare clic su **Ripristina**. La macchina virtuale viene ripristinata e registrata in Hyper-V.
 9. Riavviare XClarity Orchestrator da Hyper-V Manager.

Capitolo 3. Monitoraggio di risorse e attività

È possibile utilizzare Lenovo XClarity Orchestrator per monitorare gli inventari degli asset, la conformità di firmware e configurazione, lo stato di integrità e la cronologia degli eventi dei dispositivi gestiti.

Visualizzazione del riepilogo dell'ambiente in uso

Il dashboard è l'hub di Lenovo XClarity Orchestrator, che consente di accedere alle informazioni importanti. Contiene le schede dei report che riepilogano lo stato delle risorse e delle attività nell'ambiente, come integrità dei dispositivi, conformità e avvisi.

Per accedere al dashboard, fare clic su **Dashboard** (📊) dalla barra dei menu di XClarity Orchestrator.

È possibile modificare l'ambito del riepilogo solo su quei dispositivi gestiti da uno strumento di gestione delle risorse specifico o in un gruppo di risorse specifico utilizzando il menu a discesa **Seleziona gestione**.

È possibile fare clic su una delle statistiche collegate sul Dashboard per visualizzare un elenco filtrato dei dati che soddisfano i criteri.

Garanzia

Nella scheda Garanzia è riepilogato il periodo di garanzia per i dispositivi gestiti, inclusi i dati riportati che seguono.

- Numero di dispositivi con garanzia scaduta
- Numero di dispositivi con garanzia attiva
- Numero di dispositivi per cui non sono disponibili i dati della garanzia

Ticket di assistenza

La scheda Ticket di assistenza riepiloga i ticket di assistenza gestiti, inclusi i dati che seguono.

- Numero totale di ticket di assistenza attivi
- Numero di ticket di assistenza aperti
- Numero di ticket di assistenza in corso
- Numero di ticket di assistenza in attesa
- Numero di ticket di assistenza chiusi
- Numero di ticket di assistenza in altri stati

Conformità del firmware

Nella scheda Conformità del firmware è riepilogata la conformità ai criteri di conformità del firmware ai dispositivi gestiti in XClarity Orchestrator inclusi i dati che seguono.

- Numero di dispositivi *non* conformi
- Numero di dispositivi conformi
- Numero di dispositivi a cui *non* sono stati assegnati criteri di conformità del firmware
- Numero di dispositivi per cui la conformità non è supportata
- Numero di dispositivi per cui viene controllata la conformità rispetto ai criteri assegnati

Nota: Questi dati rappresentano la conformità del firmware in base ai criteri assegnati da XClarity Orchestrator. Non rappresentano i criteri assegnati dagli strumenti di gestione delle risorse di Lenovo XClarity Administrator.

Conformità configurazione

Nella scheda Conformità configurazione è riepilogata la conformità ai pattern di configurazione dei server sui dispositivi gestiti, inclusi i dati che seguono.

- Numero di dispositivi *non conformi* al pattern assegnato
- Numero di dispositivi conformi al pattern assegnato
- Numero di dispositivi *senza* un pattern assegnato
- Numero di dispositivi per cui è in corso un controllo della conformità della configurazione
- Numero di dispositivi per cui è richiesto un riavvio manuale per completare la distribuzione dei pattern (riavvio in sospeso)
- Numero di dispositivi per cui l'ultima distribuzione di pattern non è riuscita

Nota: Questi dati rappresentano la conformità della configurazione server per tutti i dispositivi in base ai pattern assegnati da XClarity Orchestrator. Non rappresentano i pattern assegnati dagli strumenti di gestione delle risorse di XClarity Administrator gestiti.

Correzioni di sicurezza

La scheda Correzioni di sicurezza riassume il numero di dispositivi gestiti con vulnerabilità e rischi comuni (CVE) per i quali è disponibile una correzione di sicurezza, in base alla gravità CVE più elevata.

- Numero di dispositivi con almeno vulnerabilità critiche
- Numero di dispositivi con almeno una o più vulnerabilità alte, medie o basse, ma non critiche
- Numero di dispositivi che non hanno vulnerabilità note e sono protetti

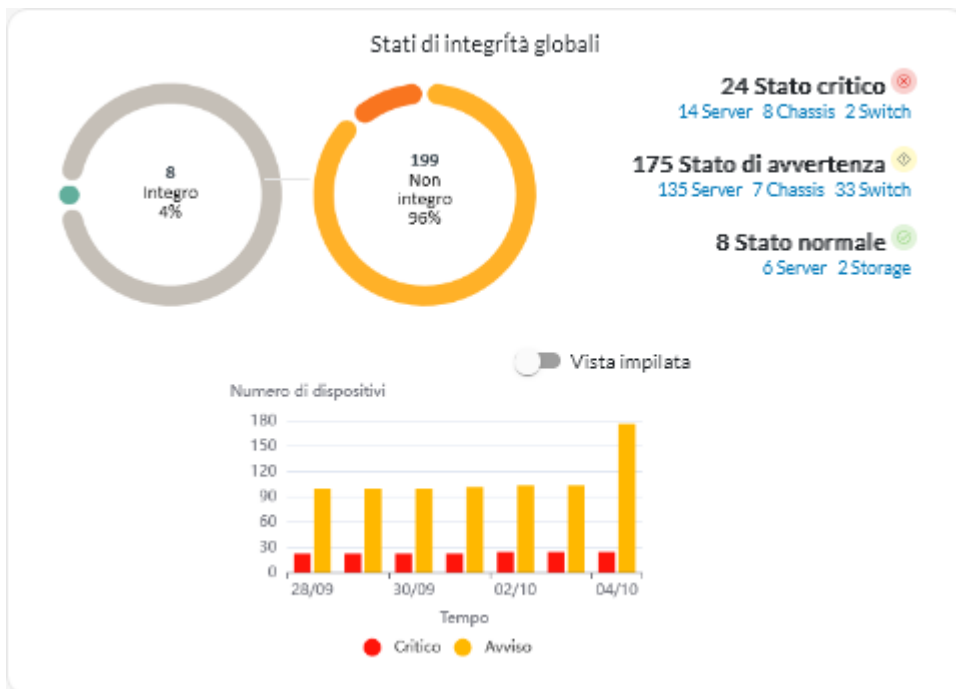
Data di creazione firmware

La scheda Data di creazione firmware riassume la data di creazione del firmware per tipo di componente.

- Numero di firmware superiori a 2 anni per ciascun tipo di componente
- Numero di firmware compresi tra 1 anno e 2 anni per ciascun tipo di componente
- Numero di firmware compresi tra 6 mesi e 1 anno per ciascun tipo di componente
- Numero di firmware inferiori a 6 mesi per ciascun tipo di componente

Stato di integrità globale

Nella scheda Stati di integrità globale vengono riassunti i dispositivi gestiti attualmente integri e non integri nell'ambiente.



In questa scheda sono inclusi i dati che seguono.

- Un grafico circolare che rappresenta la percentuale di dispositivi gestiti il cui stato è integro (normale) e non integro (critico, avvertenza e sconosciuto)

Suggerimento: ogni barra colorata nel grafico circolare indica il numero di dispositivi in uno stato specifico. È possibile passare il mouse su ogni barra colorata per ottenere ulteriori informazioni sullo stato.

- Numero totale e percentuale di dispositivi integri e non integri
- Numero di dispositivi di ciascun tipo il cui stato attualmente è critico, di avvertenza, normale e sconosciuto

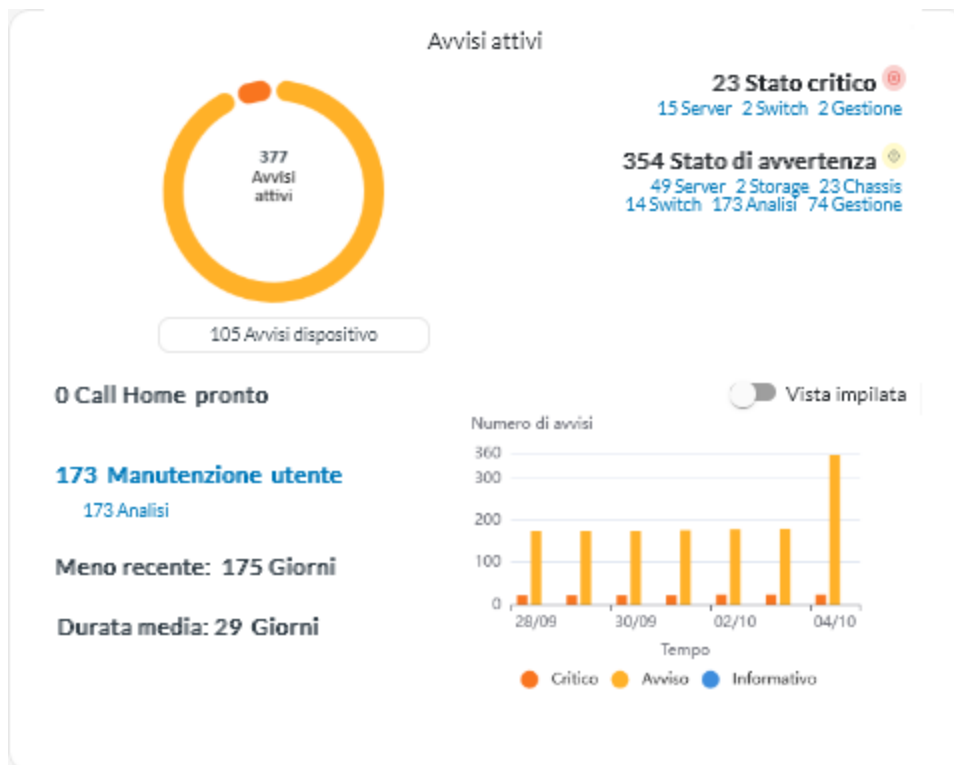
Suggerimento: è possibile fare clic sul numero di dispositivi in uno stato specifico per aprire una pagina con un elenco filtrato di dispositivi che corrispondono ai criteri.

- Un grafico a linee che rappresenta il numero di dispositivi con stato di mancata integrità nel tempo

Suggerimento: ogni barra colorata nel grafico a barre indica il numero di dispositivi in uno stato specifico. È possibile passare il mouse su ogni barra colorata per ottenere ulteriori informazioni sullo stato.

Avvisi attivi

Nella scheda Avvisi attivi dispositivi vengono riepilogati gli avvisi attivi generati dai dispositivi gestiti.



In questa scheda sono inclusi i dati che seguono.

- Un grafico circolare che rappresenta la percentuale di avvisi attivi per ogni gravità (critica, avvertenza, informativa e sconosciuta)

Suggerimento: Ogni barra colorata nel grafico circolare indica il numero di avvisi con una gravità specifica. È possibile passare il mouse su ogni barra colorata per ottenere ulteriori informazioni sulla gravità.

- Numero totale di avvisi attivi
- Numero di dispositivi con avvisi attivi

- Numero totale di avvisi attivi per ciascuna gravità e numero totale di dispositivi di ogni tipo con avvisi attivi per ogni gravità

Suggerimento: è possibile fare clic sul numero di dispositivi in uno stato specifico per aprire una pagina con un elenco filtrato di dispositivi che corrispondono ai criteri.

- Un grafico a linee che rappresenta il numero di dispositivi con stato di mancata integrità nel tempo

Suggerimento: Ogni barra colorata nel grafico a barre indica il numero di avvisi con una gravità specifica. È possibile passare il mouse su ogni barra colorata per ottenere ulteriori informazioni sulla gravità.

- Numero di avvisi attivi con un ticket di assistenza aperto presso il centro di supporto Lenovo (Call Home)
- Numero totale di avvisi attivi che richiedono l'intervento dell'utente (manutenzione) e numero di dispositivi di ogni tipo con avvisi attivi che richiedono l'intervento dell'utente
- Data dell'avviso attivo meno recente
- Durata media di tutti gli avvisi attivi

Visualizzazione dello stato e dei dettagli degli strumenti di gestione delle risorse

È possibile visualizzare il tipo, la versione, lo stato e la connettività di ogni strumento di gestione delle risorse.

Informazioni su questa attività

La colonna **Stato di integrità** identifica l'integrità globale di uno strumento di gestione delle risorse. Vengono utilizzati i seguenti stati di integrità.

- (✓) Normale
- (⚠) Avvertenza
- (✗) Critico

Procedura

Per visualizzare i dettagli degli strumenti di gestione delle risorse, fare clic su **Risorse** (⚙️) → **Strumento di gestione delle risorse** sulla barra dei menu di XClarity Orchestrator per visualizzare la scheda Strumenti di gestione delle risorse.

Strumenti di gestione delle risorse

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

🔄 📄 + 🗑️ ✍️ 📄

Tutte le azioni ▼ Filtri ▼

✕

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

0 selezionato / 2 Totale Righe per pagina: 10 ▼

Al termine

Nella scheda Strumenti di gestione delle risorse è possibile effettuare le operazioni che seguono.

- Connettere uno strumento di gestione delle risorse facendo clic sull'icona **Connetti** (+) (vedere [Connessione degli strumenti di gestione delle risorse](#)).
- Scollegare e rimuovere uno strumento di gestione delle risorse selezionato, facendo clic sull'icona **Elimina** (☒).

Nota: Se XClarity Orchestrator non riesce a connettersi allo strumento di gestione delle risorse (ad esempio, se le credenziali sono scadute o se sono presenti problemi di rete), selezionare **Forza disconnessione**.

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).

Una volta rimosso lo strumento di gestione delle risorse, verranno rimossi anche tutti i dispositivi gestiti dallo strumento di gestione delle risorse rimosso, che includono inventario dei dispositivi, log, dati di metrica e report di analisi.

- Visualizzare un riepilogo dello stato di tutti gli strumenti di gestione delle risorse o di uno specifico strumento di gestione delle risorse facendo clic su **Dashboard** (📊) sulla barra dei menu di XClarity Orchestrator. È possibile restringere l'ambito a un singolo strumento di gestione delle risorse o a un gruppo di risorse utilizzando il menu a discesa **Seleziona gestione**.

Visualizzazione dello stato dei dispositivi

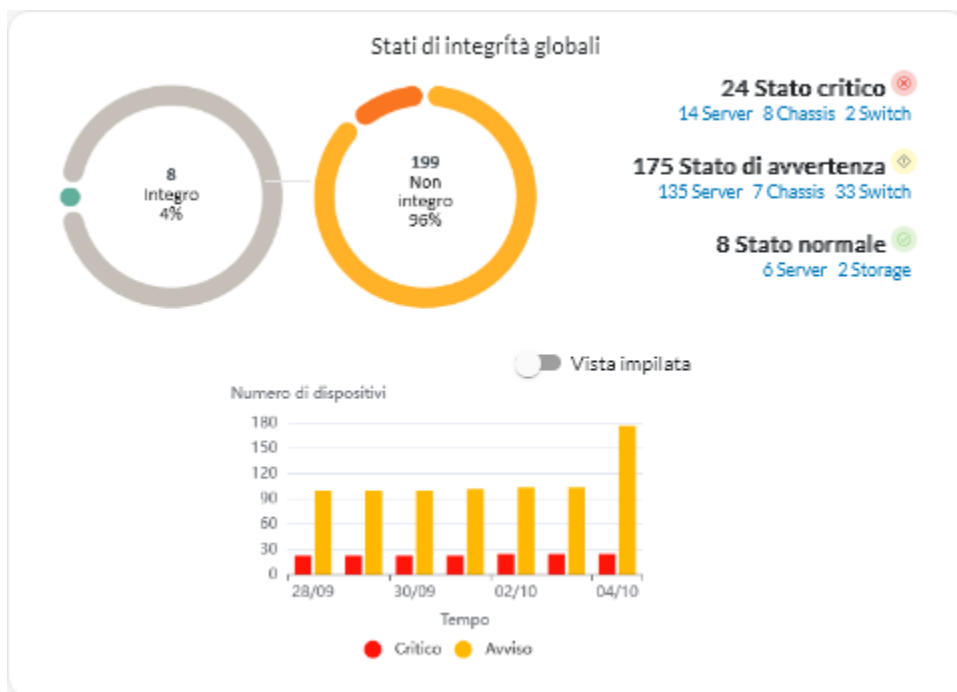
È possibile visualizzare lo stato di tutti i dispositivi gestiti da tutti gli strumenti di gestione delle risorse.

Procedura

Per visualizzare lo stato dei dispositivi gestiti, completare le seguenti operazioni.

- **Riepilogo dello stato di tutti i dispositivi** Sulla barra dei menu di XClarity Orchestrator fare clic su **Dashboard** (📊) per visualizzare le schede del dashboard con una panoramica e lo stato di tutti i dispositivi gestiti e delle altre risorse (vedere [Visualizzazione del riepilogo dell'ambiente in uso](#)).

È possibile modificare l'ambito del riepilogo solo su quei dispositivi gestiti da uno strumento di gestione delle risorse specifico o in un gruppo di risorse specifico utilizzando il menu a discesa **Seleziona gestione**.



Ogni barra colorata nei grafici a barre e circolari indica il numero di dispositivi in uno stato specifico. È possibile passare il mouse su ogni barra colorata per ottenere ulteriori informazioni sullo stato. È inoltre possibile fare clic sul numero di dispositivi in ogni stato per visualizzare un elenco di tutti i dispositivi che soddisfano i criteri.

- **Stato di tutti i dispositivi di un tipo specifico** Per visualizzare i riepiloghi globali degli avvisi attivi, fare clic su **Risorse** (🔍) sulla barra dei menu di XClarity Orchestrator, quindi sul tipo di dispositivo per mostrare una scheda con una vista tabulare di tutti i dispositivi simili. Ad esempio, se si seleziona **Server**, viene visualizzato un elenco di tutti i server rack, tower e ad alta densità e di tutti i server Flex System e ThinkSystem in uno chassis.

È possibile cambiare l'ambito del riepilogo in base alla proprietà del dispositivo nell'elenco a discesa **Analizza per**.

- **Modello tipo di macchina.** (impostazione predefinita) Questo report riepiloga l'integrità del dispositivo in base al modello MTM (Modello tipo di macchina).
- **Tipo di macchina.** Questo report riepiloga l'integrità del dispositivo in base al tipo di macchina.
- **Nome prodotto.** Questo report riepiloga l'integrità del dispositivo in base al prodotto.



XClarity Orchestrator riepiloga l'integrità del dispositivo in base a criteri specifici. Ciascun riepilogo include le seguenti informazioni.

- Un grafico circolare che mostra il numero totale di dispositivi non integri e la percentuale di dispositivi in ciascun stato di assenza di integrità (critico, avvertenza e sconosciuto).

Ogni barra colorata nel grafico circolare indica il numero di dispositivi in uno stato specifico. È possibile passare il mouse su ogni barra colorata per ottenere ulteriori informazioni sullo stato.

- Un grafico a linee che mostra il numero di dispositivi in ciascun stato di integrità su base giornaliera per il numero di giorni specificato.

Ogni barra colorata nel grafico a linee indica il numero di dispositivi in uno stato specifico. È possibile passare il mouse su ogni barra colorata per ottenere ulteriori informazioni sullo stato.

- Il numero di dispositivi di ogni tipo che non sono integri in un giorno specifico. Il giorno corrente viene visualizzato per impostazione predefinita. È possibile modificare il giorno passando il mouse su ciascun giorno nel grafico a linee.

- **Stato di un dispositivo specifico** Sulla barra dei menu di XClarity Orchestrator fare clic su **Risorse** (🔍), quindi selezionare il tipo di dispositivo per visualizzare una scheda con una vista tabulare di tutti i dispositivi simili. Ad esempio, se si seleziona **Server**, viene visualizzato un elenco di tutti i server rack, tower e ad alta densità e di tutti i server Flex System e ThinkSystem in uno chassis.

Server

Q Cerca X

Avvia Controllo remoto
 Azioni di alimentazione

 Tutte le azioni
 Filtri

<input type="checkbox"/>	Server	Stato	Connetti	Alimenta	Indirizzi	Nome pr	Tipo/mox	Firmware	Avviso	Gruppi
<input type="checkbox"/>	New...				10.24:	Leno...	719...	N3E1:	Non ...	Non di
<input type="checkbox"/>	ite-b...				10.24:	Leno...	716...	CGE1:	Non ...	Non di
<input type="checkbox"/>	Blac...				10.24:	Leno...	716...	A3EG:	Non ...	Non di
<input type="checkbox"/>	nod...				10.24:	IBM ...	791...	Non di	Non ...	Non di
<input type="checkbox"/>	IM...				10.24:	IBM ...	873...	B2E11	Non ...	Non di
<input type="checkbox"/>	Cara...				10.24:	Eagl...	791...	Non di	Non ...	Non di
<input type="checkbox"/>	blad...				10.24:	IBM ...	790...	Non di	Non ...	Non di
<input type="checkbox"/>	New...				10.24:	Leno...	719...	N3E1:	Non ...	Non di
<input type="checkbox"/>	New...				10.24:	Leno...	719...	N3E1:	Non ...	Non di
<input type="checkbox"/>	New...				10.24:	Leno...	719...	N3E1:	Non ...	Non di

0selezionato / 60 Totale Righi per pagina: 10

La colonna **Stato** identifica l'integrità globale di un dispositivo. Vengono utilizzati i seguenti stati di integrità. Se lo stato di un dispositivo non è integro, utilizzare il log avvisi per identificare e risolvere i problemi (vedere [Monitoraggio degli avvisi attivi](#)).

- Normale
- Avvertenza
- Critico

La colonna **Connettività** identifica lo stato della connessione tra il dispositivo e XClarity Orchestrator. Vengono utilizzati i seguenti stati di connettività.

- Offline
- Gestito offline
- Online
- Parziale
- In sospeso

La colonna **Alimentazione** identifica lo stato dell'alimentazione. Vengono utilizzati i seguenti stati di alimentazione.

- Attivato
- Disattivato

La colonna **Avviso** identifica il numero di avvisi per i clienti online (suggerimenti tecnici) correlati a ciascun server. Fare clic sul numero per visualizzare la scheda Avviso nella pagina dei dettagli del dispositivo per

visualizzare un elenco di avvisi per i clienti online, inclusi il riepilogo e il collegamento e per ogni avviso. Fare clic su un collegamento per aprire una pagina Web con i dettagli relativi all'avviso.

Al termine

Nelle schede dei dispositivi è possibile effettuare la seguente azione.

- Aggiungere un dispositivo selezionato a un gruppo facendo clic su **Tutte le azioni** → **Aggiungi elementi al gruppo**.
- Inoltrare report sui tipi di dispositivi specifici periodicamente a uno o più indirizzi e-mail facendo clic sull'icona **Crea server d'inoltro dei report** (+). Il report viene inviato utilizzando i filtri dati attualmente applicati alla tabella. Tutte le colonne della tabella visibili e nascoste sono incluse nel report. Per ulteriori informazioni, vedere [Inoltro di report](#).
- Aggiungere un report su un tipo di dispositivo specifico a un server d'inoltro dei report specifico utilizzando i filtri dati attualmente applicati alla tabella facendo clic sull'icona **Aggiungi al server d'inoltro dei report** (→). Se il server d'inoltro dei report include già un report per quel tipo di dispositivo, il report viene aggiornato per utilizzare i filtri dati correnti.

Visualizzazione dei dettagli dei dispositivi

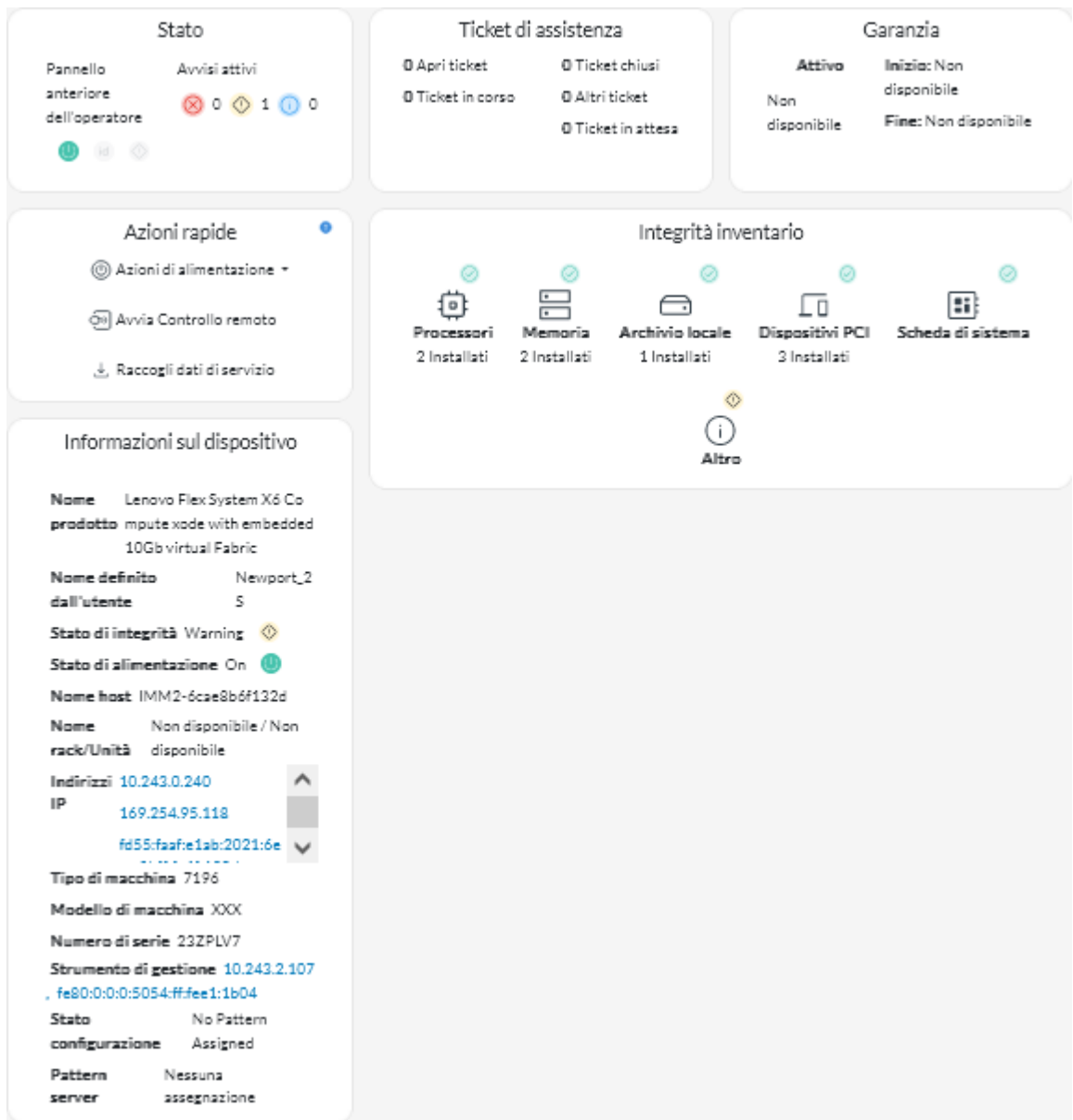
È possibile visualizzare informazioni dettagliate su ciascun dispositivo, incluso il riepilogo globale di stato e integrità dei dispositivi, inventario, avvisi ed eventi, metrica di sistema e firmware.

Procedura

Per visualizzare i dettagli relativi a un dispositivo, effettuare le operazioni che seguono.

Passo 1. Sulla barra dei menu di XClarity Orchestrator fare clic su **Risorse** (🔍), quindi sul tipo di dispositivo per visualizzare una scheda con una vista tabulare di tutti i dispositivi gestiti simili.






Passo 2. Fare clic sulla riga relativa al dispositivo per visualizzare le schede di riepilogo per quel dispositivo.



Passo 3. Completare una o più azioni seguenti.

I dettagli di ogni scheda potrebbero variare a seconda del tipo di dispositivo.

- Fare clic su **Riepilogo** per visualizzare un riepilogo globale del dispositivo, tra cui le informazioni sul dispositivo, l'inventario, l'integrità, le informazioni sul sistema operativo, le metriche di sistema, i ticket di assistenza e la garanzia. Questa pagina include anche la scheda **Azioni rapide** in cui sono elencate le azioni che è possibile eseguire sul dispositivo (come azioni di alimentazione, raccolta dei dati di servizio e avvio di una sessione di controllo remoto). In questa pagina viene visualizzato lo stato di ciascun LED sul pannello anteriore dell'operatore.
 - **LED alimentazione**
 - **Acceso** (🔌). Il dispositivo è acceso.
 - **Spento** (🔌). Il dispositivo è spento.
 - **LED di posizione**

- **Acceso** (). Il LED di posizione sul pannello di controllo è acceso.
- **Lampeggiante** (). Il LED di posizione sul pannello di controllo è acceso o lampeggiante.
- **Spento** (). Il LED di posizione sul pannello di controllo non è acceso.
- **LED di errore**
 - **Acceso** (). Il LED di errore sul pannello di controllo è acceso.
 - **Spento** (). Il LED di errore sul pannello di controllo non è acceso.
- Fare clic su **Inventario** per visualizzare i dettagli sui componenti hardware del dispositivo (come processori, moduli di memoria, unità, alimentatori, ventole, dispositivi PCI e scheda di sistema).

Nota:

- L'inventario *non* è supportato per questi dispositivi di storage: ThinkSystem DS2200, Lenovo Storage S2200 e S3200 e il nodo di storage Flex System V7000.
- I dettagli del firmware *non sono* disponibili per questi dispositivi di storage: ThinkSystem DS4200 e DS6200 e Lenovo Storage DX8200C, DX8200D e DX8200N.
- Fare clic su **Log avvisi** per visualizzare l'elenco degli avvisi attivi e le statistiche degli avvisi per il dispositivo (vedere [Monitoraggio degli avvisi attivi](#)).
- Fare clic su **Log eventi** per visualizzare l'elenco di eventi per il dispositivo (vedere [Monitoraggio degli eventi](#)).
- Fare clic su **Firmware** per visualizzare un elenco dei livelli di firmware correnti per il dispositivo e i componenti del dispositivo.
- Fare clic su **Servizio** per visualizzare le informazioni sugli archivi dei dati di servizio e i ticket di assistenza per il dispositivo.
- Fare clic su **Utilizzo** per visualizzare l'utilizzo del sistema, la temperatura e le metriche di alimentazione nel tempo per i dispositivi ThinkAgile e ThinkSystem.
- Fare clic su **Avviso** per visualizzare un elenco di avvisi dei clienti online, inclusi il riepilogo e il collegamento per ogni avviso. Fare clic su un collegamento per aprire una pagina Web con i dettagli relativi all'avviso.

Al termine

Oltre a visualizzare il riepilogo e le informazioni dettagliate su un dispositivo, da questa pagina è possibile eseguire le seguenti operazioni su un dispositivo.

- Avviare l'interfaccia Web del controller di gestione della scheda di base dalla scheda **Riepilogo**, facendo clic sull'indirizzo IP principale del dispositivo.
- Avviare l'interfaccia Web per il dispositivo dalla scheda **Riepilogo** facendo clic sull'indirizzo IP.
- Avviare l'interfaccia Web dello strumento di gestione delle risorse che gestisce il dispositivo nella scheda **Riepilogo**, facendo clic sul nome dello strumento di gestione delle risorse o sull'indirizzo IP.

Visualizzazione dello stato e dei dettagli delle risorse dell'infrastruttura

È possibile visualizzare lo stato e le informazioni dettagliate per le risorse dell'infrastruttura di data center (ad esempio, PDU e UPS) gestite tramite uno strumento di gestione delle risorse di Schneider Electric EcoStruxure IT Expert.

Prima di iniziare

La colonna **Stato** identifica l'integrità globale di una risorsa dell'infrastruttura. Vengono utilizzati i seguenti stati di integrità. Se lo stato di una risorsa dell'infrastruttura non è integro, utilizzare il log avvisi per identificare e risolvere i problemi (vedere [Monitoraggio degli avvisi attivi](#)).

- (🟢) Normale
- (🟡) Avvertenza
- (🔴) Critico

Procedura

- **Stato di una specifica risorsa dell'infrastruttura** Per visualizzare lo stato delle risorse dell'infrastruttura, fare clic su **Risorse** (⚙️) → **Infrastruttura** sulla barra dei menu di XClarity Orchestrator per visualizzare la scheda Infrastruttura. Se lo stato di una risorsa dell'infrastruttura non è integro, utilizzare il log avvisi per identificare e risolvere i problemi (vedere [Monitoraggio degli avvisi attivi](#)).

The screenshot shows the 'Infrastruttura' page in XClarity Orchestrator. It features a table with 7 columns: Nome, Stato, Nome host, Produttore, Modello, Tipo, and Gruppi. The table contains 9 rows of data. The status column uses icons: a green checkmark for 'Normale', a yellow triangle for 'Avviso', and a red 'X' for 'Critico'. The status text is also present in the same column. The bottom of the table shows '0 Selezionato/i / 9 Totale' and 'Righe per pagina: 10'.

Nome	Stato	Nome host	Produttore	Modello	Tipo	Gruppi
APC_R18	🔴 Critico	APC_R18	Server Tec...	Sentry Swit...	Rack PDU	Non dispo...
APC_R21	🔴 Critico	APC_R21	Server Tec...	Sentry Swit...	Rack PDU	Non dispo...
EcoStruxur...	🟢 Norma...	Non dispo...	Schneider ...	EcoStruxur...	Gateway	Non dispo...
Sentry3_5...	🔴 Critico	Sentry3_5...	Server Tec...	Sentry Swit...	Rack PDU	bangalore-gr
Sentry3_5...	🔴 Critico	Sentry3_5...	Server Tec...	Sentry Swit...	Rack PDU	Andrei-Testir
Sentry3_5...	🔴 Critico	Sentry3_5...	Server Tec...	Sentry Swit...	Rack PDU	Romania-PDI
Sentry3_5...	🔴 Critico	Sentry3_5...	Server Tec...	Sentry Swit...	Rack PDU	TestRefreshG
Sentry3_5...	🟡 Avviso	Sentry3_5...	Server Tec...	Sentry Swit...	Rack PDU	DemoGroup
UPSR11	🔴 Critico	UPSR11	MGE	9135 6000	UPS	Work group1

- **Dettagli di una specifica risorsa dell'infrastruttura**

1. Sulla barra dei menu di XClarity Orchestrator fare clic su **Risorse** (⚙️) → **Infrastruttura** per visualizzare la scheda Infrastruttura.
2. Fare clic sulla risorsa dell'infrastruttura per visualizzare la scheda di riepilogo della risorsa.
3. Completare una o più azioni seguenti.
 - Fare clic su **Riepilogo** per visualizzare un riepilogo della risorsa, tra cui le informazioni sul dispositivo e lo stato.
 - Fare clic sul log **Avvisi** per visualizzare l'elenco degli avvisi attivi e le statistiche degli avvisi per la risorsa (vedere [Monitoraggio degli avvisi attivi](#)).

- Fare clic sul log **Eventi** per visualizzare l'elenco di eventi per la risorsa (vedere [Monitoraggio degli eventi](#)).
- Fare clic su **Sensori** per visualizzare l'elenco di sensori nella risorsa. È possibile determinare la misurazione più recente del sensore nella scheda Sensori oppure selezionare uno o più sensori e fare clic sull'icona **Grafico** (II) per visualizzare il grafico a linee che mostra le misurazioni, nel tempo, per ciascun sensore selezionato. I sensori con la stessa unità (ad esempio, watt o amp) sono riportati sullo stesso grafico.

Nota: Schneider Electric EcoStruxure IT Expert raccoglie i dati dei sensori ogni 5 minuti e XClarity Orchestrator li sincronizza ogni ora. Al momento XClarity Orchestrator consente di salvare solo gli ultimi 60 minuti di dati.

Al termine

Oltre a visualizzare il riepilogo e le informazioni dettagliate su una risorsa dell'infrastruttura, in questa pagina è possibile effettuare le seguenti operazioni.

- Avviare l'interfaccia Web per una determinata risorsa dell'infrastruttura nella scheda **Riepilogo**, facendo clic sull'indirizzo IP della risorsa.

Monitoraggio dei processi

I *processi* sono attività a esecuzione prolungata in background. È possibile visualizzare un log di tutti i processi avviati da Lenovo XClarity Orchestrator.

Informazioni su questa attività

Se un'attività a esecuzione prolungata è destinata a più risorse viene creato un processo separato per ogni risorsa.

È possibile visualizzare lo stato e i dettagli di ciascun processo nel log dei processi. Il log dei processi può contenere massimo 500 processi o 1 GB. Quando le dimensioni massime vengono raggiunte, i processi meno recenti completati correttamente vengono eliminati. Se nel log non sono presenti processi completati correttamente, vengono eliminati i processi meno recenti completati con avvisi. Se nel log non sono presenti processi completati correttamente o con avvisi, vengono eliminati i processi meno recenti completati con errori.

Nota: I processi in esecuzione per più di 24 ore vengono arrestati e posizionati nello stato Scaduto.

Procedura

Per visualizzare i processi, effettuare una o più delle operazioni che seguono.

- **Visualizza processi pianificati** Fare clic su **Monitoraggio** (📧) → **Processi** dalla barra dei menu di XClarity Orchestrator, quindi selezionare la scheda **Processi pianificati** per visualizzare la scheda Processi pianificati. In questa scheda sono elencate le informazioni su ciascun processo pianificato, quali stato, timestamp di pianificazione del processo e timestamp di avvio del processo.
- **Visualizzazione dei processi** Fare clic su **Monitoraggio** (📧) → **Processi** sulla barra dei menu di XClarity Orchestrator per visualizzare la scheda Processi. Questa scheda elenca le informazioni su ogni processo, tra cui lo stato, l'avanzamento, i timestamp di avvio e di fine e la risorsa di destinazione.

Processi

I processi sono attività che richiedono tempi di esecuzione superiori per uno o più sistemi di destinazione. È possibile scegliere di eliminare un processo o di visualizzarne i dettagli.

Tutte le azioni ▾ Filtri ▾ Cerca

	Nome proce	Stato :	In corso :	Ora di inizio	Ora di comp	Destinazion	Categoria :	Creato da :
<input type="radio"/>	Assegna c	✓ Com	100%	5 ott 202:	5 ott 202:	Non dis...	Aggiorn...	Orches...
<input type="radio"/>	Assegna c	✓ Com	100%	5 ott 202:	5 ott 202:	Non dis...	Aggiorn...	Orches...
<input type="radio"/>	Assegna c	✓ Com	100%	5 ott 202:	5 ott 202:	Non dis...	Aggiorn...	Orches...
<input type="radio"/>	Assegna c	✓ Com	100%	5 ott 202:	5 ott 202:	Non dis...	Aggiorn...	Orches...
<input type="radio"/>	Assegna c	✓ Com	100%	5 ott 202:	5 ott 202:	Non dis...	Aggiorn...	Orches...
<input type="radio"/>	Elabora d	✗ Inter	100%	5 ott 202:	5 ott 202:	SN#Y0...	Servizio	Orches...
<input type="radio"/>	Elabora d	✗ Inter	100%	4 ott 202:	4 ott 202:	SN#Y0...	Servizio	Orches...
<input type="radio"/>	Elabora d	✗ Inter	100%	4 ott 202:	4 ott 202:	SN#Y0...	Servizio	Orches...
<input type="radio"/>	Elabora d	✗ Inter	100%	4 ott 202:	4 ott 202:	SN#Y0...	Servizio	Orches...
<input type="radio"/>	Scarica pi	✓ Com	100%	4 ott 202:	4 ott 202:	XClarit...	Aggiorn...	Orches...

0 Selezionato/i / 15 Totale Righe per pagina: 10 ▾ 1 2 >

Per visualizzare le informazioni dettagliate su un processo, fare clic sulla riga per il processo nella tabella. Vengono visualizzate le schede che elencano le informazioni su ogni processo secondario (inclusi lo stato, l'avanzamento, i timestamp di avvio e di fine, i dispositivi di destinazione e il log dei processi).

Connetti gestore 10.243.10.122

Tutte le azioni ▾ Filtri ▾ Cerca

	Nome processo :	Stato :	In corso :	Ora di inizio :	Ora di completam	Destinazione :
▾	Connetti gest	ⓘ Completato	100%	4 ott 2022, 09:2	4 ott 2022, 09:2	Non disponibile
	Importa ce	ⓘ Completato	100%	4 ott 2022, 09:2	4 ott 2022, 09:2	Non disponibile
	Verifica de	ⓘ Completato	100%	4 ott 2022, 09:2	4 ott 2022, 09:2	Non disponibile
	Verifica au	ⓘ Completato	100%	4 ott 2022, 09:2	4 ott 2022, 09:2	Non disponibile
	Controllo	ⓘ Completato	100%	4 ott 2022, 09:2	4 ott 2022, 09:2	Non disponibile
▸	Configura:	ⓘ Completato	100%	4 ott 2022, 09:2	4 ott 2022, 09:2	Non disponibile
	Salvataggi	ⓘ Completato	100%	4 ott 2022, 09:2	4 ott 2022, 09:2	Non disponibile

7 Totale Righe per pagina: 10 ▾

Al termine

Nella scheda Processi è possibile effettuare le operazioni che seguono.

- Eliminare una sottoattività o un processo *completato* o *scaduto* dal log dei processi selezionando uno o più processi o sottoattività e facendo clic sull'icona **Elimina** (🗑️).

Monitoraggio degli avvisi attivi

Gli *avvisi* sono eventi hardware o di Orchestrator che richiedono l'analisi e l'intervento dell'utente. Lenovo XClarity Orchestrator esegue il polling degli strumenti di gestione delle risorse in modo asincrono e visualizza gli avvisi ricevuti da questi strumenti.

Informazioni su questa attività

Non è presente alcun limite al numero di avvisi attivi memorizzati nel repository locale.

Nella scheda Avvisi è possibile visualizzare un elenco di tutti gli avvisi attivi.

Avvisi

Gli avvisi indicano condizioni hardware o di gestione che necessitano di analisi e intervento dell'utente.

Tutte le azioni ▾ Filtri ▾

Cerca

	Data e ora ▾	Gravità :	Avviso :	Risorsa :	Intervento :	Tipo di risorsa	Tipo di origini	Gruppi :	
<input type="radio"/>	05/10/...	⚠️	Av...	La connes	XClarit...	Ne...	Chassis	Gestione	Non disp
<input type="radio"/>	05/10/...	⚠️	Av...	La connes	XClarit...	Ne...	Chassis	Gestione	Non disp
<input type="radio"/>	05/10/...	⚠️	Av...	La connes	XClarit...	Ne...	Switch	Gestione	Non disp
<input type="radio"/>	05/10/...	⚠️	Av...	La connes	XClarit...	Ne...	Switch	Gestione	Non disp
<input type="radio"/>	05/10/...	⚠️	Av...	La connes	XClarit...	Ne...	Switch	Gestione	Non disp
<input type="radio"/>	05/10/...	⚠️	Av...	La connes	XClarit...	Ne...	Switch	Gestione	Non disp
<input type="radio"/>	05/10/...	⚠️	Av...	La connes	XClarit...	Ne...	Switch	Gestione	Non disp
<input type="radio"/>	05/10/...	⚠️	Av...	La connes	XClarit...	Ne...	Switch	Gestione	Non disp
<input type="radio"/>	05/10/...	⚠️	Av...	La connes	XClarit...	Ne...	Switch	Gestione	Non disp
<input type="radio"/>	05/10/...	⚠️	Av...	La connes	XClarit...	Ne...	Switch	Gestione	Non disp



351 Totale Righe per pagina: 10 ▾

1 2 3 4 5

La colonna **Gravità** identifica la gravità dell'avviso. Vengono utilizzate le seguenti gravità.

- (i) **Informativo**. Nessuna azione richiesta.
- (⚠️) **Avvertenza**. L'azione può essere rinviata oppure non è richiesta alcuna azione.
- (❌) **Critico**. È richiesta un'azione immediata.

La colonna **Intervento richiesto** indica se il dispositivo richiede un intervento e il responsabile che generalmente esegue l'intervento. Vengono utilizzati i seguenti tipi di interventi richiesti.

- **Nessuna.** L'avviso è informativo e non richiede intervento.
-  **Utente.** Intraprende l'azione di ripristino appropriata per risolvere il problema.
-  **Supporto.** Se Call Home è abilitato per XClarity Orchestrator o per strumento di gestione delle risorse che gestisce il dispositivo associato, l'avviso viene in genere inviato al centro di supporto Lenovo, tranne se non è già disponibile un ticket di assistenza aperto per lo stesso ID di avviso per il dispositivo (vedere [Apertura automatica dei ticket di assistenza mediante Call Home](#) nella documentazione online di XClarity Orchestrator). Se Call Home non è abilitato, si consiglia di aprire manualmente un ticket di assistenza per risolvere il problema (vedere [Apertura manuale di un ticket di assistenza nel centro di supporto Lenovo](#) nella documentazione online di XClarity Orchestrator).

Se sono presenti avvisi attivi, nella scheda Analisi avvisi vengono visualizzate le statistiche degli avvisi. È possibile visualizzare le statistiche degli avvisi per gravità, origine, risorsa e intervento richiesto per il giorno corrente e per un periodo di tempo specifico (vedere [Analisi di avvisi attivi](#)).




Procedura

Per visualizzare gli avvisi attivi, completare una o più delle operazioni che seguono.

- **Visualizzare tutti gli avvisi attivi** Fare clic su **Monitoraggio**  → **Avvisi** sulla barra dei menu di XClarity Orchestrator per visualizzare la scheda Avvisi.

Per visualizzare le informazioni su un avviso specifico, fare clic sulla descrizione nella colonna **Avviso**. Verrà visualizzato un popup con le informazioni sull'origine dell'avviso, la spiegazione e le azioni per il ripristino.

- **Visualizzare avvisi attivi per un dispositivo specifico**

1. Sulla barra dei menu di XClarity Orchestrator fare clic su **Risorse** , quindi sul tipo di dispositivo per visualizzare una scheda con una vista tabulare di tutti i dispositivi gestiti simili.

2. Fare clic sulla riga relativa a un dispositivo per visualizzare le schede di riepilogo per quel dispositivo.
3. Fare clic su **Log avvisi** per visualizzare l'elenco degli avvisi attivi per il dispositivo sulla scheda Analisi avvisi. Per visualizzare le informazioni su un avviso specifico, fare clic sulla descrizione nella colonna **Avviso**. Verrà visualizzato un popup con le informazioni sull'origine dell'avviso, la spiegazione e le azioni per il ripristino.

Monitoraggio degli eventi

Da Lenovo XClarity Orchestrator, è possibile accedere a un elenco cronologico di tutti gli eventi di controllo e delle risorse.

Ulteriori informazioni:  [Come monitorare gli eventi di dispositivi specifici](#)




Informazioni su questa attività

Un *evento risorsa* identifica una condizione hardware o di Orchestrator che si è verificata su un dispositivo gestito, uno strumento di gestione delle risorse o su XClarity Orchestrator. È possibile utilizzare questi eventi per tenere traccia e analizzare i problemi relativi al server Orchestrator e all'hardware.



Un *evento di controllo* è un record delle attività utente eseguite da uno strumento di gestione delle risorse o da XClarity Orchestrator. È possibile utilizzare questi eventi di controllo per tenere traccia e analizzare i problemi relativi all'autenticazione.

Il log eventi contiene gli eventi di controllo e risorse. Può contenere fino a 100.000 eventi da tutte le origini. Fino a 50.000 eventi possono riguardare un singolo strumento di gestione delle risorse e i relativi dispositivi gestiti. Fino a 1.000 eventi possono riguardare un singolo dispositivo gestito. Quando il numero massimo di eventi viene raggiunto, l'evento meno recente viene rimosso quando viene ricevuto il nuovo evento.

La colonna **Gravità** identifica la gravità dell'evento. Vengono utilizzate le seguenti gravità.

-  **Informativo**. Nessuna azione richiesta.
-  **Avvertenza**. L'azione può essere rinviata oppure non è richiesta alcuna azione.
-  **Critico**. È richiesta un'azione immediata.

La colonna **Intervento richiesto** indica se il dispositivo richiede un intervento e il responsabile che generalmente esegue l'intervento. Vengono utilizzati i seguenti tipi di interventi richiesti.

- **Nessuna**. L'avviso è informativo e non richiede intervento.
-  **Utente**. Intraprende l'azione di ripristino appropriata per risolvere il problema.
-  **Supporto**. Se Call Home è abilitato per XClarity Orchestrator o per strumento di gestione delle risorse che gestisce il dispositivo associato, l'avviso viene in genere inviato al centro di supporto Lenovo, tranne se non è già disponibile un ticket di assistenza aperto per lo stesso ID di avviso per il dispositivo (vedere [Apertura automatica dei ticket di assistenza mediante Call Home](#) nella documentazione online di nella documentazione online di XClarity Orchestrator). Se Call Home non è abilitato, si consiglia di aprire manualmente un ticket di assistenza per risolvere il problema (vedere [Apertura manuale di un ticket di assistenza nel centro di supporto Lenovo](#) nella documentazione online di nella documentazione online di XClarity Orchestrator).

Procedura

Per visualizzare eventi, effettuare una o più delle operazioni che seguono.

- **Visualizzare tutti gli eventi risorsa o di controllo** Fare clic su **Monitoraggio** (📊) → **Eventi** sulla barra dei menu di XClarity Orchestrator per visualizzare la scheda Eventi. Quindi, fare clic sulla scheda **Eventi risorse** o **Eventi di controllo** per visualizzare le voci di log.

Eventi

Il log eventi fornisce una cronologia delle condizioni hardware e di gestione rilevate (eventi delle risorse) e un audit trail delle azioni utente (eventi di controllo).

Eventi risorse Eventi di controllo

🔄 📄 📄 ➔ 📄 📄 Tutte le azioni ▾ Filtri ▾ 🔍 Cerca ✕

Data e ora ▾	Gravità ▾	Evento ▾	Risorsa ▾	Intervento ric	Tipo di risorsa	Gruppi ▾
05/10/22...	⚠️ Avviso	Lo stato di ii	Not Availab	Ness...	Non disponi	Non disponi
05/10/22...	⚠️ Avviso	Asserzione	Not Availab	Ness...	Non disponi	Non disponi
05/10/22...	ℹ️ Infor...	Impossibile	IO Module :	Ness...	Switch	Non disponi
05/10/22...	ℹ️ Infor...	Annullamer	Not Availab	Ness...	Non disponi	Non disponi
05/10/22...	ℹ️ Infor...	Impossibile	IO Module :	Ness...	Switch	Non disponi
05/10/22...	ℹ️ Infor...	Impossibile	IO Module :	Ness...	Switch	Non disponi
05/10/22...	⚠️ Avviso	Lo stato di ii	Not Availab	Ness...	Non disponi	Non disponi
05/10/22...	⚠️ Avviso	Asserzione	Not Availab	Ness...	Non disponi	Non disponi
05/10/22...	ℹ️ Infor...	Impossibile	IO Module :	Ness...	Switch	Non disponi
05/10/22...	⚠️ Avviso	Asserzione	Not Availab	Ness...	Non disponi	Non disponi

9336 Totale Righe per pagina: 10 ▾

⏪ < 1 2 3 4 5 > ⏩

- **Visualizzare eventi risorsa o di controllo per un dispositivo specifico**
 1. Fare clic su **Risorse** (📊) sulla barra dei menu di XClarity Orchestrator, quindi sul tipo di dispositivo per visualizzare una scheda con una vista tabulare di tutti i dispositivi gestiti simili.
 2. Fare clic sulla riga relativa a un dispositivo per visualizzare le schede di riepilogo per quel dispositivo.
 3. Fare clic sulla scheda **Log eventi** per visualizzare la pagina Eventi per il dispositivo.

Esclusione di avvisi ed eventi

Se vengono visualizzati eventi e avvisi attivi che non interessano l'utente, è possibile escludere tali eventi e avvisi attivi da tutte le pagine e i riepiloghi in cui vengono visualizzati. Gli avvisi e gli avvisi esclusi rimangono continuano a essere presenti nel log ma non vengono visualizzati in nessuna delle pagine dedicate a eventi e avvisi, incluse le visualizzazioni del log e lo stato delle risorse.

Informazioni su questa attività

Gli eventi esclusi vengono nascosti per tutti gli utenti, non solo per l'utente che imposta la configurazione.

Quando si esclude un evento a cui è associato un avviso, viene escluso anche l'avviso.

Procedura

Per escludere eventi e avvisi, attenersi alla procedura descritta di seguito.

Passo 1. Dalla barra dei menu di XClarity Orchestrator, fare clic su **Monitoraggio** (📊) → **Avvisi** o **Monitoraggio** (📊) → **Eventi** per visualizzare la scheda Avvisi o Eventi.

Passo 2. Selezionare gli avvisi o gli eventi da escludere e fare clic sull'icona **Escludi** (🚫). Viene visualizzata la finestra di dialogo Escludi avvisi o Escludi eventi.

Passo 3. Selezionare una delle seguenti opzioni.

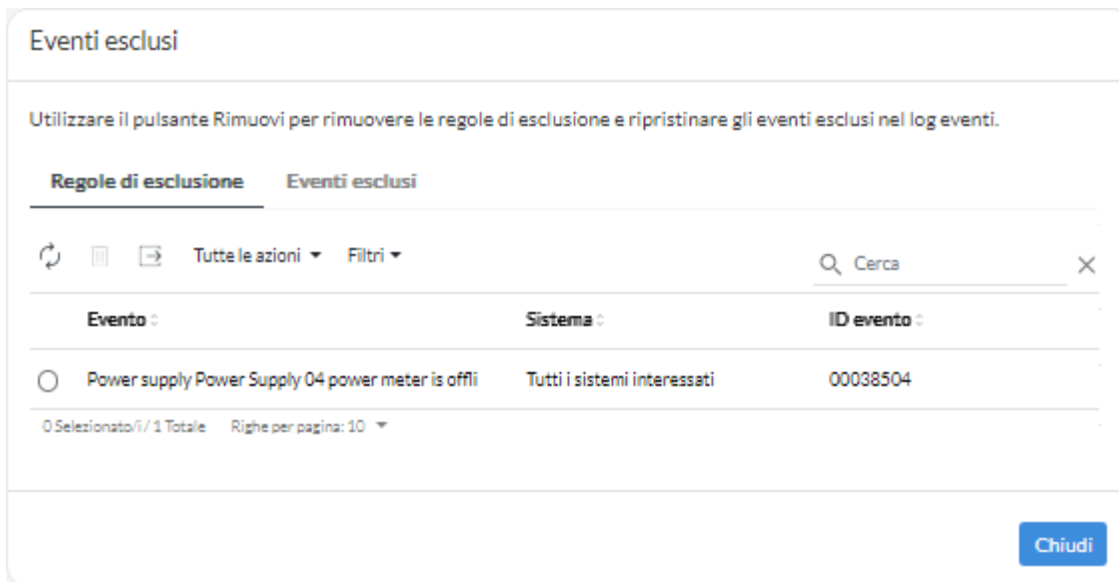
- **Escludi eventi selezionati da tutti i dispositivi.** Esclude gli eventi selezionati da tutti i dispositivi gestiti.
- **Escludi eventi solo dai dispositivi nell'ambito dell'istanza selezionata.** Esclude gli eventi selezionati dai dispositivi gestiti a cui si applicano.

Passo 4. Fare clic su **Salva**.

Al termine

Quando si escludono gli eventi, XClarity Orchestrator crea regole di esclusione in base alle informazioni fornite.

- Visualizzare un elenco delle regole di esclusione e degli eventi e degli avvisi esclusi facendo clic sull'icona **Visualizza esclusioni** (🔍) per visualizzare la finestra di dialogo Avvisi esclusi o Eventi esclusi. Fare clic sulla scheda **Regole di esclusione** per visualizzare le regole di esclusione oppure selezionare la scheda **Avvisi esclusi** o **Eventi esclusi** per visualizzare gli avvisi o gli eventi esclusi.



- Ripristinare gli eventi esclusi nei log rimuovendo la regola di esclusione appropriata. Per rimuovere una regola di esclusione, fare clic sull'icona **Visualizza esclusioni** (🔍) per visualizzare la finestra di dialogo Avvisi esclusi o Eventi esclusi, selezionare le regole di esclusione da ripristinare, quindi fare clic sull'icona **Elimina** (🗑️).

Inoltro di dati di eventi, inventario e metrica

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

Informazioni su questa attività

Dati di eventi

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

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

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

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

Dati dell'inventario e degli eventi

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

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

Dati di metrica

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

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

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

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

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

Procedura

Per inoltrare i dati, completare le seguenti operazioni.

Passo 1. Creare una destinazione del server d'inoltro.

Le *destinazioni del server d'inoltro* sono configurazioni comuni che possono essere utilizzate da più server d'inoltro dei dati. La destinazione del server d'inoltro identifica la posizione in cui devono essere inviati i dati per un tipo specifico di server d'inoltro.

Passo 2. Creare filtri per eventi e risorse (solo per i server d'inoltro degli eventi).

È possibile assegnare *filtri di inoltro dei dati* comuni a più server d'inoltro dei dati. Questi filtri vengono utilizzati per definire criteri specifici per determinare quali eventi inoltrare per quali risorse.

Se non si assegnano filtri al server d'inoltro dei dati, tutti gli eventi per tutte le risorse vengono inoltrati alla destinazione del server d'inoltro selezionata.

Passo 3. Creare e abilitare un server d'inoltro dei dati.

È possibile creare e abilitare i server d'inoltro dei dati per inoltrare i dati degli eventi a un'applicazione esterna specifica. È necessario scegliere una destinazione del server d'inoltro applicabile al tipo di server d'inoltro che si sta creando.

Creazione di filtri di inoltro dei dati

È possibile definire comuni *filtri d'inoltro dei dati* che possono essere utilizzati da più server d'inoltro per attivare l'inoltro di dati che soddisfano criteri specifici.

Informazioni su questa attività

È possibile creare i seguenti tipi di filtri:


- *Filtri eventi* che inoltrano eventi corrispondenti a codici di eventi o proprietà specifiche (tra cui classi di eventi, gravità degli eventi e tipi di assistenza).
 - Tutti i codici e tutte le proprietà si applicano a tutte le origini evento.
 - Se nessuna proprietà delle classi è selezionata, vengono associate tutte le proprietà delle classi.
 - Se nessuna proprietà di manutenzione è selezionata, vengono associate tutte le proprietà di manutenzione.
 - Se nessuna proprietà di gravità è selezionata, vengono associate tutte le proprietà di gravità.
 - Se nessun codice evento viene specificato, vengono associati tutti i codici evento.
- *Filtri per risorsa* che inoltrano dati generati da risorse specifiche (XClarity Orchestrator, strumenti di gestione delle risorse e dispositivi). È possibile scegliere un sottoinsieme di risorse selezionando uno o più gruppi di risorse.
 - Se un tipo di risorsa è disabilitato, nessun dato di quel tipo di risorsa verrà inoltrato.
 - Se un tipo di risorsa è abilitato e nessun gruppo è selezionato, tutti i dati di quel tipo di risorsa vengono inoltrati.
 - Se un tipo di risorsa è abilitato e uno o più gruppi sono selezionati, vengono inoltrati solo i dati generati dalle risorse dei gruppi selezionati.

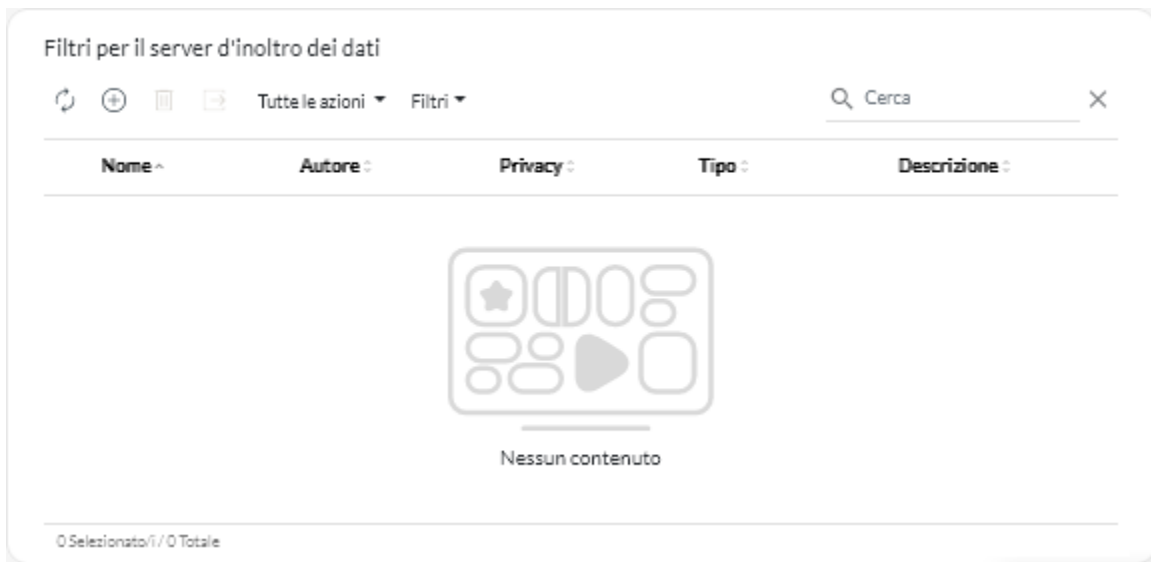
È possibile riutilizzare i filtri per risorse ed eventi in più server d'inoltro, ma è possibile aggiungere al massimo un filtro eventi e un filtro per risorsa a ciascun server d'inoltro.

Procedura

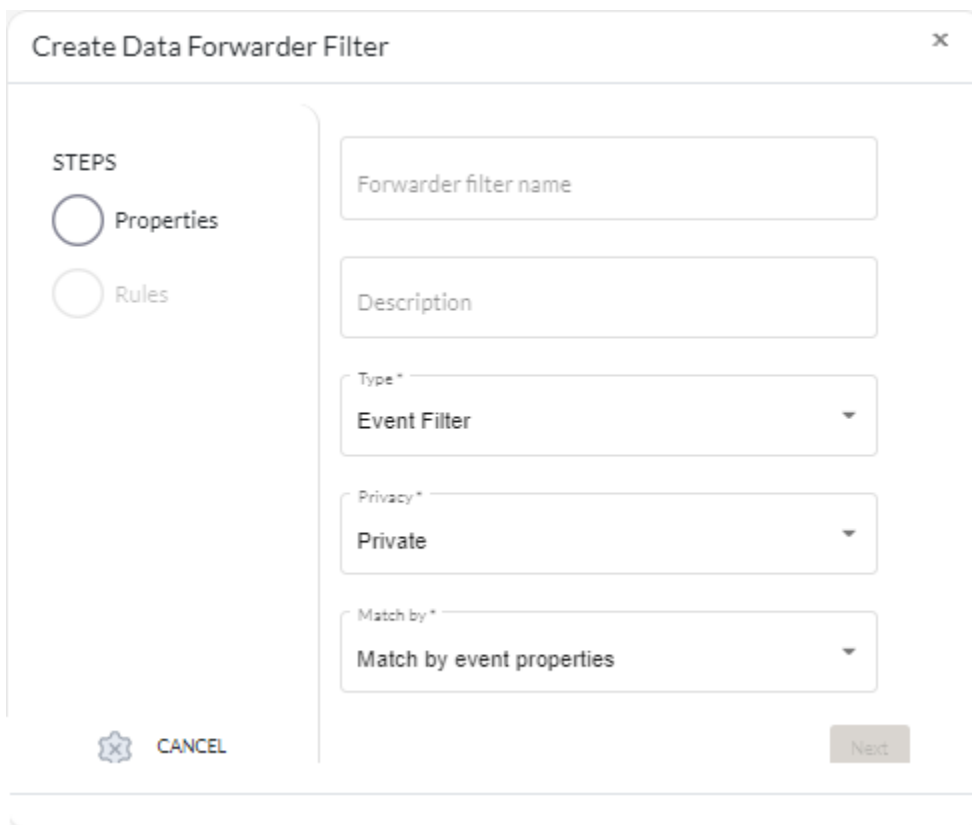
Per creare un filtro di inoltro dei dati, attenersi a una delle procedure che seguono a seconda del tipo di filtro che si desidera realizzare.

• Filtri eventi

1. Sulla barra dei menu di XClarity Orchestrator fare clic su **Monitoraggio**  → **Inoltro** e selezionare **Filtri per il server d'inoltro dei dati** nel riquadro di navigazione sinistro per visualizzare la scheda Filtri per il server d'inoltro dei dati.



2. Fare clic sull'icona **Crea** (+) per visualizzare la finestra di dialogo Crea filtro per il server d'inoltro dei dati.



3. Specificare il nome del filtro e la descrizione facoltativa.
4. Selezionare **Filtro eventi** come tipo di filtro.
5. Selezionare il tipo di privacy.
 - **Privato**. Solo l'utente che ha creato il filtro lo può utilizzare.
 - **Pubblico**. Qualsiasi utente può utilizzare il filtro.
6. Scegliere le proprietà evento o i codici evento come criteri per questo filtro.

7. Fare clic su **Regole** e selezionare i criteri per questo filtro in base al tipo di criteri selezionati nel passaggio precedente.
 - **Associa eventi per proprietà.** Selezionare uno o più proprietà di gravità, manutenzione e classe. Vengono inoltrati solo gli eventi che corrispondono a una proprietà selezionata. Ad esempio, se si scelgono gravità critiche e di avvertenza e classi di schede e memoria, i dati degli eventi verranno inoltrati solo per eventi di memoria di avvertenza, eventi di memoria critica, eventi di schede di avvertenza ed eventi di schede critiche, indipendentemente dall'intervento richiesto per l'evento. Se si seleziona solo l'intervento richiesto dall'utente, i dati degli eventi verranno inoltrati solo per gli eventi con interventi richiesti dall'utente, indipendentemente dalla gravità o dalla classe.

Nota:

- Se non si seleziona una proprietà delle classi, vengono associate tutte le proprietà delle classi.
 - Se non si seleziona una proprietà di manutenzione, vengono associate tutte le proprietà di manutenzione.
 - Se non si seleziona una proprietà di gravità, vengono associate tutte le proprietà di gravità.
- **Associa eventi per codice.** Immettere un codice evento che si desidera filtrare, quindi fare clic sull'icona **Aggiungi** (+) per aggiungere il codice evento all'elenco. Ripetere l'operazione per ogni codice evento che si desidera aggiungere. È possibile eliminare un codice evento facendo clic sull'icona **Elimina** (III) accanto al codice specifico. Solo gli eventi associati a uno dei codici evento elencati vengono inoltrati.

È possibile specificare un codice evento completo o parziale. Ad esempio, FQXXOCO0001I è associato all'evento specifico, FQXXOSE è associato a tutti gli eventi di sicurezza di XClarity Orchestrator e CO001 è associato a tutti gli eventi che contengono quei caratteri.

Se non viene specificato un codice evento, vengono associati tutti i codici evento.

Per un elenco dei codici evento disponibili, vedere [Messaggi di eventi e avvisi](#) nella documentazione online di XClarity Orchestrator.

8. Fare clic su **Crea** per creare il filtro. Il filtro viene aggiunto alla tabella.

• **Filtri per risorsa**

1. Sulla barra dei menu di XClarity Orchestrator fare clic su **Monitoraggio** (📧) → **Inoltro** e selezionare **Filtri per il server d'inoltro dei dati** nel riquadro di navigazione sinistro per visualizzare la scheda Filtri per il server d'inoltro dei dati.
2. Fare clic sull'icona **Crea** (+) per visualizzare la finestra di dialogo Crea filtro per il server d'inoltro dei dati.
3. Specificare il nome del filtro e la descrizione facoltativa.
4. Selezionare **Filtro per risorsa** come tipo di filtro.
5. Selezionare il tipo di privacy.
 - **Privato.** Solo l'utente che ha creato il filtro lo può utilizzare.
 - **Pubblico.** Qualsiasi utente può utilizzare il filtro.
6. Fare clic su **Risorse** e selezionare l'origine degli eventi per questo filtro.
 - **Associa qualsiasi evento di XClarity Orchestrator.** Inoltra gli eventi generati da questo XClarity Orchestrator. Questa opzione è disabilitata per impostazione predefinita.
 - **Associa a qualsiasi evento dello strumento di gestione delle risorse.** Inoltra gli eventi generati da uno strumento di gestione delle risorse. Questa opzione è disabilitata per impostazione predefinita.
 - Se si disabilita questa opzione, gli eventi non verranno inoltrati da alcun strumento di gestione delle risorse.
 - Se si abilita questa opzione, ma non si seleziona alcun gruppo di strumenti di gestione, vengono inoltrati gli eventi generati da tutti gli strumenti di gestione delle risorse.

- Se si abilita questa opzione e si seleziona uno o più gruppi di strumenti di gestione, vengono inoltrati solo gli eventi generati dagli strumenti di gestione delle risorse dei gruppi selezionati.

Suggerimento: è possibile creare gruppi di strumenti di gestione tramite questa scheda facendo clic sull'icona **Crea** (+).

- **Associa qualsiasi evento di dispositivo.** Inoltra gli eventi generati da un dispositivo. Questa opzione è abilitata per impostazione predefinita.
 - Se si disabilita questa opzione, gli eventi non verranno inoltrati da alcun dispositivo.
 - Se si abilita questa opzione, ma non si seleziona alcun gruppo di dispositivi, vengono inoltrati gli eventi generati da tutti i dispositivi.
 - Se si abilita questa opzione e si seleziona uno o più gruppi di dispositivi, vengono inoltrati gli eventi generati solo dai dispositivi dei gruppi selezionati.

Suggerimento: è possibile creare gruppi di dispositivi tramite questa scheda facendo clic sull'icona **Crea** (+).

7. Fare clic su **Crea** per creare il filtro. Il filtro viene aggiunto alla tabella.

Al termine

Nella scheda Filtri per il server d'inoltro dei dati è possibile effettuare la seguente operazione.

- Rimuovere un file selezionato facendo clic sull'icona **Elimina** (III). Non è possibile eliminare un filtro assegnato a un server d'inoltro.

Inoltro di eventi a SAP Data Intelligence

È possibile configurare Lenovo XClarity Orchestrator per inoltrare gli eventi a SAP Data Intelligence (Intelligent Insights).

Prima di iniziare

Attenzione: La connessione tra XClarity Orchestrator e SAP Data Intelligence utilizza il trasporto crittografato ma non verifica il certificato TLS del sistema remoto.

Informazioni su questa attività

Se il controllo degli accessi basato sulle risorse è abilitato, i dati vengono inoltrati solo per le risorse accessibili mediante gli elenchi di controllo degli accessi. Se non si è un membro di un gruppo a cui è assegnato il ruolo predefinito di **Supervisore**, è necessario assegnare uno o più elenchi di controllo degli accessi ai server d'inoltro creati. Se si desidera inviare i dati per tutte le risorse a cui è possibile accedere, selezionare tutti gli elenchi di controllo degli accessi associati disponibili. Se si è un membro di un gruppo a cui è assegnato il ruolo predefinito di **Supervisore**, è possibile scegliere di inviare i dati per tutte le risorse oppure di assegnare gli elenchi di controllo degli accessi per limitare le risorse.

Non è possibile filtrare i dati che vengono inoltrati a SAP Data Intelligence.

L'esempio che segue mostra il formato predefinito dei dati inoltrati a SAP Data Intelligence. Le parole tra parentesi quadre doppie sono attributi che vengono sostituiti con i valori effettivi quando i dati vengono inoltrati.

```
{ "msg": "[EventMessage]", "eventID": "[EventID]", "serialnum":
  "[EventSerialNumber]", "senderUUID": "[EventSenderUUID]", "flags":
  "[EventFlags]", "userid": "[EventUserName]", "localLogID":
  "[EventLocalLogID]", "systemName": "[DeviceFullPathName]", "action":
  "[EventActionNumber]", "failFRUNumbers": "[EventFailFRUs]", "severity":
  "[EventSeverityNumber]", "sourceID": "[EventSourceUUID]" }
```

```

\ "sourceLogSequence\":[[EventSourceLogSequenceNumber]],\ "failFRUSNs\":
\ "[[EventFailSerialNumbers]]\",\ "failFRUUUIDs\":\ "[[EventFailFRUUUIDs]]\",
\ "eventClass\":[[EventClassNumber]],\ "componentID\":[[EventComponentUUID]]\",
\ "mtm\":[[EventMachineTypeModel]]\",\ "msgID\":[[EventMessageID]]\",
"sequenceNumber\":[[EventSequenceID]]\",\ "timeStamp\":[[EventTimeStamp]]\",
\ "args\":[[EventMessageArguments]],\ "service\":[[EventServiceNumber]],
\ "commonEventID\":[[CommonEventID]]\",\ "eventDate\":[[EventDate]]\"}

```

Procedura

Per inoltrare dati degli eventi a SAP Data Intelligence, effettuare le operazioni che seguono.

- Passo 1. Dalla barra del menu di XClarity Orchestrator fare clic su **Monitoraggio** (📊) → **Inoltro eventi**, quindi su **Server d'inoltro dei dati** nel riquadro di navigazione sinistro per visualizzare la scheda Server d'inoltro dei dati.
- Passo 2. Fare clic sull'icona **Crea** (+) per visualizzare la finestra di dialogo Crea server d'inoltro dei dati.
- Passo 3. Specificare il nome del server d'inoltro e la descrizione facoltativa.
- Passo 4. Scegliere di abilitare o disabilitare il server d'inoltro facendo clic sull'opzione di attivazione/disattivazione **Stato**.
- Passo 5. Selezionare **Intelligent Insights** come tipo di server d'inoltro.
- Passo 6. Fare clic su **Configurazione** e immettere le informazioni specifiche del protocollo.
 - Immettere il nome host o l'indirizzo IP di SAP Data Intelligence.
 - Immettere la porta da utilizzare per l'inoltro di eventi. Il valore predefinito è 443.
 - Immettere il percorso della risorsa in cui il server d'inoltro pubblicherà gli eventi (ad esempio, /rest/test).
 - Selezionare il metodo REST. È possibile selezionare uno dei seguenti valori.
 - **PUT**
 - **POST**
 - Selezionare il protocollo da utilizzare per l'inoltro di eventi. È possibile selezionare uno dei seguenti valori.
 - **HTTP**
 - **HTTPS**
 - Immettere il periodo di timeout (in secondi) per la richiesta. Il valore predefinito è 30 secondi.
 - Se l'autenticazione è obbligatoria, selezionare uno dei tipi di autenticazione che seguono.
 - **Base**. Esegue l'autenticazione al server specificato utilizzando tenant, ID utente e password specificati.
 - **Token**. Esegue l'autenticazione al server specificato utilizzando il nome e il valore dell'intestazione del token.
- Passo 7. Fare clic su **Elenchi di controllo accessi** e selezionare uno o più elenchi di controllo degli accessi che si desidera associare a questo server d'inoltro.

Se l'accesso basato sulle risorse è abilitato, è necessario selezionare almeno un elenco di controllo degli accessi.

Suggerimento: gli utenti che sono membri di un gruppo a cui è assegnato il ruolo predefinito di **Supervisore** possono selezionare facoltativamente **Associa tutto** invece di selezionare gli elenchi di controllo degli accessi, in modo che i dati inoltrati non siano limitati.

- Passo 8. Fare clic su **Crea** per creare il server d'inoltro.

Al termine

Nella scheda Server d'inoltrato dei dati è possibile effettuare le operazioni che seguono.

- Abilitare o disabilitare un server d'inoltrato specifico selezionando l'interruttore nella colonna **Stato**.
- Modificare un server d'inoltrato selezionato facendo clic sull'icona **Modifica** (✎).
- Rimuovere un server d'inoltrato selezionato facendo clic sull'icona **Elimina** (🗑).

Inoltrato di eventi a un servizio Web REST

È possibile configurare Lenovo XClarity Orchestrator in modo che inoltri eventi specifici a un servizio Web REST.

Prima di iniziare

Attenzione: Non viene stabilita una connessione sicura durante l'inoltrato dei dati a questo servizio. I dati vengono inviati tramite un protocollo in testo semplice.

Informazioni su questa attività

Se il controllo degli accessi basato sulle risorse è abilitato, i dati vengono inoltrati solo per le risorse accessibili mediante gli elenchi di controllo degli accessi. Se non si è un membro di un gruppo a cui è assegnato il ruolo predefinito di **Supervisore**, è necessario assegnare uno o più elenchi di controllo degli accessi ai server d'inoltrato creati. Se si desidera inviare i dati per tutte le risorse a cui è possibile accedere, selezionare tutti gli elenchi di controllo degli accessi associati disponibili. Se si è un membro di un gruppo a cui è assegnato il ruolo predefinito di **Supervisore**, è possibile scegliere di inviare i dati per tutte le risorse oppure di assegnare gli elenchi di controllo degli accessi per limitare le risorse.

I comuni *filtri per i server d'inoltrato dei dati* vengono utilizzati per definire l'ambito degli eventi che si desidera inoltrare, in base ai codici, alle classi e alla gravità degli eventi, nonché ai tipi di servizio e alla risorsa che ha generato l'evento. Verificare che i filtri eventi e per risorsa da utilizzare per questo server d'inoltrato dei dati siano già stati creati (vedere [Creazione di filtri di inoltrato dei dati](#)).

L'esempio che segue mostra il formato predefinito dei dati inoltrati a un servizio Web REST. Le parole tra parentesi quadre doppie sono attributi che vengono sostituiti con i valori effettivi quando i dati vengono inoltrati.

```
{ "msg": "[EventMessage]", "eventID": "[EventID]", "serialnum": "[EventSerialNumber]", "senderUUID": "[EventSenderUUID]", "flags": "[EventFlags]", "userid": "[EventUserName]", "localLogID": "[EventLocalLogID]", "systemName": "[DeviceFullPathName]", "action": "[EventActionNumber]", "failFRUNumbers": "[EventFailFRUs]", "severity": "[EventSeverityNumber]", "sourceID": "[EventSourceUUID]", "sourceLogSequence": "[EventSourceLogSequenceNumber]", "failFRUSNs": "[EventFailSerialNumbers]", "failFRUUUIDs": "[EventFailFRUUUIDs]", "eventClass": "[EventClassNumber]", "componentID": "[EventComponentUUID]", "mtm": "[EventMachineTypeModel]", "msgID": "[EventMessageID]", "sequenceNumber": "[EventSequenceID]", "timeStamp": "[EventTimeStamp]", "args": "[EventMessageArguments]", "service": "[EventServiceNumber]", "commonEventID": "[CommonEventID]", "eventDate": "[EventDate]" }
```

Procedura

Per inoltrare dati a un servizio Web REST, effettuare le operazioni che seguono.

Passo 1. Dalla barra del menu di XClarity Orchestrator fare clic su **Monitoraggio** (📊) → **Inoltrato eventi**, quindi su **Server d'inoltrato dei dati** nel riquadro di navigazione sinistro per visualizzare la scheda Server d'inoltrato dei dati.

Passo 2. Fare clic sull'icona **Crea** (+) per visualizzare la finestra di dialogo Crea server d'inoltrato dei dati.

- Passo 3. Specificare il nome del server d'inoltro e la descrizione facoltativa.
- Passo 4. Scegliere di abilitare o disabilitare il server d'inoltro facendo clic sull'opzione di attivazione/disattivazione **Stato**.
- Passo 5. Selezionare **REST** come tipo di server d'inoltro.
- Passo 6. Fare clic su **Configurazione** e immettere le informazioni specifiche del protocollo.
- Immettere il nome host o l'indirizzo IP del server REST.
 - Immettere la porta da utilizzare per l'inoltro di eventi. Il valore predefinito è 80.
 - Immettere il percorso della risorsa in cui il server d'inoltro pubblicherà gli eventi (ad esempio, /rest/test).
 - Selezionare il metodo REST. È possibile selezionare uno dei seguenti valori.
 - **PUT**
 - **POST**
 - Selezionare il protocollo da utilizzare per l'inoltro di eventi. È possibile selezionare uno dei seguenti valori.
 - **HTTP**
 - **HTTPS**
 - Immettere il periodo di timeout (in secondi) per la richiesta. Il valore predefinito è 30 secondi.
 - Se l'autenticazione è obbligatoria, selezionare uno dei tipi di autenticazione che seguono.
 - **Base**. Esegue l'autenticazione server specificato utilizzando l'ID utente e la password specificati.
 - **Token**. Esegue l'autenticazione al server specificato utilizzando il nome e il valore dell'intestazione del token.

Passo 7. Fare clic su **Filtri** e, facoltativamente, selezionare i filtri da utilizzare per questo server d'inoltro.

È possibile selezionare al massimo un filtro eventi e un filtro per risorsa.

Se non si seleziona un filtro, i dati vengono inoltrati per tutti gli eventi generati da tutte le risorse (dispositivi, strumenti di gestione delle risorse e XClarity Orchestrator).

Da questa scheda è anche possibile scegliere di inoltrare l'evento escluso impostando l'interruttore **Eventi esclusi** su **Sì**.

Passo 8. Fare clic su **Elenchi di controllo accessi** e selezionare uno o più elenchi di controllo degli accessi che si desidera associare a questo server d'inoltro.

Se l'accesso basato sulle risorse è abilitato, è necessario selezionare almeno un elenco di controllo degli accessi.

Suggerimento: gli utenti che sono membri di un gruppo a cui è assegnato il ruolo predefinito di **Supervisore** possono selezionare facoltativamente **Associa tutto** invece di selezionare gli elenchi di controllo degli accessi, in modo che i dati inoltrati non siano limitati.

Passo 9. Fare clic su **Crea** per creare il server d'inoltro.

Al termine

Nella scheda Server d'inoltro dei dati è possibile effettuare le operazioni che seguono.

- Abilitare o disabilitare un server d'inoltro specifico selezionando l'interruttore nella colonna **Stato**.
- Modificare un server d'inoltro selezionato facendo clic sull'icona **Modifica** (✎).
- Rimuovere un server d'inoltro selezionato facendo clic sull'icona **Elimina** (🗑).

Inoltro di eventi a un servizio e-mail tramite SMTP

È possibile configurare Lenovo XClarity Orchestrator affinché inoltri eventi specifici a uno o più indirizzi e-mail tramite SMTP.

Prima di iniziare

Attenzione: Non viene stabilita una connessione sicura durante l'inoltro dei dati a questo servizio. I dati vengono inviati tramite un protocollo in testo semplice.

Per inoltrare l'e-mail a un servizio e-mail basato sul Web (ad esempio Gmail, Hotmail o Yahoo), il server SMTP deve supportare l'inoltro della posta elettronica Web.

Prima di configurare un server d'inoltro degli eventi a un servizio Web di Gmail, consultare le informazioni in [Inoltro di eventi a un servizio SMTP di Gmail](#).

Informazioni su questa attività

Se il controllo degli accessi basato sulle risorse è abilitato, i dati vengono inoltrati solo per le risorse accessibili mediante gli elenchi di controllo degli accessi. Se non si è un membro di un gruppo a cui è assegnato il ruolo predefinito di **Supervisore**, è necessario assegnare uno o più elenchi di controllo degli accessi ai server d'inoltro creati. Se si desidera inviare i dati per tutte le risorse a cui è possibile accedere, selezionare tutti gli elenchi di controllo degli accessi associati disponibili. Se si è un membro di un gruppo a cui è assegnato il ruolo predefinito di **Supervisore**, è possibile scegliere di inviare i dati per tutte le risorse oppure di assegnare gli elenchi di controllo degli accessi per limitare le risorse.

I comuni *filtri per i server d'inoltro dei dati* vengono utilizzati per definire l'ambito degli eventi che si desidera inoltrare, in base ai codici, alle classi e alla gravità degli eventi, nonché ai tipi di servizio e alla risorsa che ha generato l'evento. Verificare che i filtri eventi e per risorsa da utilizzare per questo server d'inoltro dei dati siano già stati creati (vedere [Creazione di filtri di inoltro dei dati](#)).

L'esempio che segue mostra il formato predefinito dei dati inoltrati a un servizio e-mail. Le parole tra parentesi quadre doppie sono attributi che vengono sostituiti con i valori effettivi quando i dati vengono inoltrati.

Oggetto dell'e-mail

Event Forwarding

Corpo dell'e-mail

```
{
  "groups": [],
  "acls": [],
  "local": null,
  "eventID": "FQXHMEM02161",
  "severity": "Warning",
  "sourceID": "FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF",
  "componentID": "FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF",
  "msg": "The event forwarder destination cannot be reached. Therefore new events are not being
        forwarded.",
  "description": "The event forwarder destination cannot be reached. Therefore new events are not
                being forwarded.",
  "userAction": "Look in the online documentation to determinate more information about this event
                based on the eventID. At the moment the orchestrator server can not offer more
                information.",
  "recoveryURL": null,
  "flags": [],
  "userid": null,
  "action": "None",
```





```

"eventClass": "System",
"args": [],
"service": "None",
"lxcaUUID": "23C87F0A2CB6491097489193447A655C",
"managerID": "23C87F0A2CB6491097489193447A655C",
"failFRUNumbers": null,
"failFRUSNs": null,
"failFRUUUIDs": "[FFFFFFFFFFFFFFFFFFFFFFFFFFFFFFFF]",
"msgID": null,
"timestamp": "2021-03-12T18:32:14.000Z",
"eventDate": "2021-03-12T18:32:14Z",
"commonEventID": "FQXHEM0216I",
"sequenceNumber": "17934247",
"details": null,
"device": {
  "name": "xhmc194.labs.lenovo.com",
  "mtm": null,
  "serialNumber": null
},
"resourceType": "XClarity Administrator",
"componentType": "XClarity Administrator",
"sourceType": "Management",
"resourceName": "xhmc194.labs.lenovo.com",
"fruType": "other",
"ipAddress": "10.243.2.107",
"_id": 252349
}

```

Procedura

Per inoltrare dati a un servizio e-mail tramite SMTP, effettuare le operazioni che seguono.

- Passo 1. Dalla barra del menu di XClarity Orchestrator fare clic su **Monitoraggio**  → **Inoltro eventi**, quindi su **Server d'inoltro dei dati** nel riquadro di navigazione sinistro per visualizzare la scheda Server d'inoltro dei dati.
- Passo 2. Fare clic sull'icona **Crea**  per visualizzare la finestra di dialogo Crea server d'inoltro dei dati.
- Passo 3. Specificare il nome del server d'inoltro e la descrizione facoltativa.
- Passo 4. Scegliere di abilitare o disabilitare il server d'inoltro facendo clic sull'opzione di attivazione/disattivazione **Stato**.
- Passo 5. Selezionare **E-mail** come tipo di server d'inoltro.
- Passo 6. Fare clic su **Configurazione** e immettere le informazioni specifiche del protocollo.
 - Immettere il nome host o l'indirizzo IP del server SMTP.
 - Immettere la porta da utilizzare per l'inoltro di eventi. Il valore predefinito è 25.
 - Immettere il periodo di timeout (in secondi) per la richiesta. Il valore predefinito è 30 secondi.
 - Immettere l'indirizzo e-mail per ciascun destinatario. Separare gli indirizzi e-mail con una virgola.
 - **Facoltativo:** immettere l'indirizzo e-mail del mittente dell'e-mail (ad esempio, john@company.com) e il dominio del server. Se non viene specificato un indirizzo e-mail, l'indirizzo del mittente è `LXCO.<source_identifier>@<smtp_host>` per impostazione predefinita.

Se viene specificato solo il dominio del mittente, il formato dell'indirizzo del mittente è `<LXCO_host_name>@<sender_domain>` (ad esempio, XClarity1@company.com).

Nota:

- Se si configura un server SMTP affinché richieda un nome host per l'inoltro delle e-mail e non si configura un nome host per XClarity Orchestrator, è possibile che il server SMTP rifiuti gli eventi inoltrati. Se XClarity Orchestrator non dispone di un nome host, l'evento viene inoltrato con l'indirizzo IP. Se l'indirizzo IP non può essere ottenuto, verrà inviato "localhost". Ciò potrebbe far sì che il server SMTP rifiuti l'evento.
- Se viene specificato il dominio del mittente, la fonte non si identifica nell'indirizzo del mittente. Vengono, invece, incluse le informazioni sulla fonte dell'evento nel corpo dell'e-mail, tra cui il nome di sistema, l'indirizzo IP, il tipo o il modello e il numero di serie.
- Se il server SMTP accetta solo le e-mail inviate da un utente registrato, l'indirizzo predefinito del mittente (`LXC0.<source_identifier>@{smtp_host}`) viene rifiutato. In questo caso, è necessario specificare almeno un nome di dominio nel campo **Da utente**.
- Per stabilire una connessione protetta al server SMTP, selezionare uno dei tipi di connessione che seguono.
 - **SSL**. Utilizzare il protocollo SSL per creare una comunicazione protetta.
 - **STARTTLS**. Utilizzare il protocollo TLS per formare una comunicazione protetta su un canale non protetto.

Se viene selezionato uno di questi tipi di connessione, XClarity Orchestrator tenta di scaricare e importare il certificato del server SMTP nell'archivio attendibile XClarity Orchestrator. Viene chiesto di accettare il certificato.
- Se l'autenticazione è obbligatoria, selezionare uno dei tipi di autenticazione che seguono.
 - **Regolare**. Esegue l'autenticazione server SMTP specificato utilizzando l'ID utente e la password specificati.
 - **OAUTH2**. Utilizza il protocollo Simple Authentication and Security Layer (SASL) per eseguire l'autenticazione al server SMTP specificato utilizzando il nome utente e il token di sicurezza specificati. Generalmente, il nome utente è l'indirizzo e-mail.

Attenzione: il token di sicurezza scade dopo un breve periodo di tempo. L'aggiornamento del token di sicurezza è responsabilità dell'utente.

 - **Nessuna**. Non viene utilizzata nessuna autenticazione.

Passo 7. Fare clic su **Filtri** e, facoltativamente, selezionare i filtri da utilizzare per questo server d'inoltro.

È possibile selezionare al massimo un filtro eventi e un filtro per risorsa.

Se non si seleziona un filtro, i dati vengono inoltrati per tutti gli eventi generati da tutte le risorse (dispositivi, strumenti di gestione delle risorse e XClarity Orchestrator).

Da questa scheda è anche possibile scegliere di inoltrare l'evento escluso impostando l'interruttore **Eventi esclusi** su **Sì**.

Passo 8. Fare clic su **Elenchi di controllo accessi** e selezionare uno o più elenchi di controllo degli accessi che si desidera associare a questo server d'inoltro.

Se l'accesso basato sulle risorse è abilitato, è necessario selezionare almeno un elenco di controllo degli accessi.

Suggerimento: gli utenti che sono membri di un gruppo a cui è assegnato il ruolo predefinito di **Supervisore** possono selezionare facoltativamente **Associa tutto** invece di selezionare gli elenchi di controllo degli accessi, in modo che i dati inoltrati non siano limitati.

Passo 9. Fare clic su **Crea** per creare il server d'inoltro.

Al termine

Nella scheda Server d'inoltro dei dati è possibile effettuare le operazioni che seguono.

- Abilitare o disabilitare un server d'inoltro specifico selezionando l'interruttore nella colonna **Stato**.
- Modificare un server d'inoltro selezionato facendo clic sull'icona **Modifica** (✎).
- Rimuovere un server d'inoltro selezionato facendo clic sull'icona **Elimina** (🗑).

Inoltro di eventi a un servizio SMTP di Gmail

È possibile configurare Lenovo XClarity Orchestrator affinché inoltri eventi a un servizio e-mail basato su Web, come ad esempio Gmail.

Utilizzare i seguenti esempi di configurazione per impostare il server d'inoltro degli eventi affinché utilizzi il servizio SMTP di Gmail.

Nota: Gmail consiglia di utilizzare il metodo di autenticazione OAUTH2 per comunicazioni più sicure. Se si sceglie di utilizzare l'autenticazione regolare, verrà inviata un'e-mail per indicare che un'applicazione ha tentato di utilizzare l'account senza gli standard di sicurezza più recenti. Il messaggio include le istruzioni per la configurazione dell'account e-mail affinché accetti questi tipi di applicazioni.

Per informazioni sulla configurazione di un server SMTP di Gmail, vedere <https://support.google.com/a/answer/176600?hl=en>.

Autenticazione regolare mediante SSL sulla porta 465

Questo esempio comunica con il server SMTP di Gmail tramite il protocollo SSL sulla porta 465 ed esegue l'autenticazione mediante un account utente e una password Gmail validi.

Parametro	Valore
Host	smtp.gmail.com
Porta	465
SSL	Seleziona
STARTTLS	Cancella
Autenticazione	Regolare
Utente	Indirizzo e-mail Gmail valido
Password	Password di autenticazione Gmail
Indirizzo di provenienza	(facoltativo)

Autenticazione regolare mediante TLS sulla porta 587

Questo esempio comunica con il server SMTP di Gmail tramite il protocollo TLS sulla porta 587 ed esegue l'autenticazione mediante un account utente e una password Gmail validi.

Parametro	Valore
Host	smtp.gmail.com
Porta	587
SSL	Cancella
STARTTLS	Seleziona
Autenticazione	Regolare
Utente	Indirizzo e-mail Gmail valido

Parametro	Valore
Password	Password di autenticazione Gmail
Indirizzo di provenienza	(facoltativo)

Autenticazione OAUTH2 mediante TLS sulla porta 587

Questo esempio comunica con il server SMTP di Gmail tramite il protocollo TLS sulla porta 587 ed esegue l'autenticazione mediante un account utente e un token di sicurezza Gmail validi.

Utilizzare la seguente procedura di esempio per ottenere il token di sicurezza.

1. Creare un progetto in Google Developers Console e recuperare l'ID e il client secret. Per ulteriori informazioni, visitare il sito Web [Pagina Web per l'accesso di Google ai siti Web](#).
 - a. Da un browser Web, aprire la [Pagina Web delle API Google](#).
 - b. Dal menu di quella pagina Web, fare clic su **Seleziona un progetto → Crea progetto**. Viene visualizzata la finestra di dialogo Nuovo progetto.
 - c. Immettere un nome, selezionare **Sì** per accettare l'accordo di licenza e fare clic su **Crea**.
 - d. Nella scheda **Panoramica** utilizzare il campo di ricerca per cercare "gmail". Fare clic su **GMAIL API** nei risultati della ricerca.
 - e. Fare clic su **Abilita**.
 - f. Fare clic sulla scheda **Credenziali**.
 - g. Fare clic su **Schermata consenso OAuth**.
 - h. Immettere un nome nel campo **Nome del prodotto visualizzato dagli utenti** e fare clic su **Salva**.
 - i. Fare clic su **Crea credenziali → ID client OAuth**.
 - j. Selezionare **Altro** e immettere un nome.
 - k. Fare clic su **Crea**. Viene visualizzata la finestra di dialogo Client OAuth con l'ID e il segreto client.
 - l. Prendere nota dell'ID e del segreto client per utilizzarli in futuro.
 - m. Fare clic su **OK** per chiudere la finestra di dialogo.
2. Utilizzare lo script Python [oauth2.py](#) per generare e autorizzare un token di sicurezza fornendo l'ID e il segreto client generato al momento della creazione del progetto.

Nota: per completare questa operazione è necessario Python versione 2.7. È possibile scaricare ed installare Python 2.7 dal [Sito Web di Python](#).

- a. Da un browser Web, aprire la [Pagina Web gmail-oauth2-tools](#).
- b. Fare clic su **Non elaborato** e salvare il contenuto in un file denominato `oauth2.py` sul sistema locale.
- c. Eseguire il seguente comando come terminale (Linux) o come riga di comando (Windows):

```
py oauth2.py --user={your_email} --client_id={client_id}
--client_secret={client_secret} --generate_oauth2_token
```

Ad esempio

```
py oauth2.py --user=jon@gmail.com
--client_id=884243132302-458elfqjiebpuvdmvdackp6elip8kl63.apps.googleusercontent.com
--client_secret=3tnyXgEiBibT2m00zqnlTszk --generate_oauth2_token
```

Questo comando restituisce un URL da utilizzare per autorizzare il token e per recuperare un codice di verifica dal sito Web di Google, ad esempio:

To authorize token, visit this url and follow the directions:

```
https://accounts.google.com/o/oauth2/auth?client_id=884243132302
-458elfqjiebpuvdmvdackp6elip8kl63.apps.googleusercontent.com&redirect_uri=
urn%3Aietf%3Aawg%3Aoauth%3A2.0%3Aob&response_type=code&scope=https%3A%2F%2Fmail.
```

google.com%2F

Enter verification code:

- d. Da un browser Web, aprire l'URL che è stato restituito nel passaggio precedente.
- e. Fare clic su **Consenti** per accettare questo servizio. Viene restituito un codice di verifica.
- f. Immettere il codice di verifica nel comando `oauth2.py`. Il comando restituisce il token di sicurezza e aggiorna il token, ad esempio:
Refresh Token: 1/K8lPGx6UQQajj7tQGyKq8mVG8LVvGIVzHqzxFIMeYEQMEudVrK5jSpoR30zcRFq6
Access Token: ya29.CjHXAsyoH9GuCZutgIOxm1SGSqKrUkjIoH14SGMnljZ6rwp3gZmK7SrGDPCQx_KN-34f
Access Token Expiration Seconds: 3600

Importante: il token di sicurezza scade dopo un periodo di tempo. È possibile utilizzare lo script Python `oauth2.py` e il token di aggiornamento per generare un nuovo token di sicurezza. La generazione del nuovo token di sicurezza e l'aggiornamento del server di inoltro degli eventi tramite il nuovo token in Lenovo XClarity Orchestrator è responsabilità dell'utente.

3. Dall'interfaccia Web di Lenovo XClarity Orchestrator configurare il server di inoltro degli eventi per e-mail utilizzando gli attributi che seguono.

Parametro	Valore
Host	smtp.gmail.com
Porta	587
SSL	Cancela
STARTTLS	Seleziona
Autenticazione	OAuth2
Utente	Indirizzo e-mail Gmail valido
Token	Token di sicurezza
Indirizzo di provenienza	(facoltativo)

Inoltro di inventario ed eventi a Splunk

È possibile configurare Lenovo XClarity Orchestrator per inoltrare inventario ed eventi in un formato predefinito a un'applicazione Splunk. È quindi possibile utilizzare Splunk per creare grafici e diagrammi in base ai dati per analizzare le condizioni e prevedere i problemi nell'ambiente.

Prima di iniziare

Attenzione: Non viene stabilita una connessione sicura durante l'inoltro dei dati a questo servizio. I dati vengono inviati tramite un protocollo in testo semplice.

Informazioni su questa attività

Splunk è uno strumento per gli operatori di data center che permette di monitorare e analizzare i log eventi e gli altri dati. Lenovo fornisce un'app XClarity Orchestrator per Splunk che analizza gli eventi inoltrati da XClarity Orchestrator e presenta l'analisi in una serie di dashboard. In questa app è possibile monitorare i dashboard per individuare potenziali problemi dell'ambiente utilizzato, in modo da agire prima che si verifichino problemi gravi. Per ulteriori informazioni, consultare la [Guida per l'utente dell'app XClarity Orchestrator per Splunk](#) nella documentazione online di XClarity Orchestrator.



È possibile definire più configurazioni Splunk, ma XClarity Orchestrator può inoltrare gli eventi a una sola istanza di Splunk. Pertanto, è possibile abilitare solo una configurazione Splunk alla volta.

Se il controllo degli accessi basato sulle risorse è abilitato, i dati vengono inoltrati solo per le risorse accessibili mediante gli elenchi di controllo degli accessi. Se non si è un membro di un gruppo a cui è assegnato il ruolo predefinito di **Supervisore**, è necessario assegnare uno o più elenchi di controllo degli accessi ai server d'inoltro creati. Se si desidera inviare i dati per tutte le risorse a cui è possibile accedere, selezionare tutti gli elenchi di controllo degli accessi associati disponibili. Se si è un membro di un gruppo a cui è assegnato il ruolo predefinito di **Supervisore**, è possibile scegliere di inviare i dati per tutte le risorse oppure di assegnare gli elenchi di controllo degli accessi per limitare le risorse.

Non è possibile filtrare i dati inoltrati alle applicazioni Splunk.

Procedura

Per inoltrare dati di inventario ed eventi a un'applicazione Splunk, effettuare le operazioni che seguono.

- Passo 1. Dalla barra del menu di XClarity Orchestrator fare clic su **Monitoraggio**  → **Inoltro eventi**, quindi su **Server d'inoltro dei dati** nel riquadro di navigazione sinistro per visualizzare la scheda Server d'inoltro dei dati.
- Passo 2. Fare clic sull'icona **Crea**  per visualizzare la finestra di dialogo Crea server d'inoltro dei dati.
- Passo 3. Specificare il nome del server d'inoltro e la descrizione facoltativa.
- Passo 4. Scegliere di abilitare o disabilitare il server d'inoltro facendo clic sull'opzione di attivazione/disattivazione **Stato**.
- Passo 5. Selezionare **Splunk** come tipo di server d'inoltro.
- Passo 6. Fare clic su **Configurazione** e immettere le informazioni specifiche del protocollo.
 - Immettere il nome host o l'indirizzo IP dell'applicazione Splunk.
 - Specificare l'account utente e la password da utilizzare per eseguire il login al servizio Splunk.
 - Specificare l'API REST e i numeri di porta dati da utilizzare per connettersi al servizio Splunk.
 - Specificare uno o più indici dello strumento di raccolta degli eventi HTTP. L'indice predefinito è **lxco**.
 - Immettere il periodo di timeout (in secondi) per la richiesta. Il valore predefinito è 30 secondi.
- Passo 7. Fare clic su **Elenchi di controllo accessi** e selezionare uno o più elenchi di controllo degli accessi che si desidera associare a questo server d'inoltro.



Se l'accesso basato sulle risorse è abilitato, è necessario selezionare almeno un elenco di controllo degli accessi.

Suggerimento: gli utenti che sono membri di un gruppo a cui è assegnato il ruolo predefinito di **Supervisore** possono selezionare facoltativamente **Associa tutto** invece di selezionare gli elenchi di controllo degli accessi, in modo che i dati inoltrati non siano limitati.

- Passo 8. Fare clic su **Crea** per creare il server d'inoltro.

Al termine

Nella scheda Server d'inoltro dei dati è possibile effettuare le operazioni che seguono.

- Abilitare o disabilitare un server d'inoltro specifico selezionando l'interruttore nella colonna **Stato**.
- Modificare un server d'inoltro selezionato facendo clic sull'icona **Modifica** .
- Rimuovere un server d'inoltro selezionato facendo clic sull'icona **Elimina** .

Inoltro di eventi a un syslog

È possibile configurare Lenovo XClarity Orchestrator in modo che inoltri eventi specifici a un syslog.

Prima di iniziare

Attenzione: Non viene stabilita una connessione sicura durante l'inoltro dei dati a questo servizio. I dati vengono inviati tramite un protocollo in testo semplice.

Informazioni su questa attività

Se il controllo degli accessi basato sulle risorse è abilitato, i dati vengono inoltrati solo per le risorse accessibili mediante gli elenchi di controllo degli accessi. Se non si è un membro di un gruppo a cui è assegnato il ruolo predefinito di **Supervisore**, è necessario assegnare uno o più elenchi di controllo degli accessi ai server d'inoltro creati. Se si desidera inviare i dati per tutte le risorse a cui è possibile accedere, selezionare tutti gli elenchi di controllo degli accessi associati disponibili. Se si è un membro di un gruppo a cui è assegnato il ruolo predefinito di **Supervisore**, è possibile scegliere di inviare i dati per tutte le risorse oppure di assegnare gli elenchi di controllo degli accessi per limitare le risorse.

I comuni *filtri per i server d'inoltro dei dati* vengono utilizzati per definire l'ambito degli eventi che si desidera inoltrare, in base ai codici, alle classi e alla gravità degli eventi, nonché ai tipi di servizio e alla risorsa che ha generato l'evento. Verificare che i filtri eventi e per risorsa da utilizzare per questo server d'inoltro dei dati siano già stati creati (vedere [Creazione di filtri di inoltro dei dati](#)).

L'esempio che segue mostra il formato predefinito dei dati inoltrati a un syslog. Le parole tra parentesi quadre doppie sono attributi che vengono sostituiti con i valori effettivi quando i dati vengono inoltrati.

```
{
  "appl": "LXCO",
  "groups": [],
  "acls": [],
  "local": null,
  "eventID": "FQXMEM0216I",
  "severity": "Warning",
  "sourceID": "FFFFFFFFFFFFFFFFFFFFFFFF",
  "componentID": "FFFFFFFFFFFFFFFFFFFFFFFF",
  "msg": "The event forwarder destination cannot be reached. Therefore new events are not being
        forwarded.",
  "description": "The event forwarder destination cannot be reached. Therefore new events are not
                 being forwarded.",
  "userAction": "Look in the online documentation to determinate more information about this event
                based on the eventID. At the moment the orchestrator server can not offer more
                information.",
  "recoveryURL": null,
  "flags": [],
  "userid": null,
  "action": "None",
  "eventClass": "System",
  "args": [],
  "service": "None",
  "lxcaUUID": "23C87F0A2CB6491097489193447A655C",
  "managerID": "23C87F0A2CB6491097489193447A655C",
  "failFRUNumbers": null,
  "failFRUSNs": null,
  "failFRUUUIDs": "[FFFFFFFFFFFFFFFFFFFFFFFF]",
  "msgID": null,
  "timeStamp": "2021-03-12T18:32:14.000Z",
  "eventDate": "2021-03-12T18:32:14Z",
  "commonEventID": "FQXMEM0216I",
  "sequenceNumber": "17934247",
  "details": null,
  "device": {
    "name": "xhmc194.labs.lenovo.com",
    "mtm": null,
  }
}
```

```

    "serialNumber": null
  },
  "resourceType": "XClarity Administrator",
  "componentType": "XClarity Administrator",
  "sourceType": "Management",
  "resourceName": "xhmc194.labs.lenovo.com",
  "fruType": "other",
  "ipAddress": "10.243.2.107",
  "_id": 252349
}

```

Procedura

Per inoltrare dati a syslog, effettuare le operazioni che seguono.

Passo 1. Dalla barra del menu di XClarity Orchestrator fare clic su **Monitoraggio** (📊) → **Inoltro eventi**, quindi su **Server d'inoltro dei dati** nel riquadro di navigazione sinistro per visualizzare la scheda Server d'inoltro dei dati.

Passo 2. Fare clic sull'icona **Crea** (+) per visualizzare la finestra di dialogo Crea server d'inoltro dei dati.

Passo 3. Specificare il nome del server d'inoltro e la descrizione facoltativa.

Passo 4. Scegliere di abilitare o disabilitare il server d'inoltro facendo clic sull'opzione di attivazione/disattivazione **Stato**.

Passo 5. Selezionare **Syslog** come tipo di server d'inoltro.

Passo 6. Fare clic su **Configurazione** e immettere le informazioni specifiche del protocollo.

- Immettere il nome host o l'indirizzo IP del syslog.
- Immettere la porta da utilizzare per l'inoltro di eventi. Il valore predefinito è 514.
- Selezionare il protocollo da utilizzare per l'inoltro di eventi. È possibile selezionare uno dei seguenti valori.
 - **UDP**
 - **TCP**
- Immettere il periodo di timeout (in secondi) per la richiesta. Il valore predefinito è 30 secondi.
- **Facoltativo:** selezionare il formato di data/ora del syslog. È possibile selezionare uno dei seguenti valori.
 - **Ora locale.** Il formato predefinito, ad esempio Fri Mar 31 05:57:18 EDT 2017.
 - **Ora GMT.** Standard internazionale (ISO8601) per la data e l'ora, ad esempio 2017-03-31T05:58:20-04:00.

Passo 7. Fare clic su **Filtri** e, facoltativamente, selezionare i filtri da utilizzare per questo server d'inoltro.

È possibile selezionare al massimo un filtro eventi e un filtro per risorsa.

Se non si seleziona un filtro, i dati vengono inoltrati per tutti gli eventi generati da tutte le risorse (dispositivi, strumenti di gestione delle risorse e XClarity Orchestrator).

Da questa scheda è anche possibile scegliere di inoltrare l'evento escluso impostando l'interruttore **Eventi esclusi** su **Sì**.

Passo 8. Fare clic su **Elenchi di controllo accessi** e selezionare uno o più elenchi di controllo degli accessi che si desidera associare a questo server d'inoltro.

Se l'accesso basato sulle risorse è abilitato, è necessario selezionare almeno un elenco di controllo degli accessi.

Suggerimento: gli utenti che sono membri di un gruppo a cui è assegnato il ruolo predefinito di **Supervisore** possono selezionare facoltativamente **Associa tutto** invece di selezionare gli elenchi di controllo degli accesso, in modo che i dati inoltrati non siano limitati.

Passo 9. Fare clic su **Crea** per creare il server d'inoltro.

Al termine

Nella scheda Server d'inoltro dei dati è possibile effettuare le operazioni che seguono.

- Abilitare o disabilitare un server d'inoltro specifico selezionando l'interruttore nella colonna **Stato**.
- Modificare un server d'inoltro selezionato facendo clic sull'icona **Modifica** (✎).
- Rimuovere un server d'inoltro selezionato facendo clic sull'icona **Elimina** (🗑).

Inoltro dei dati di metrica a Lenovo TruScale Infrastructure Services

È possibile configurare Lenovo XClarity Orchestrator in modo che inoltri i dati di metrica (telemetria) a Lenovo TruScale Infrastructure Services.

Prima di iniziare

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

Attenzione: Queste operazioni di configurazione sono destinate solo ai tecnici dell'assistenza Lenovo.

Non viene stabilita una connessione sicura durante l'inoltro dei dati a TruScale Infrastructure Services.

Verificare che sia in esecuzione XClarity Orchestrator v1.2.0 o versioni successive.

Assicurarsi che gli strumenti di gestione delle risorse di Lenovo XClarity Administrator che gestiscono i dispositivi per cui si desidera inoltrare i dati delle metriche stiano eseguendo la versione 3.0.0 con il pacchetto di correzione o versioni successive.

Accertarsi che gli strumenti di gestione delle risorse appropriati di XClarity Administrator siano collegati a XClarity Orchestrator (vedere [Connessione degli strumenti di gestione delle risorse](#)).

Verificare che i dispositivi per cui si desidera inoltrare i dati delle metriche stiano eseguendo il firmware più recente di Lenovo XClarity Controller (vedere [Applicazione e attivazione degli aggiornamenti agli strumenti di gestione delle risorse](#)).

Verificare che le impostazioni di data e ora siano configurate correttamente nelle seguenti risorse.

- XClarity Orchestrator (vedere [Configurazione di data e ora](#))
- Strumento di gestione delle risorse di XClarity Administrator (vedere [Impostazione di data e ora](#) nella documentazione online di XClarity Administrator)
- Controller di gestione della scheda di base di ciascun dispositivo (vedere [Impostazione di data e ora di XClarity Controller](#) nella documentazione online di Lenovo XClarity Controller)

Verificare che le impostazioni di rete in XClarity Orchestrator siano configurate correttamente.

Verificare che i dati delle metriche vengano raccolti per i dispositivi gestiti, visualizzando i grafici sull'utilizzo nella pagina di riepilogo dei dispositivi (vedere [Visualizzazione dei dettagli dei dispositivi](#)). Se i dati delle metriche non vengono visualizzati, vedere [Risoluzione dei problemi di inoltro dei dati](#).

Per ulteriori informazioni su Lenovo TruScale Infrastructure Services, vedere [Sito Web di TruScale Infrastructure Services](#).

Informazioni su questa attività

È possibile definire più configurazioni Lenovo TruScale Infrastructure Services, ma XClarity Orchestrator può inoltrare gli eventi a una sola istanza di Lenovo TruScale Infrastructure Services. Pertanto, è possibile abilitare solo una configurazione Lenovo TruScale Infrastructure Services alla volta.

Se il controllo degli accessi basato sulle risorse è abilitato, i dati vengono inoltrati solo per le risorse accessibili mediante gli elenchi di controllo degli accessi. Se non si è un membro di un gruppo a cui è assegnato il ruolo predefinito di **Supervisore**, è necessario assegnare uno o più elenchi di controllo degli accessi ai server d'inoltro creati. Se si desidera inviare i dati per tutte le risorse a cui è possibile accedere, selezionare tutti gli elenchi di controllo degli accessi associati disponibili. Se si è un membro di un gruppo a cui è assegnato il ruolo predefinito di **Supervisore**, è possibile scegliere di inviare i dati per tutte le risorse oppure di assegnare gli elenchi di controllo degli accessi per limitare le risorse.

Non è possibile filtrare i dati inoltrati a Lenovo TruScale Infrastructure Services.

L'esempio che segue mostra il formato predefinito dei dati inoltrati a Lenovo TruScale Infrastructure Services. Le parole tra parentesi quadre doppie sono attributi che vengono sostituiti con i valori effettivi quando i dati vengono inoltrati.

```
{ "msg": "[EventMessage]", "eventID": "[EventID]", "serialnum": "[EventSerialNumber]", "senderUUID": "[EventSenderUUID]", "flags": "[EventFlags]", "userid": "[EventUserName]", "localLogID": "[EventLocalLogID]", "systemName": "[DeviceFullPathName]", "action": "[EventActionNumber]", "failFRUNumbers": "[EventFailFRUs]", "severity": "[EventSeverityNumber]", "sourceID": "[EventSourceUUID]", "sourceLogSequence": "[EventSourceLogSequenceNumber]", "failFRUSNs": "[EventFailSerialNumbers]", "failFRUUIDs": "[EventFailFRUUIDs]", "eventClass": "[EventClassNumber]", "componentID": "[EventComponentUUID]", "mtm": "[EventMachineTypeModel]", "msgID": "[EventMessageID]", "sequenceNumber": "[EventSequenceID]", "timeStamp": "[EventTimeStamp]", "args": "[EventMessageArguments]", "service": "[EventServiceNumber]", "commonEventID": "[CommonEventID]", "eventDate": "[EventDate]" }
```

Procedura

Per inoltrare dati a Lenovo TruScale Infrastructure Services, effettuare le operazioni che seguono.

Passo 1. Aggiungere i certificati SSL attendibili forniti da Lenovo TruScale Infrastructure Services.

1. Dalla barra dei menu di XClarity Orchestrator, fare clic sulla barra dei menu di XClarity Orchestrator e selezionare **Amministrazione** (🔒) → **Sicurezza**, quindi fare clic su **Certificati attendibili** nel riquadro di navigazione sinistro per visualizzare la scheda Certificati attendibili.
2. Fare clic sull'icona **Aggiungi** (+) per aggiungere un certificato. Viene visualizzata la finestra di dialogo Aggiungi certificato.
3. Copiare e incollare i dati del certificato in formato PEM.
4. Fare clic su **Aggiungi**.

Passo 2. Dalla barra del menu di XClarity Orchestrator fare clic su **Monitoraggio** (📊) → **Inoltro eventi**, quindi su **Server d'inoltro dei dati** nel riquadro di navigazione sinistro per visualizzare la scheda Server d'inoltro dei dati.

Passo 3. Fare clic sull'icona **Crea** (+) per visualizzare la finestra di dialogo Crea server d'inoltro dei dati.

Passo 4. Specificare il nome del server d'inoltro e la descrizione facoltativa.

Passo 5. Scegliere di abilitare o disabilitare il server d'inoltro facendo clic sull'opzione di attivazione/disattivazione **Stato**.

Passo 6. Selezionare **TruScale Infrastructure Services** come tipo di server d'inoltro.

Passo 7. Fare clic su **Configurazione** e immettere le informazioni specifiche del protocollo.

- Immettere il nome host o l'indirizzo IP di TruScale Infrastructure Service.
- Immettere la porta da utilizzare per l'inoltro di eventi. Il valore predefinito è 9092.
- Facoltativamente immettere la frequenza, in minuti, di inoltro dei dati. Il valore predefinito è 60 minuti.
- Immettere il nome dell'argomento.
- Immettere il periodo di timeout (in secondi) per la richiesta. Il valore predefinito è 300 secondi.

Passo 8. Fare clic su **Convalida connessione** per verificare che sia possibile stabilire una connessione in base alla configurazione.

Attenzione: La convalida della connessione potrebbe richiedere diversi minuti. È possibile chiudere il messaggio popup e continuare a creare il server d'inoltro senza interrompere il processo di convalida. Al termine della convalida, viene visualizzato un altro messaggio popup per notificare se è stata stabilita la connessione.

Passo 9. Fare clic su **Elenchi di controllo accessi** e selezionare uno o più elenchi di controllo degli accessi che si desidera associare a questo server d'inoltro.

Se l'accesso basato sulle risorse è abilitato, è necessario selezionare almeno un elenco di controllo degli accessi.

Suggerimento: gli utenti che sono membri di un gruppo a cui è assegnato il ruolo predefinito di **Supervisore** possono selezionare facoltativamente **Associa tutto** invece di selezionare gli elenchi di controllo degli accessi, in modo che i dati inoltrati non siano limitati.

Passo 10. Fare clic su **Crea** per creare il server d'inoltro.

Al termine

Nella scheda Server d'inoltro dei dati è possibile effettuare le operazioni che seguono.

- Abilitare o disabilitare un server d'inoltro specifico selezionando l'interruttore nella colonna **Stato**.
- Modificare un server d'inoltro selezionato facendo clic sull'icona **Modifica** (✎).
- Rimuovere un server d'inoltro selezionato facendo clic sull'icona **Elimina** (🗑).

Inoltro di report

È possibile inoltrare report periodicamente a uno o più indirizzi e-mail mediante un servizio Web SMTP.

Informazioni su questa attività

Un *report* è costituito da dati visualizzati sotto forma di tabella nell'interfaccia utente. I seguenti report sono attualmente supportati.

- Avvisi attivi
- Eventi di controllo e risorse
- Dispositivi gestiti (server, storage, switch e chassis)
- Conformità del firmware dei dispositivi
- Conformità della configurazione server
- Stato della garanzia per i server
- Ticket di assistenza attivi

Creazione di configurazioni di destinazione del server d'inoltro

È possibile definire configurazioni di destinazione comuni che possano essere utilizzate da più server d'inoltro dei report. La destinazione identifica la posizione di invio dei report.

Procedura

Per creare una configurazione di destinazione per i server d'inoltro dei report, completare le seguenti operazioni.

- Passo 1. Sulla barra dei menu di XClarity Orchestrator fare clic su **Monitoraggio** (📧) → **Inoltro**, quindi su **Destinazioni server d'inoltro** nel riquadro di navigazione sinistro per visualizzare la scheda Destinazioni server d'inoltro.
- Passo 2. Fare clic sull'icona **Crea** (+) per visualizzare la finestra di dialogo Crea destinazioni server d'inoltro.
- Passo 3. Specificare il nome del server d'inoltro dei report e la descrizione facoltativa.
- Passo 4. Selezionare **SMTP** come tipo di destinazione.
- Passo 5. Fare clic su **Configurazione** e immettere le informazioni specifiche del protocollo.
 - Immettere il nome host o l'indirizzo IP del server SMTP (e-mail).
 - Immettere la porta da utilizzare per la destinazione. Il valore predefinito è 25.
 - Immettere il periodo di timeout (in secondi) per la richiesta. Il valore predefinito è 30 secondi.
 - Immettere l'indirizzo e-mail per ciascun destinatario. Separare gli indirizzi e-mail con una virgola.
 - **Facoltativo:** immettere l'indirizzo e-mail del mittente dell'e-mail (ad esempio, john@company.com) e il dominio del server. Se non viene specificato un indirizzo e-mail, l'indirizzo del mittente è `LXCO.{source_identifier}@{smtp_host}` per impostazione predefinita.

Se viene specificato solo il dominio del mittente, il formato dell'indirizzo del mittente è `{LXCO_host_name}@{sender_domain}` (ad esempio, XClarity1@company.com).

Nota:

- Se si configura un server SMTP affinché richieda un nome host per l'inoltro dell'e-mail e non si configura un nome host per XClarity Orchestrator, è possibile che il server SMTP rifiuti l'e-mail. Se XClarity Orchestrator non dispone di un nome host, l'e-mail viene inoltrata con l'indirizzo IP. Se l'indirizzo IP non può essere ottenuto, verrà inviato "localhost". Ciò potrebbe far sì che il server SMTP rifiuti l'e-mail.
 - Se viene specificato il dominio del mittente, la fonte non si identifica nell'indirizzo del mittente. Vengono, invece, incluse le informazioni sull'origine dati nel corpo dell'e-mail, tra cui il nome di sistema, l'indirizzo IP, il tipo/modello della macchina e il numero di serie.
 - Se il server SMTP accetta solo le e-mail inviate da un utente registrato, l'indirizzo predefinito del mittente (`LXCO.<source_identifier>@{smtp_host}`) viene rifiutato. In questo caso, è necessario specificare almeno un nome di dominio nel campo **Da utente**.
 - Per stabilire una connessione protetta al server SMTP, selezionare uno dei tipi di connessione che seguono.
 - **SSL.** Utilizzare il protocollo SSL per creare una comunicazione protetta.
 - **STARTTLS.** Utilizzare il protocollo TLS per formare una comunicazione protetta su un canale non protetto.
- Se viene selezionato uno di questi tipi di connessione, XClarity Orchestrator tenta di scaricare e importare il certificato del server SMTP nell'archivio attendibile XClarity Orchestrator. Viene chiesto di accettare il certificato.
- Se l'autenticazione è obbligatoria, selezionare uno dei tipi di autenticazione che seguono.

- **Regolare.** Eseguire l'autenticazione server SMTP specificato utilizzando l'ID utente e la password specificati.
- **OAUTH2.** Utilizza il protocollo Simple Authentication and Security Layer (SASL) per eseguire l'autenticazione al server SMTP specificato utilizzando il nome utente e il token di sicurezza specificati. Generalmente, il nome utente è l'indirizzo e-mail.

Attenzione: il token di sicurezza scade dopo un breve periodo di tempo. L'aggiornamento del token di sicurezza è responsabilità dell'utente.

- **Nessuna.** Non viene utilizzata nessuna autenticazione.

Passo 6. Fare clic su **Crea** per creare la configurazione di destinazione.

Al termine

Nella scheda Destinazioni server d'inoltro è possibile effettuare le azioni che seguono.

- Modificare una destinazione selezionata facendo clic sull'icona **Modifica** (✎).
- Rimuovere una destinazione selezionata facendo clic sull'icona **Elimina** (🗑️). Non è possibile eliminare una destinazione assegnata a un server d'inoltro.

Inoltro di report tramite e-mail

È possibile inoltrare report periodicamente a uno o più indirizzi e-mail mediante un servizio Web SMTP.

Informazioni su questa attività

Un *report* è costituito da dati visualizzati sotto forma di tabella nell'interfaccia utente. I seguenti report sono attualmente supportati.

- Avvisi attivi
- Eventi di controllo e risorse
- Dispositivi gestiti (server, storage, switch e chassis)
- Conformità del firmware dei dispositivi
- Conformità della configurazione server
- Stato della garanzia per i server
- Ticket di assistenza attivi

Ogni server d'inoltro del report può includere un solo report di ciascun tipo.

Il report viene creato come file di archivio e salvato sull'host del server Orchestrator. Se il file ha una dimensione inferiore a 10 MB, verrà inoltrato come allegato e-mail. Se le dimensioni del file sono maggiori di 10 MB, l'e-mail include la posizione dei file. È inoltre possibile scaricare il file di archivio facendo clic su **Cronologia report** e selezionando **Scarica** nella riga del report.

Lenovo XClarity Orchestrator memorizza un massimo di 100 report. Se viene raggiunto il numero massimo di report, XClarity Orchestrator elimina il report meno recente prima di generarne uno nuovo.








Procedura

Per inoltrare un report tramite e-mail, completare una delle seguenti operazioni.

- **Invio di dati non filtrati**
 1. Sulla barra del menu di XClarity Orchestrator fare clic su **Monitoraggio** (📊) → **Inoltro eventi**, quindi su **Server d'inoltro dei report** nel riquadro di navigazione sinistro per visualizzare la scheda Report.
 2. Fare clic sull'icona **Crea** (+) per visualizzare la finestra di dialogo Crea report.



3. Specificare il nome del server d'inoltro dei report e la descrizione facoltativa.
4. Scegliere di abilitare o disabilitare il server d'inoltro dei report facendo clic sull'opzione di attivazione/disattivazione **Stato**.
5. Fare clic su **Elenco contenuto** e selezionare uno o più report che si desidera inoltrare.
6. Fare clic su **Destinazione server d'inoltro** e selezionare la destinazione (vedere [Creazione di configurazioni di destinazione del server d'inoltro](#)).
7. Fare clic su **Pianificazioni** e specificare il giorno della settimana, l'ora, la durata (data di inizio e di fine) in cui si desidera inviare i report. Il report viene inviato lo stesso giorno e alla stessa ora di ogni settimana durante l'intervallo di tempo specificato.
8. Fare clic su **Crea** per creare il server d'inoltro.

- **Invio di dati filtrati**

1. Sulla barra dei menu di XClarity Orchestrator aprire la scheda che contiene il report da inviare. Sono supportati i seguenti report.
 - Dati del dispositivo (fare clic su **Risorse**  → {device_type})
 - Dati avvisi attivi (fare clic su **Monitoraggio**  → **Avvisi**)
 - Dati degli eventi di controllo e delle risorse (fare clic su **Monitoraggio**  → **Eventi**)
 - Conformità del firmware (fare clic su **Provisioning**  → **Aggiornamenti** → **Applica e attiva** → **Dispositivi**)
 - Conformità della configurazione del server (fare clic su **Provisioning**  → **Configurazione server** → **Assegna e distribuisce**)
 - Dati di garanzia del dispositivo (fare clic su **Amministrazione**  → **Assistenza e supporto** → **Garanzia**)
 - Ticket di assistenza attivi (fare clic su **Amministrazione**  → **Assistenza e supporto** → **Ticket di assistenza**)
2. Facoltativamente, limitare il set di dati unicamente alle informazioni che interessano, restringendo l'ambito dei dati solo alle risorse di gruppi e strumenti di gestione delle risorse specifici e utilizzando i filtri e la ricerca per includere dati che corrispondono a criteri specifici (vedere [Suggerimenti e tecniche dell'interfaccia utente](#)).
3. Fare clic su **Tutte le azioni** → **Crea server d'inoltro dei report** per visualizzare la finestra di dialogo Crea server d'inoltro dei report.
4. Specificare il nome del server d'inoltro dei report e la descrizione facoltativa.
5. Scegliere di abilitare o disabilitare il server d'inoltro dei report facendo clic sull'opzione di attivazione/disattivazione **Stato**.
6. Fare clic su **Destinazione server d'inoltro** e selezionare la destinazione (vedere [Creazione di configurazioni di destinazione del server d'inoltro](#)).
7. Fare clic su **Pianificazioni** e specificare il giorno della settimana, l'ora, la durata (data di inizio e di fine) in cui si desidera inviare i report. Il report viene inviato lo stesso giorno e alla stessa ora di ogni settimana durante l'intervallo di tempo specificato.
8. Fare clic su **Crea** per creare il server d'inoltro.

Al termine

Nella scheda Server d'inoltro dei report è possibile effettuare le azioni che seguono.

- Abilitare o disabilitare un server d'inoltro dei report specifico selezionando l'opzione di attivazione/disattivazione nella colonna **Stato**.
- Modificare un server d'inoltro dei report selezionato facendo clic sull'icona **Modifica** .
- Rimuovere un server d'inoltro dei report selezionato facendo clic sull'icona **Elimina** .

- Salvare i report nel sistema locale facendo clic sulla scheda **Cronologia report**, quindi su **Scarica** nella riga di ciascun report.

È possibile aggiungere un report a un server d'oltro dei report esistente da qualsiasi scheda di report supportata utilizzando i filtri dati attualmente applicati alla tabella e facendo clic su **Tutte le azioni → Aggiungi contenuto al server d'oltro dei report esistente** da tale scheda. Se il server d'oltro dei report include già un report di quel tipo, il report viene aggiornato per utilizzare i filtri dati correnti.

Capitolo 4. Gestione delle risorse

È possibile utilizzare Lenovo XClarity Orchestrator per gestire le risorse, come la visualizzazione dei dettagli dei dispositivi offline.

Creazione dei gruppi di risorse

Un *gruppo di risorse* è una serie di risorse che è possibile visualizzare e utilizzare collettivamente in Lenovo XClarity Orchestrator. Sono supportati diversi tipi di gruppi di risorse.

Ulteriori informazioni:  [Come creare un gruppo di risorse](#)

Informazioni su questa attività


Sono supportati diversi tipi di gruppi di risorse.

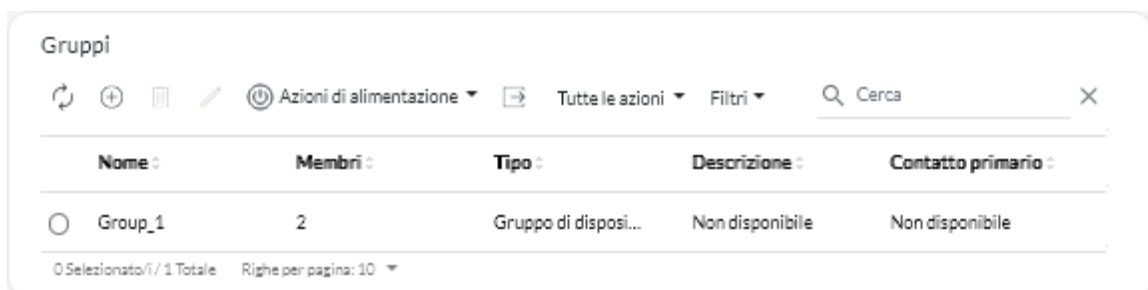
- *Gruppi di dispositivi dinamici* contenenti una serie dinamica di dispositivi in base a criteri specifici.
- *Gruppi di dispositivi* contenenti una serie statica di dispositivi specifici.
- *Gruppi di strumenti di gestione* contenenti una serie statica di strumenti di gestione delle risorse specifici e lo stesso prodotto XClarity Orchestrator.
- *Gruppi di infrastrutture* contenenti una serie di dispositivi di rete. Quando si utilizza uno strumento di gestione delle risorse Schneider Electric EcoStruxure IT Expert, XClarity Orchestrator clona automaticamente le raccolte di "gruppi" definite in tale strumento Esperto EcoStruxure IT gestito. Il gruppo clonato è denominato $\{domain\}\{groupName\}$ nel repository locale. Tenere presente che le raccolte di tipo posizione (sito, edificio, ambiente, fila o rack) non sono clonate.


Nota: Non è possibile creare un gruppo di risorse con un insieme di dispositivi, strumenti di gestione delle risorse e risorse dell'infrastruttura.

Procedura

Per creare un gruppo di risorse e gestire l'appartenenza, completare le seguenti operazioni.

- **Creare un gruppo di dispositivi dinamico e aggiungere dispositivi.**
 1. Sulla barra dei menu di XClarity Orchestrator fare clic su **Risorse**  → **Gruppi** per visualizzare la scheda Gruppi.



2. Fare clic sull'icona **Crea**  per visualizzare la finestra di dialogo Crea gruppo.
3. Selezionare **Gruppo di dispositivi dinamici** come tipo di gruppo.
4. Specificare il nome e la descrizione facoltativa del gruppo.

5. Fare clic su **Criteri di gruppo** e selezionare le regole da utilizzare per l'appartenenza al gruppo.

The screenshot shows a 'Crea gruppo' dialog box with the following elements:

- Tab: **Proprietà**
- Field: Tipo di gruppo * (Dropdown menu: Gruppo di dispositivi)
- Field: Nome del gruppo *
- Field: Descrizione
- Buttons: Dispositivi disponibili >, Crea

- Scegliere se il dispositivo deve corrispondere a **una** (una o più) o **tutte** le regole dall'elenco a discesa di corrispondenza **Criteri**.
 - Specificare l'attributo, l'operatore e il valore di ogni regola. Fare clic su **Aggiungi criteri** per aggiungere un'altra regola.
6. Fare clic su **Informazioni sul contatto** e facoltativamente selezionare un contatto di supporto primario (nella colonna **Contatti primari**) e uno o più contatti secondari (nella colonna **Contatti secondari**) da assegnare a tutti i dispositivi del gruppo.
 7. Fare clic su **Crea**. Il gruppo viene aggiunto alla tabella.
- **Creare un gruppo di risorse statico e aggiungere risorse.**
 1. Sulla barra dei menu di XClarity Orchestrator fare clic su **Risorse** (⚙️) → **Gruppi** per visualizzare la scheda Gruppi.
 2. Fare clic sull'icona **Crea** (+) per visualizzare la finestra di dialogo Crea gruppo.
 3. Selezionare **Gruppo di dispositivi** o **Gruppo di strumenti di gestione** come tipo di gruppo.
 4. Specificare il nome e la descrizione facoltativa del gruppo.
 5. Fare clic su **Dispositivi disponibili** o **Strumenti di gestione delle risorse disponibili**, a seconda del tipo di gruppo, e selezionare le risorse che si desidera includere nel gruppo.
 6. Fare clic su **Informazioni sul contatto** e facoltativamente selezionare un contatto di supporto primario (nella colonna **Contatti primari**) e uno o più contatti secondari (nella colonna **Contatti secondari**) da assegnare a tutti i dispositivi del gruppo.
 7. Fare clic su **Crea**. Il gruppo viene aggiunto alla tabella.
 - **Aggiungere dispositivi a un gruppo di dispositivi statico.**
 1. Sulla barra dei menu di XClarity Orchestrator fare clic su **Risorse** (⚙️) e selezionare il tipo di dispositivo (ad esempio, Server o Switch) per visualizzare una scheda con l'elenco di tutti i dispositivi simili.

Server

Cerca X

Avvia Controllo remoto
 Azioni di alimentazione

 Tutte le azioni
 Filtri

<input type="checkbox"/>	Server	Stato	Connetti	Alimenta	Indirizzi	Nome pr	Tipo/nor	Firmware	Avviso	Gruppi
<input type="checkbox"/>	New...				10.24...	Leno...	719...	N3E1f	Non ...	Non di
<input type="checkbox"/>	ite-b...				10.24...	Leno...	716...	CGE1f	Non ...	Non di
<input type="checkbox"/>	Blac...				10.24...	Leno...	716...	A3EGf	Non ...	Non di
<input type="checkbox"/>	nod...				10.24...	IBM ...	791...	Non di	Non ...	Non di
<input type="checkbox"/>	IM...				10.24...	IBM ...	873...	B2E11	Non ...	Non di
<input type="checkbox"/>	Cara...				10.24...	Eagl...	791...	Non di	Non ...	Non di
<input type="checkbox"/>	blad...				10.24...	IBM ...	790...	Non di	Non ...	Non di
<input type="checkbox"/>	New...				10.24...	Leno...	719...	N3E1f	Non ...	Non di
<input type="checkbox"/>	New...				10.24...	Leno...	719...	N3E1f	Non ...	Non di
<input type="checkbox"/>	New...				10.24...	Leno...	719...	N3E1f	Non ...	Non di

0 selezionato / 60 Totale Righe per pagina: 10

2. Selezionare uno o più dispositivi da aggiungere a un gruppo.

3. Fare clic sull'icona **Aggiungi elemento al gruppo** ().

4. Selezionare un gruppo esistente o specificare un nome e una descrizione facoltativa per creare un nuovo gruppo e fare clic su **Applica**.

• **Aggiungere strumenti di gestione delle risorse a un gruppo di strumenti di gestione statico.**

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

2. Selezionare uno o più strumenti di gestione delle risorse da aggiungere a un gruppo.

3. Fare clic sull'icona **Aggiungi elemento al gruppo** ().

4. Selezionare un gruppo esistente o specificare un nome e una descrizione facoltativa per creare un nuovo gruppo e fare clic su **Applica**.

Al termine

Nella scheda Gruppi è possibile effettuare le operazioni che seguono.

• Modificare le proprietà e l'appartenenza di un gruppo selezionato facendo clic sull'icona **Modifica** ().

Nota: Per i gruppi di infrastrutture clonate da Schneider Electric EcoStruxure IT Expert, utilizzare Schneider Electric EcoStruxure IT Expert per modificare il nome del gruppo, la descrizione e l'appartenenza.

• Eliminare un gruppo selezionato facendo clic sull'icona **Elimina** ().

- Visualizzare i membri di un gruppo di risorse facendo clic sul nome del gruppo per visualizzare la finestra di dialogo Visualizza gruppo, quindi sulla scheda **Riepilogo membri**.

Gestione dei dispositivi offline

Se un dispositivo attualmente non è gestito da uno strumento di gestione delle risorse, è possibile utilizzare Lenovo XClarity Orchestrator per gestire i dispositivi in *modalità offline* importando un archivio dei dati di servizio associato al dispositivo.

Informazioni su questa attività

Solo i server con controller di gestione della scheda di base IMM2 o XCC possono essere gestiti offline. Questi dispositivi vengono identificati nell'interfaccia Web utilizzando lo stato di connettività "Gestito offline".

È possibile effettuare le seguenti azioni sui dispositivi gestiti offline. Tutte le altre azioni sono disabilitate.

- Visualizzare l'inventario dei dispositivi
- Escludere avvisi ed eventi
- Gestire i dati di servizio
- Aprire i ticket di assistenza al centro di supporto Lenovo utilizzando Call Home e gestire i ticket di assistenza
- Recupero delle informazioni sulla garanzia
- Funzioni di analisi per la previsione e l'analisi dei problemi con questi dispositivi

Importante: XClarity Orchestrator non comunica con i dispositivi offline per recuperare i dati aggiornati.

Procedura

Per gestire i dispositivi offline, completare le seguenti operazioni.

Passo 1. Dalla barra dei menu di Lenovo XClarity Orchestrator, fare clic su **Risorse** (🔍) → **Server**. Verrà visualizzata la pagina Server.

Passo 2. Fare clic sull'icona **Importa** (📁) per importare gli archivi dei dati di servizio.

Passo 3. Trascinare e rilasciare uno o più archivi dei dati di servizio (in formato .gz, .tzz o .tgz) nella finestra di dialogo Importa oppure fare clic su **Browser** per individuare l'archivio.

Passo 4. Abilitare facoltativamente l'opzione **Aggiungi il server nei dati di servizio all'inventario solo per la visualizzazione** per gestire il server applicabile in modalità di gestione offline (vedere [Gestione dei dispositivi offline](#)).

Passo 5. Fare clic sull'icona **Importa** per importare e analizzare l'archivio. Al termine dell'analisi, il campo **Stato analisi** per l'archivio importato viene modificato in "Analizzato".

È possibile monitorare lo stato del processo di importazione e analisi dal log dei processi ([Monitoraggio dei processi](#)).

Al termine

È possibile annullare la gestione di un dispositivo selezionato gestito offline facendo clic sull'icona **Non gestire** (🗑️).

Esecuzione di azioni di alimentazione sui server gestiti

È possibile utilizzare Lenovo XClarity Orchestrator per accendere, spegnere e riavviare i server gestiti.

Prima di iniziare








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

I server ThinkSystem richiedono un sistema operativo per eseguire le operazioni di alimentazione.


Verificare che il sistema operativo sul server sia conforme allo standard ACPI (Advanced Configuration and Power Interface) e che sia configurato per consentire operazioni di arresto.

Informazioni su questa attività

XClarity Orchestrator supporta le azioni di alimentazione che seguono.

-  **Accendi**. Accende i server selezionati che sono in quel momento spenti.
-  **Spegni normalmente**. Arresta il sistema operativo e spegne i server selezionati che sono in quel momento accesi.
-  **Spegni immediatamente**. Spegne i server selezionati che sono in quel momento accesi.
-  **Riavvia normalmente**. Arresta il sistema operativo e riavvia i server selezionati che sono in quel momento accesi.
-  **Riavvia immediatamente**. Riavvia i server selezionati che sono in quel momento accesi.
-  **Riavvia con la configurazione di sistema**. Riavvia con la configurazione BIOS/UEFI (F1) per i server selezionati.
-  **Riavvia controller di gestione**. Riavvia il controller di gestione della scheda di base per i server selezionati.

Nota:


- Per i dispositivi client ThinkEdge è supportata solo l'opzione  **Riavvia normalmente**.
- Lo stato di connettività del server deve essere online. Non è possibile eseguire azioni di alimentazione sui dispositivi offline, inclusi i dispositivi gestiti offline.

È possibile eseguire azioni di alimentazione su un massimo di 25 dispositivi contemporaneamente.


• Procedura

Per accendere, spegnere o riavviare server, attenersi alla procedura descritta di seguito.

Per un singolo server

- Nel menu XClarity Orchestrator fare clic su **Risorse**  → **Server**. Verrà visualizzata la scheda Server contenente una vista tabulare di tutti i server gestiti.
- Fare clic sulla riga relativa al server per visualizzare le schede di riepilogo per quel server.
- Nella scheda Azioni rapide fare clic su **Azioni di alimentazione**, quindi sull'azione di alimentazione desiderata.
- Fare clic su **Conferma**.

Per più server

- Nel menu XClarity Orchestrator fare clic su **Risorse**  → **Server**. Verrà visualizzata la scheda Server contenente una vista tabulare di tutti i server gestiti.
- Selezionare uno o più server. È possibile selezionare un massimo di 25 server.
- Fare clic su **Azioni di alimentazione**, quindi sull'azione di alimentazione desiderata.

Verrà visualizzata una finestra di dialogo con un elenco di dispositivi selezionati. I dispositivi non applicabili (che non supportano le azioni di alimentazione) sono disabilitati.

- d. Fare clic su **Conferma**.

Per tutti i server di un gruppo

- a. Sulla barra dei menu di XClarity Orchestrator fare clic su **Risorse** (🔍) → **Gruppi**. Verrà visualizzata la scheda Gruppi contenente una vista tabulare di tutti i gruppi.
- b. Selezionare un gruppo di server.
- c. Nella scheda Azioni rapide fare clic su **Azioni di alimentazione**, quindi sull'azione di alimentazione desiderata.

Verrà visualizzata una finestra di dialogo con un elenco di dispositivi selezionati. I dispositivi non applicabili (che non supportano le azioni di alimentazione) sono disabilitati.

- d. Selezionare i server specifici nel gruppo su cui intervenire. È possibile selezionare un massimo di 25 server.
- e. Fare clic su **Conferma**.

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).

Apertura di una sessione di controllo remoto per server gestiti

È possibile aprire una sessione di controllo remoto per un server gestito, come con una console locale. È possibile quindi utilizzare la sessione di controllo remoto per eseguire operazioni, quali accensione o spegnimento del server e montaggio logico di un'unità locale o remota.

Apertura di una sessione di controllo remoto per i server ThinkSystem o ThinkAgile

È possibile aprire una sessione di controllo remoto per un server ThinkSystem o ThinkAgile gestito, come con una console locale. È quindi possibile utilizzare la sessione di controllo remoto per eseguire le operazioni di gestione.

Prima di iniziare

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

Il server gestito deve avere uno stato di integrità normale e uno stato di connettività online. Per ulteriori informazioni sulla visualizzazione dello stato dei server, vedere [Visualizzazione dei dettagli dei dispositivi](#).

Esaminare le seguenti considerazioni per i server ThinkSystem SR635 e SR655.

- È necessario il firmware del controller di gestione della scheda di base v2.94 o versioni successive.
- È supportata solo la modalità utente multiplo; la modalità utente singolo non è supportata.
- Internet Explorer 11 non è supportato.
- Non è possibile accendere o spegnere un server da una sessione di controllo remoto.

Informazioni su questa attività

È possibile avviare una sessione di controllo remoto per un singolo server ThinkSystem o ThinkAgile.

Per ulteriori informazioni sull'utilizzo della console remota e delle funzioni dei supporti, consultare la documentazione del server ThinkSystem o ThinkAgile.

Nota: Per i server ThinkSystem e ThinkAgile, non è richiesto un ambiente JRE (Java Runtime Environment) con supporto Java WebStart.

Procedura

Per aprire una sessione di controllo remoto per un server ThinkSystem o ThinkAgile, completare i seguenti passaggi.

Passo 1. Nel menu XClarity Orchestrator fare clic su **Risorse** (🔍) → **Server**. Verrà visualizzata la scheda Server contenente una vista tabulare di tutti i server gestiti.

Passo 2. Selezionare il server da controllare in remoto.

Passo 3. Fare clic sull'icona **Avvia controllo remoto** (🔗).

Passo 4. Accettare tutti gli avvisi di sicurezza del browser Web.

Al termine

Se la sessione di controllo remoto non si apre correttamente, vedere [Problemi di controllo remoto](#) nella documentazione online di XClarity Orchestrator..

Apertura di una sessione di controllo remoto per i server ThinkServer

È possibile aprire una sessione di controllo remoto per server ThinkServer gestiti, come con una console locale. È possibile quindi utilizzare la sessione di controllo remoto per eseguire operazioni di alimentazione e ripristino, montare a livello logico un'unità locale o di rete sul server, acquisire schermate e registrare video.

Prima di iniziare

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

Il server gestito deve avere uno stato di integrità normale e uno stato di connettività online. Per ulteriori informazioni sulla visualizzazione dello stato dei server, vedere [Visualizzazione dei dettagli dei dispositivi](#).

La chiave FoD (Feature on Demand) per ThinkServer System Manager Premium Upgrade deve essere installata sul server gestito. Per ulteriori informazioni sulle chiavi FoD installate nei server, vedere [Visualizzazione delle chiavi FoD \(Feature on Demand\)](#) nella documentazione online di Lenovo XClarity Administrator.

Sul server locale è necessario installare un ambiente Java Runtime Environment (JRE) con supporto Java WebStart (ad esempio, Adopt OpenJDK 8 con il plug-in IcedTea-Web v1.8).

Informazioni su questa attività

È possibile aprire una sessione di controllo remoto solo per un singolo server ThinkServer.

Per ulteriori informazioni sull'utilizzo della console remota ThinkServer e delle funzioni dei supporti, consultare la documentazione del server ThinkServer.

Procedura

Per aprire una sessione di controllo remoto per un server ThinkSystem o ThinkAgile, completare i seguenti passaggi.

Passo 1. Nel menu XClarity Orchestrator fare clic su **Risorse** (🔍) → **Server**. Verrà visualizzata la scheda Server contenente una vista tabulare di tutti i server gestiti.

Passo 2. Selezionare il server da controllare in remoto.

Passo 3. Fare clic sull'icona **Avvia controllo remoto** (🔗).

Passo 4. Accettare tutti gli avvisi di sicurezza del browser Web.

Al termine

Se la sessione di controllo remoto non si apre correttamente, vedere [Problemi di controllo remoto](#) nella documentazione online di XClarity Orchestrator..

Apertura di una sessione di controllo remoto per i server System x

È possibile aprire una sessione di controllo remoto per server System x gestiti, come con una console locale. È possibile quindi utilizzare la sessione di controllo remoto per eseguire operazioni di alimentazione e ripristino, montare a livello logico un'unità locale o di rete sul server, acquisire schermate e registrare video.

Prima di iniziare

Prima di aprire una sessione di controllo remoto, esaminare le considerazioni relative a sicurezza, prestazioni e tastiera. Per ulteriori informazioni su queste considerazioni, vedere [Considerazioni sul controllo remoto](#).

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

Il server gestito deve avere uno stato di integrità normale e uno stato di connettività online. Per ulteriori informazioni sulla visualizzazione dello stato dei server, vedere [Visualizzazione dei dettagli dei dispositivi](#).

Utilizzare l'account utente di Lenovo XClarity Orchestrator per eseguire il login alla sessione di controllo remoto. L'account utente deve disporre delle autorizzazioni utente necessarie per accedere a un server e gestirlo.

Sul server locale è necessario installare un ambiente Java Runtime Environment (JRE) con supporto Java WebStart (ad esempio, Adopt OpenJDK 8 con il plug-in IcedTea-Web v1.8).

La chiave FOD (Feature on Demand) per la presenza remota deve essere installata e abilitata sul server gestito. È possibile determinare se la presenza remota è abilitata o disabilitata nella pagina Server e facendo clic su **Filtri** → **Presenza remota**. Se disabilitata:

- Verificare che il server sia in uno stato di integrità normale e in uno stato di connettività online.
- Verificare che il livello XClarity Controller Enterprise o l'aggiornamento avanzato MM sia abilitato per i server in cui queste funzioni non sono già attivate per impostazione predefinita.

La sessione di controllo remoto utilizza le impostazioni internazionali e della lingua di visualizzazione definite per il sistema operativo sul sistema locale.


Informazioni su questa attività

È possibile avviare più sessioni di controllo remoto. Ogni sessione può gestire più server.

Nota: Per i server Flex System x280, x480 e x880, è possibile avviare una sessione di controllo remoto solo per il nodo primario. Se si tenta di avviare una sessione di controllo remoto per un nodo non primario in un sistema multinodo, la finestra di dialogo di controllo remoto si avvia ma non viene visualizzato alcun video.

Procedura

Per aprire una sessione di controllo remoto per un server System x, effettuare le seguenti operazioni.

Passo 1. Nel menu XClarity Orchestrator fare clic su **Risorse**  → **Server**. Verrà visualizzata la scheda Server contenente una vista tabulare di tutti i server gestiti.

Passo 2. Selezionare il server da controllare in remoto.

Se non si seleziona un server, viene aperta una sessione di controllo remoto non assegnata.

Passo 3. Fare clic sull'icona **Avvia controllo remoto** .

Passo 4. Accettare tutti gli avvisi di sicurezza del browser Web.

Passo 5. Quando richiesto, selezionare una delle seguenti modalità di connessione:

- **Modalità utente singolo.** Stabilisce una sessione di controllo remoto esclusiva con il server. Tutte le altre sessioni di controllo remoto a questo server sono bloccate fino alla disconnessione dal server. Questa opzione è disponibile solo se non sono presenti altre sessioni di controllo remoto al server.
- **Modalità multiutente.** Consente di stabilire più sessioni di controllo remoto con lo stesso server. XClarity Orchestrator supporta fino a sei sessioni di controllo remoto simultanee a un singolo server.

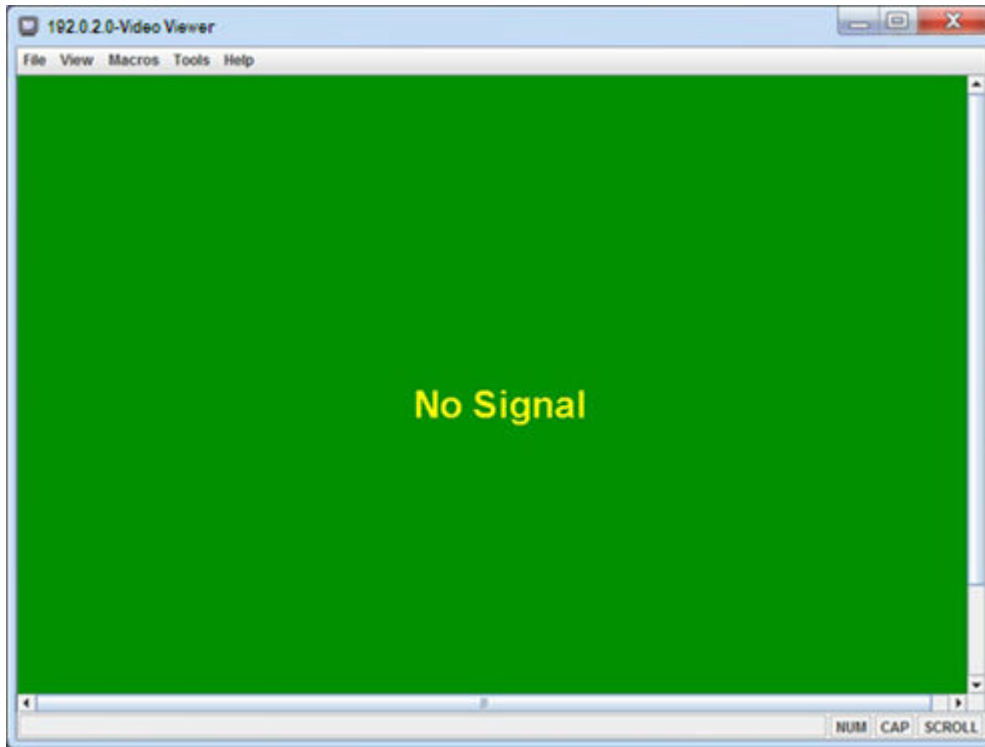
Passo 6. Fare clic su **Avvia controllo remoto**.

Passo 7. Quando richiesto, scegliere la posizione dove salvare un collegamento alla sessione di controllo remoto sul sistema locale. È possibile utilizzare questo collegamento per avviare una sessione di controllo remoto senza accedere all'interfaccia Web di XClarity Orchestrator. Il collegamento contiene un link che apre una sessione di controllo remoto vuota, a cui è possibile aggiungere manualmente i server.

Nota: Il sistema locale deve avere accesso a XClarity Orchestrator per convalidare l'account utente con il server di autenticazione XClarity Orchestrator.

Al termine

La sessione di controllo remoto dispone di una miniatura (icona) per ciascun server attualmente gestito tramite la sessione.




Se la sessione di controllo remoto non si apre correttamente, vedere [Problemi di controllo remoto](#) nella documentazione online di XClarity Orchestrator.





È possibile procedere come segue nella sessione di controllo remoto.

- Visualizzare più console del server e passare da una all'altra facendo clic su una miniatura. La console del server viene visualizzata nell'area delle sessioni video. Se si accede a più server rispetto al numero massimo visualizzabile nell'area icone, fare clic sull'icona **Scorri a destra** (») e sull'icona **Scorri a sinistra** («) per scorrere le miniature aggiuntive dei server. Fare clic sull'icona **Tutte le sessioni** (🖥️) per visualizzare un elenco di tutte le sessioni server aperte.
- Aggiungere una console del server alla sessione di controllo remoto corrente facendo clic sull'icona **Aggiungi server** (+).
- Nascondere o mostrare l'area miniature facendo clic sull'icona **Attiva/Disattiva miniature** (🔍).
- Visualizzare la sessione di controllo remoto in una finestra o a schermo intero facendo clic sull'icona **Schermo** (🖥️), quindi su **Attiva schermo intero** o **Disattiva schermo intero**.
- È possibile utilizzare i pulsanti con tasti permanenti Ctrl, Alt e Maiusc per inviare la sequenza tasti direttamente al server. Quando si fa clic su un tasto permanente, il tasto rimane attivo finché non viene premuto nuovamente un tasto della tastiera o non si fa nuovamente clic sul pulsante. Per inviare le combinazioni di tasti Ctrl o Alt, fare clic su Ctrl o Alt nella barra degli strumenti, posizionare il cursore nell'area delle sessioni video e premere un tasto sulla tastiera.

Nota: Se viene abilitata la modalità di acquisizione mouse, premere il tasto Alt sinistro per spostare il cursore all'esterno dell'area delle sessioni video. Anche se la modalità di acquisizione mouse è disabilitata per impostazione predefinita, è possibile abilitarla dalla pagina della barra degli strumenti (vedere [Impostazione delle preferenze di controllo remoto](#)).

- Definire sequenze di tasti personalizzate, note come softkey, facendo clic sull'icona **Tastiera** (🗂️). Le definizioni di softkey sono memorizzate nel sistema da cui è stata avviata la sessione di controllo remoto.

Pertanto, se si avvia la sessione di controllo remoto da un altro sistema, è necessario definire nuovamente i tasti softkey. È possibile esportare le impostazioni utente, inclusi i tasti softkey, facendo clic sull'icona **Preferenza** () , sulla scheda **Impostazioni utente** e infine su **Importa**.

- Acquisire una cattura della schermata della sessione del server selezionata e salvarla in vari formati, facendo clic sull'icona **Schermo** () , quindi su **Screenshot**.
- Montare supporti remoti (come CD, DVD o dispositivi USB, immagini disco o ISO) sul server selezionato oppure spostare un dispositivo montato su un altro server facendo clic sull'icona **Supporti remoti** () .
- Caricare le immagini su un server dai supporti remoti facendo clic sull'icona **Supporti remoti** () , quindi su **Monta supporti remoti** e infine su **Carica l'immagine su IMM**.
- Accendere o spegnere il server da una console remota facendo clic sull'icona **Alimentazione** () .
- Modificare le preferenze di controllo remoto, inclusa la frequenza di aggiornamento dell'icona del server (vedere [Impostazione delle preferenze di controllo remoto](#)).

Considerazioni sul controllo remoto

Esaminare le considerazioni su sicurezza, prestazioni e tastiera relative all'accesso ai server gestiti tramite una sessione di controllo remoto.

Considerazioni sulla sicurezza

L'account utente utilizzato per avviare la sessione di controllo remoto deve essere un account utente valido definito nel server di autenticazione Lenovo XClarity Orchestrator. L'account utente deve disporre di livelli sufficienti di autorizzazione utente per accedere e gestire un server.

Per impostazione predefinita, è possibile stabilire sessioni di controllo remoto a un server. Tuttavia, quando si avvia una sessione di controllo remoto, è possibile avviare la sessione in modalità utente singolo, che stabilisce una sessione esclusiva con il server. Tutte le altre sessioni di controllo remoto a questo server sono bloccate fino alla disconnessione dal server.

Nota: Questa opzione è disponibile solo se al momento non sono presenti altre sessioni di controllo remoto al server.

Per utilizzare lo standard FIPS (Federal Information Processing Standard) 140, è necessario abilitarlo manualmente completando le seguenti operazioni sul sistema locale:

1. Individuare il nome del fornitore del sistema di crittografia certificato FIPS 140 installato sul sistema locale.
2. Modificare il file `$(java.home)/lib/security/java.security`.
3. Modificare la riga che include `com.sun.net.ssl.internal.ssl.Provider` aggiungendo il nome del fornitore del sistema di crittografia certificato FIPS 140. Ad esempio, modificare:
`security.provider.4=com.sun.net.ssl.internal.ssl.Provider`
in:
`security.provider.4=com.sun.net.ssl.internal.ssl.Provider SunPKCS11-NSS`

Considerazioni sulle prestazioni

Se una sessione di controllo remoto è lenta o bloccata, chiudere tutti i video e le sessioni dei supporti remoti stabilite con il server selezionato per ridurre il numero di connessioni aperte con il server. Inoltre, è possibile aumentare le prestazioni modificando le seguenti preferenze. Per ulteriori informazioni, vedere [Impostazione delle preferenze di controllo remoto](#).

- **KVM**
 - Ridurre la percentuale della larghezza di banda video utilizzata dall'applicazione. La qualità delle immagini della sessione di controllo remoto verrà ridotta.

- Ridurre la percentuale dei frame aggiornati dall'applicazione. La velocità di aggiornamento della sessione di controllo remoto verrà ridotta.
- **Miniature**
 - Aumentare la velocità dell'intervallo di aggiornamento delle miniature. L'applicazione aggiornerà le miniature a una velocità inferiore.
 - Disattivare completamente la visualizzazione delle miniature.

La dimensione della finestra della sessione di controllo remoto e il numero di sessioni attive potrebbero incidere sull'utilizzo delle risorse della workstation, come memoria e larghezza di banda della rete, riducendo le prestazioni. La sessione di controllo remoto utilizza un limite flessibile di 32 sessioni aperte. Se vengono aperte più di 32 sessioni, le prestazioni potrebbero essere notevolmente ridotte e la sessione di controllo remoto potrebbe bloccarsi. È possibile visualizzare la riduzione delle prestazioni con meno di 32 sessioni aperte, se le risorse, come larghezza di banda della rete e memoria locale, non sono sufficienti.

Considerazioni sulla tastiera

La sessione di controllo remoto supporta i seguenti tipi di tastiera:

- Belga a 105 tasti
- Brasiliano
- Cinese
- Francese a 105 tasti
- Tedesco a 105 tasti
- Italiano a 105 tasti
- Giapponese a 109 tasti
- Coreano
- Portoghese
- Russo
- Spagnolo a 105 tasti
- Svizzero a 105 tasti
- Regno Unito a 105 tasti
- Stati Uniti a 104 tasti


Per informazioni sulle preferenze delle tastiere, vedere [Impostazione delle preferenze di controllo remoto](#).

Impostazione delle preferenze di controllo remoto

È possibile modificare le impostazioni delle preferenze per la sessione di controllo remoto corrente.

Procedura

Completare le seguenti operazioni per modificare le preferenze di controllo remoto.

Passo 1. Per modificare le preferenze di controllo remoto, fare clic sull'icona **Preferenze** (). Tutte le modifiche saranno effettive immediatamente.

- **KVM**
 - **Percentuale della larghezza di banda video.** L'aumento della larghezza di banda migliora la qualità di visualizzazione della sessione di controllo remoto ma potrebbe incidere sulle prestazioni della sessione di controllo remoto.
 - **Percentuale di frame aggiornati.** L'aumento della percentuale di frame aggiornati incrementa l'intervallo di aggiornamento della sessione di controllo remoto ma potrebbe incidere sulle prestazioni della sessione di controllo remoto.
 - **Tipo di tastiera.** Selezionare il tipo di tastiera che si utilizza per la sessione di controllo remoto. Il tipo di tastiera selezionato deve corrispondere alle configurazioni della tastiera del sistema locale e dell'host remoto.

Nota: Se si seleziona una tastiera internazionale ed è necessario immettere una combinazione di tasti che richiede l'utilizzo del tasto AltGr (Alternate Graphics), verificare che il sistema operativo della workstation usata per richiamare la sessione di controllo remoto sia dello stesso tipo di quello del server a cui si desidera accedere in remoto. Ad esempio, se sul server è in esecuzione Linux, assicurarsi di richiamare l'applicazione di controllo remoto da una workstation Linux.

- **Adatta immagine a finestra.** Selezionare questa opzione per adattare l'immagine video ricevuta dal server alla dimensione dell'area delle sessioni video.

- **Protezione**

- **Preferisci connessioni modalità utente singolo.** Specificare se le connessioni modalità utente singolo sono l'impostazione predefinita per il collegamento a un server. Quando viene stabilita una connessione in modalità utente singolo, solo un utente per volta può essere collegato a un server. Se questa casella non è selezionata, la funzione predefinita è il collegamento al server in modalità multiutente.
- **Richiedi connessioni tunneling (sicure).** Selezionare questa opzione per accedere a un server tramite il nodo di gestione. È possibile utilizzare questa opzione per accedere a un server da un client che non si trova nella stessa rete del server.

Nota: L'applicazione di controllo remoto tenta sempre di collegarsi direttamente al server dal sistema locale dove il controllo remoto è stato avviato. Se la workstation client non può accedere direttamente al server, selezionando questa opzione, l'applicazione di controllo remoto accede al server tramite Lenovo XClarity Orchestrator.

- **Barra degli strumenti**

Nota: Fare clic su **Ripristina valori predefiniti** per ripristinare tutte le impostazioni in questa pagina ai valori predefiniti

- **Aggiungi la barra degli strumenti alla finestra.** Per impostazione predefinita, la barra degli strumenti è nascosta sopra la finestra della sessione di controllo remoto e viene visualizzata solo al passaggio del mouse. Se si seleziona questa opzione, la barra di strumenti viene aggiunta alla finestra e viene sempre visualizzata tra il pannello della miniatura e la finestra della sessione di controllo remoto.
- **Mostra pulsanti tastiera.** Consente di specificare se visualizzare le icone dei pulsanti della tastiera (BlocMaiusc, BlocNum e BlocScorr) sulla barra degli strumenti.
- **Mostra controllo alimentazione.** Consente di specificare se visualizzare le opzioni di controllo dell'alimentazione sulla barra degli strumenti.
- **Mostra pulsanti con tasti permanenti.** Consente di specificare se visualizzare le icone dei pulsanti con tasti permanenti (Ctrl, Alt e Canc) sulla barra degli strumenti.
- **Nascondi puntatore mouse locale.** Consente di specificare se visualizzare il puntatore del mouse locale quando si posiziona il cursore nella sessione server attualmente visualizzata nell'area delle sessioni video.
- **Abilita modalità di acquisizione mouse.** Per impostazione predefinita, la modalità di acquisizione del mouse è disabilitata. Ciò significa che è possibile spostare liberamente il cursore all'interno e all'esterno dell'area delle sessioni video. Se si abilita la modalità di acquisizione mouse, è necessario premere il tasto Alt sinistro prima di poter spostare il cursore all'esterno dell'area delle sessioni video. Se la modalità di acquisizione mouse è abilitata, è possibile specificare se utilizzare i tasti Ctrl+Alt per uscire dalla modalità di acquisizione mouse. L'impostazione predefinita è l'uso del tasto Alt sinistro.
- **Specifica opacità sfondo barra degli strumenti.** La riduzione della percentuale di opacità consente di visualizzare un'area maggiore della sessione video attraverso lo sfondo della barra degli strumenti.

Nota: Questa opzione è disponibile solo quando la barra degli strumenti non è stata aggiunta alla finestra.

- **Miniature**

- **Mostra miniature.** Selezionare questa opzione per mostrare l'area miniature nella sessione di controllo remoto.
- **Specifica intervallo di aggiornamento miniature.** Riducendo l'intervallo di aggiornamento delle miniature viene aumentata la frequenza di aggiornamento delle miniature dei server.

- **Generale**

- **Modalità di debug.** Consente di specificare se impostare la modalità di debug per l'applicazione di controllo remoto. Le impostazioni determinano la granularità degli eventi registrati nei file di log. Per impostazione predefinita, vengono registrati solo gli eventi gravi.
- **Eredita impostazioni aspetto sistema.** Questa impostazione modifica l'aspetto in modo che corrisponda alla combinazione di colori configurata per il server locale (basato su Windows). Per rendere effettive queste impostazioni, è necessario riavviare l'applicazione di controllo remoto.
- **Crea icona sul desktop.** Questa impostazione crea un'icona sul desktop del sistema locale in modo da poter avviare l'applicazione di controllo remoto direttamente dal sistema. È necessario disporre dell'accesso al software di gestione del sistema.
- **Sincronizza con il server di gestione.** Questa impostazione verifica che i dati del server visualizzati nell'applicazione di controllo remoto corrispondano ai dati del server visualizzati dal software di gestione.

Capitolo 5. Provisioning delle risorse

È possibile utilizzare Lenovo XClarity Orchestrator per eseguire il provisioning delle risorse gestite, ad esempio la distribuzione degli aggiornamenti agli strumenti di gestione delle risorse di Lenovo XClarity Administrator e ai server gestiti e la configurazione dei server gestiti.

Provisioning delle configurazioni dei server

I pattern di configurazione dei server vengono utilizzati per configurare rapidamente più server di un singolo insieme di impostazioni di configurazione definite. Ciascun pattern definisce le caratteristiche della configurazione di un tipo specifico di server. È possibile creare un pattern server apprendendo le impostazioni da un server esistente.

Prima di iniziare

Accertarsi che i server che si desidera configurare siano aggiornati con il firmware più recente.

Informazioni su questa attività

La configurazione dei server con l'utilizzo dei pattern è supportata solo per i server ThinkSystem (esclusi SR635 e SR655).

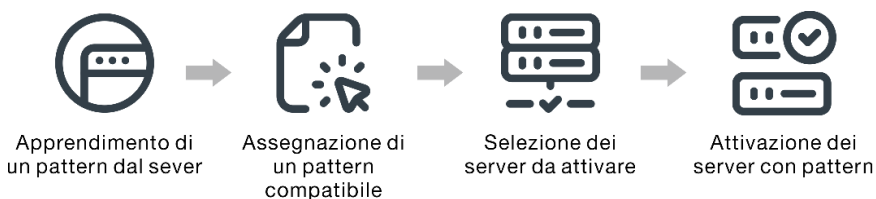
È possibile utilizzare pattern di configurazione dei server per configurare le impostazioni e le definizioni del controller di gestione della scheda di base e UEFI (Unified Extensible Firmware Interface) nei server gestiti. I pattern integrano il supporto per la virtualizzazione degli indirizzi I/O, pertanto è possibile virtualizzare le connessioni fabric del server oppure reimpiegare i server senza interruzione nel fabric.

Non è possibile configurare le seguenti impostazioni.

- Ordine di avvio
- Storage locale e suddivisione in zone SAN
- Adattatori I/O
- Account utenti locali
- Server LDAP

Procedura

La seguente figura mostra il flusso di lavoro per la configurazione di server gestiti.



Passo 1. Creazione di un pattern server

È possibile creare pattern per rappresentare configurazioni differenti utilizzate nel centro dati apprendendo le definizioni e le impostazioni di configurazione dei server esistenti.

Importante: Valutare la possibilità di creare un pattern server per ciascun tipo di server nel proprio centro dati. Ad esempio, creare un pattern server per tutti i server ThinkSystem SR650 e un

altro pattern server per tutti i server ThinkSystem SR850. Non distribuire in un tipo di server un pattern di configurazione server creato per un altro tipo.

Per ulteriori informazioni sulla creazione di pattern server, vedere [Apprendere un pattern di configurazione server da un server esistente](#).

Passo 2. **Assegnazione del pattern a uno o più server gestiti**

È possibile assegnare un pattern a più server. Tuttavia a ogni server può essere assegnato un solo pattern XClarity Orchestrator.

Valutare la possibilità di creare un pattern server per ciascun tipo di server nel proprio centro dati. Ad esempio, creare un pattern server per tutti i server ThinkSystem SR650 e un altro pattern server per tutti i server ThinkSystem SR850.

Non assegnare né distribuire in un tipo di server un pattern server creato per un altro tipo.

Dopo aver assegnato un pattern applicabile a uno o più server di destinazione, XClarity Orchestrator esegue un controllo di conformità sui server per determinare se la configurazione dei server corrisponde al pattern. I server non conformi al pattern assegnato sono segnalati.

Per ulteriori informazioni sulla creazione di pattern server, vedere [Applicazione e attivazione degli aggiornamenti agli strumenti di gestione delle risorse](#).

Passo 3. **Distribuzione del pattern assegnato su server di destinazione**

È possibile distribuire pattern assegnati a uno o più server specifici oppure a gruppi di server. Quando si distribuisce un pattern, le definizioni e le impostazioni di configurazione di tale pattern vengono scritte nella memoria condivisa e successivamente attivate. Alcune impostazioni richiedono un riavvio del sistema prima di essere attivate.

I server devono essere riavviati per attivare determinate modifiche della configurazione, quali le impostazioni delle configurazioni del controller di gestione della scheda di base e UEFI (Unified Extensible Firmware Interface). È possibile scegliere quando attivare le modifiche:

- **Attivazione rinviata** attiva tutte le modifiche della configurazione dopo il successivo riavvio del server. Il server di destinazione deve essere riavviato manualmente per continuare il processo di distribuzione.

Importante: Utilizzare **Riavvia normalmente** per riavviare il server e continuare il processo di aggiornamento. *Non* utilizzare **Riavvia immediatamente**.

Nota: Le impostazioni di un server possono diventare non conformi al relativo pattern se le impostazioni vengono modificate direttamente nel server invece che nei pattern assegnati o se si è verificato un problema durante la distribuzione del pattern assegnato, a causa di un errore del firmware o di un'impostazione non valida. È possibile determinare lo stato di conformità di ciascun server nella scheda **Assegna e distribuisci**.

Attenzione: XClarity Orchestrator non assegna indirizzi IP e I/O ai singoli server in caso di distribuzione di pattern server.

Per ulteriori informazioni sulla creazione di criteri di conformità degli aggiornamenti, vedere [Assegnazione e distribuzione di un pattern di configurazione server](#).

Passo 4. **Modifica e redistribuzione di un pattern** È possibile apportare successive modifiche della configurazione a un pattern esistente. Una volta salvato il pattern, XClarity Orchestrator esegue un controllo di conformità sui server a cui è stato assegnato il pattern per determinare se la

configurazione dei server corrisponde al pattern. È quindi possibile ridistribuire il pattern modificato a tutti i server assegnati o a un sottoinsieme di questi.

Considerazioni sulla configurazione dei server

Prima di iniziare la configurazione dei server con Lenovo XClarity Orchestrator, esaminare le seguenti considerazioni importanti.

Considerazioni sui server

- La configurazione dei server con l'utilizzo dei pattern è supportata solo per i server ThinkSystem (esclusi SR635 e SR655).
- Accertarsi che i server che si desidera configurare siano aggiornati con il firmware più recente.

Considerazioni sui pattern di configurazione

- È possibile assegnare un pattern a più server. Tuttavia a ogni server può essere assegnato un solo pattern XClarity Orchestrator.

Nota: XClarity Orchestrator non impedisce l'assegnazione o la distribuzione di un pattern di configurazione server a un server a cui è assegnato un pattern o un profilo del server in Lenovo XClarity Administrator. La distribuzione di un pattern mediante XClarity Orchestrator potrebbe incidere sulla conformità dei pattern in XClarity Administrator.

- È possibile utilizzare pattern di configurazione dei server per configurare le impostazioni e le definizioni del controller di gestione della scheda di base e UEFI (Unified Extensible Firmware Interface) nei server gestiti. I pattern integrano il supporto per la virtualizzazione degli indirizzi I/O, pertanto è possibile virtualizzare le connessioni fabric del server oppure reimpiegare i server senza interruzione nel fabric.

Non è possibile configurare le seguenti impostazioni.

- Ordine di avvio
 - Storage locale e suddivisione in zone SAN
 - Adattatori I/O
 - Account utenti locali
 - Server LDAP
- Valutare la possibilità di creare un pattern server per ciascun tipo di server nel proprio centro dati. Ad esempio, creare un pattern server per tutti i server ThinkSystem SR650 e un altro pattern server per tutti i server ThinkSystem SR850.
 - Non assegnare né distribuire in un tipo di server un pattern server creato per un altro tipo.
 - Le impostazioni di un server possono diventare non conformi al pattern assegnato nelle seguenti istanze. È possibile determinare lo stato di conformità di ciascun server nella scheda **Assegna e distribuisci**.
 - Le impostazioni di configurazione sono state modificate direttamente sul server invece che nei pattern assegnati.
 - Si è verificato un problema durante la distribuzione dei pattern, ad esempio un errore del firmware o un'impostazione non valida.
 - L'aggiornamento del firmware ha modificato le definizioni e le impostazioni di configurazione.

Nota: La distribuzione potrebbe avere esito negativo se il pattern assegnato si basa su livelli di firmware precedenti. In questo caso, si consiglia di scegliere di apprendere un nuovo pattern basato sul firmware attualmente installato o di modificare il pattern esistente per escludere la configurazione di elementi specifici prima di distribuire il pattern.

Considerazioni sul processo di configurazione

- Mentre la configurazione è in corso, il server di destinazione è bloccato. Non è possibile avviare altre attività di gestione sul server di destinazione finché il processo di configurazione non è completo.

- Una volta distribuito un pattern di configurazione in un server, potrebbero essere necessari uno o più riavvii per attivare completamente le modifiche. È possibile scegliere di attivare tutte le modifiche riavviando immediatamente il server. Se si sceglie di riavviare il server immediatamente, in XClarity Orchestrator viene ridotto al minimo il numero di riavvii richiesti. Se si sceglie l'attivazione rinviata, tutte le modifiche vengono attivate al successivo riavvio del server. Se si sceglie l'attivazione parziale, le modifiche che non richiedono il riavvio del server vengono immediatamente attivate e tutte le altre modifiche vengono attivate al successivo riavvio del server.
- Verificare che nessun processo sia attualmente in esecuzione sul server di destinazione. Se sono in esecuzione dei processi, il processo di configurazione viene messo in coda fino al completamento di tutti gli altri.
- Alcune funzioni avanzate del server vengono attivate utilizzando le chiavi FoD (Feature 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 FoD (Feature on Demand) corrispondente.

Apprendere un pattern di configurazione server da un server esistente

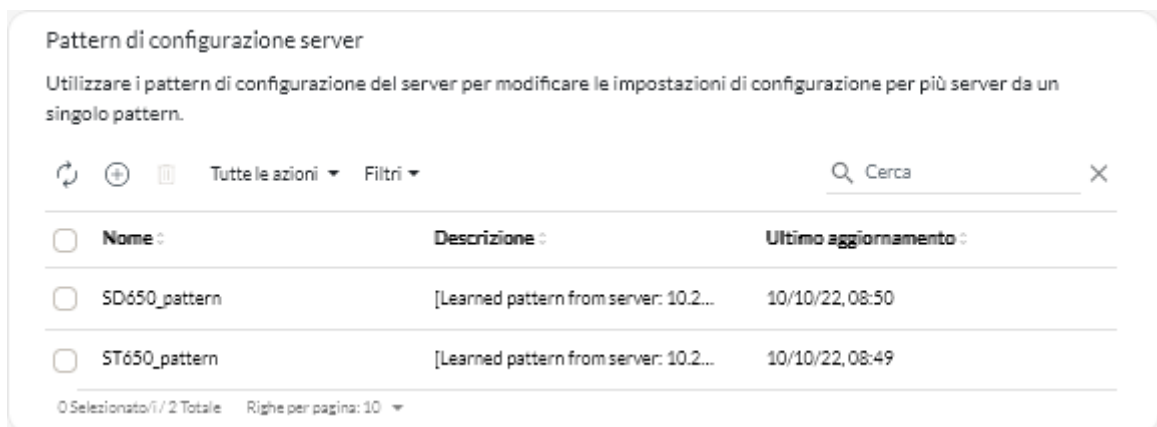
I pattern di configurazione server definiscono le caratteristiche della configurazione di un tipo specifico di server. È possibile creare un pattern server apprendendo le impostazioni da un server esistente.

Prima di iniziare

- Assicurarsi di leggere le considerazioni sulla configurazione dei server prima di creare un pattern di configurazione server (vedere [Considerazioni sulla distribuzione degli aggiornamenti](#)).
- Verificare che il server che si desidera utilizzare per creare il pattern sia online.
- Identificare i gruppi di server con le stesse opzioni hardware e che si desidera configurare allo stesso modo. È possibile utilizzare un pattern server per distribuire le stesse impostazioni di configurazione su più server, in modo da controllare una configurazione comune da una singola postazione.

Per creare un pattern apprendendo la configurazione di un server esistente, completare la seguente procedura.

Passo 1. Sulla barra dei menu di XClarity Orchestrator fare clic su **Provisioning** (🔒) → **Configurazione server**, quindi sulla scheda **Pattern** per visualizzare la scheda Pattern di configurazione server.



Passo 2. Fare clic sull'icona **Crea** (+) per visualizzare la finestra di dialogo Crea pattern di configurazione server.

Crea pattern di configurazione server
✕

Specificare il nome del pattern e la descrizione

Nome

Descrizione

Selezionare un server da richiamare come configurazione base ●

🔄 Tutte le azioni ▾ Filtri ▾
🔍 Cerca ✕

	Dispositivi :	Indirizzi IP :	Nome prodotto :
<input type="radio"/>	Colossus-ST650V2-1	10.240.211.65, 2002:97bc:2bt	ThinkSystem ST650V2
<input type="radio"/>	Mehlow-ST250-1	10.240.211.39, 169.254.95.11	ThinkSystem ST250
<input type="radio"/>	OceanCat-SDV-6	10.240.211.221, 2002:97bc:2t	Lenovo ThinkSystem SD650

0 Selezionato/i / 3 Totale Righe per pagina: 10 ▾

Scopri

Passo 3. Specificare il nome e la descrizione facoltativa del pattern.

Passo 4. Selezionare il server che si desidera utilizzare come base per questo pattern.

Nota: I modelli di dispositivo non supportati vengono visualizzati in grigio e non possono essere selezionati.

Passo 5. Fare clic su **Apprendi**.

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).

Al termine

Nella scheda Pattern è possibile effettuare le azioni che seguono.

- Visualizzare i dettagli del pattern facendo clic sulla riga corrispondente.
- Copiare un pattern selezionato facendo clic sull'icona **Copia** (📄).
- Modificare le impostazioni di configurazione di un pattern facendo clic sulla riga del pattern per visualizzare i dettagli del pattern, apportando le modifiche necessarie e infine facendo clic su **Salva**. Per impostazione predefinita, tutte le impostazioni apprese sono incluse nel pattern. È possibile escludere le impostazioni dal pattern selezionando **Escludi/Includi impostazioni nel pattern** e cancellando le impostazioni che non si desidera includere nel pattern. Le impostazioni cancellate (contrassegnate per l'esclusione) vengono evidenziate in giallo. Quando si fa clic su **Salva**, vengono elencate solo le impostazioni incluse nel pattern. Se sono state escluse impostazioni, è possibile includerle nuovamente.

facendo clic su **Escludi/Includi impostazioni nel pattern**, quindi su **Visualizza impostazioni escluse** e infine selezionando le impostazioni che si desidera includere. Le impostazioni selezionate (contrassegnate per l'inclusione) vengono evidenziate in verde.

Nota: Il controllo di conformità si basa solo sulle impostazioni incluse. Le impostazioni escluse non vengono verificate.

Una volta salvato il pattern modificato, XClarity Orchestrator esegue un controllo di conformità sui server a cui è stato assegnato il pattern per determinare se la configurazione dei server corrisponde al pattern. È quindi possibile distribuire il pattern modificato sui server non conformi (vedere [Assegnazione e distribuzione di un pattern di configurazione server](#)).

The screenshot displays the 'Configurazione pattern' (Pattern Configuration) interface. On the left, a sidebar shows a navigation menu with 'Configurazione pattern' selected, and two other options: 'BMC esteso' and 'UEFI esteso'. Below the menu are two toggle switches: 'Escludi/Includi impostazioni in questo pattern' (checked) and 'Visualizza impostazioni escluse' (checked). At the bottom of the sidebar, there are two colored boxes: a red one labeled 'Esclusi' and a green one labeled 'Inclusi'. The main content area is titled 'Configurazione pattern' and contains a form with the following fields: 'Nome*' (SD650_pattern) and 'Descrizione' ([Learned pattern from server: 10.240.211.221 on 2022-10-10]). Below the form is a list of configuration categories, each with a checked checkbox and a right-pointing arrow: 'Integrated Management Module' (expanded), 'Login Profile', 'General Settings', 'Network Settings Interface', 'UEFI' (expanded), 'System Recovery' (expanded), 'POST Watchdog Timer' (Disable), 'POST Watchdog Timer Value' (5), 'Reboot System on NMI' (Disable), 'Post Load Setup Default' (Disable), '<F1> Start Control' (Auto), 'Devices and I/O Ports', 'Processors', and 'Physical Presence Policy Configuration'.

- Copiare un pattern di configurazione facendo clic sulla riga del pattern per visualizzare i dettagli del pattern, quindi facendo clic su **Salva con nome**.
- Eliminare un pattern selezionato facendo clic sull'icona **Elimina** (🗑️). Se il pattern viene assegnato a uno o più server, viene visualizzata una finestra di dialogo con un elenco di server applicabili. Quando viene confermata la richiesta di eliminazione, verrà annullata l'assegnazione del pattern da questi server.

Nota: Non è possibile eliminare un pattern distribuito attivamente nei server.

- Assegnare e distribuire un pattern a uno o più server di destinazione (vedere [Assegnazione e distribuzione di un pattern di configurazione server](#)).

Assegnazione e distribuzione di un pattern di configurazione server

È possibile assegnare e distribuire un pattern di configurazione server in uno o più server gestiti.

Prima di iniziare

- Assicurarsi di leggere le considerazioni sulla configurazione dei server prima di assegnare o distribuire un pattern a un server (vedere [Considerazioni sulla distribuzione degli aggiornamenti](#)).
- Accertarsi che i server che si desidera configurare siano aggiornati con il firmware più recente.
- Non assegnare né distribuire in un tipo di server un pattern server creato per un altro tipo.
- XClarity Orchestrator non impedisce l'assegnazione o la distribuzione di un pattern di configurazione server a un server a cui è assegnato un pattern o un profilo del server in Lenovo XClarity Administrator. La distribuzione di un pattern mediante XClarity Orchestrator potrebbe incidere sulla conformità dei pattern in XClarity Administrator.
- XClarity Orchestrator non assegna indirizzi IP e I/O ai singoli server in caso di distribuzione di pattern server.

Informazioni su questa attività


Quando un pattern viene assegnato a un server, XClarity Orchestrator esegue un controllo di conformità per confrontare le impostazioni di configurazione correnti sul server con le impostazioni nel pattern di configurazione e aggiorna la colonna **Stato conformità** in base ai risultati. Lo stato della conformità può essere:

- **Conforme.** Tutte le impostazioni di configurazione nel pattern assegnato corrispondono alle impostazioni del server.
- **Non conforme.** Una o più impostazioni di configurazione nel pattern assegnato *non* corrispondono alle impostazioni del server. Passare il mouse sulla cella della tabella per visualizzare un popup in cui sono elencati i valori e le impostazioni senza corrispondenza.
- **In sospeso.** È in corso una distribuzione di pattern o un controllo di conformità.
- **Riavvio in sospeso.** Il server deve essere riavviato per attivare le modifiche della configurazione dopo la distribuzione dei pattern.
- **Non disponibile.** Un pattern non è assegnato al server.

Quando si distribuisce un pattern a un server, XClarity Orchestrator modifica le impostazioni del server in modo che corrispondano al pattern di configurazione server assegnato. Al termine della distribuzione, XClarity Orchestrator esegue il controllo della conformità per verificare che le impostazioni nel pattern assegnato corrispondano all'impostazione del server, quindi aggiorna lo stato di conformità del server.






Procedura

Per assegnare e distribuire un pattern di configurazione server a uno o più server gestiti, completare le seguenti operazioni.

- Passo 1. Sulla barra dei menu di XClarity Orchestrator fare clic su **Provisioning**  → **Configurazione server**, quindi sulla scheda **Assegna e distribuisce** per visualizzare la scheda **Assegna e distribuisce** pattern di configurazione server.

Assegna e distribuisci


Modificare le impostazioni di configurazione su più server assegnando un pattern applicabile e distribuendo il pattern ai server. ⓘ






 Tutte le azioni ▾ Filtri ▾ Cerca X

<input type="checkbox"/> Dispositivi	Stato	Pattern assegnato	Stato conformità	Gruppi
<input type="checkbox"/> Colossus-ST650V2	⊗ Critico	Nessuna ass... ▾	i Nessun patterr	Non disponibile
<input type="checkbox"/> Mehlow-ST250-1	⊗ Critico	Nessuna ass... ▾	i Nessun patterr	Non disponibile
<input type="checkbox"/> OceanCat-SDV-6	⊙ Normale	Nessuna ass... ▾	i Nessun patterr	Non disponibile

0 Selezionato/i / 3 Totale Righi per pagina: 10 ▾

Passo 2. Assegnare un pattern a uno o più server.

1. Selezionare uno o più server.
2. Fare clic sull'icona **Assegna**  per visualizzare la finestra di dialogo Assegna pattern di configurazione server.

Assegna pattern di configurazione server X

Scegliere un pattern da assegnare ai server selezionati. Il pattern è assegnato solo ai server applicabili.

Pattern da assegnare:

Applica a gruppi di risorse specifici:

Assegna pattern a:

- Tutti i dispositivi applicabili (sovrascrivi i pattern assegnati)
- Dispositivi applicabili senza assegnazione pattern
- Solo i dispositivi applicabili selezionati (sovrascrivi i pattern assegnati)
- Solo i dispositivi applicabili selezionati senza un'assegnazione pattern

3. Selezionare il pattern che si desidera assegnare.

Nota:

- Questo elenco mostra tutti i pattern applicabili per i server specifici. L'elenco potrebbe essere incompleto se il server Orchestrator sta ancora calcolando i pattern applicabili. In

questo caso chiudere la finestra di dialogo, attendere qualche istante, quindi riaprire la finestra di dialogo.

- Selezionare il pattern **Nessuna assegnazione** per annullare l'assegnazione di un pattern dall'elenco dei dispositivi selezionati.
4. Selezionare la regola di assegnazione. È possibile selezionare uno dei seguenti valori.
 - **Tutti i dispositivi applicabili (sovrascrivono i pattern assegnati)**
 - **Dispositivi applicabili senza assegnazione pattern**
 - **Solo i dispositivi applicabili selezionati (sovrascrivono i pattern assegnati)**
 - **Solo i dispositivi applicabili selezionati senza un'assegnazione pattern**
 5. Fare clic su **Assegna**.

Passo 3. Distribuire il pattern assegnato su server specifici.

1. Selezionare uno o più server.

Nota: I modelli di dispositivo non supportati vengono visualizzati in grigio e non possono essere selezionati.

2. Fare clic sull'icona **Distribuisci** (☑) per visualizzare la finestra di dialogo Distribuisci pattern di configurazione server.

Distribuisci pattern di configurazione server

Selezionare la regola di attivazione, quindi fare clic su Distribuisci per distribuire e attivare il pattern sui server selezionati.

NOTA: Il processo viene eseguito in background e potrebbe richiedere alcuni minuti per essere completato. È possibile accedere alla pagina Processi per visualizzare lo stato di avanzamento del processo.

Applica a gruppi di risorse specifici: Gruppi di dispositivi

Regola di attivazione Attivazione rinviata

Distribuisci

3. Scegliere quando attivare gli aggiornamenti.
 - **Attivazione rinviata** attiva tutte le modifiche della configurazione dopo il successivo riavvio del server. Il server di destinazione deve essere riavviato manualmente per continuare il processo di distribuzione.

Importante: Utilizzare **Riavvia normalmente** per riavviare il server e continuare il processo di aggiornamento. *Non* utilizzare **Riavvia immediatamente**.

4. Fare clic su **Distribuisci**. 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).

Al termine

Nella scheda Pattern è possibile effettuare le azioni che seguono.

- Eseguire manualmente un controllo della conformità della configurazione sui server selezionati facendo clic su **Tutte le azioni** → **Controllo della conformità**.
- Annullare l'assegnazione di un pattern da uno o più server di destinazione assegnando il pattern **Nessuna assegnazione**.
- Inoltrare report sul controllo della conformità di configurazione periodicamente a uno o più indirizzi e-mail facendo clic sull'icona **Crea server d'inoltro dei report** (+). Il report viene inviato utilizzando i filtri dati attualmente applicati alla tabella. Tutte le colonne della tabella visibili e nascoste sono incluse nel report. Per ulteriori informazioni, vedere [Inoltro di report](#).
- Aggiungere un report sulla conformità della configurazione a un server d'inoltro dei report specifico utilizzando i filtri dati attualmente applicati alla tabella facendo clic sull'icona **Aggiungi al server d'inoltro dei report** (→). Se il server d'inoltro dei report include già un report sulla conformità della configurazione, il report viene aggiornato per utilizzare i filtri dati correnti.

Gestione della conformità della configurazione server

Le impostazioni di un server possono diventare non conformi al relativo profilo se le impostazioni sono state modificate senza utilizzare i pattern di configurazione, si è verificato un problema durante l'applicazione di un pattern di configurazione (ad esempio, se il pattern è stato creato da un livello di firmware precedente a quello del server) oppure durante l'applicazione di un aggiornamento firmware che modifica la configurazione del server (ad esempio, con l'aggiunta o l'eliminazione delle impostazioni, la modifica dei comportamenti delle impostazioni, l'aggiunta di nuove opzioni o la variazione degli intervalli dei valori).

Informazioni su questa attività

È possibile determinare lo stato della conformità di ciascun server nella colonna **Stato conformità** della pagina Configurazione server: assegnazione e distribuzione. Se un server non è conforme, passare il cursore sullo stato per determinare il motivo.

Procedura

Per risolvere i problemi di conformità della configurazione, effettuare una delle operazioni che seguono.

- Apprendere un nuovo pattern di configurazione basato sul livello di firmware corrente (vedere [Apprendere un pattern di configurazione server da un server esistente](#)). Quindi, assegnare e applicare il pattern al server (vedere [Assegnazione e distribuzione di un pattern di configurazione server](#)).
- Modificare il pattern di configurazione applicabile per correggere le impostazioni di mancata conformità facendo clic sulla riga del pattern per visualizzare i dettagli del pattern, apportando le modifiche necessarie e infine facendo clic su **Salva**. Per impostazione predefinita, tutte le impostazioni apprese sono incluse nel pattern. È possibile escludere le impostazioni dal pattern selezionando **Escludi/Includi impostazioni nel pattern** e cancellando le impostazioni che non si desidera includere nel pattern. Le impostazioni cancellate (contrassegnate per l'esclusione) vengono evidenziate in giallo. Quando si fa clic su **Salva**, vengono elencate solo le impostazioni incluse nel pattern. Se sono state escluse impostazioni, è possibile includerle nuovamente facendo clic su **Escludi/Includi impostazioni nel pattern**, quindi su **Visualizza impostazioni escluse** e infine selezionando le impostazioni che si desidera includere. Le impostazioni selezionate (contrassegnate per l'inclusione) vengono evidenziate in verde.

Nota: Il controllo di conformità si basa solo sulle impostazioni incluse. Le impostazioni escluse non vengono verificate.

Una volta salvato il pattern modificato, XClarity Orchestrator esegue un controllo di conformità sui server a cui è stato assegnato il pattern per determinare se la configurazione dei server corrisponde al pattern. È quindi possibile distribuire il pattern modificato sui server non conformi (vedere [Assegnazione e distribuzione di un pattern di configurazione server](#)).

- Creare una copia modificata del pattern di configurazione facendo clic sulla riga del pattern per visualizzare i dettagli del pattern, apportando le modifiche necessarie e infine facendo clic su **Salva con nome**. Quindi, assegnare e applicare il pattern al server non conforme (vedere [Assegnazione e distribuzione di un pattern di configurazione server](#)).

Provisioning dei sistemi operativi

È possibile utilizzare Lenovo XClarity Orchestrator per gestire il repository delle immagini del sistema operativo e distribuire le immagini del sistema operativo.

Prima di iniziare

XClarity Orchestrator non distribuisce direttamente i sistemi operativi ai dispositivi. Invia le richieste allo strumento di gestione delle risorse applicabile per eseguire la distribuzione. Accertarsi che lo strumento di gestione delle risorse disponga delle licenze necessarie per eseguire le funzioni di distribuzione del sistema operativo.

Esaminare le considerazioni sulla distribuzione del sistema operativo prima di tentare di distribuire i sistemi operativi ai dispositivi gestiti (vedere [Considerazioni sulla distribuzione del sistema operativo](#)).

Verificare che l'intero firmware sul server gestito sia ai livelli più recenti (vedere [Provisioning degli aggiornamenti alle risorse gestite](#)).

Verificare che la configurazione sul server gestito sia aggiornata (vedere [Provisioning delle configurazioni dei server](#)).

Attenzione: si consiglia di *non* utilizzare XClarity Orchestrator per eseguire una distribuzione del sistema operativo bare metal sulle appliance Converged e ThinkAgile.

Nota: Accertarsi che i server siano gestiti utilizzando XClarity Administrator 4.0 o versioni successive.

Informazioni su questa attività

XClarity Orchestrator fornisce un modo semplice per distribuire le immagini del sistema operativo sui server *bare metal*, su cui generalmente non è installato un sistema operativo. Se si distribuisce un sistema operativo su un server su cui è installato un sistema operativo, XClarity Orchestrator esegue una nuova installazione che sovrascrive le partizioni sui dischi di destinazione.

La quantità di tempo necessaria per distribuire un sistema operativo su un server è determinata da vari fattori.

- La quantità di RAM installata nel server, che incide sul tempo che il server impiega per l'avvio.
- Il numero e i tipi di adattatori I/O installati nel server, che incide sulla quantità di tempo che impiega per raccogliere i dati di inventario. Incide, inoltre, sulla quantità di tempo necessaria per l'avvio del firmware UEFI quando il server viene avviato. Durante una distribuzione del sistema operativo, il server viene riavviato più volte.
- La quantità di traffico di rete. L'immagine del sistema operativo viene scaricata sul server mediante la rete di dati o la rete di distribuzione del sistema operativo.
- La quantità di RAM, processori e storage delle unità disco fisso disponibili per il server e gli strumenti di gestione delle risorse di Orchestrator.

Procedura

La seguente figura mostra il flusso di lavoro per la distribuzione di un'immagine del sistema operativo su un server.



Passo 1. Importare le immagini del sistema operativo.

Prima di poter distribuire un sistema operativo su un server, è necessario prima importare l'immagine del sistema operativo nel repository delle immagini del sistema operativo nello strumento di gestione delle risorse di XClarity Orchestrator. Quando si importa un'immagine del sistema operativo:

- Verifica che ci sia spazio sufficiente nel repository di immagini del sistema operativo prima di importare il sistema operativo. Se non si dispone di spazio sufficiente per l'importazione di un'immagine, eliminare un'immagine esistente dal repository delle immagini del sistema operativo e tentare di importare nuovamente la nuova immagine.
- Crea uno o più profili dell'immagine e memorizza il profilo nel repository di immagini del sistema operativo. Ciascun *profilo* include l'immagine del sistema operativo e le opzioni di installazione.

Per ulteriori informazioni sui profili predefiniti dell'immagine del sistema operativo, vedere [Profili immagine del sistema operativo](#).

Un *sistema operativo di base* è l'immagine completa del sistema operativo importata nel repository di immagini del sistema operativo. L'immagine di base importata contiene i profili predefiniti che descrivono le configurazioni di installazione per l'immagine. Inoltre, è possibile creare profili personalizzati basati sui profili predefiniti nel sistema operativo di base, che possono essere distribuiti per configurazioni specifiche.

Per un elenco di sistemi operativi di base e personalizzati supportati, vedere [Sistemi operativi supportati](#).

Passo 2. Personalizzare e assegnare il profilo del sistema operativo

I profili del sistema operativo vengono creati automaticamente quando si importa un sistema operativo. I profili creati sono basati sul tipo e sulla versione del sistema operativo. È possibile modificare il profilo, tra cui le credenziali del sistema operativo, il nome host, le impostazioni di rete e di storage, le chiavi di licenza e la posizione di storage.

Passo 3. Assegnare e distribuire il profilo del sistema operativo

È possibile assegnare un profilo del sistema operativo a uno o più server di destinazione e quindi distribuire il profilo a tali server. Ricordare che, per distribuire un sistema operativo, lo stato di distribuzione del server deve essere **Pronto**.

XClarity Orchestrator non distribuisce direttamente i sistemi operativi ai dispositivi. Invia invece una richiesta allo strumento di gestione delle risorse applicabile per eseguire la distribuzione, quindi tiene traccia dell'avanzamento della richiesta. XClarity Orchestrator trasferisce le immagini applicabili allo strumento di gestione delle risorse e crea una richiesta di avvio di un processo sullo strumento di gestione delle risorse per eseguire la distribuzione.

Prima di tentare la distribuzione di un'immagine del sistema operativo, ricontrollare [Considerazioni sulla distribuzione del sistema operativo](#).

Per ulteriori informazioni sull'assegnazione e sulla distribuzione di un profilo del sistema operativo, vedere [Distribuzione di un'immagine del sistema operativo](#).

Considerazioni sulla distribuzione del sistema operativo

Prima di tentare la distribuzione di un'immagine del sistema operativo, esaminare le seguenti considerazioni.

Considerazioni sugli strumenti di gestione delle risorse

- Per i dispositivi gestiti mediante Lenovo XClarity Administrator, verificare che l'istanza di XClarity Administrator disponga delle licenze o del periodo di prova necessari per eseguire le funzioni di distribuzione del sistema operativo.
- La distribuzione del sistema operativo non è supportata sui dispositivi gestiti da Lenovo XClarity Management Hub.

Considerazioni sui dispositivi gestiti

- Verificare che la funzione di distribuzione del sistema operativo sia supportata per i dispositivi di destinazione.
- Verificare che nessun processo sia attualmente in esecuzione sul server di destinazione. Per visualizzare un elenco dei processi attivi, fare clic su **Monitoraggio** → **Processi**.
- Verificare che l'intero firmware sul server gestito sia ai livelli più recenti (vedere [Provisioning degli aggiornamenti alle risorse gestite](#)).

- Verificare che la configurazione sul server gestito sia aggiornata (vedere [Provisioning delle configurazioni dei server](#)). Verificare inoltre che il dispositivo di destinazione non abbia un pattern server rinviato o parziale attivato. Se un pattern server è stato rinviato o parzialmente attivato sul server gestito, è necessario riavviare il server per applicare tutte le impostazioni di configurazione. Non tentare di distribuire un sistema operativo su un server con un pattern server parzialmente attivato.

Per determinare lo stato di configurazione del server, consultare il campo **Stato configurazione** nella pagina Riepilogo del server gestito (vedere [Visualizzazione dei dettagli dei dispositivi](#)).

- Accertarsi che sia stata definita una password per l'account radice utilizzato per distribuire il sistema operativo. Per ulteriori informazioni sull'impostazione della password, vedere [Configurazione dei profili del sistema operativo](#).
- Verificare che non sia montato alcun supporto (ad esempio, ISO) sul server di destinazione. Assicurarsi inoltre che non siano attive sessioni di supporti remoti sul controller di gestione.
- Assicurarsi che il timestamp del BIOS sia impostato su data e ora correnti.
- Per i server ThinkSystem
 - Verificare che l'opzione BIOS legacy sia disabilitata. Da Setup Utility del BIOS/UEFI (F1), fare clic su **Configurazione UEFI → Impostazioni di sistema** e verificare che l'opzione BIOS legacy sia impostata su Disabilitato.
 - La funzione XClarity Controller Enterprise è richiesta per la distribuzione del sistema operativo.
- Per i server System x
 - Verificare che l'opzione BIOS legacy sia disabilitata. Da Setup Utility del BIOS/UEFI (F1), fare clic su **Configurazione UEFI → Impostazioni di sistema** e verificare che l'opzione BIOS legacy sia impostata su Disabilitato.
 - Accertarsi che sia installata una chiave FoD (Feature on Demand) per la presenza remota. È possibile determinare se la presenza remota è abilitata, disabilitata o non installata su un server dalla pagina Server (vedere [Visualizzazione dei dettagli dei dispositivi](#)).
- Per i server Flex System, verificare che lo chassis sia acceso.
- Verificare che una chiave FoD (Feature on Demand) per la presenza remota sia installata sui server NeXtScale. È possibile determinare se la presenza remota è abilitata, disabilitata o non installata su un server dalla pagina Server (vedere [Visualizzazione dei dettagli dei dispositivi](#)).
- Per le appliance Converged e ThinkAgile si consiglia di *non* utilizzare XClarity Orchestrator per eseguire una distribuzione del sistema operativo bare metal.

Considerazioni sul sistema operativo

- Verificare di possedere tutte le licenze del sistema operativo applicabili per attivare i sistemi operativi installati. L'utente sarà responsabile dell'acquisizione delle licenze direttamente dal produttore del sistema operativo.
- Verificare che l'immagine del sistema operativo che si intende distribuire sia già caricata nel repository di immagini del sistema operativo. Per informazioni sull'importazione delle immagini, vedere [Importazione delle immagini del sistema operativo](#).
- Le immagini del sistema operativo nel repository di immagini del sistema operativo potrebbero non essere supportate solo su determinate piattaforme hardware. È possibile determinare se un sistema operativo è compatibile con un server specifico da [Sito Web della guida all'interoperabilità del sistema operativo Lenovo](#).
- Installare sempre il sistema operativo più recente per accertarsi di possedere i driver di dispositivo predefiniti dell'adattatore I/O più recenti. Per VMware, utilizzare l'immagine personalizzata Lenovo per ESXi più aggiornata, che include il supporto per gli adattatori più recenti. Per informazioni su come ottenere questa immagine, consultare il [Supporto VMware - Pagina Web dei download](#).

Per ulteriori informazioni sulle limitazioni di sistemi operativi specifici, vedere [Sistemi operativi supportati](#).

Considerazioni sulla rete

- Verificare che tutte le porte richieste siano aperte (vedere [Disponibilità della porta per i sistemi operativi distribuiti](#)).
- Accertarsi che lo strumento di gestione delle risorse sia configurato per utilizzare le reti di dati e di gestione.
- Verificare che lo strumento di gestione delle risorse possa comunicare con il server di destinazione (sia con il controller di gestione della scheda di base sia con la rete di dati dei server) tramite interfacce di rete di dati e di gestione. Per specificare un'interfaccia da utilizzare per la distribuzione del sistema operativo, vedere [Configurazione dell'accesso alla rete](#) nella documentazione online di XClarity Administrator.

Per ulteriori informazioni sulle interfacce e la rete di distribuzione del sistema operativo, vedere [Considerazioni sulla rete](#) nella documentazione online di XClarity Administrator.

- Se la rete è lenta o instabile, è possibile visualizzare i risultati imprevedibili durante la distribuzione dei sistemi operativi.
- È necessario utilizzare gli indirizzi IP assegnati dinamicamente mediante DHCP. Gli indirizzi IP statici non sono supportati.

Per ulteriori informazioni sulle interfacce e la rete di distribuzione del sistema operativo, vedere [Configurazione dell'accesso alla rete](#) e [Considerazioni sulla rete](#) nella documentazione online di XClarity Administrator.

Considerazioni su storage e opzioni di avvio

- È possibile installare il sistema operativo solo su un'unità disco locale. Hypervisor incorporato, driver M.2 e storage SAN non sono supportati.
- Ciascun server deve essere dotato di un adattatore RAID hardware o di HBA SAS/SATA installato e configurato. Il software RAID generalmente presente sull'adattatore di storage SATA Intel integrato o lo storage configurato come JBOD non è supportato. Tuttavia, se non è presente un adattatore RAID hardware, in alcuni casi potrebbe essere possibile abilitare la modalità SATA AHCI dell'adattatore SATA per la distribuzione del sistema operativo oppure impostare i dischi validi non configurati su JBOD. Per ulteriori informazioni, vedere [Il programma di installazione del sistema operativo non è in grado di trovare l'unità disco su cui si desidera eseguire l'installazione](#) nella documentazione online di XClarity Orchestrator.
- Prima di distribuire un sistema operativo, verificare che l'opzione di avvio UEFI sul server di destinazione sia impostata su "Solo avvio UEFI". Le opzioni di avvio "Solo legacy" e "Prima UEFI, poi legacy" non sono supportate per la distribuzione del sistema operativo.
- Ciascun server deve essere dotato di un adattatore RAID hardware installato e configurato.

Attenzione:

- È supportato solo lo storage configurato con RAID hardware.
- Il software RAID generalmente presente sull'adattatore di storage SATA Intel integrato o lo storage configurato come JBOD non è supportato. Tuttavia, se non è presente un adattatore RAID hardware, in alcuni casi potrebbe essere possibile abilitare la modalità **SATA AHCI** dell'adattatore SATA per la distribuzione del sistema operativo oppure impostare i dischi validi non configurati su JBOD.
- Se è abilitato un adattatore SATA, la modalità SATA *non deve* essere impostata su "IDE."
- Lo storage NVMe non è connesso a una scheda madre del server o il controller HBA non è supportato e non deve essere installato nel dispositivo. In caso contrario, la distribuzione del sistema operativo sullo storage non NVMe avrà esito negativo.
- Verificare che la modalità di avvio sicuro sia disabilitata per il server. Se si sta distribuendo un sistema operativo con la modalità di avvio sicuro abilitata (Windows, ad esempio), disabilitare la modalità di avvio sicuro, distribuire il sistema operativo, quindi riabilitare la modalità di avvio sicuro.
- Per i server ThinkServer accertarsi che siano rispettati i seguenti requisiti.

- Le impostazioni di avvio sul server devono includere criteri OpROM di storage impostati su UEFI Only.
- Se si sta distribuendo ESXi e sono presenti adattatori di rete con avvio PXE, disabilitare il supporto PXE degli adattatori di rete prima di distribuire il sistema operativo. La distribuzione è stata completata: è possibile riabilitare il supporto PXE, se desiderato.
- Se si distribuendo ESXi e sono presenti periferiche avviabili nell'elenco dell'ordine di avvio diverse dall'unità su cui deve essere installato il sistema operativo, rimuovere le periferiche avviabili dall'elenco dell'ordine di avvio prima di distribuire il sistema operativo. Una volta completata la distribuzione, è possibile aggiungere nuovamente la periferica avviabile all'elenco. Verificare che l'unità installata sia la prima dell'elenco.

Per ulteriori informazioni sulle impostazioni delle posizioni dello storage, vedere [Configurazione dei profili del sistema operativo](#).

Sistemi operativi supportati

Lenovo XClarity Orchestrator supporta la distribuzione di diversi sistemi operativi. Solo le versioni supportate dei sistemi operativi possono essere caricate nel XClarity Orchestrator repository di immagini del sistema operativo.

Importante:

- Per ulteriori informazioni sulle limitazioni di distribuzione del sistema operativo per dispositivi specifici, vedere [Hardware e software supportati](#) nella documentazione online di XClarity Orchestrator.
- La funzione di gestione della crittografia di XClarity Orchestrator consente la comunicazione delle limitazioni di determinate modalità SSL/TLS minime. Ad esempio, se si seleziona TLS 1.2, solo i sistemi operativi con un processo di installazione che supporta TLS 1.2 e algoritmi di crittografia avanzati possono essere distribuiti tramite XClarity Orchestrator.
- Le immagini del sistema operativo nel repository di immagini del sistema operativo potrebbero non essere supportate solo su determinate piattaforme hardware. È possibile determinare se un sistema operativo è compatibile con un server specifico da [Sito Web della guida all'interoperabilità del sistema operativo Lenovo](#).
- Per informazioni sul supporto e la relativa compatibilità di Hypervisor e sistema operativo e sulle risorse per le soluzioni e i server Lenovo, vedere [Pagina Web del centro di supporto del sistema operativo del server](#).

La seguente tabella riporta i sistemi operativi a 64 bit che possono essere distribuiti da XClarity Orchestrator.

Sistema operativo	Versioni	Note
Red Hat® Enterprise Linux (RHEL) Server	7.2 and later 8.x	<p>Include KVM</p> <p>Nota:</p> <ul style="list-style-type: none"> Tutte le versioni minori esistenti e future sono supportate se non diversamente indicato. Quando si importa la versione DVD dell'immagine del sistema operativo, è supportato solo DVD1. Quando si installa RHEL sui server ThinkSystem, è consigliato RHEL v7.4 o versioni successive.
SUSE® Linux Enterprise Server (SLES)	12.3 and later 15.2 and later	<p>Include gli hypervisor Xen e KVM</p> <p>Nota:</p> <ul style="list-style-type: none"> Tutti i service pack esistenti e futuri sono supportati se non diversamente indicato. Quando si importa la versione DVD dell'immagine del sistema operativo, è supportato solo DVD1.
VMware vSphere® Hypervisor (ESXi)	6.0.x 6.5.x 6.7.x 7.0.x	<p>Le immagini base di VMware vSphere Hypervisor (ESXi) e le immagini di Lenovo VMware ESXi Custom sono supportate.</p> <p>Le immagini Lenovo VMware ESXi Custom sono personalizzate per determinati hardware, in modo da fornire la gestione online della piattaforma, con aggiornamenti e configurazione del firmware, diagnostica della piattaforma e avvisi hardware avanzati. Gli strumenti di gestione Lenovo supportano inoltre la gestione semplificata di ESXi con alcuni server System x. Questa immagine è disponibile per il download da Supporto VMware - Pagina Web dei download. La licenza fornita con l'immagine è una versione di prova gratuita di 60 giorni. L'utente sarà responsabile della soddisfazione di tutti i requisiti di licenza VMware.</p> <p>Importante:</p> <ul style="list-style-type: none"> Tutti i pacchetti di aggiornamento esistenti e futuri sono supportati se non diversamente indicato. Le immagini ESXi base (senza personalizzazione Lenovo) includono solo i driver di dispositivo integrati per rete e storage. L'immagine base non include i driver di dispositivo più recenti (inclusi nelle immagini Lenovo VMware ESXi personalizzate). Per alcune versioni delle immagini Lenovo VMware ESXi Custom potrebbero essere disponibili immagini separate per ThinkSystem, System x e ThinkServer. Nel repository delle immagini del sistema operativo, può essere presente solo un'immagine per ogni specifica versione. La distribuzione di ESXi non è supportata per alcuni server più vecchi. Per ulteriori informazioni sui server supportati, vedere Sito Web della guida all'interoperabilità del sistema operativo Lenovo.

Profili immagine del sistema operativo

L'importazione di un'immagine del sistema operativo genera profili predefiniti del sistema operativo. Ogni profilo predefinito include l'immagine del sistema operativo e le opzioni di installazione dell'immagine.

È possibile modificare i profili per configurare credenziali, rete e impostazioni di storage. È inoltre possibile creare nuovi profili in base ai criteri predefiniti del sistema operativo. Per ulteriori informazioni, vedere [Configurazione dei profili del sistema operativo](#).

La seguente tabella elenca i profili predefiniti delle immagini del sistema operativo create quando si importa un'immagine del sistema operativo. Questa tabella elenca inoltre i pacchetti inclusi in ogni profilo.

Sistema operativo	profilo	Pacchetti inclusi nel profilo	
Red Hat Enterprise Linux (RHEL) Nota: Include KVM	Base	@X Window System @Desktop @Fonts compat-libstdc++-33 compat-libstdc++-33.i686 compat-libstdc++-296 libstdc++.i686 pam.i686	
	Minimo	compat-libstdc++-33 compat-libstdc++-33.i686 compat-libstdc++-296 libstdc++.i686 pam.i686	
	Virtualizzazione	%packages @virtualization @virtualization-client @virtualization-platform @virtualization-tools # begin additional packages @basic-desktop @desktop-debugging @desktop-platform @fonts @general-desktop @graphical-admin-tools @kde-desktop @remote-desktop-clients @x11 @^graphical-server-environment @gnome-desktop @x11 @virtualization-client # end additional packages	libconfig libsysfs libc lm_sensors-libs net-snmp net-snmp-libs redhat-lsb compat-libstdc++-33 compat-libstdc++-296 # begin additional rpms xterm xorg-x11-xdm rdesktop tigervnc-server device-mapper-multipath # end additional rpms
SUSE Linux Enterprise Server (SLES) 12.3 e versioni successive	Base	<pattern>32bit</pattern> <pattern>Basis-Devel</pattern> <pattern>Minimal</pattern> <pattern>WBEM</pattern> <pattern>apparmor</pattern> <pattern>base</pattern> <pattern>documentation</pattern> <pattern>file_server</pattern> <pattern>fips</pattern> <pattern>gateway_server</pattern> <pattern>lamp_server</pattern> <pattern>mail_server</pattern> <pattern>ofed</pattern> <pattern>printing</pattern> <pattern>sap_server</pattern> <pattern>x11</pattern>	
	Minimo	<pattern>Minimal</pattern> <pattern>file_server</pattern> <pattern>sap_server</pattern>	

Sistema operativo	profilo	Pacchetti inclusi nel profilo
	Virtualizzazione-KVM	<pattern>32bit</pattern> <pattern>Minimal</pattern> <pattern>apparmor</pattern> <pattern>base</pattern> <pattern>documentation</pattern> <pattern>file_server</pattern> <pattern>fips</pattern> <pattern>kvm_server</pattern> <pattern>kvm_tools</pattern> <pattern>sap_server</pattern> <pattern>x11</pattern>
	Virtualizzazione-Xen	<pattern>32bit</pattern> <pattern>Minimal</pattern> <pattern>apparmor</pattern> <pattern>base</pattern> <pattern>documentation</pattern> <pattern>file_server</pattern> <pattern>fips</pattern> <pattern>sap_server</pattern> <pattern>x11</pattern> <pattern>xen_server</pattern> <pattern>xen_tools</pattern>
SUSE Linux Enterprise Server (SLES) 15.2 e versioni successive	Base	<pattern>apparmor</pattern> <pattern>devel_basis</pattern> <pattern>enhanced_base</pattern> <pattern>base</pattern> <pattern>basesystem</pattern> <pattern>minimal_base</pattern> <pattern>print_server</pattern> <pattern>sw_management</pattern> <pattern>x11</pattern> <pattern>x11_enhanced</pattern> <pattern>x11_yast</pattern> <pattern>yast2_basis</pattern> <package>wget</package>
	Minimo	<pattern>base</pattern> <pattern>minimal_base</pattern> <pattern>yast2_basis</pattern> <package>wget</package>
	Virtualizzazione-KVM	<pattern>apparmor</pattern> <pattern>devel_basis</pattern> <pattern>enhanced_base</pattern> <pattern>base</pattern> <pattern>basesystem</pattern> <pattern>minimal_base</pattern> <pattern>print_server</pattern> <pattern>sw_management</pattern> <pattern>x11</pattern> <pattern>x11_enhanced</pattern> <pattern>x11_yast</pattern> <pattern>yast2_basis</pattern> <pattern>xen_server</pattern> <pattern>xen_tools</pattern> <package>wget</package>

Sistema operativo	profilo	Pacchetti inclusi nel profilo
	Virtualizzazione-Xen	<pre> <pattern>apparmor</pattern> <pattern>devel_basis</pattern> <pattern>enhanced_base</pattern> <pattern>base</pattern> <pattern>basesystem</pattern> <pattern>minimal_base</pattern> <pattern>print_server</pattern> <pattern>sw_management</pattern> <pattern>x11</pattern> <pattern>x11_enhanced</pattern> <pattern>x11_yast</pattern> <pattern>yast2_basis</pattern> <pattern>xen_server</pattern> <pattern>xen_tools</pattern> <package>wget</package> </pre>
VMware vSphere® Hypervisor (ESXi)	Virtualizzazione	Le immagini base di VMware vSphere Hypervisor (ESXi) e le immagini di Lenovo VMware ESXi Custom sono supportate.

Disponibilità della porta per i sistemi operativi distribuiti

Alcune porte sono bloccate da determinati profili di sistema operativo. Nelle seguenti tabelle sono riportate le porte aperte (non bloccate).

Verificare che l'hypervisor che sta eseguendo l'appliance Lenovo XClarity Orchestrator consenta il traffico di rete (TCP/UDP) sulle porte 139, 445, 3001, 3900, 8443. Queste porte sono necessarie per distribuzione del sistema operativo.

Profilo di virtualizzazione RHEL

Per impostazione predefinita, il profilo di virtualizzazione RHEL (Red Hat Enterprise Linux) blocca tutte le porte, tranne quelle riportate nella seguente tabella.

Tabella 1. Disponibilità della porta per i profili di virtualizzazione RHEL

Porta	TCP o UDP	Direzione	Descrizione comunicazione
22	TCP	In ingresso	Comunicazione SSH
53	TCP, UDP	In uscita/in ingresso	Comunicazione con i dispositivi di rete KVM RHEL
67	TCP, UDP	In uscita/in ingresso	Comunicazione con i dispositivi di rete KVM RHEL
161	UDP	In uscita	Comunicazione con gli agent SNMP
162	UDP	In ingresso	Comunicazione con gli agent SNMP
427	TCP, UDP	In uscita/in ingresso	Comunicazione con l'agent di servizio SLP, agent di directory SLP
3001	TCP	In uscita/in ingresso	Comunicazione con il servizio di distribuzione delle immagini del software di gestione
15988	TCP	In uscita	Comunicazione CIM-XML su HTTP
15989	TCP	In uscita	Comunicazione CIM-XML su HTTP
49152 - 49215	TCP	In uscita/in ingresso	Comunicazione del server virtuale KVM

Profili minimi e di base RHEL

Per impostazione predefinita, i profili minimi e di base RHEL bloccano tutte le porte, tranne quelle riportate nella seguente tabella.

Tabella 2. Disponibilità della porta per i profili minimi e di base RHEL

Porta	TCP o UDP	Direzione	Descrizione comunicazione
22	TCP	In ingresso	Comunicazione SSH
3001	TCP	In uscita/in ingresso	Comunicazione con il servizio di distribuzione delle immagini del software di gestione

Virtualizzazione SLES, profili minimi e di base

Per SLES (SUSE Linux Enterprise Server), alcune porte aperte vengono assegnate dinamicamente in base a versione e profili del sistema operativo. Per un elenco completo delle porte aperte, consultare la documentazione di SUSE Linux Enterprise Server.

Profilo di virtualizzazione VMware ESXi

Per un elenco completo delle porte aperte per VMware vSphere Hypervisor (ESXi) con Personalizzazione Lenovo, consultare la documentazione di VMware per ESXi sul [Sito Web della knowledge base di VMware](#).

Importazione delle immagini del sistema operativo

Prima di poter distribuire un sistema operativo con licenza sui server gestiti, è necessario importare l'immagine nel repository di immagini del sistema operativo .

Informazioni su questa attività

Per informazioni sulle immagini del sistema operativo che è possibile importare e distribuire, inclusi i sistemi operativi base e personalizzati supportati, vedere [Sistemi operativi supportati](#).

Solo per ESXi, è possibile importare più immagini ESXi con la stessa versione principale/minore nel repository delle immagini del sistema operativo.

Solo per ESXi, è possibile importare più immagini ESXi personalizzate con la stessa versione principale/minore e lo stesso numero di build nel repository delle immagini del sistema operativo.

Durante l'importazione di un'immagine del sistema operativo, XClarity Orchestrator:

- Verifica che ci sia spazio sufficiente nel repository di immagini del sistema operativo prima di importare il sistema operativo. Se non si dispone di spazio sufficiente per l'importazione di un'immagine, eliminare un'immagine esistente dal repository e tentare di importare nuovamente la nuova immagine.
- Crea uno o più profili dell'immagine e memorizza il profilo nel repository di immagini del sistema operativo. Ciascun *profilo* include l'immagine del sistema operativo e le opzioni di installazione. Per ulteriori informazioni sui profili predefiniti dell'immagine del sistema operativo, vedere [Profili immagine del sistema operativo](#).

Nota: I browser Internet Explorer e Microsoft Edge hanno un limite di caricamento di 4 GB. Se il file che si sta importando supera 4 GB, considerare l'utilizzo di un altro browser Web (ad esempio Chrome o Firefox).

Procedura

Per importare un'immagine del sistema operativo nel repository di immagini del sistema operativo, completare le seguenti operazioni.

Passo 1. Procurarsi un'immagine ISO del sistema operativo con licenza.

Nota: l'utente sarà responsabile dell'acquisizione delle licenze applicabili per il sistema operativo.

Passo 2. Dalla barra dei menu di XClarity Orchestrator, fare clic su **Provisioning** (🔗) → **Distribuzione sistema operativo** e selezionare la scheda **Gestione sistema operativo** per visualizzare la pagina Gestione sistema operativo.

Passo 3. Fare clic su **Immagini del sistema operativo** nel riquadro di navigazione sinistro per visualizzare la scheda Immagini del sistema operativo.

Gestione sistema operativo

Di seguito è riportato l'elenco delle immagini del sistema operativo gestite e memorizzate in questo server di gestione. È possibile importare una nuova immagine del sistema operativo dalla workstation locale oppure eliminare un'immagine del sistema operativo da questo repository.

Utilizzo dello storage del sistema operativo: 394.2 MB di 185.8 GB.

Immagini sistema operativo

🔄 📁 🗑️ ➡️ Tutte le azioni ▾ Filtri ▾ 🔍 Cerca ✕

<input type="checkbox"/>	Nome sistema operativo ^v	Versione ^v	Stato ^v
<input type="checkbox"/>	esxi7.0_3-20036589.1	7.0	Pronto

0 selezionato / 1 Totale Righi per pagina: 10 ▾

Passo 4. Fare clic sull'icona **Importa file** (📁) per visualizzare la finestra di dialogo Importa immagini del sistema operativo.

Passo 5. Trascinare e rilasciare l'immagine .iso che si desidera importare oppure fare clic su **Sfoglia** per individuare l'immagine ISO che si desidera importare.

Passo 6. **Facoltativo:** selezionare il tipo di checksum e copiare e incollare il valore di checksum nel campo di testo fornito.

Se si seleziona un tipo di checksum, è necessario specificare un valore di checksum per verificare l'integrità e la sicurezza dell'immagine del sistema operativo caricata. Il valore deve provenire da una un'origine sicura, da un'organizzazione attendibile. Se l'immagine caricata corrisponde al valore di checksum, è possibile continuare la distribuzione in tutta sicurezza. Altrimenti, è necessario caricare nuovamente l'immagine oppure controllare il valore di checksum.

Sono supportati i seguenti tipi di checksum: MD5, SHA1 e SHA256.

Passo 7. Fare clic su **Importa**.

XClarity Orchestrator carica l'immagine del sistema operativo nel repository di immagini del sistema operativo e aggiunge i profili predefiniti del sistema operativo alla scheda **Profili sistema operativo**.

Suggerimento: l'immagine ISO viene caricata su una connessione di rete sicura. Pertanto, l'affidabilità e le prestazioni della rete incidono sui tempi di importazione dell'immagine.

Al termine

Da questa pagina, è possibile completare le seguenti azioni.

- Eliminare un'immagine del sistema operativo selezionata facendo clic sull'icona **Elimina** (🗑️).
- Visualizzare e modificare i profili del sistema operativo facendo clic sulla barra dei menu di XClarity Orchestrator e selezionando **Provisioning** (🔗) → **Distribuzione sistema operativo**. Quindi fare clic su **Profili sistema operativo**, selezionare il profilo e fare clic sull'icona **Modifica** (✎) (vedere Configurazione dei profili del sistema operativo).
- Eliminare i profili del sistema operativo facendo clic sulla barra dei menu di XClarity Orchestrator e selezionando **Provisioning** (🔗) → **Distribuzione sistema operativo**. Quindi fare clic sulla scheda **Profili sistema operativo**, selezionare i profili e fare clic sull'icona **Elimina** (🗑️).

Nota: Se si elimina l'ultimo profilo rimanente di un sistema operativo, anche il sistema operativo viene eliminato.

Configurazione dei profili del sistema operativo

I profili del sistema operativo vengono creati automaticamente quando si importa un sistema operativo. I profili creati sono basati sul tipo e sulla versione del sistema operativo. È possibile modificare il profilo, tra cui le credenziali del sistema operativo, il nome host, le impostazioni di rete e di storage, le chiavi di licenza e la posizione di storage.

Prima di iniziare

Esaminare le considerazioni prima di distribuire un sistema operativo su un dispositivo server gestito. Per informazioni, vedere [Considerazioni sulla distribuzione del sistema operativo](#).

Procedura

Per configurare un profilo del sistema operativo per la distribuzione, attenersi alla procedura descritta di seguito.

- Passo 1. Dalla barra dei menu di XClarity Orchestrator, fare clic su **Provisioning** (🔗) → **Distribuzione sistema operativo** e selezionare la scheda **Profili sistema operativo** per visualizzare la pagina Profili sistema operativo.
- Passo 2. Selezionare il profilo del sistema operativo.
- Passo 3. Fare clic sull'icona **Modifica** (✎) per visualizzare la scheda Dettagli profilo sistema operativo.

Profilo sistema operativo
Basato su esxi7.0_3-20036589.1 e sul profilo Virtualization.

Nome
esxi7.0_3-20036589.1-x86_64-install-Virtualization

Descrizione
Generated by default

Credenziali sistema operativo
ESXi/Linux

Nome utente
root

Nuova password

Conferma password

Nome host

Utilizza nome host predefinito

Impostazione di rete

Utilizza DHCP

Impostazione indirizzo MAC

Utilizza AUTOMATICO

Storage

Utilizza unità disco

Passo 4. Configurare gli attributi del profilo.

- **Nome.** La modifica del nome del profilo crea un nuovo profilo del sistema operativo.
- **Descrizione.** Modificare la descrizione per questo profilo del sistema operativo.
- **Credenziali sistema operativo.** Inserire le credenziali del sistema operativo per l'account amministratore da utilizzare per eseguire il login al sistema operativo.
- **Nome host.** Selezionare le opzioni da utilizzare per il nome host. È possibile scegliere uno dei seguenti valori.
 - **Utilizza nome host predefinito** (predefinito). Il nome host è "nodo", seguito dai primi 11 caratteri dell'ID del dispositivo, ad esempio nodoABC31213310
- **Impostazione di rete.** Selezionare le impostazioni IP per questo profilo. È possibile scegliere uno dei seguenti valori.
 - **DHCP** (predefinito). Utilizzare l'infrastruttura DHCP esistente per assegnare gli indirizzi IPv4 ai server.
- **Impostazione indirizzo MAC.** Selezionare l'indirizzo MAC della porta sull'host in cui deve essere installato il sistema operativo. È possibile scegliere uno dei seguenti valori.

Nota: Le porte di rete virtuali non sono supportate. Non utilizzare una porta di rete fisica per simulare più porte di rete virtuali.

- **Utilizza AUTO** (predefinito). Rileva automaticamente le porte Ethernet che possono essere configurate e utilizzate per la distribuzione. Il primo indirizzo MAC (porta) rilevato viene utilizzato per impostazione predefinita. Se viene rilevata la connettività su un indirizzo MAC differente, il server viene riavviato automaticamente per utilizzare l'indirizzo MAC appena rilevato per la distribuzione. Lo strumento di gestione delle risorse di XClarity Administrator può rilevare automaticamente le porte di rete negli slot 1-16. Almeno una porta negli slot 1-16 deve disporre di una connessione allo strumento di gestione delle risorse applicabile.

Se si desidera utilizzare una porta di rete nello slot 17 o superiore per l'indirizzo MAC, non è possibile utilizzare l'opzione AUTO.

- **Storage.** Selezionare la posizione di storage dove si desidera distribuire l'immagine del sistema operativo.
 - **Utilizza unità disco.** Installare l'immagine del sistema operativo sulla prima unità disco RAID locale enumerata nel server gestito. Sono supportate solo unità disco collegate a un controller RAID o HBA SAS/SATA.

Se la configurazione RAID sul server non è configurata correttamente o se è inattiva, potrebbe non vedere il disco locale sul server Orchestrator. Per risolvere il problema, abilitare la configurazione RAID tramite i pattern di configurazione (vedere [Apprendere un pattern di configurazione server da un server esistente](#)) o tramite il software di gestione RAID sul server.




Nota:

- Se è presente anche un'unità M.2, l'unità disco deve essere configurata per la modalità RAID hardware.
- Se è abilitato un adattatore SATA, la modalità SATA *non deve* essere impostata su **IDE**.
- Per i server ThinkServer, la configurazione è disponibile solo mediante il software di gestione RAID sul server.

Passo 5. Fare clic su **Salva**.

Al termine

È possibile eseguire le seguenti azioni.

- Assegnare un profilo del sistema operativo a uno o più server dalla scheda **Assegna e distribuisci** facendo clic durante la selezione dei server e quindi scegliendo l'icona **Assegna** () oppure facendo clic sull'icona **Assegna** () e quindi selezionando un gruppo di server. Dopo avere selezionato il profilo del sistema operativo, è possibile scegliere di assegnarlo a:
 - **Tutti i dispositivi applicabili (sovrascrivi i profili assegnati)**
 - **Dispositivi applicabili senza assegnazione del profilo**
 - **Solo i dispositivi applicabili selezionati (sovrascrivi i profili assegnati)**
 - **Solo i dispositivi applicabili selezionati senza assegnazione del profilo**
- Eliminare i profili del sistema operativo selezionato facendo clic sull'icona **Elimina** ()

Nota: Se si elimina l'ultimo profilo rimanente di un sistema operativo, anche il sistema operativo viene eliminato.

Distribuzione di un'immagine del sistema operativo

È possibile utilizzare Lenovo XClarity Orchestrator per distribuire un sistema operativo sui server gestiti.

Prima di iniziare

Leggere le relative considerazioni sulla distribuzione del sistema operativo prima di tentare di distribuire i sistemi operativi sui server gestiti (vedere [Considerazioni sulla distribuzione del sistema operativo](#)).

Attenzione: Se il server dispone attualmente di un sistema operativo installato, la distribuzione dell'immagine del sistema operativa sovrascriverà il sistema operativo corrente.

Procedura

Per distribuire un'immagine del sistema operativo su uno o più server gestiti, completare una delle seguenti procedure.

- **Per dispositivi specifici**

1. Dalla barra dei menu di XClarity Orchestrator fare clic su **Provisioning** (🔧) → **Distribuzione sistema operativo**, quindi sulla scheda **Assegna e distribuisce** per visualizzare la scheda Assegna e distribuisce pattern di configurazione server.



2. Selezionare uno o più server sui quali distribuire il sistema operativo.
3. Per ciascun server di destinazione, selezionare il profilo dell'immagine del sistema operativo da distribuire nell'elenco a discesa **Profili sistema operativo**. Accertarsi di selezionare un profilo del sistema operativo compatibile con il server di destinazione.
4. Verificare che lo stato di distribuzione nella colonna **Stato** sia Pronto per tutti i server selezionati.
5. Fare clic sull'icona **Distribuisce** (☺) per visualizzare la finestra di dialogo Distribuisce profilo.
6. Fare clic sull'icona **Distribuisce** per avviare la distribuzione del sistema operativo. 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).

- **Per tutti i dispositivi di un gruppo specifico**

1. Dalla barra dei menu di XClarity Orchestrator fare clic su **Provisioning** (🔧) → **Distribuzione sistema operativo**, quindi sulla scheda **Assegna e distribuisce** per visualizzare la scheda Assegna e distribuisce pattern di configurazione server.
2. Assegnare un profilo del sistema operativo al gruppo di server.
 - a. Fare clic sull'icona **Assegna** (🔗) per visualizzare la finestra di dialogo Assegna profilo.

- b. Selezionare il profilo da assegnare.
 - c. Selezionare il gruppo di dispositivi da assegnare.
 - d. Scegliere i dispositivi nel gruppo da assegnare.
 - **Tutti i dispositivi applicabili (sovrascrivi i profili assegnati)**
 - **Dispositivi applicabili senza assegnazione del profilo**
 - **Solo i dispositivi applicabili selezionati (sovrascrivi i profili assegnati)**
 - **Solo i dispositivi applicabili selezionati senza assegnazione del profilo**
 - e. Fare clic su **Distribuisci**.
3. Fare clic sull'icona **Distribuisci** (☑) per visualizzare la finestra di dialogo Distribuisci profilo.

4. Selezionare il gruppo di dispositivi su cui si desidera distribuire il profilo del sistema operativo assegnato.

5. Fare clic sull'icona **Distribuisci** per avviare la distribuzione del sistema operativo. 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).

Provisioning degli aggiornamenti alle risorse gestite

È possibile utilizzare Lenovo XClarity Orchestrator per gestire i livelli software correnti sugli strumenti di gestione delle risorse e i server gestiti di Lenovo XClarity Administrator. È possibile utilizzare il catalogo degli aggiornamenti per conoscere i livelli software disponibili, utilizzare i criteri di conformità degli aggiornamenti per identificare quali risorse devono essere aggiornate in base ai criteri personalizzati e quindi distribuire gli aggiornamenti a queste risorse.

Procedura

La seguente figura mostra il flusso di lavoro per l'aggiornamento delle risorse gestite.



Passo 1. Aggiornare il catalogo

Il *repository degli aggiornamenti* contiene un catalogo e i pacchetti di aggiornamento applicabili alle risorse gestite.

Il *catalogo* contiene informazioni sugli aggiornamenti attualmente disponibili. Il catalogo organizza gli aggiornamenti per tipi di risorsa (piattaforme) e componenti. Quando si aggiorna il catalogo, XClarity Orchestrator recupera le informazioni sugli ultimi aggiornamenti disponibili dal sito Web del supporto Lenovo e le memorizza nel *repository degli aggiornamenti*.

Importante: XClarity Orchestrator deve essere collegato a Internet per aggiornare il catalogo.

Quando i nuovi pacchetti di aggiornamento diventano disponibili è necessario importare i pacchetti di aggiornamento applicabili, prima di poter applicare un aggiornamento. L'aggiornamento del catalogo non importa automaticamente i pacchetti di aggiornamento.

Quando XClarity Orchestrator viene installato per la prima volta, il *repository degli aggiornamenti* è vuoto.

Passo 2. Scaricare o importare i pacchetti di aggiornamento nel repository

Se XClarity Orchestrator è collegato a Internet, è possibile scaricare i pacchetti di aggiornamento elencati nel catalogo degli aggiornamenti direttamente dal sito Web del supporto Lenovo. Se XClarity Orchestrator non è collegato a Internet, è possibile importare manualmente i pacchetti di aggiornamento scaricati in precedenza dal [Sito Web dell'Assistenza del Centro Dati Lenovo](#) in una workstation con accesso di rete all'host XClarity Orchestrator.

Se si sceglie di scaricare una versione secondaria, verranno scaricati anche i pacchetti di aggiornamento prerequisiti.

Quando si importano manualmente i pacchetti del repository, è necessario importare il payload (.tgz), i metadati (.xml), il log delle modifiche (.chg) e il file readme (.txt).

Quando si importano manualmente gli aggiornamenti, è necessario importare i file richiesti in base al tipo di risorsa.

- Per i server ThinkSystem V3, importare il singolo pacchetto di aggiornamento (*.zip). Il file zip contiene il payload, i file di metadati (diversi file *.json), il file della cronologia delle modifiche (*.chg) e il file readme (*.txt).
- Per i dispositivi client ThinkEdge, importare il payload (Windows.exe). Il file readme (.txt) è facoltativo. Nota: al momento è supportato solo l'aggiornamento del **pacchetto di utilità flash del BIOS per Windows**.
- Per XClarity Management Hub e XClarity Management Hub 2.0, importare il singolo file del pacchetto di aggiornamento (.tgz). Questo file contiene payload, metadati, cronologia delle modifiche e file readme.
- Per tutte le altre risorse (inclusi XClarity Administrator, i server ThinkEdge, ThinkSystem V1 e V2, nonché di dispositivi legacy), importare il payload (.zip, .uxz, .tar.gz, .tar, .bin), i metadati (.xml), il registro delle modifiche (.chg) e il file leggimi (.txt).

Per ulteriori informazioni sull'importazione degli aggiornamenti, vedere [Download e importazione degli aggiornamenti](#).

Passo 3. **Creazione e assegnazione di criteri di conformità degli aggiornamenti**

I *criteri di conformità degli aggiornamenti* permettono di verificare che il software o il firmware di determinate risorse gestite sia aggiornato, contrassegnando le risorse che richiedono attenzione. Ciascuno dei criteri di conformità degli aggiornamenti identifica le risorse da monitorare e il livello software o firmware da installare affinché le risorse risultino conformi. XClarity Orchestrator utilizza quindi tali criteri per verificare lo stato degli strumenti di gestione delle risorse e identificare le risorse non conformi.

Quando si creano criteri di conformità degli aggiornamenti, è possibile scegliere di utilizzare XClarity Orchestrator per contrassegnare una risorsa quando il software o firmware della risorsa è inferiore al livello richiesto.

Una volta assegnato un criterio di conformità degli aggiornamenti a una risorsa, XClarity Orchestrator controlla lo stato di conformità della risorsa quando il repository degli aggiornamenti viene modificato. Se il software o il firmware sulla risorsa non è conforme ai criteri assegnati, XClarity Orchestrator contrassegna tale risorsa come non conforme nella pagina Applica/Attiva, in base alle regole specificate nei criteri di conformità degli aggiornamenti.

Ad esempio, è possibile creare criteri di conformità degli aggiornamenti che definiscono il livello software di base per XClarity Administrator e quindi assegnare tali criteri a tutti gli strumenti di gestione delle risorse di XClarity Administrator. Quando il catalogo degli aggiornamenti viene aggiornato e viene scaricato o importato un nuovo aggiornamento, le istanze XClarity Administrator potrebbero risultare non conformi. Quando ciò si verifica, XClarity Orchestrator aggiorna la pagina Applica/Attiva per mostrare quali istanze XClarity Administrator non sono conformi e genera un avviso.

Per ulteriori informazioni sulla creazione di criteri di conformità degli aggiornamenti, vedere [Creazione e assegnazione di criteri di conformità degli aggiornamenti](#).

Passo 4. **Applicare e attivare gli aggiornamenti**

XClarity Orchestrator non applica automaticamente gli aggiornamenti. Per aggiornare le risorse software è necessario applicare manualmente e attivare l'aggiornamento alle risorse selezionate che non sono conformi ai criteri di conformità degli aggiornamenti assegnati.

XClarity Orchestrator non aggiorna direttamente le risorse. Invia invece una richiesta allo strumento di gestione delle risorse applicabile per eseguire l'aggiornamento, quindi tiene traccia dell'avanzamento della richiesta. XClarity Orchestrator identifica le dipendenze necessarie per eseguire l'aggiornamento, verifica che le risorse di destinazione vengano aggiornate nell'ordine corretto, trasferisce i pacchetti di aggiornamento applicabili allo strumento di gestione delle risorse e crea una richiesta di avvio di un processo sullo strumento di gestione delle risorse per eseguire l'aggiornamento.

Per ulteriori informazioni sull'applicazione degli aggiornamenti, vedere [Applicazione e attivazione degli aggiornamenti agli strumenti di gestione delle risorse](#) e [Applicazione e attivazione degli aggiornamenti ai server gestiti](#).

Considerazioni sulla distribuzione degli aggiornamenti

Prima di distribuire gli aggiornamenti mediante Lenovo XClarity Orchestrator, valutare le seguenti considerazioni importanti.

- Per prestazioni ottimali, verificare che gli strumenti di gestione delle risorse di Lenovo XClarity Administrator stiano eseguendo la versione 3.2.1 o successive
- Accertarsi che il repository degli aggiornamenti contenga i pacchetti di aggiornamento che si intende applicare. In caso contrario, aggiornare il catalogo prodotti e scaricare gli aggiornamenti appropriati (vedere [Download e importazione degli aggiornamenti](#)).
- Verificare che nessun processo sia attualmente in esecuzione sulla risorsa di destinazione. Se sono in esecuzione dei processi, il processo di aggiornamento viene messo in coda fino al completamento di tutti gli altri processi.
- Se alla risorsa sono assegnati criteri di conformità degli aggiornamenti che determinano violazioni della conformità, queste devono essere corrette modificando i criteri di conformità o assegnando criteri alternativi.
- Se si sceglie di installare un pacchetto di aggiornamento firmware che contiene aggiornamenti per più componenti, vengono aggiornati tutti i componenti a cui viene applicato il pacchetto di aggiornamento.

Considerazioni sulle risorse

- La funzione di aggiornamento supporta l'aggiornamento solo di server e strumenti di gestione delle risorse. Per i server ThinkSystem SR635 e SR655 sono supportati solo gli aggiornamenti firmware UEFI e BMC.

Per i dispositivi ThinkSystem e ThinkAgile, gli aggiornamenti firmware non sono supportati per il controller gestito della scheda di base e i banchi di backup UEFI. Aggiornare il banco primario e abilitare quindi la promozione automatica.

- Prima di aggiornare i dispositivi gestiti, leggere le importanti considerazioni sull'aggiornamento (vedere [Considerazioni sugli aggiornamenti firmware](#) nella documentazione online di XClarity Administrator).
- Prima di aggiornare gli strumenti di gestione delle risorse di XClarity Administrator verificare di aver letto le considerazioni sugli aggiornamenti per XClarity Administrator (vedere [Aggiornamento del server di gestione di XClarity Administrator](#) nella documentazione online di XClarity Administrator).
- Prima di aggiornare gli strumenti di gestione delle risorse di XClarity Administrator, eseguire il backup dell'appliance virtuale creando un clone (vedere [Backup di XClarity Administrator](#) nella documentazione online di XClarity Administrator).

- Verificare che alle risorse che si desidera aggiornare sia stato assegnato un criterio di conformità degli aggiornamenti.
- XClarity Orchestrator trasferisce gli aggiornamenti applicabili allo strumento di gestione delle risorse durante il processo di aggiornamento. Verificare che sul disco del server di gestione sia disponibile spazio sufficiente per gli aggiornamenti.
- Per i dispositivi client ThinkEdge, sono supportati solo gli aggiornamenti BIOS sui server con sistema operativo Windows 10 versione 1809 o successiva a 64 bit. Le edizioni speciali (come 10 S o 10x) attualmente non sono supportate.
- Non è possibile scaricare gli aggiornamenti del firmware per i seguenti IBM dall'interfaccia Web. Scaricare manualmente gli aggiornamenti dal sito ibm.com e importarli.
 - IBM System x iDataPlex dx360 M4
 - IBM System series M4
 - IBM System x3100 M5 e x3250 M
 - IBM System x3850 X5 e x3950 X5
 - IBM System x3850 X6 e x3950 X6
 - IBM Flex System

Considerazioni sul repository

- Accertarsi che il repository degli aggiornamenti contenga i pacchetti di aggiornamento che si intende applicare. In caso contrario, aggiornare il catalogo prodotti e scaricare gli aggiornamenti appropriati (vedere [Download e importazione degli aggiornamenti](#)). È possibile scegliere di installare gli aggiornamenti prerequisiti, oltre all'aggiornamento di destinazione. Tutti gli aggiornamenti prerequisiti devono essere scaricati nel repository prima di poterli applicare.

In alcuni casi, potrebbero essere necessarie più versioni per applicare un aggiornamento e tutte le versioni devono essere scaricate nel repository.

Considerazioni sul processo di aggiornamento

- Se si sceglie di installare un pacchetto di aggiornamento firmware che contiene aggiornamenti per più componenti, vengono aggiornati tutti i componenti a cui viene applicato il pacchetto di aggiornamento.
- Quando si effettua una richiesta di applicazione degli aggiornamenti a uno strumento di gestione delle risorse e a uno o più dispositivi gestiti da questo strumento di gestione delle risorse, gli aggiornamenti vengono applicati prima allo strumento di gestione delle risorse.
- Mentre è in corso un aggiornamento, la risorsa di destinazione è bloccata. Non è possibile avviare altre attività di gestione sulla risorsa di destinazione finché il processo di aggiornamento non è completo.
- Una volta applicato un aggiornamento a una risorsa, potrebbero essere necessari uno o più riavvii per attivare completamente l'aggiornamento. È possibile scegliere se riavviare la risorsa immediatamente, ritardare l'attivazione o dare priorità all'attivazione. Se si sceglie il riavvio immediato, XClarity Orchestrator riduce al minimo il numero di riavvii richiesti. Se si sceglie l'attivazione ritardata, gli aggiornamenti vengono attivati al successivo riavvio della risorsa. Se si sceglie di dare priorità all'attivazione, gli aggiornamenti vengono attivati immediatamente sul controller di gestione della scheda di base e tutti gli altri aggiornamenti vengono attivati al successivo riavvio del dispositivo.
- Se si sceglie di riavviare la risorsa durante il processo di aggiornamento (*attivazione immediata*), accertarsi che tutti i carichi di lavoro in esecuzione siano stati arrestati oppure, se si sta lavorando in un ambiente virtualizzato, siano stati spostati su una risorsa differente.
- Alcuni aggiornamenti firmware richiedono il collegamento di un monitor al dispositivo di destinazione. Il processo di aggiornamento potrebbe non riuscire se non è collegato un monitor.

Download e importazione degli aggiornamenti

Gli aggiornamenti dei pacchetti devono essere disponibili nel repository degli aggiornamenti per poterli applicare alle risorse gestite.

Prima di iniziare

Per recuperare le informazioni più recenti sui pacchetti di aggiornamento, selezionare il tipo di risorsa e fare clic su **Controlla aggiornamenti** → **Aggiornamento selezionato** per ottenere informazioni su tutti i pacchetti di aggiornamento disponibili oppure fare clic su **Controlla aggiornamenti** → **Aggiornamento selezionato - Solo più recente** per ottenere informazioni solo sul pacchetto di aggiornamento più recente per tale risorsa. Ordinare quindi la tabella utilizzando la colonna **Nome** per ordinare gli aggiornamenti per versione.

XClarity Orchestrator utilizza un'unità separata per il repository degli aggiornamenti. Il requisito minimo di dimensioni per questa unità è 100 GB.

Informazioni su questa attività

È possibile scaricare o importare un singolo pacchetto del repository XClarity Administrator o uno o più pacchetti di aggiornamento alla volta.








- **Pacchetti del repository XClarity Administrator** I pacchetti del repository Lenovo XClarity Administrator contengono i più recenti aggiornamenti firmware disponibili in una data specifica per la maggior parte dei dispositivi supportati e i criteri di conformità del firmware predefiniti aggiornati. Quando si scarica un pacchetto del repository dalla [Pagina Web di download di XClarity Administrator](#), ogni pacchetto di aggiornamento nel pacchetto del repository viene estratto e importato nel repository degli aggiornamenti e viene eliminato il file payload del repository. I criteri di conformità del firmware predefiniti aggiornati vengono importati anche come criteri predefiniti. Non è possibile modificare questo criterio predefinito.

Sono disponibili i seguenti pacchetti del repository.

- **Invgy_sw_lxca_cmmswitchrepo $x-x.x.x$ _anyos_noarch**. Contiene gli aggiornamenti firmware per tutti i CMM e gli switch Flex System.
- **Invgy_sw_lxca_storagerackswitchrepo $x-x.x.x$ _anyos_noarch**. Contiene gli aggiornamenti firmware per tutti gli switch RackSwitch e i dispositivi Lenovo Storage.
- **Invgy_sw_lxca_systemxrepo $x-x.x.x$ _anyos_noarch**. Contiene gli aggiornamenti firmware per i server Converged serie HX, Flex System e System x.
- **Invgy_sw_thinksystemrepo $x-x.x.x$ _anyos_noarch**. Contiene gli aggiornamenti firmware per tutti i server ThinkSystem.
- **Invgy_sw_lxca_thinksystemv2repo $x-x.x.x$ _anyos_noarch**. Contiene gli aggiornamenti firmware per tutti i server ThinkSystem V2.
- **Invgy_sw_lxca_thinksystemv3repo $x-x.x.x$ _anyos_noarc**. Contiene gli aggiornamenti firmware per tutti i server ThinkAgile e ThinkSystem V3.

Quando si importano manualmente i pacchetti del repository, è necessario importare il payload (.tgz), i metadati (.xml), il log delle modifiche (.chg) e il file readme (.txt).

È possibile determinare lo stato di un pacchetto del repository dalla colonna **Stato** nella pagina Gestione repository. Questa colonna contiene i seguenti valori.

-  **Non scaricato**. Il pacchetto del repository è disponibile sul Web ma non è stato scaricato ed estratto nel repository degli aggiornamenti.
-  **Download in sospeso**. Il pacchetto del repository è in coda per il download da Internet.
-  **In download**. È in corso il download del pacchetto del repository da Internet.
-  **Applicazione in sospeso**. Il pacchetto del repository è in coda per l'estrazione dei pacchetti di aggiornamento nel pacchetto del repository nel repository degli aggiornamenti.
-  **Applicazione**. I pacchetti di aggiornamento nel pacchetto del repository sono in fase di estrazione nel repository degli aggiornamenti.
-  **x di y scaricati**. Alcuni pacchetti del repository sono stati scaricati ed estratti nel repository degli aggiornamenti. I numeri tra parentesi indicano il numero di aggiornamenti scaricati e disponibili.
-  **Scaricato**. Tutti i pacchetti di aggiornamento nel pacchetto del repository vengono memorizzati nel repository degli aggiornamenti e il file payload del pacchetto del repository viene eliminato.

- **Pacchetti di aggiornamento** Se XClarity Orchestrator è collegato a Internet, è possibile scaricare i pacchetti di aggiornamento elencati nel catalogo degli aggiornamenti direttamente dal sito Web del supporto Lenovo. Se XClarity Orchestrator non è collegato a Internet, è possibile importare manualmente i pacchetti di aggiornamento scaricati in precedenza dal [Sito Web dell'Assistenza del Centro Dati Lenovo](#) in una workstation con accesso di rete all'host XClarity Orchestrator.






Se si sceglie di scaricare una versione secondaria, verranno scaricati anche i pacchetti di aggiornamento prerequisites.

Quando si importano manualmente gli aggiornamenti, è necessario importare i file richiesti in base al tipo di risorsa.

- Per i server ThinkSystem V3, importare il singolo pacchetto di aggiornamento (*.zip). Il file zip contiene il payload, i file di metadati (diversi file *.json), il file della cronologia delle modifiche (*.chg) e il file readme (*.txt).
- Per i dispositivi client ThinkEdge, importare il payload (Windows.exe). Il file readme (.txt) è facoltativo. Nota: al momento è supportato solo l'aggiornamento del **pacchetto di utilità flash del BIOS per Windows**.
- Per XClarity Management Hub e XClarity Management Hub 2.0, importare il singolo file del pacchetto di aggiornamento (.tgz). Questo file contiene payload, metadati, cronologia delle modifiche e file readme.
- Per tutte le altre risorse (inclusi XClarity Administrator, i server ThinkEdge, ThinkSystem V1 e V2, nonché di dispositivi legacy), importare il payload (.zip, .uxz, .tar.gz, .tar, .bin), i metadati (.xml), il registro delle modifiche (.chg) e il file leggimi (.txt).

Importante: La dimensione massima di tutti i file che è possibile importare contemporaneamente è di 8 GB.


È possibile determinare se specifici file di aggiornamento vengono memorizzati nel repository degli aggiornamenti dalla colonna **Stato** nella pagina Gestione repository. Questa colonna contiene i seguenti valori.

-  **Non scaricato.** L'intero pacchetto di aggiornamento o i singoli aggiornamenti sono disponibili sul Web, ma attualmente non sono memorizzati nel repository.
-  **Download in sospeso.** Il pacchetto di aggiornamento è in coda per il download da Internet.
-  **In download.** È in corso il download del pacchetto di aggiornamento da Internet.
-  **x di y scaricati.** Non tutti gli aggiornamenti nel pacchetto di aggiornamento sono memorizzati nel repository. I numeri tra parentesi indicano il numero di aggiornamenti memorizzati e disponibili.
-  **Scaricato.** L'intero pacchetto di aggiornamento o i singoli aggiornamenti vengono memorizzati nel repository.

Nota: Alcuni pacchetti di aggiornamento sono utilizzati da più piattaforme. Se si seleziona un pacchetto di aggiornamento nella tabella, viene selezionato in ogni piattaforma che lo utilizza.

Procedura

Per scaricare o importare manualmente i pacchetti di aggiornamento e i pacchetti del repository, completare una delle seguenti operazioni.

- Se XClarity Orchestrator è collegato a Internet, scaricare i pacchetti di aggiornamento elencati nel catalogo.
 1. Dalla barra dei menu di XClarity Orchestrator, fare clic su **Provisioning**  → **Aggiornamenti** e selezionare **Gestione repository** per visualizzare la scheda Gestione repository. La scheda Gestione repository elenca le informazioni sui pacchetti di aggiornamento in una struttura ad albero, organizzata per tipi di risorsa, componenti e pacchetti di aggiornamento. Per impostazione predefinita, nella tabella sono elencati solo i tipi di risorse per le risorse *gestite*. Fare clic su **Mostra**

4. Fare clic sull'icona **Scarica aggiornamenti** (📄) per scaricare gli aggiornamenti selezionati. 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).

Al termine del download, il valore **Stato del download** per gli aggiornamenti selezionati viene modificato in "Scaricato".

- Se XClarity Orchestrator non è collegato a Internet, importare manualmente i pacchetti di aggiornamento e i pacchetti del repository.
 1. Scaricare i file per ciascun pacchetto del repository e pacchetto di aggiornamento in una workstation con accesso di rete all'host di XClarity Orchestrator mediante un browser Web. Utilizzare questi collegamenti per scaricare gli aggiornamenti applicabili.
 - Per gli aggiornamenti di Lenovo XClarity Administrator, visitare il [Pagina Web di download di XClarity Administrator](#). È inoltre possibile scaricare gli aggiornamenti di XClarity Administrator utilizzando i comandi Lenovo XClarity Essentials OneCLI. Nel seguente esempio viene scaricato l'aggiornamento più recente (incluso il payload) nella directory /lxca-updates, mentre i file di log vengono memorizzati nella directory /logs/lxca-updates. Per ulteriori informazioni su OneCLI, vedere [comando acquisisci](#) nella documentazione online di Lenovo XClarity Essentials OneCLI.
`Onecli.exe update acquire --lxca --ostype none --mt lxca --scope latest --superseded --xml --dir ./lxca-updates --output ./logs/lxca-updates`
 - Per i pacchetti del repository degli aggiornamenti firmware, visitare il [Pagina Web di download di XClarity Administrator](#).
 - Per gli aggiornamenti firmware, visitare il [Sito Web dell'Assistenza del Centro Dati Lenovo](#).
 2. Dalla barra dei menu di XClarity Orchestrator, fare clic su **Provisioning** (🔧) → **Aggiornamenti** e selezionare **Gestione repository** per visualizzare la scheda Gestione repository.
 3. Fare clic sull'icona **Importa** (📁) per visualizzare la finestra di dialogo Importa aggiornamenti.
 4. Trascinare e rilasciare i file scaricati nella finestra di dialogo Importa oppure fare clic su **Sfoglia** per individuare i file.

Attenzione:

- Per i dispositivi client ThinkEdge, è necessario importare il file payload per ogni pacchetto di aggiornamento. Il file readme è facoltativo.
 - Per tutti gli altri dispositivi, è necessario importare il file di metadati, nonché i file di immagine e del payload, il file della cronologia delle modifiche e il file readme per ciascun pacchetto del repository e pacchetto di aggiornamento. Tutti i file selezionati ma non specificati nel file dei metadati vengono eliminati. Se non si include il file dei metadati, l'aggiornamento non viene importato.
 - Non importare altri file che potrebbero essere disponibili nei siti Web di download Lenovo.
 - Se non si include il file di metadati (.xml o .json) per il pacchetto del repository o il pacchetto di aggiornamento, il pacchetto del repository o il pacchetto di aggiornamento non viene importato.
5. Fare clic su **Importa**. Viene creato un processo per eseguire questa operazione. È possibile monitorare l'avanzamento del processo dalla scheda **Monitoraggio** (📊) → **Processi**. Se il processo non è stato completato correttamente, fare clic sul relativo collegamento per visualizzare i dettagli sul processo (vedere).

Quando i file vengono importati e memorizzati nel repository, la colonna **Stato del download** viene modificata in "Scaricato".

Al termine

Nella scheda Gestione repository è possibile effettuare le operazioni che seguono.

- Esaminare il file leggimi, il file della cronologia delle modifiche e l'elenco di vulnerabilità e rischi comuni fissi (CVE) per un aggiornamento specifico facendo clic sull'icona delle informazioni (📄) nella colonna **Note sulla versione**. È inoltre possibile trovare un elenco di CVE fissi, posizionando il cursore sulla colonna **CVE fissi**. Fare clic sull'ID CVE per visualizzare le informazioni dettagliate sul CVE dal sito Web NVD (National Vulnerability Data).

Le colonne **Note di rilascio** e **CVE fissi** sono nascoste per impostazione predefinita. Per visualizzare queste colonne nella tabella, fare clic su **Tutte le azioni → Attiva/Disattiva colonne**.

- Eliminare solo l'immagine del file (payload) per ciascun aggiornamento selezionato facendo clic sull'icona **Elimina solo file payload** (🗑️). Le informazioni sull'aggiornamento (il file di metadati XML) restano nel repository e lo stato del download viene modificato in "Non scaricato".

Importante:

- Il payload per i pacchetti del repository viene eliminato automaticamente una volta estratti i pacchetti di aggiornamento durante il processo di download o importazione.
- Non è possibile eliminare i payload dai pacchetti di aggiornamento utilizzati nei criteri di conformità dell'aggiornamento. È necessario innanzitutto rimuovere il pacchetto di aggiornamento dai criteri (vedere [Creazione e assegnazione di criteri di conformità degli aggiornamenti](#)).
- Alcuni pacchetti di aggiornamento sono comuni per più piattaforme e componenti. L'eliminazione di un pacchetto di aggiornamento comune interessa tutte le piattaforme e i componenti che lo utilizzano.

Creazione e assegnazione di criteri di conformità degli aggiornamenti

È possibile creare criteri di conformità degli aggiornamenti in base agli aggiornamenti acquisiti nel repository degli aggiornamenti. È quindi possibile assegnare i criteri a uno o più strumenti di gestione delle risorse o server gestiti.

Prima di iniziare

Quando si creano criteri di conformità degli aggiornamenti è necessario selezionare la versione dell'aggiornamento di destinazione da applicare alle risorse che verranno assegnate al criterio. Verificare che i file di aggiornamento per la versione di destinazione si trovino nel repository degli aggiornamenti prima di creare i criteri.

Quando si scarica o si importa un pacchetto del repository degli aggiornamenti firmware, i criteri di conformità del firmware predefiniti nel pacchetto del repository vengono aggiunti al repository degli aggiornamenti. Questo viene considerato un *criterio predefinito* che non può essere modificato o eliminato.

Informazioni su questa attività

I *criteri di conformità degli aggiornamenti* permettono di verificare che il software o il firmware di determinate risorse gestite sia aggiornato, contrassegnando le risorse che richiedono attenzione. Ciascuno dei criteri di conformità degli aggiornamenti identifica le risorse da monitorare e il livello software o firmware da installare affinché le risorse risultino conformi. XClarity Orchestrator utilizza quindi tali criteri per verificare lo stato degli strumenti di gestione delle risorse e identificare le risorse non conformi.

Quando si creano criteri di conformità degli aggiornamenti, è possibile scegliere di utilizzare XClarity Orchestrator per contrassegnare una risorsa quando il software o firmware della risorsa è inferiore al livello richiesto.

Una volta assegnato un criterio di conformità degli aggiornamenti a una risorsa, XClarity Orchestrator controlla lo stato di conformità della risorsa quando il repository degli aggiornamenti viene modificato. Se il software o il firmware sulla risorsa non è conforme ai criteri assegnati, XClarity Orchestrator contrassegna

tale risorsa come non conforme nella pagina Applica/Attiva, in base alle regole specificate nei criteri di conformità degli aggiornamenti.

Ad esempio, è possibile creare criteri di conformità degli aggiornamenti che definiscono il livello software di base per XClarity Administrator e quindi assegnare tali criteri a tutti gli strumenti di gestione delle risorse di XClarity Administrator. Quando il catalogo degli aggiornamenti viene aggiornato e viene scaricato o importato un nuovo aggiornamento, le istanze XClarity Administrator potrebbero risultare non conformi. Quando ciò si verifica, XClarity Orchestrator aggiorna la pagina Applica/Attiva per mostrare quali istanze XClarity Administrator non sono conformi e genera un avviso.

Procedura

Per creare e assegnare un criterio di conformità degli aggiornamenti, completare le seguenti operazioni.

Passo 1. Creare un criterio di conformità degli aggiornamenti.

1. Sulla barra dei menu di XClarity Orchestrator fare clic su **Provisioning** (🔑) → **Aggiornamenti** e selezionare **Gestione criteri** per visualizzare la scheda Gestione criteri.

Gestione criteri

Gestione criteri consente di creare o modificare nel repository firmware un criterio in base agli aggiornamenti acquistati.

Impossibile modificare o eliminare un criterio di conformità assegnato.

Tutte le azioni ▾ Filtri ▾ Cerca

<input type="checkbox"/>	Nome criterio di com	Stato di utilizzo	Origine criterio di co	Ultima modifica	Descrizione
<input type="checkbox"/>	ThinkAgile_VX_0...	← Non assegnato	Definito dall'...	04/10/22, 18:08	ThinkAgile VX M...
<input type="checkbox"/>	v2.6.0-2020-01-...	→ Assegnato	Definito dall'...	04/10/22, 18:23	Production firmw...
<input type="checkbox"/>	v3.2.0-2021-07-...	← Non assegnato	Definito dall'...	04/10/22, 18:34	Production firmw...
<input type="checkbox"/>	v3.6.0-2022-06-...	← Non assegnato	Definito dall'...	04/10/22, 18:42	Production firmw...
<input type="checkbox"/>	ThinkAgile-VX-Se...	← Non assegnato	Definito dall'...	04/10/22, 18:54	System and Com...
<input type="checkbox"/>	ThinkAgile-VX-Se...	← Non assegnato	Definito dall'...	04/10/22, 19:07	System and Com...
<input type="checkbox"/>	v3.6.0-2022-06-...	← Non assegnato	Definito dall'...	04/10/22, 19:25	Production firmw...
<input type="checkbox"/>	v3.6.0-2022-06-...	← Non assegnato	Definito dall'...	04/10/22, 19:33	Production firmw...
<input type="checkbox"/>	v2.6.0-2019-12-...	← Non assegnato	Definito dall'...	04/10/22, 19:41	Production firmw...

0 Selezionato / 9 Totale Righe per pagina: 10

2. Fare clic sull'icona **Crea** (+) per visualizzare la finestra di dialogo Crea criterio di conformità.
3. Specificare il nome e la descrizione facoltativa del criterio.
4. Specificare il trigger per il criterio. È possibile selezionare uno dei seguenti valori.
 - **Segnala in caso di coincidenza non esatta.** Se la versione del software o del firmware installata sulla risorsa è *precedente* o *successiva* alla versione del firmware di destinazione nei criteri di conformità dell'aggiornamento, la risorsa viene contrassegnata come non conforme. Se, ad esempio, si sostituisce una scheda di rete in un server e il firmware sulla scheda di rete è diverso da quello della versione del firmware di destinazione nei criteri di

conformità dell'aggiornamento assegnati, il server viene contrassegnato come non conforme.

- **Non segnalare.** Le risorse non conformi non vengono segnalati.
5. Fare clic su scheda **Regole** per aggiungere le regole di conformità per questo criterio.
 - a. Selezionare il tipo di risorsa per questo criterio.
 - b. Specificare l'obiettivo di conformità per le risorse e i componenti applicabili. Per le risorse con componenti, è possibile scegliere uno dei seguenti valori.
 - **Personalizzato.** La destinazione di conformità di ciascun componente della risorsa ha il valore predefinito della versione corrente più recente nel repository di questo componente.
 - **Non aggiornare.** La destinazione di conformità per ciascun componente della risorsa ha il valore predefinito **Non aggiornare**. Tenere presente che se si modifica il valore predefinito per qualsiasi componente, la destinazione di conformità per la risorsa globale viene modificata in **Personalizzato**. Per le risorse senza componente e per ciascun componente è possibile scegliere uno dei seguenti valori.
 - *{firmware_level}*. Specifica che la versione di firmware del componente deve essere quella di base selezionata.
 - **Non aggiornare.** Specifica che il firmware del componente non deve essere aggiornato. Tenere presente che il firmware del controller di gestione di backup (secondario) non viene aggiornato per impostazione predefinita.
 - c. Fare clic sull'icona **Aggiungi** (+) per aggiungere regole aggiuntive e fare clic sull'icona **Elimina** (☒) per eliminare le regole.
 6. Fare clic su **Crea**.

Passo 2. Dalla barra dei menu di XClarity Orchestrator, fare clic su **Provisioning** (☰) → **Aggiornamenti e** selezionare **Applica e attiva** per visualizzare la scheda Applica e attiva.

Passo 3. Assegnare il criterio di conformità dell'aggiornamento alle risorse.

- **A una singola risorsa** Per ciascuna risorsa, selezionare un criterio dall'elenco a discesa della colonna **Criterio di conformità assegnato**.

È possibile scegliere da un elenco dei criteri di conformità applicabili alla risorsa. Se un criterio non è attualmente assegnato alla risorsa, il criterio assegnato è impostato su **Nessuna assegnazione**. Se non vi sono criteri applicabili alla risorsa, il criterio assegnato è impostato su **Nessun criterio applicabile**.

- **A più risorse**


1. Selezionare una o più risorse a cui si desidera assegnare il criterio.
2. Fare clic sull'icona **Assegna** (☰) per visualizzare la finestra di dialogo Assegna criteri.
3. Selezionare il criterio che si desidera assegnare. È possibile scegliere da un elenco dei criteri di conformità applicabili a tutte le risorse selezionate. Se un criterio non è attualmente assegnato alla risorsa, il criterio assegnato è impostato su **Nessuna assegnazione**. Se non vi sono criteri applicabili alla risorsa, il criterio assegnato è impostato su **Nessun criterio applicabile**. Se le risorse non sono state selezionate prima di aprire la finestra di dialogo, vengono elencati tutti i criteri.

Nota: Selezionare **Nessuna assegnazione** per rimuovere l'assegnazione dei criteri dalla risorsa selezionata.

4. Selezionare uno dei seguenti ambiti per l'assegnazione dei criteri.
 - **Tutti i dispositivi applicabili che sono...**
 - **Solo i dispositivi applicabili selezionati che sono...**

5. Selezionare uno o più criteri.
 - **Senza un criterio assegnato**
 - **Non conformi (sovrascrivere i criteri attualmente assegnati)**
 - **Conformi (sovrascrivere i criteri attualmente assegnati)**
6. Fare clic su **Applica**. Il nome dei criteri assegnati nella colonna Criteri assegnati della pagina "Aggiornamenti firmware: repository" viene modificato in base al nome dei criteri di conformità del firmware selezionati.


- **A gruppi di risorse**

1. Fare clic sull'icona **Assegna**  per visualizzare la finestra di dialogo Assegna criteri.
2. Selezionare il criterio che si desidera assegnare. È possibile scegliere da un elenco dei criteri di conformità del firmware applicabili a tutte le risorse nel gruppo. Se un criterio non è attualmente assegnato alla risorsa, il criterio assegnato è impostato su **Nessuna assegnazione**. Se non vi sono criteri applicabili alla risorsa, il criterio assegnato è impostato su **Nessun criterio applicabile**.



Nota: Selezionare **Nessuna assegnazione** per rimuovere l'assegnazione dei criteri dalle risorse nel gruppo.
3. Selezionare uno o più gruppi di risorse a cui si desidera assegnare il criterio.
4. Selezionare uno dei seguenti ambiti per l'assegnazione dei criteri.
 - **Tutti i dispositivi applicabili che sono...**
 - **Solo i dispositivi applicabili selezionati che sono...**
5. Selezionare uno o più criteri.
 - **Senza un criterio assegnato**
 - **Non conformi (sovrascrivere i criteri attualmente assegnati)**
 - **Conformi (sovrascrivere i criteri attualmente assegnati)**
6. Fare clic su **Applica**. Il nome dei criteri assegnati nella colonna Criteri assegnati della pagina "Aggiornamenti firmware: repository" viene modificato in base al nome dei criteri di conformità del firmware selezionati.

Al termine


Nella scheda Gestione criteri è possibile effettuare le operazioni che seguono.

- Visualizzare i dettagli dei criteri facendo clic sulla riga nella tabella.
- Modificare un criterio selezionato facendo clic sull'icona **Modifica** .

Nota: Non è possibile modificare un criterio assegnato a una o più risorse. È innanzitutto necessario annullare l'assegnazione dei criteri.

- Copiare e modificare un criterio selezionato facendo clic sull'icona **Copia** .
- Eliminare un criterio *definito dall'utente* selezionato facendo clic sull'icona **Elimina** .

Nota: Non è possibile eliminare un criterio assegnato a una o più risorse. È innanzitutto necessario annullare l'assegnazione dei criteri.

Nella scheda Applica e attiva è possibile annullare l'assegnazione dei criteri per una risorsa selezionata facendo clic sull'icona **Assegna** , selezionando il criterio **Nessuna assegnazione**, quindi scegliendo se applicare la modifica a tutte le risorse con un'assegnazione di criteri o solo alle risorse selezionate.

Applicazione e attivazione degli aggiornamenti agli strumenti di gestione delle risorse

XClarity Orchestrator non applica automaticamente gli aggiornamenti. Per aggiornare il software è necessario applicare manualmente e attivare l'aggiornamento sugli strumenti di gestione delle risorse selezionati di Lenovo XClarity Administrator che non sono conformi ai criteri di conformità degli aggiornamenti assegnati.

Prima di iniziare

Prima di tentare di applicare e attivare gli aggiornamenti su qualsiasi risorsa, assicurarsi di aver letto le considerazioni sugli aggiornamenti (vedere [Considerazioni sulla distribuzione degli aggiornamenti](#)).

Verificare che alla risorsa di destinazione sia assegnato un criterio di conformità degli aggiornamenti (vedere [Creazione e assegnazione di criteri di conformità degli aggiornamenti](#)).

Non è possibile applicare un aggiornamento di un livello software analogo o precedente a quello attualmente installato.

Informazioni su questa attività

È possibile applicare gli aggiornamenti firmware agli strumenti di gestione delle risorse di XClarity Administrator con criteri di conformità degli aggiornamenti assegnati e non conformi a questi criteri. È possibile aggiornare il software nei seguenti modi.

- Per strumenti di gestione non conformi specifici
- Per strumenti di gestione non conformi in gruppi specifici
- Per strumenti di gestione non conformi assegnati a un criterio di conformità dell'aggiornamento specifico
- Per strumenti di gestione non conformi in gruppi specifici assegnati a un criterio di conformità dell'aggiornamento specifico
- Per strumenti di gestione non conformi assegnati a un criterio e non conformi a questi criteri

XClarity Orchestrator non aggiorna direttamente le risorse. Invia invece una richiesta allo strumento di gestione delle risorse applicabile per eseguire l'aggiornamento, quindi tiene traccia dell'avanzamento della richiesta. XClarity Orchestrator identifica le dipendenze necessarie per eseguire l'aggiornamento, verifica che le risorse di destinazione vengano aggiornate nell'ordine corretto, trasferisce i pacchetti di aggiornamento applicabili allo strumento di gestione delle risorse e crea una richiesta di avvio di un processo sullo strumento di gestione delle risorse per eseguire l'aggiornamento.

Durante il processo di aggiornamento, la risorsa di destinazione potrebbe essere riavviata automaticamente diverse volte finché l'intero processo di aggiornamento non viene completato. Accertarsi di sospendere tutte le applicazioni sulla risorsa di destinazione prima di procedere.

Se si verifica un errore durante l'aggiornamento di uno dei componenti in una risorsa di destinazione, il processo di aggiornamento non aggiorna il componente. Il processo di aggiornamento tuttavia continua ad aggiornare gli altri componenti nella risorsa e tutte le risorse di destinazione nel processo di aggiornamento corrente.

Gli aggiornamenti prerequisiti non vengono applicati automaticamente.

Suggerimento:

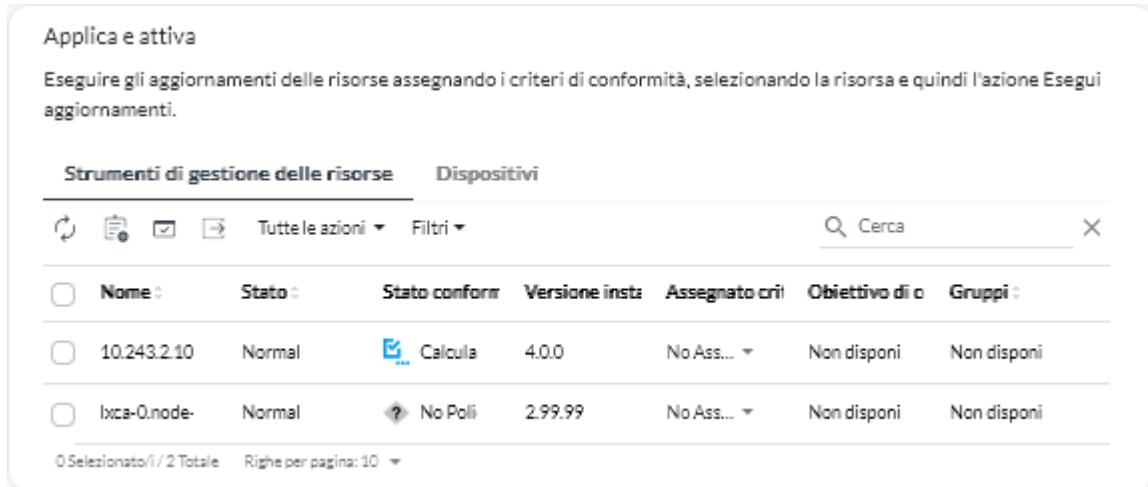
- Nella tabella sono elencati solo gli strumenti di gestione delle risorse che possono essere aggiornati.
- Le colonne **Numero build** e **Numero build di destinazione conformità** sono nascoste per impostazione predefinita. È possibile visualizzare queste colonne facendo clic su **Tutte le azioni → Attiva/Disattiva colonne**.

Procedura

Completare una delle seguenti operazioni per applicare gli aggiornamenti agli strumenti di gestione delle risorse di XClarity Orchestrator.

- **Per strumenti di gestione delle risorse non conformi specifici**

1. Sulla barra dei menu di XClarity Orchestrator fare clic su **Provisioning** (🔑) → **Aggiornamenti** e selezionare **Applica e attiva** per visualizzare la scheda Applica e attiva.



2. Fare clic sulla scheda **Strumenti di gestione delle risorse**.
3. Selezionare uno o più strumenti di gestione delle risorse a cui si desidera applicare gli aggiornamenti.
4. Fare clic sull'icona **Applica aggiornamento** (🔄) per visualizzare la finestra di dialogo Riepilogo aggiornamenti.
5. Fare clic su **Esegui aggiornamenti** per applicare gli aggiornamenti. 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).

- **Per strumenti di gestione delle risorse non conformi in gruppi specifici o assegnati a un criterio di conformità dell'aggiornamento specifico**

1. Dalla barra dei menu di XClarity Orchestrator, fare clic su **Provisioning** (🔑) → **Aggiornamenti** e selezionare **Applica e attiva** per visualizzare la scheda Applica e attiva.
2. Fare clic sulla scheda **Strumenti di gestione delle risorse**.
3. Fare clic sull'icona **Applica aggiornamento** (🔄) per visualizzare la finestra di dialogo Riepilogo aggiornamenti.
4. Selezionare i gruppi e i criteri di conformità dell'aggiornamento.
 - Se non si seleziona un criterio o un gruppo, tutti gli strumenti di gestione con un criterio assegnato e che non sono conformi a questo criterio vengono aggiornati.
 - Se si seleziona un criterio ma non un gruppo, tutti gli strumenti di gestione a cui è assegnato tale criterio e che non sono conformi a questo criterio vengono aggiornati.
 - Se si seleziona uno o più gruppi e non criterio, tutti gli strumenti di gestione nel gruppo che non sono conformi al criterio assegnato vengono aggiornati.
 - Se si seleziona un criterio e uno o più gruppi, tutti gli strumenti di gestione nel gruppo che sono assegnati a tale criterio e non sono conformi al criterio vengono aggiornati.

5. Fare clic su **Esegui aggiornamenti** per applicare gli aggiornamenti. 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).

Applicazione e attivazione degli aggiornamenti ai server gestiti

Lenovo XClarity Orchestrator non applica automaticamente gli aggiornamenti. Per aggiornare il firmware è necessario applicare manualmente e attivare l'aggiornamento sui dispositivi selezionati che non sono conformi ai criteri di conformità degli aggiornamenti assegnati.

Prima di iniziare

Prima di tentare di applicare e attivare gli aggiornamenti su qualsiasi dispositivo, assicurarsi di aver letto le considerazioni sugli aggiornamenti (vedere [Considerazioni sulla distribuzione degli aggiornamenti](#)).

Verificare che al dispositivo di destinazione sia assegnato un criterio di conformità degli aggiornamenti (vedere [Creazione e assegnazione di criteri di conformità degli aggiornamenti](#)).

È possibile applicare gli aggiornamenti firmware solo ai server gestiti.

Quando si aggiorna il firmware su più dispositivi contemporaneamente, utilizzare XClarity Orchestrator v1.3.1 o successive e Lenovo XClarity Administrator v3.2.1 o successive per ottenere prestazioni migliori.

Informazioni su questa attività

È possibile applicare gli aggiornamenti firmware ai dispositivi con criteri di conformità degli aggiornamenti assegnati e non conformi a questi criteri. È possibile aggiornare il firmware nei seguenti modi.

- Per dispositivi non conformi specifici
- Per dispositivi non conformi in gruppi specifici
- Per dispositivi non conformi assegnati a un criterio di conformità dell'aggiornamento specifico
- Per dispositivi non conformi in gruppi specifici assegnati a un criterio di conformità dell'aggiornamento specifico
- Per dispositivi non conformi assegnati a un criterio e non conformi a questi criteri

Un server è contrassegnato come Non conforme quando la versione del firmware installata di uno o più componenti è *precedente o successiva* alla versione del firmware di destinazione nei criteri di conformità dell'aggiornamento. Se la versione del firmware installata è *successiva* alla versione del firmware di destinazione, è necessario selezionare l'opzione **Aggiornamento forzato** durante l'applicazione dell'aggiornamento per eseguire il downgrade del firmware sui componenti. Se l'opzione **Aggiornamento forzato** non è selezionata, vengono applicate solo le versioni del firmware di destinazione successive a quelle installate.

Nota: Solo alcune opzioni di dispositivo, adattatori e unità supportano il downgrade. Consultare la documentazione hardware per determinare se il downgrade è supportato.

XClarity Orchestrator non aggiorna direttamente le risorse. Invia invece una richiesta allo strumento di gestione delle risorse applicabile per eseguire l'aggiornamento, quindi tiene traccia dell'avanzamento della richiesta. XClarity Orchestrator identifica le dipendenze necessarie per eseguire l'aggiornamento, verifica che le risorse di destinazione vengano aggiornate nell'ordine corretto, trasferisce i pacchetti di aggiornamento applicabili allo strumento di gestione delle risorse e crea una richiesta di avvio di un processo sullo strumento di gestione delle risorse per eseguire l'aggiornamento.

Durante il processo di aggiornamento, il dispositivo di destinazione potrebbe essere riavviata automaticamente diverse volte finché l'intero processo di aggiornamento non viene completato. Accertarsi di sospendere tutte le applicazioni sul dispositivo di destinazione prima di procedere.

Se si verifica un errore durante l'aggiornamento di uno dei componenti in un dispositivo di destinazione, il processo di aggiornamento non aggiorna il componente. Il processo di aggiornamento tuttavia continua ad aggiornare gli altri componenti nel dispositivo e tutti i dispositivi di destinazione nel processo di aggiornamento corrente.

Gli aggiornamenti prerequisiti non vengono applicati automaticamente.

Suggerimenti:

- Nella tabella sono elencati solo i dispositivi che possono essere aggiornati.
- Le colonne **Numero build**, **Numero build di destinazione conformità** e **Nome prodotto** sono nascoste per impostazione predefinita. È possibile visualizzare queste colonne facendo clic su **Tutte le azioni** → **Attiva/Disattiva colonne**.
- Per i server ThinkSystem SR635, SR645, SR655 e SR665, per applicare sia il firmware in banda che quello fuori banda, applicare innanzitutto gli aggiornamenti ai controller di gestione della scheda di base e quindi applicare gli aggiornamenti firmware alle opzioni restanti.

Procedura

Per applicare gli aggiornamenti ai dispositivi gestiti, completare una delle seguenti procedure.

- **Per dispositivi non conformi specifici**

1. Dalla barra dei menu di XClarity Orchestrator, fare clic su **Provisioning** (🔗) → **Aggiornamenti** e selezionare **Applica e attiva** per visualizzare la scheda Applica e attiva.
2. Fare clic sulla scheda **Dispositivi**.
3. Selezionare uno o più dispositivi a cui si desidera applicare gli aggiornamenti.
4. Fare clic sull'icona **Applica aggiornamento** (📄) per visualizzare la finestra di dialogo Riepilogo aggiornamenti.
5. Selezionare quando attivare gli aggiornamenti.
 - **Attivazione con priorità.** Gli aggiornamenti firmware sul controller di gestione della scheda di base vengono attivati immediatamente; tutti gli altri aggiornamenti firmware vengono attivati al successivo riavvio del dispositivo. Riavvii aggiuntivi vengono quindi eseguiti fino a che l'operazione di aggiornamento non è completa. Un evento si verifica quando lo stato viene modificato in Modalità di manutenzione firmware in sospenso per notificare quando il server deve essere riavviato.
 - **Attivazione ritardata.** Alcune ma non tutte le operazioni di aggiornamento sono state eseguite. I dispositivi di destinazione devono essere riavviati manualmente per continuare il processo di aggiornamento. Riavvii aggiuntivi vengono quindi eseguiti fino a che l'operazione di aggiornamento non è completa. Un evento si verifica quando lo stato viene modificato in Modalità di manutenzione firmware in sospenso per notificare quando il server deve essere riavviato.

Se un dispositivo di destinazione viene riavviato per un qualsiasi motivo, il processo di aggiornamento ritardato viene terminato.

Importante:

- Utilizzare **Riavvia normalmente** per riavviare il server e continuare il processo di aggiornamento. *Non* utilizzare **Riavvia immediatamente**.

- Non scegliere Attivazione ritardata per più di 50 dispositivi contemporaneamente. XClarity Orchestrator monitora attivamente i dispositivi con attivazione ritardata in modo che tale attivazione venga eseguita al riavvio di un dispositivo. Se si desidera applicare aggiornamenti con attivazione ritardata a oltre 50 dispositivi, suddividere la selezione degli aggiornamenti in batch di 50 dispositivi alla volta.
- **Attivazione immediata** Durante il processo di aggiornamento, il dispositivo di destinazione potrebbe essere riavviata automaticamente diverse volte finché l'intero processo di aggiornamento non viene completato. Accertarsi di sospendere tutte le applicazioni sul dispositivo di destinazione prima di procedere.

Nota:

- Per i server gestiti da XClarity Management Hub 2.0 e per i dispositivi client ThinkEdge, è supportata solo l'opzione Attivazione immediata, a prescindere dalla regola di attivazione selezionata.
 - Se abilitata, l'opzione di avvio WOL (Wake-on-LAN) può interferire con le operazioni di Lenovo XClarity Administrator che spengono il server, inclusi gli aggiornamenti firmware se nella rete è presente un client Wake-on-LAN che genera comandi "Magic Packet per riattivazione".
6. **Facoltativo:** selezionare **Aggiornamento forzato** per aggiornare il firmware nei componenti selezionati anche se il livello di firmware è già aggiornato oppure per applicare un aggiornamento del firmware precedente a quello attualmente installato sui componenti installati.
 7. **Facoltativo:** selezionare **Pianifica aggiornamento** per scegliere la data e l'ora in cui si desidera eseguire l'aggiornamento firmware. Se l'opzione non viene selezionata, il firmware viene aggiornato immediatamente.
 8. Fare clic su **Esegui aggiornamenti** per applicare gli aggiornamenti. 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).
- **Per dispositivi non conformi in gruppi specifici assegnati a un criterio di conformità dell'aggiornamento specifico**
 1. Dalla barra dei menu di XClarity Orchestrator, fare clic su **Provisioning** (🔗) → **Aggiornamenti** e selezionare **Applica e attiva** per visualizzare la scheda Applica e attiva.
 2. Fare clic sulla scheda **Dispositivi**.
 3. Selezionare uno o più gruppi di dispositivi a cui si desidera applicare gli aggiornamenti.
 4. Fare clic sull'icona **Applica aggiornamento** (👌) per visualizzare la finestra di dialogo Riepilogo aggiornamenti.
 5. Selezionare i gruppi e i criteri di conformità dell'aggiornamento.
 - Se non si seleziona un criterio o un gruppo, tutti i dispositivi con un criterio assegnato e che non sono conformi a questo criterio vengono aggiornati.
 - Se si seleziona un criterio ma non un gruppo, tutti i dispositivi a cui è assegnato tale criterio e che non sono conformi a questo criterio vengono aggiornati.
 - Se si seleziona uno o più gruppi e non criterio, tutti i dispositivi nel gruppo che non sono conformi al criterio assegnato vengono aggiornati.
 - Se si seleziona un criterio e uno o più gruppi, tutti i dispositivi nel gruppo che sono assegnati a tale criterio e non sono conformi al criterio vengono aggiornati.
 6. Selezionare quando attivare gli aggiornamenti.
 - **Attivazione con priorità.** Gli aggiornamenti firmware sul controller di gestione della scheda di base vengono attivati immediatamente; tutti gli altri aggiornamenti firmware vengono attivati al successivo riavvio del dispositivo. Riavvii aggiuntivi vengono quindi eseguiti fino a che l'operazione di aggiornamento non è completa. Un evento si verifica quando lo stato viene modificato in

Modalità di manutenzione firmware in sospenso per notificare quando il server deve essere riavviato.

- **Attivazione ritardata.** Alcune ma non tutte le operazioni di aggiornamento sono state eseguite. I dispositivi di destinazione devono essere riavviati manualmente per continuare il processo di aggiornamento. Riavvii aggiuntivi vengono quindi eseguiti fino a che l'operazione di aggiornamento non è completa. Un evento si verifica quando lo stato viene modificato in Modalità di manutenzione firmware in sospenso per notificare quando il server deve essere riavviato.

Se un dispositivo di destinazione viene riavviato per un qualsiasi motivo, il processo di aggiornamento ritardato viene terminato.

Importante:

- Utilizzare **Riavvia normalmente** per riavviare il server e continuare il processo di aggiornamento. *Non* utilizzare **Riavvia immediatamente**.
- Non scegliere Attivazione ritardata per più di 50 dispositivi contemporaneamente. XClarity Orchestrator monitora attivamente i dispositivi con attivazione ritardata in modo che tale attivazione venga eseguita al riavvio di un dispositivo. Se si desidera applicare aggiornamenti con attivazione ritardata a oltre 50 dispositivi, suddividere la selezione degli aggiornamenti in batch di 50 dispositivi alla volta.
- **Attivazione immediata** Durante il processo di aggiornamento, il dispositivo di destinazione potrebbe essere riavviato automaticamente diverse volte finché l'intero processo di aggiornamento non viene completato. Accertarsi di sospendere tutte le applicazioni sul dispositivo di destinazione prima di procedere.

Nota:

- Per i server gestiti da XClarity Management Hub 2.0 e per i dispositivi client ThinkEdge, è supportata solo l'opzione Attivazione immediata, a prescindere dalla regola di attivazione selezionata.
 - Se abilitata, l'opzione di avvio WOL (Wake-on-LAN) può interferire con le operazioni di Lenovo XClarity Administrator che spengono il server, inclusi gli aggiornamenti firmware se nella rete è presente un client Wake-on-LAN che genera comandi "Magic Packet per riattivazione".
7. **Facoltativo:** selezionare **Aggiornamento forzato** per aggiornare il firmware nei componenti selezionati anche se il livello di firmware è già aggiornato oppure per applicare un aggiornamento del firmware precedente a quello attualmente installato sui componenti installati.
 8. **Facoltativo:** selezionare **Pianifica aggiornamento** per scegliere la data e l'ora in cui si desidera eseguire l'aggiornamento firmware. Se l'opzione non viene selezionata, il firmware viene aggiornato immediatamente.
 9. Fare clic su **Esegui aggiornamenti** per applicare gli aggiornamenti. 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).

Al termine

Nella scheda Pattern è possibile effettuare le azioni che seguono.

- Inoltrare report sulla conformità del firmware periodicamente a uno o più indirizzi e-mail facendo clic sull'icona **Crea server d'inoltro dei report** (+). Il report viene inviato utilizzando i filtri dati attualmente applicati alla tabella. Tutte le colonne della tabella visibili e nascoste sono incluse nel report. Per ulteriori informazioni, vedere [Inoltro di report](#).
- Aggiungere un report sulla conformità del firmware a un server d'inoltro dei report specifico utilizzando i filtri dati attualmente applicati alla tabella facendo clic sull'icona **Aggiungi al server d'inoltro dei report** (

⇒). Se il server d'oltro dei report include già un report sulla conformità del firmware, il report viene aggiornato per utilizzare i filtri dati correnti.

È possibile annullare un processo di aggiornamento firmware pianificato non ancora in esecuzione facendo clic su **Monitoraggio** (📈) → **Processi** dalla barra dei menu di XClarity Orchestrator e selezionando la scheda **Pianificazioni** per visualizzare la scheda Processi pianificati. Selezionare il processo pianificato, quindi fare clic sull'icona **Annullato** (🗑️).

Capitolo 6. Analisi delle tendenze e previsione dei problemi

Lenovo XClarity Orchestrator genera avvisi di analisi basati su problemi hardware e firmware noti, monitora le tendenze per rilevare le anomalie che si verificano nelle risorse gestite e sviluppa euristiche che possono calcolare la probabilità di problemi o errori imminenti. Le tendenze vengono visualizzate come query, grafici e diagrammi che mostrano lo stato di conformità, la cronologia dei problemi e la suddivisione delle risorse più problematiche. È quindi possibile analizzare queste tendenze per ottenere informazioni dettagliate sulla causa dei problemi e risolverli rapidamente.

Importante:

- Le funzioni di analisi sono supportate per i server ThinkAgile, ThinkSystem e ThinkEdge che eseguono il firmware XCC 1.4 o versioni successive.
- Per utilizzare le funzioni di analisi, è necessaria una licenza di analisi di Lenovo XClarity Orchestrator per ogni dispositivo che le supporta. Una licenza *non* è legata a dispositivi specifici. Per ulteriori informazioni, vedere [Applicazione delle licenze per XClarity Orchestrator](#) nella documentazione online di XClarity Orchestrator.

Creazione di report di analisi personalizzati

I rapporti di analisi vengono eseguiti costantemente in background per fornire informazioni sulla modalità di funzionamento del data center in tempo reale.

Informazioni su questa attività

Lenovo XClarity Orchestrator fornisce diversi report di analisi predefiniti, basati sui dati di eventi, inventario o metriche raccolti dalle risorse gestite. Questi dati vengono quindi visualizzati come statistiche (in formato tabella) oppure come grafici a barre o a torta. È possibile visualizzare gli esempi di questi report nelle pagine **Analisi (🔍) → Analisi predefinite**.

È inoltre possibile creare report personalizzati per rappresentare i dati di maggior interesse.

Procedura

Per creare report di analisi personalizzati, effettuare le seguenti operazioni.

Passo 1. Creare avvisi personalizzati.

XClarity Orchestrator genera avvisi di analisi basati su problemi noti relativi all'hardware e al firmware. È inoltre possibile creare avvisi personalizzati da utilizzare nei report personalizzati.

Passo 2. Creare report personalizzati (query).

È possibile aggiungere report grafici personalizzati a XClarity Orchestrator definendo le query in base ai dati di maggiore interesse.

Creazione di regole per avvisi di analisi personalizzati

Lenovo XClarity Orchestrator genera avvisi basati su problemi noti relativi all'hardware e al firmware. È possibile definire *regole di avviso* personalizzate per generare avvisi di analisi, quando si verifica un evento specifico o una metrica specifica viene violata. È quindi possibile utilizzare questi avvisi per generare report di analisi personalizzati (query).

Informazioni su questa attività

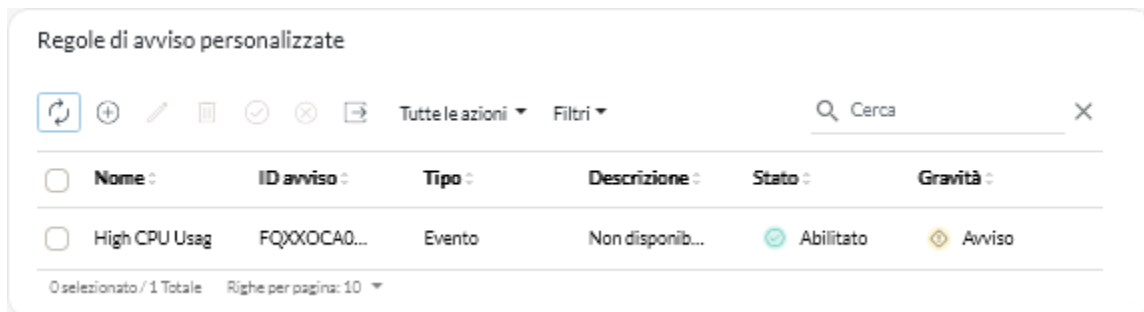
Gli eventi vengono generati per tutti gli avvisi, inclusi gli avvisi di analisi personalizzati. Lo stesso codice evento viene utilizzato per l'avviso attivo e l'evento con il formato FQXX0CAxxxxc, dove xxxx è l'identificatore univoco e c la gravità.

Gli avvisi personalizzati sono inclusi nell'elenco degli avvisi attivi per lo stato di integrità. Tutti gli avvisi attivi, inclusi gli avvisi personalizzati, vengono visualizzati in una singola vista unificata (vedere [Monitoraggio degli avvisi attivi](#)).

Procedura

Per creare una regola di avviso personalizzata, effettuare le seguenti operazioni.

Passo 1. Dalla barra dei menu di XClarity Orchestrator fare clic su **Analisi** (🔍) → **Avvisi personalizzati** per visualizzare la scheda Regole di avviso personalizzate.



Passo 2. Fare clic sull'icona **Crea** (+) per visualizzare la finestra di dialogo Crea regola di avviso personalizzato.

Passo 3. Specificare un nome univoco e una descrizione facoltativa per l'avviso personalizzato.

Passo 4. Selezionare il tipo di origine per questa regola.

- **Evento.** Genera un avviso quando si verifica un evento specifico, in base ai criteri delle regole.
- **Metrica.** Genera un avviso quando una metrica specifica viene violata, in base ai criteri delle regole.

Passo 5. Fare clic su **Dettagli di attivazione regole** e specificare i criteri per questa regola. I criteri variano a seconda del tipo di origine.

- **Regole avvisi basati su eventi**

- Specificare il tipo di destinazione per questo avviso.
 - **Dispositivo.** Genera un avviso quando l'evento si verifica su qualsiasi dispositivo. Il nome del dispositivo è incluso in questo avviso.
 - **Gruppo di dispositivi.** Genera un avviso quando l'evento si verifica su un dispositivo in qualsiasi gruppo di dispositivi. Il nome del gruppo è incluso nell'avviso.
- Specificare l'ID dell'evento che attiva un avviso. Per un elenco degli ID evento, vedere [Messaggi di eventi e avvisi](#) nella documentazione online di XClarity Orchestrator.
- Specificare il numero di volte (conteggio) che l'evento deve verificarsi nell'intervallo specificato prima che venga generato un avviso.
- Selezionare il periodo di tempo (intervallo), in minuti, in cui l'evento si verifica prima che venga visualizzato un avviso.

- **Regole avvisi basati su metriche**

- Selezionare la modalità del criterio.
 - **medio.** Genera un avviso quando il valore medio della metrica supera la soglia (in base al criterio di confronto) durante un intervallo specifico.

Ad esempio è possibile creare una regola per generare un avviso quando la temperatura media della CPU (**metric**) in un periodo di 24 ore (**interval**) è maggiore di (**operator**) 40 °C (**threshold**).

- **conteggio**. Genera un avviso quando la metrica supera la soglia (in base al criterio di confronto) un determinato numero di volte durante un intervallo specifico.

Ad esempio è possibile creare una regola per generare un avviso quando la temperatura della CPU (**metric**) è maggiore di (**operator**) 40 °C (**threshold**) per 5 volte (**count**) in un periodo di 24 ore (**interval**).

- **semplice**. Genera un avviso quando la soglia viene superata (in base al criterio di confronto).

Ad esempio è possibile creare una regola per generare un avviso quando la temperatura della CPU (**metric**) è maggiore di (**operator**) 40 °C (**threshold**).

- Selezionare la misurazione (metriche) per questo avviso da un elenco di misurazioni supportate per le risorse gestite.
- Se la modalità del criterio è "conteggio", specificare il numero di volte che il valore viene utilizzato nell'intervallo specificato prima che venga generato un avviso.
- Selezionare la funzione di confronto.
 - >=. Maggiore o uguale a
 - <=. Minore o uguale a
 - >. Maggiore di
 - <. Minore di
 - =. Uguale a
 - !=. Non uguale a
- Specificare il valore di soglia da confrontare con il valore metrico.
- Se la modalità del criterio è "medio" o "conteggio", selezionare il periodo di tempo (intervallo), in minuti, in cui la metrica viene valutata.

Passo 6. Fare clic su **Dettagli avvisi ed eventi** e specificare le informazioni da visualizzare per l'avviso e l'evento.

1. Specificare il messaggio, la descrizione e l'intervento dell'utente da visualizzare per l'avviso e l'evento associati. È possibile includere variabili racchiudendo il nome del campo (variabile) tra parentesi quadre, ad esempio, [[DeviceName]]. Un elenco dei campi disponibili (in base alla misurazione selezionata) viene visualizzato nella tabella a destra dei campi di immissione.
2. Selezionare la gravità per questa regola di avviso.
 - **Avvertenza**. L'utente può decidere se è necessaria l'azione.
 - **Critico**. L'azione è necessaria immediatamente e l'ambito è ampio (potrebbe causare un'interruzione immediata di una risorsa critica).
3. Specificare un numero univoco a 4 cifre da utilizzare come codice evento per questo avviso. È possibile specificare un numero da 0001 a 9999, che non sia già in uso.

Passo 7. Facoltativamente è possibile modificare lo stato in **Abilitato** per abilitare XClarity Orchestrator, in modo da generare un avviso di analisi quando vengono soddisfatti i criteri per l'avviso personalizzato.

Passo 8. Fare clic su **Crea**.

Al termine

È possibile visualizzare l'elenco degli avvisi di analisi generati in base alle regole di avvisi personalizzati abilitate facendo clic su **Monitoraggio** (📧) → **Avvisi**.

Nella scheda Regole di avvisi personalizzati è possibile effettuare le operazioni che seguono.

- Modificare le proprietà di una regola di avviso personalizzato selezionata, facendo clic sull'icona **Modifica** (✎).
- Eliminare una regola di avviso personalizzato selezionata, facendo clic sull'icona **Elimina** (🗑).
- Per abilitare o disabilitare una o più regole di avviso personalizzate selezionate, fare clic sull'icona **Abilita** (☑) o **Disabilita** (☒).

Creazione di report personalizzati (query)

È possibile aggiungere report grafici e tabulari personalizzati in Lenovo XClarity Orchestrator definendo le query basate sui dati raccolti, ad esempio avvisi, eventi, inventario, metriche di dispositivi o metriche personalizzate (aggregazioni).

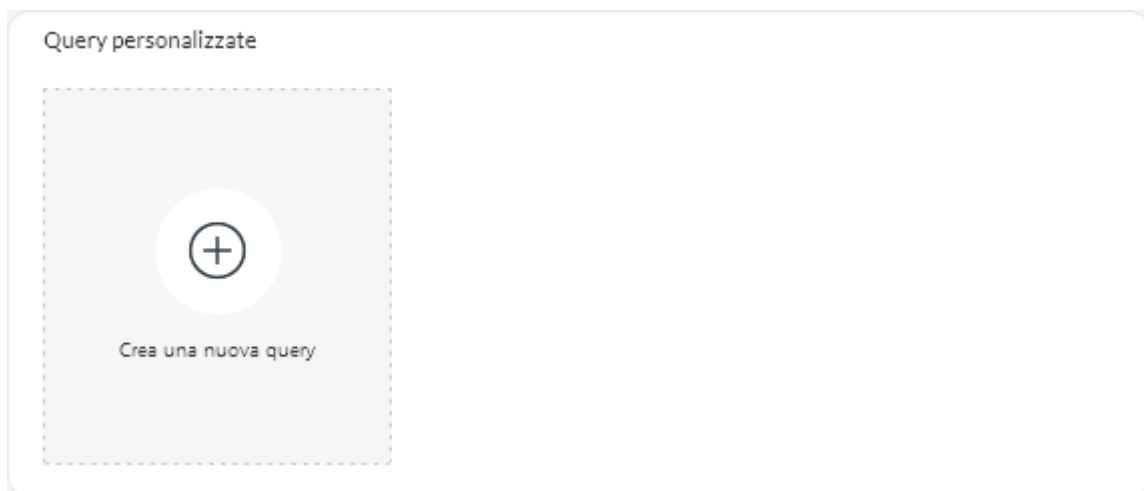
Prima di iniziare

Importante: La creazione di report di analisi e personalizzati in XClarity Orchestrator richiede una conoscenza di base dei database e delle query di database.

Informazioni su questa attività

Per creare un report personalizzato, effettuare le seguenti operazioni.

Passo 1. Dalla barra dei menu di XClarity Orchestrator, fare clic su **Analisi** (🔍) → **Query personalizzate** per visualizzare la scheda Query personalizzate.



Passo 2. Fare clic sull'icona **Crea** (+) per visualizzare la finestra di dialogo Crea query personalizzata.

Passo 3. Specificare un nome univoco per la query personalizzata.

Passo 4. Selezionare il tipo di dati che si desidera utilizzare come origine per questa query.

È possibile scegliere uno dei seguenti tipi di origine dati.

- **Avvisi.** Condizioni hardware o di gestione che richiede l'analisi e l'intervento dell'utente
- **Eventi.** Eventi di controllo e risorse
- **Eventi-Risorsa.** Condizione hardware o di Orchestrator che si è verificata su un dispositivo gestito, uno strumento di gestione delle risorse o su XClarity Orchestrator
- **Eventi-Controllo.** Attività utente eseguite da uno strumento di gestione delle risorse o da XClarity Orchestrator.
- **Inventari-Strumento di gestione.** I dati di inventario per gli strumenti di gestione delle risorse
- **Inventari-Dispositivo.** I dati di inventario per tutti i tipi di dispositivi gestiti
- **Inventari-Dispositivo-Server.** I dati di inventario per i server gestiti
- **Inventari-Dispositivo-Switch.** I dati di inventario per gli switch gestiti

- **Inventari-Dispositivo-Storage.** I dati di inventario per i dispositivi di storage gestiti
- **Inventari-Dispositivo-Chassis.** I dati di inventario per gli chassis gestiti
- **Temperatura CPU.** I dati di metrica per la temperatura, in Celsius, di ciascun processore in un dispositivo gestito. La metrica viene acquisita ogni minuto.
- **Statistiche di utilizzo CPU.** I dati di metrica per l'utilizzo del processore, come una percentuale, per un dispositivo gestito. La metrica viene acquisita ogni minuto.
- **Temperatura aria in ingresso.** I dati di metrica per la temperatura dell'aria in ingresso, in Celsius, di un dispositivo gestito. La temperatura viene acquisita ogni minuto.
- **Statistiche di utilizzo memoria.** I dati di metrica per la memoria utilizzata, come una percentuale, da un dispositivo gestito. La metrica viene acquisita ogni minuto.
- **Metrica di alimentazione.** I dati di metrica per il consumo energetico, in watt, da tutti i processori, i moduli di memoria o l'intero sistema per un dispositivo gestito. Queste metriche vengono acquisite ogni 30 secondi.
- **Statistiche alimentatore.** I dati di metrica per l'ingresso e l'uscita dell'alimentatore, in watt, per un dispositivo gestito. Queste metriche vengono acquisite ogni 30 secondi.

I tipi di origini dati (avvisi, eventi, inventari e metriche) elencati variano in base ai dati disponibili in XClarity Orchestrator. Ad esempio, se sono disponibili dati di avvisi, viene elencato il tipo **Avvisi**. Se sono disponibili i dati degli eventi vengono elencati tutti i tipi **Eventi-***.

L'origine dati selezionata ha effetto sui dati disponibili nella scheda **Condizioni di query**. Se si seleziona un tipo generico, ad esempio **Inventari-Dispositivi** vengono elencati solo gli attributi comuni a tutti i dispositivi. Se si seleziona **Inventari-Dispositivo-Server** vengono elencati gli attributi comuni a tutti i server.

Passo 5. Fare clic su **Condizioni di query** per definire le condizioni di query per il report.

1. Restringere i dati che si desidera utilizzare per questa query.
 - a. Selezionando uno o più campi dall'elenco a discesa **Campi filtrati**. I campi elencati in base al tipo di origine dati selezionato nel [passaggio 4](#).
 - b. Se sono stati selezionati più campi Filtro, scegliere l'operatore da utilizzare per creare la query. È possibile selezionare uno dei seguenti valori.
 - **AND.** Tutti i valori devono corrispondere.
 - **OR.** È necessario che uno o più valori corrispondano.
 - **E (negato).** Tutti i valori non devono corrispondere.
 - **O (negato).** È necessario che uno o più valori non corrispondano.
 - c. Per ciascun campo filtrato selezionato, scegliere l'operatore di confronto dall'elenco a discesa **Confronto** e il valore del campo. Gli operatori di confronto disponibili differiscono in base al tipo di dati per l'attributo.
 - **>=.** Confronta i valori *maggiori o uguali* a un valore specificato
 - **<=.** Confronta i valori *minori o uguali* a un valore specificato
 - **>.** Confronta i valori *maggiori* a un valore specificato
 - **<.** Confronta i valori *minori* a un valore specificato
 - **=.** Confronta i valori *uguali* a un valore specificato
 - **!=.** Confronta tutti i valori *diversi da* un valore specificato
 - **Contiene.** (Solo per le query di inventario ed eventi) Confronta qualsiasi valore parziale specificato in una matrice
 - **In.** (Solo per le query di inventario ed eventi) Confronta qualsiasi valore specificato in una matrice
 - **Non in.** (Solo per le query di inventario ed eventi) Confronta nessun valore specificato in una matrice

Suggerimento: per individuare i valori correnti per qualsiasi campo, creare una nuova query con lo stesso tipo di origine dati, selezionare il nome del campo dall'elenco a

discesa **Campi raggruppati**, specificare 0 per il **Limite** e fare clic su **Salva**. La scheda **Opzioni grafico** viene visualizzata con un elenco di tutti i valori correnti.

2. Facoltativamente, scegliere una funzione di aggregazione nella sezione **Aggregazione risultati** per creare un nuovo campo in base ai dati filtrati e specificare un nome (alias) per il nuovo campo. Per alcune funzioni di aggregazione, come Media e Massima, è necessario specificare anche il campo in cui si desidera applicare la funzione.

Per le query di eventi e inventario è possibile scegliere una delle seguenti funzioni.

- **Media**. Media statistica di tutti i valori
- **Somma**. Somma di tutti i valori
- **Conteggio**. Numero di valori
- **Massimo**. Valore più elevato
- **Minimo**. Valore più basso
- **Primo**. Valore con il timestamp meno recente
- **Ultimo**. Valore con il timestamp più recente

Per le query di metriche è possibile scegliere una delle seguenti funzioni.

- **Conteggio**. Numero di valori non null
 - **Distinto**. Elenco di valori univoci
 - **Intero**. Valore medio del campo
 - **Media**. Media aritmetica dei valori
 - **Mediano**. Valore medio
 - **Modalità**. Valore più frequente
 - **Estensione**. Differenza tra i valori minimo e massimo
 - **Devstd**. Deviazione standard
 - **Somma**. Somma di tutti i valori
3. È possibile scegliere i campi che si desidera utilizzare per raggruppare i risultati della query dall'elenco a discesa **Campi raggruppati**. Quando si sceglie un campo raggruppato, XClarity Orchestrator rimuove (decostruisce) i dati, in modo da creare un punto dati per ciascun valore dei campi selezionati.
 4. Scegliere facoltativamente come ordinare i risultati della query selezionando un campo dall'elenco a discesa **Ordina per campo** e l'ordinamento dall'elenco a discesa **Ordinamento**. Per le query di metriche è possibile ordinare solo per ora.
 5. Specificare facoltativamente il numero di punti dati da restituire nei risultati della query nel campo **Limite**. Il limite predefinito è 10. Se si specifica 0 o si lascia vuoto il campo vengono restituiti tutti i punti dati.

È inoltre possibile specificare facoltativamente il numero di punti dati che si desidera ignorare nei risultati della query nel campo **Offset**.

6. (Solo per query di metriche) Se si selezionano i campi raggruppati, specificare facoltativamente il numero di set di dati da restituire nei risultati della query nel campo **Limite serie**. Il limite predefinito è vuoto (0). Se si specifica 0 o si lascia il campo vuoto vengono restituiti tutti i set di dati.

È inoltre possibile specificare facoltativamente il numero di set di dati che si desidera ignorare nei risultati della query nel campo **Offset serie**.

7. Fare clic su **Salva** per salvare la query e generare il report.

Passo 6. Fare clic su **Opzioni grafico** per scegliere l'aspetto del report. Sono disponibili i seguenti tipi di grafici.

- **Tabella**. Visualizza i dati in formato tabulare.
- **Barra**. Visualizza i dati in un grafico a barre. Scegliere i campi che si desidera utilizzare per l'asse x e y.

- **Torta.** Visualizza i dati in un grafico a torta. Scegliere i campi che si desidera utilizzare per l'asse x e y. È possibile scegliere di utilizzare un grafico a torta solo quando i dati non sono raggruppati.

Passo 7. Fare clic su **Crea** per aggiungere una nuova scheda che contiene un report con i risultati della query corrente.

Al termine

Nella scheda Query personalizzate è possibile effettuare le operazioni che seguono.

- Ingrandire un report personalizzato facendo clic sull'icona **Ingrandisci** (🔍) nella scheda del report personalizzato. Per i report tabulari, l'icona del report nella scheda Query personalizzate mostra solo le prime quattro colonne della tabella. È possibile ingrandire il report per visualizzare tutte le colonne nella tabella.

Il collegamento **Visualizza dettagli** in una colonna della tabella indica che la colonna contiene più campi di dati. Fare clic sul collegamento **Visualizza dettagli** per visualizzare una tabella a comparsa in cui sono elencati i dati aggiuntivi.

- Modificare le proprietà di un report personalizzato facendo clic sull'icona **Modifica** (✎) sulla scheda.
- Eliminare un report personalizzato facendo clic sull'icona **Elimina** (🗑️) sulla scheda.

Analisi dei tempi di avvio dei dispositivi

Il pannello Analisi contiene schede di riepilogo in cui sono riportati i tempi di avvio dei dispositivi gestiti. Il *tempo di avvio* è la quantità di tempo, in secondi, necessaria per completare l'avvio del sistema prima che il sistema operativo sia pronto per l'uso.

Per visualizzare i report relativi al tempo di avvio, fare clic su **Analisi** (🔍) → **Analisi predefinite**, quindi su **Tempi di avvio** per visualizzare le schede con le analisi correlate.

Nota: Le statistiche di avvio sono disponibili solo per i dispositivi ThinkSystem e ThinkAgile con firmware XCC v1.40 o versioni successive.

Tempi di avvio

Questa scheda di riepilogo include un grafico a barre che mostra la quantità di tempo necessaria per il completamento degli avvii, per i dispositivi con il più lungo dei tempi di avvio più recenti.

Analisi dei problemi di connettività

Il pannello Analisi contiene schede di riepilogo che mostrano statistiche sui problemi di connettività.

La perdita di connettività viene segnalata utilizzando l'evento che segue.

- **FQXHMDM0163J.** La connessione tra lo strumento di gestione delle risorse e il controller di gestione della scheda di base nel dispositivo è offline.

Per visualizzare i report relativi alla perdita di connettività, fare clic su **Analisi** (🔍) → **Analisi predefinite**, quindi su **Problemi di connettività** per visualizzare le schede con le analisi correlate.

Problemi di connettività in base al tempo

Questa scheda di riepilogo include un grafico a barre che mostra il numero di problemi di connettività che si sono verificati durante il giorno o il mese corrente per ciascuna risorsa.

È possibile scegliere di visualizzare i dati per un intervallo di tempo specifico selezionando l'icona **Impostazioni** (⚙️) nell'angolo in alto a destra della scheda.

Primi 10 dispositivi per numero di problemi di connettività

Questa scheda di riepilogo include un grafico a barre che mostra i primi 10 dispositivi con il numero totale più elevato di problemi di connettività. È possibile fare clic su un elemento della legenda per ottenere maggiori informazioni su una risorsa specifica.

Analisi delle correzioni di sicurezza

Il pannello Analisi contiene schede di riepilogo con analisi sulle correzioni di sicurezza per vulnerabilità e rischi comuni (CVE) noti.

Per visualizzare i report CVE, fare clic su **Analisi** (🔍) → **Analisi predefinite**, quindi su **Correzioni di sicurezza** per visualizzare le schede con le analisi correlate.

Correzioni di sicurezza

Questa scheda del report include le statistiche e i grafici seguenti.

- Un grafico circolare che mostra il numero di dispositivi gestiti con vulnerabilità e rischi comuni (CVE) per i quali è disponibile una correzione di sicurezza, in base alla gravità CVE più elevata.
 - **Critico**. Numero di dispositivi con almeno una gravità CVE critica
 - **Non critico**. Numero di dispositivi con almeno una gravità CVE alta, media o bassa, ma non critica
 - **Protetto**. Numero di dispositivi che non hanno gravità CVE note e sono protetti
- Un grafico circolare che mostra il numero di CVE univoci per i quali sono disponibili correzioni di sicurezza, in base alla gravità (critica, alta, media o bassa).

È possibile passare il mouse su ogni barra colorata nei grafici circolari per ottenere ulteriori informazioni sullo stato. È inoltre possibile fare clic sul numero accanto a ciascuno stato per visualizzare un elenco di tutti i dispositivi che soddisfano i criteri.

Dispositivi

Nella scheda Dispositivi è elencato il numero totale di CVE per cui è disponibile una correzione di sicurezza e la gravità più elevata per ogni dispositivo. È possibile espandere il dispositivo per visualizzare un elenco di componenti del dispositivo con correzioni di sicurezza e il numero di correzioni di sicurezza disponibili grazie agli aggiornamenti firmware scaricati nel repository degli aggiornamenti.

È possibile fare clic sul numero di correzioni di sicurezza per aprire una finestra di dialogo con un elenco filtrato di CVE applicabili per il componente specificato. In questa finestra di dialogo è possibile fare clic sul collegamento CVE per ottenere informazioni dettagliate sul CVE sul Web.

È possibile mostrare o nascondere la scheda Dispositivi facendo clic sull'interruttore **Mostra/Nascondi dispositivi**. L'interruttore passa automaticamente su **Mostra dispositivi** quando si fa clic su un numero nei grafici.

Analisi dell'integrità dell'unità

Il pannello "Analisi" contiene schede di report che mostrano l'analisi dell'integrità e gli errori previsti delle unità disco fisso e delle unità SSD nei server ThinkAgile e ThinkSystem gestiti.

Per visualizzare i report relativi al firmware, fare clic su **Analisi** (🔍) → **Analisi predefinite**, quindi su **Analisi predittiva dell'unità** per visualizzare le schede con le analisi correlate.

Le analisi sono supportate per i seguenti tipi di modelli di unità.

Unità disco fisso

- ST2000NX0253

- ST8000NM0055
- ST10000NM0086
- ST12000NM0008

Unità SSD

- Intel SSDSC2BB800G4

Importante: Le unità con firmware meno recenti non sono idonee per l'analisi. Aggiornare le unità al livello firmware più recente per abilitare l'analisi predittiva.

Unità a rischio

Questa scheda del report contiene un grafico a torta che mostra il numero di unità e il relativo stato di integrità (normale o a rischio).

Cronologia unità a rischio

Questa scheda del report contiene un diagramma a barre che mostra il numero di unità guaste nell'ultimo anno o settimana. Passare il cursore su ogni barra del grafico per visualizzare un elenco filtrato di unità guaste, per dispositivo, in un determinato giorno.

Unità con errore previsto

La scheda del report contiene una tabella che elenca i dispositivi con unità guaste. Fare clic su un dispositivo per elencare i dettagli di ogni unità a rischio nel dispositivo.

Analisi del firmware

Il pannello Analisi contiene schede di riepilogo con analisi sul firmware.

Per visualizzare i report relativi al firmware, fare clic su **Analisi** (🔍) → **Analisi predefinite**, quindi su **Analisi firmware** per visualizzare le schede con le analisi correlate.

Analisi firmware

Questa scheda di riepilogo include un grafico a barre che mostra il numero di firmware installati sui dispositivi gestiti in base alla categoria e all'età del firmware.

Il firmware è raggruppato nelle seguenti categorie.

- Controller di gestione
- Strumenti di sistema
- UEFI

Le età del firmware sono raggruppate nei seguenti intervalli

- **Meno di 6 mesi**
- **6-12 mesi**
- **1-2 anni**
- **Oltre 2 anni**

È possibile filtrare i dispositivi inclusi nel report utilizzando i campi di immissione **Filtri**. È inoltre possibile salvare le query filtrate che si desidera utilizzare regolarmente.

È possibile mostrare o nascondere la scheda Dispositivi facendo clic sull'interruttore **Mostra/Nascondi dispositivi**. La scheda Dispositivi elenca i tipi e le età dei firmware per tutti i dispositivi inclusi nel grafico.

Analisi degli eventi persi

Il pannello Analisi contiene schede di riepilogo con statistiche sugli eventi persi. Gli eventi persi sono determinati da un gap nella sequenza numerica.

Gli eventi hanno un numero di sequenza che indica l'ordine in cui si è verificato ogni evento su un dispositivo specifico. I numeri di sequenza degli eventi devono essere consecutivi per un dispositivo specifico. Se sono presenti numeri di sequenza non consecutivi, il gap potrebbe indicare che uno o più eventi sono stati persi.

Per visualizzare i report relativi agli eventi persi, fare clic su **Analisi** (🔍) → **Analisi predefinite** e selezionare **Eventi persi** per visualizzare le schede con le analisi correlate.

Eventi persi per ora

Questa scheda di riepilogo include un grafico a barre che mostra il numero di eventi persi durante il giorno o il mese corrente per ciascuna risorsa.

È possibile scegliere di visualizzare i dati per un intervallo di tempo specifico selezionando l'icona **Impostazioni** (⚙️) nell'angolo in alto a destra della scheda.

Primi 10 dispositivi per numero di eventi persi

Questa scheda di riepilogo include un grafico a barre che mostra i primi 10 dispositivi con il numero totale più elevato di eventi persi.

Analisi e previsione della capacità degli strumenti di gestione delle risorse

Il pannello Analisi contiene schede di riepilogo con le previsioni di quando gli strumenti di gestione delle risorse supereranno il numero massimo di dispositivi gestiti. Per gli strumenti di gestione delle risorse di Lenovo XClarity Administrator sono supportati fino a 1.000 dispositivi gestiti.

Per visualizzare i report relativi alla capacità degli strumenti di gestione delle risorse, fare clic su **Analisi avanzata** (🔍) → **Analisi predefinite**, quindi su **Previsione capacità di gestione delle risorse** per visualizzare le schede con le analisi correlate.

Capacità degli strumenti di gestione

Questo report elenca la capacità del dispositivo per ogni strumento di gestione delle risorse, inclusi il numero di dispositivi gestiti e lo stato della capacità, che indica se la capacità è sovraccarica. Vengono utilizzati i seguenti stati di capacità.

- (✅) **Normale**. Numero di dispositivi gestiti inferiore al numero massimo di dispositivi supportati.
- (⚠️) **Avvertenza**. Numero di dispositivi gestiti prossimo al numero massimo di dispositivi supportati.
- (❌) **Critico**. Numero di dispositivi gestiti superiore al numero massimo di dispositivi supportati.

Gestisci tendenza della capacità

Questa scheda di riepilogo include un grafico a linee che mostra il numero di dispositivi gestiti, nel tempo, per uno strumento di gestione delle risorse specifico e la tendenza prevista quando il numero di dispositivi gestiti raggiunge la capacità massima supportata dallo strumento di gestione delle risorse.

Fare clic su una riga nella tabella Capacità degli strumenti di gestione per visualizzare le tendenze di capacità dello strumento di gestione delle risorse.

È possibile modificare il periodo di tempo visualizzato facendo clic sul menu a discesa. È possibile scegliere di visualizzare i dati per anno, mese o giorno. È inoltre possibile modificare il numero di periodi visualizzati nel grafico utilizzando la casella di zoom del grafico.

Analisi e previsione delle tendenze di utilizzo

Il pannello Analisi contiene schede di riepilogo che mostrano l'utilizzo cronologico e previsto di processore, storage e memoria sui dispositivi e sulle risorse virtuali (come host, cluster e macchine virtuali).

Importante: Questa funzione richiede una connessione allo strumento di gestione delle risorse di VMware vRealize Operations Manager (vedere [Connessione degli strumenti di gestione delle risorse](#)).

Per visualizzare i report delle tendenze di utilizzo, fare clic su **Analisi avanzata** (☺) → **Analisi predefinite** e selezionare **Tendenza utilizzo carico di lavoro**. Verranno visualizzate le schede con le analisi correlate.

Selezione delle risorse

Questo report elenca i dispositivi e le risorse virtuali gestiti dal server Orchestrator.

Fare clic su una riga nella tabella per visualizzare le tendenze di utilizzo di quella risorsa.

Tendenza utilizzo CPU

Questa scheda di riepilogo include un grafico a linee che mostra l'utilizzo del processore, nel tempo, per una risorsa virtuale specifica e la tendenza prevista quando l'utilizzo del processore raggiungerà la capacità massima supportata per la risorsa virtuale.

È possibile modificare il periodo di tempo visualizzato per i dati cronologici e previsti, rispettivamente nei menu a discesa **Cronologia** e **Proiezione**. È inoltre possibile modificare il numero di periodi visualizzati nel grafico utilizzando la casella di zoom del grafico.

Tendenza utilizzo memoria

Questa scheda di riepilogo include un grafico a linee che mostra l'utilizzo della memoria, nel tempo, per una risorsa virtuale specifica e la tendenza prevista quando l'utilizzo della memoria raggiungerà la capacità massima supportata per la risorsa virtuale.

È possibile modificare il periodo di tempo visualizzato per i dati cronologici e previsti, rispettivamente nei menu a discesa **Cronologia** e **Proiezione**. È inoltre possibile modificare il numero di periodi visualizzati nel grafico utilizzando la casella di zoom del grafico.

Tendenza utilizzo storage

Questa scheda di riepilogo include un grafico a linee che mostra l'utilizzo dello storage, nel tempo, per una risorsa virtuale specifica e la tendenza prevista quando l'utilizzo dello storage raggiungerà la capacità massima supportata per la risorsa virtuale.

È possibile modificare il periodo di tempo visualizzato per i dati cronologici e previsti, rispettivamente nei menu a discesa **Cronologia** e **Proiezione**. È inoltre possibile modificare il numero di periodi visualizzati nel grafico utilizzando la casella di zoom del grafico.

Analisi delle metriche di prestazioni e utilizzo

Il pannello Analisi contiene le schede del report che mostrano le mappe termiche in base a metriche e risorse specifiche per le ultime 24 ore.

Per visualizzare le mappe termiche delle prestazioni, fare clic su **Analisi avanzata** (🔍) → **Analisi predefinite**, quindi su **Mappa termica delle prestazioni** per visualizzare le schede con le analisi correlate.

Mappa termica delle prestazioni

Questa scheda di report include una mappa termica che illustra il numero di dispositivi con valori di metrica all'interno di un numero specifico di intervalli per un determinato periodo di tempo.

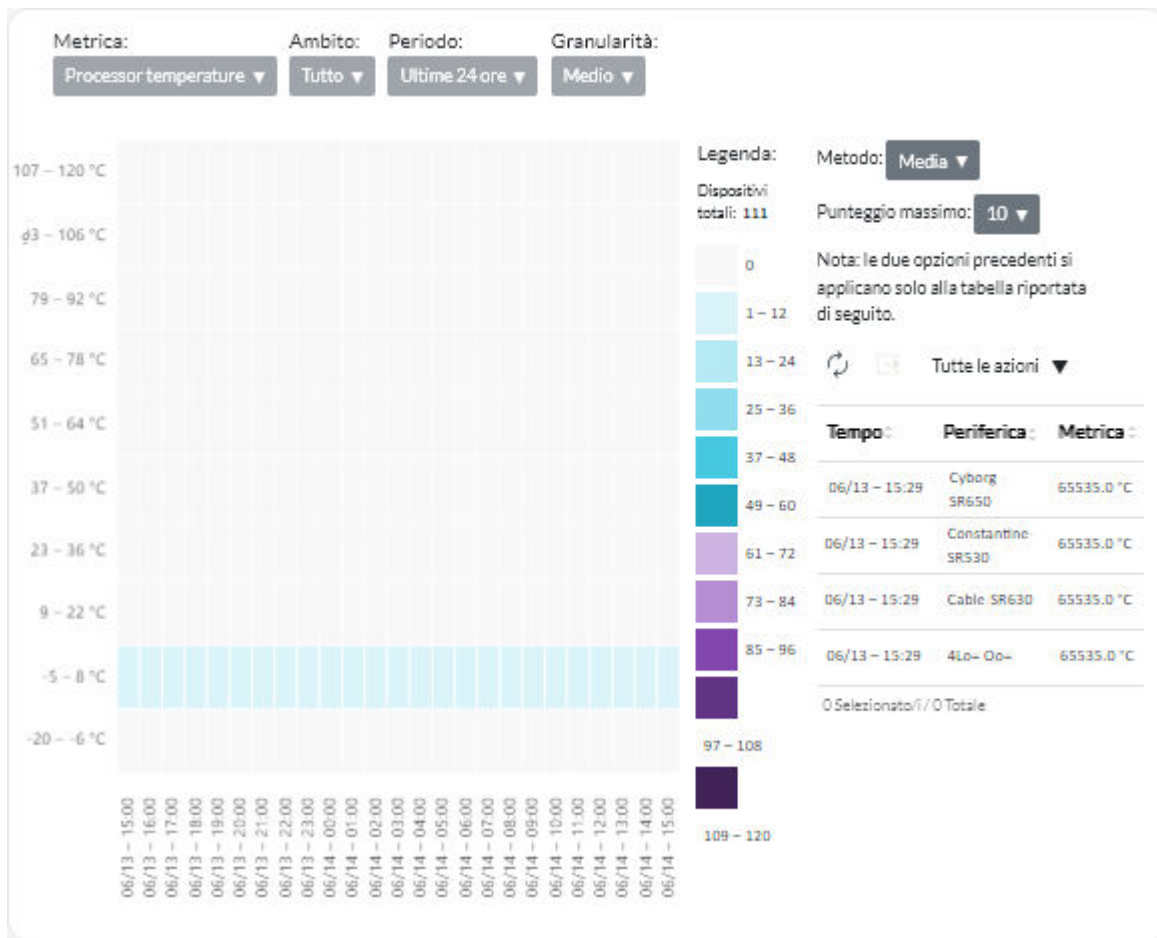
È possibile fare clic su qualsiasi cella nella mappa termica per visualizzare un elenco a discesa di dispositivi rappresentati da questa cella, con informazioni sul valore metrico effettivo per ciascun dispositivo e il timestamp in cui è stata raccolta la metrica.

È possibile configurare la mappa termica per visualizzare solo le informazioni desiderate.

- È possibile visualizzare i dati per una delle seguenti metriche.
 - Temperatura del processore
 - Utilizzo del processore
 - Utilizzo della memoria
- È possibile scegliere di aggregare i dati di metrica in base alla media o al valore di picco (massimo).
- È possibile filtrare la mappa termica per includere solo i dati di metrica per i dispositivi in uno specifico gruppo di dispositivi.

Nota: Se l'ambito dell'interfaccia utente viene ristretto a uno specifico strumento di gestione delle risorse, solo i dati per i dispositivi nei gruppi selezionati che sono gestiti anche dallo strumento di gestione delle risorse vengono inclusi nella mappa termica.

- È inoltre possibile scegliere gli intervalli di valori numerici da visualizzare sull'asse x della mappa termica. Il numero di valori tra massimo e minimo è suddiviso in parti uguali in base al numero scelto. È possibile scegliere 10, 15 o 20.
- È inoltre possibile scegliere di elencare i primi 10, 15 o 20 dispositivi con i valori più alti e il timestamp in cui è stata raccolta la metrica.



Analisi degli eventi ripetuti

Il pannello "Analisi" contiene le schede dei report che riepilogano gli eventi ripetuti per ciascun dispositivo.

Gli *eventi ripetuti* vengono generati quando si verificano le seguenti condizioni:

- **FQXXOIS0002J**. Un evento di avvertenza o critico con lo stesso ID è stato generato una o più volte per lo stesso dispositivo in almeno tre periodi consecutivi di 5 minuti.
- **FQXXOIS0003J**. Più di cinque eventi di avvertenza o critici sono stati generati per lo stesso dispositivo ogni ora per due o più ore consecutive.

Per visualizzare i report relativi agli eventi ripetuti, fare clic su **Analisi avanzata** (🔍) → **Analisi predefinite**, quindi su **Eventi ripetuti** per visualizzare le schede con le analisi correlate.

Eventi ripetuti

Questa scheda di riepilogo include un grafico a barre che mostra il numero totale di eventi ripetuti, per ogni dispositivo.

Eventi ripetuti per ora

Questa scheda di riepilogo include un grafico a barre che mostra il numero di eventi ripetuti generati il giorno corrente, per ogni dispositivo.

Analisi dei tentativi di accesso non autorizzato

Il pannello Analisi contiene schede di riepilogo in cui sono elencati i tentativi di accesso non autorizzato (login non riuscito).

Per visualizzare i report degli accessi non autorizzati, fare clic su **Analisi** (🔍) → **Analisi predefinite**, quindi su **Tentativi di accesso non autorizzato** per visualizzare le schede con le analisi degli accessi non autorizzati.

Numero di tentativi di login non riusciti per utente

Questa scheda di riepilogo include un grafico che mostra il numero totale di tentativi di accesso non autorizzato per ogni utente (per nome utente). È possibile visualizzare i dati come grafico a barre (📊) o grafico a torta (📈) facendo clic sull'icona appropriata nell'angolo superiore sinistro della scheda.

È possibile posizionare il puntatore del mouse su ogni barra o parte del grafico per ottenere maggiori informazioni, come l'ultima occorrenza.

Numero di tentativi di login non riusciti per utente, in ciascun periodo

Questa scheda di riepilogo include un grafico a barre che mostra il numero di tentativi di accesso non autorizzato che si sono verificati nel giorno corrente per ogni utente (per nome utente).

Numero di tentativi di login non riusciti per indirizzo IP

Questa scheda di riepilogo include un grafico a barre che mostra il numero totale di tutti i tentativi di accesso non autorizzato per ogni utente (per indirizzo IP). È possibile visualizzare i dati come grafico a barre (📊) o grafico a torta (📈) facendo clic sull'icona appropriata nell'angolo superiore sinistro della scheda.

È possibile posizionare il puntatore del mouse su ogni barra o parte del grafico per ottenere maggiori informazioni, come l'ultima occorrenza.

Numero di tentativi di login non riusciti per indirizzo IP dell'utente, in ciascun periodo

Questa scheda di riepilogo include un grafico a barre che mostra il numero di tentativi di accesso non autorizzato che si sono verificati nel giorno corrente per ogni utente (per indirizzo IP).

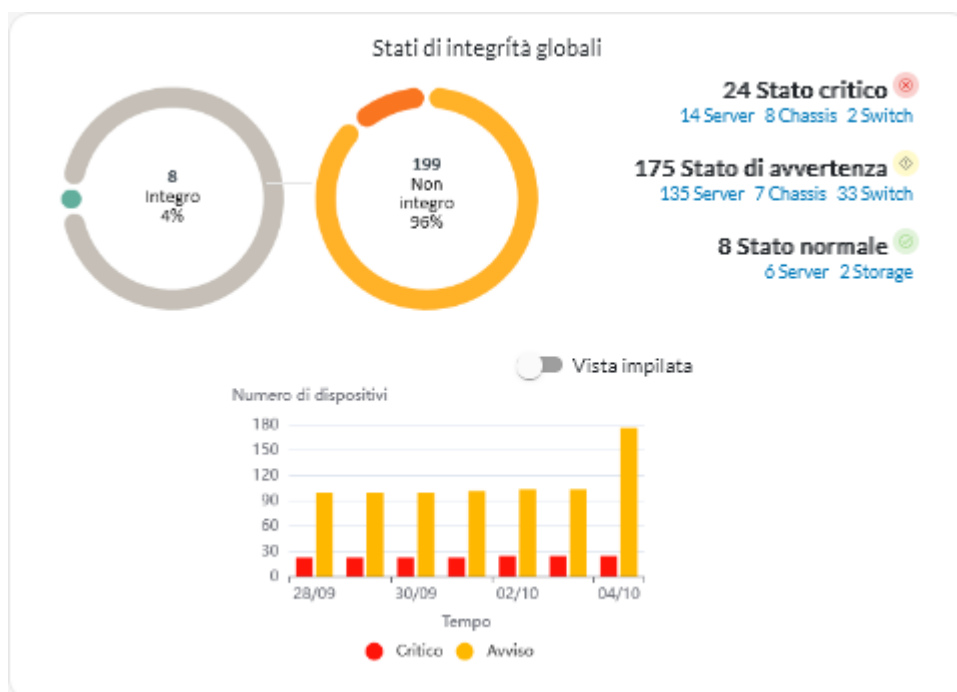
Analisi dell'integrità del dispositivo

La scheda con lo stato di integrità globale sul dashboard e la scheda con l'analisi del dispositivo su ciascuna pagina dei dispositivi riepilogano l'integrità globale dei dispositivi gestiti.

Riepilogo dello stato di tutti i dispositivi

Sulla barra dei menu di XClarity Orchestrator fare clic su **Dashboard** (🏠) per visualizzare le schede del dashboard con una panoramica e lo stato di tutti i dispositivi gestiti e delle altre risorse (vedere [Visualizzazione del riepilogo dell'ambiente in uso](#)).

È possibile modificare l'ambito del riepilogo solo su quei dispositivi gestiti da uno strumento di gestione delle risorse specifico o in un gruppo di risorse specifico utilizzando il menu a discesa **Seleziona gestione**.



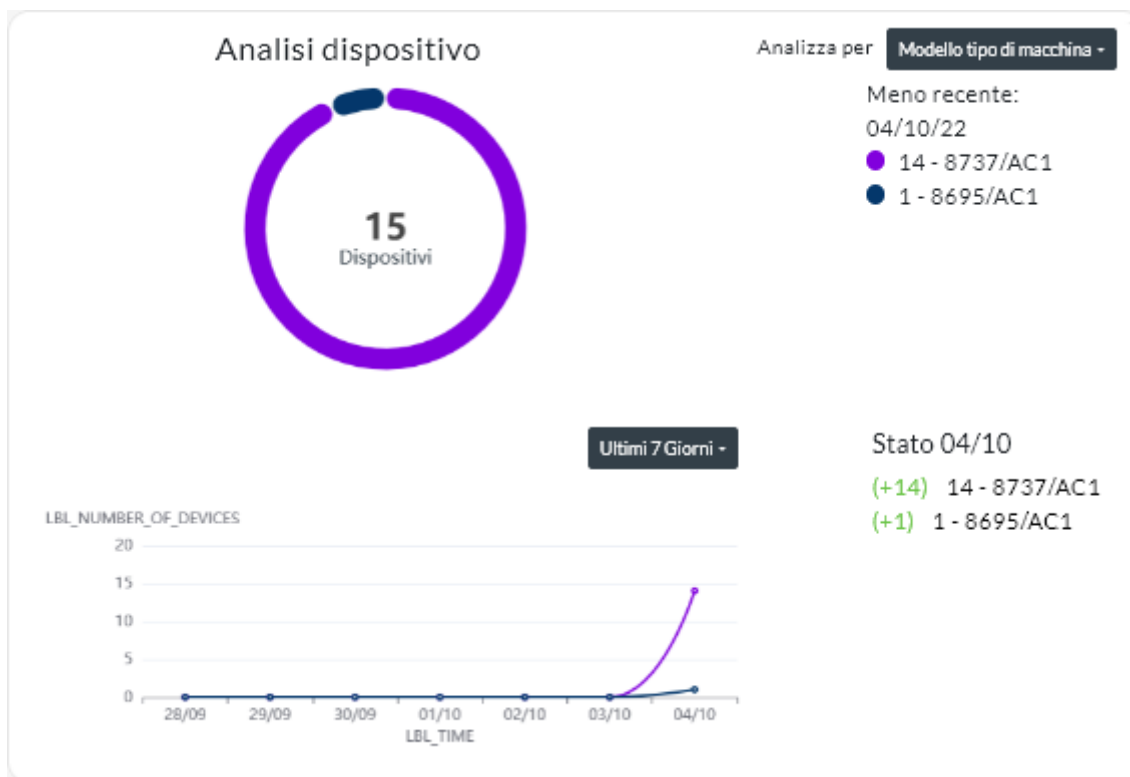
Ogni barra colorata nei grafici a barre e circolari indica il numero di dispositivi in uno stato specifico. È possibile passare il mouse su ogni barra colorata per ottenere ulteriori informazioni sullo stato. È inoltre possibile fare clic sul numero di dispositivi in ogni stato per visualizzare un elenco di tutti i dispositivi che soddisfano i criteri.

Riepilogo dello stato di tutti i dispositivi di un tipo specifico

Per visualizzare i riepiloghi globali degli avvisi attivi, fare clic su **Risorse** (🔍) sulla barra dei menu di XClarity Orchestrator, quindi sul tipo di dispositivo per mostrare una scheda con una vista tabulare di tutti i dispositivi simili. Ad esempio, se si seleziona **Server**, viene visualizzato un elenco di tutti i server rack, tower e ad alta densità e di tutti i server Flex System e ThinkSystem in uno chassis.

È possibile cambiare l'ambito del riepilogo in base alla proprietà del dispositivo nell'elenco a discesa **Analizza per**.

- **Modello tipo di macchina.** (impostazione predefinita) Questo report riepiloga l'integrità del dispositivo in base al modello MTM (Modello tipo di macchina).
- **Tipo di macchina.** Questo report riepiloga l'integrità del dispositivo in base al tipo di macchina.
- **Nome prodotto.** Questo report riepiloga l'integrità del dispositivo in base al prodotto.



XClarity Orchestrator riassume l'integrità del dispositivo in base a criteri specifici. Ciascun riepilogo include le seguenti informazioni.

- Un grafico circolare che mostra il numero totale di dispositivi non integri e la percentuale di dispositivi in ciascun stato di assenza di integrità (critico, avvertenza e sconosciuto).
 Ogni barra colorata nel grafico circolare indica il numero di dispositivi in uno stato specifico. È possibile passare il mouse su ogni barra colorata per ottenere ulteriori informazioni sullo stato.
- Un grafico a linee che mostra il numero di dispositivi in ciascun stato di integrità su base giornaliera per il numero di giorni specificato.
 Ogni barra colorata nel grafico a linee indica il numero di dispositivi in uno stato specifico. È possibile passare il mouse su ogni barra colorata per ottenere ulteriori informazioni sullo stato.
- Il numero di dispositivi di ogni tipo che non sono integri in un giorno specifico. Il giorno corrente viene visualizzato per impostazione predefinita. È possibile modificare il giorno passando il mouse su ciascun giorno nel grafico a linee.

Analisi dell'integrità delle risorse dell'infrastruttura

È possibile determinare l'integrità globale e l'andamento dei sensori delle risorse dell'infrastruttura.

Stato di integrità delle risorse dell'infrastruttura

Sulla barra dei menu di Lenovo XClarity Orchestrator fare clic su **Risorse** (⚙️) → **Infrastruttura** per visualizzare la scheda Infrastruttura. È possibile determinare lo stato di integrità di ogni risorsa nella colonna **Stato**.

Andamento dei sensori

Sulla barra dei menu di XClarity Orchestrator fare clic su **Risorse** (🔧) → **Infrastruttura** per accedere alla scheda Infrastruttura, quindi su una risorsa dell'infrastruttura nella tabella per visualizzare un elenco di sensori per la risorsa e l'ultima misurazione di ciascuno.

Selezionare uno o più sensori, quindi fare clic sull'icona **Grafico** (📊) per visualizzare il grafico a linee che mostra le misurazioni, nel tempo, per ciascun sensore selezionato. Per impostazione predefinita, i sensori con la stessa unità (ad esempio, watt o amp) sono riportati sullo stesso grafico.

Nota: Schneider Electric EcoStruxure IT Expert raccoglie i dati dei sensori ogni 5 minuti e XClarity Orchestrator li sincronizza ogni ora. Al momento XClarity Orchestrator consente di salvare solo gli ultimi 60 minuti di dati.

Analisi di avvisi attivi

Nella scheda Analisi avvisi sono riepilogati gli avvisi attivi.

Lenovo XClarity Orchestrator riepiloga gli avvisi attivi in base a criteri specifici. Ciascun riepilogo include le seguenti informazioni.

- Un grafico circolare che mostra il numero totale di avvisi attivi e la percentuale di avvisi associati a ciascun tipo di riepilogo.
- Il numero di avvisi attivi per ogni tipo di riepilogo.
- La data di creazione dell'avviso attivo meno recente
- Un grafico a linee che mostra il numero di avvisi attivi per ogni tipo di riepilogo su base giornaliera per il numero di giorni specificato
- Il numero di avvisi attivi per ogni tipo di riepilogo in un giorno specifico. Il giorno corrente viene visualizzato per impostazione predefinita. È possibile modificare il giorno passando il mouse su ciascun giorno nel grafico a linee.

Avvisi attivi globali

Per visualizzare i riepiloghi degli avvisi attivi globali, completare le seguenti operazioni.

1. Sulla barra dei menu di XClarity Orchestrator fare clic su **Monitoraggio** (📊) → **Avvisi** per visualizzare la scheda Analisi avvisi.
2. Selezionare il periodo di tempo dall'elenco a discesa al di sopra del grafico a linee. Per impostazione predefinita, vengono presi in esame gli ultimi sette giorni.
3. Selezionare il tipo di riepilogo dall'elenco a discesa **Analizza per**.
 - **Gravità** (impostazione predefinita). Questo report riepiloga gli avvisi attivi per gravità: critici, di avvertenza e informativi.
 - **Tipo di origine**. Questo report riepiloga gli avvisi attivi generati da ogni tipo di origine, quali dispositivi, gestione e analisi.
 - **Tipo di risorsa**. Questo report riepiloga gli avvisi attivi per ogni tipo di risorsa, quali dispositivi, strumenti di gestione delle risorse e XClarity Orchestrator.
 - **Intervento richiesto**. Questo report riepiloga gli avvisi attivi associati a ciascun tipo di intervento richiesto: **nessuno** (intervento non richiesto), **utente** (intervento eseguito dall'utente), **manutenzione** (intervento eseguito da Lenovo).

Avvisi attivi per uno specifico dispositivo

Per visualizzare l'avviso attivo per uno specifico dispositivo, completare le seguenti operazioni.

1. Sulla barra dei menu di XClarity Orchestrator fare clic su **Risorse** (🔧), quindi sul tipo di dispositivo per visualizzare una scheda con una vista tabulare di tutti i dispositivi gestiti simili.
2. Fare clic sulla riga relativa al dispositivo per visualizzare le schede di riepilogo per quel dispositivo.
3. Fare clic su **Log avvisi** per visualizzare l'elenco degli avvisi attivi per il dispositivo e la scheda "Analisi avvisi".
4. Nella scheda Analisi avvisi selezionare il periodo di tempo dall'elenco a discesa sopra il grafico a linee. Per impostazione predefinita, vengono presi in esame gli ultimi sette giorni.
5. Selezionare il tipo di riepilogo dall'elenco a discesa **Analizza per**.
 - **Tipo di origine.** Questo report riepiloga gli avvisi attivi generati da ogni tipo di origine, quali dispositivi, gestione e analisi.
 - **Tipo di intervento richiesto.** Questo report riepiloga gli avvisi attivi associati a ciascun tipo di intervento richiesto: nessuno (intervento non richiesto), utente (intervento eseguito dall'utente), manutenzione (intervento eseguito da Lenovo).
 - **Gravità.** Questo report riepiloga gli avvisi attivi per gravità: critici, di avvertenza e informativi.

Capitolo 7. Utilizzo di assistenza e supporto

Lenovo XClarity Orchestrator fornisce un set di strumenti che è possibile utilizzare per raccogliere e inviare file di servizio a Supporto Lenovo, configurare notifiche automatiche per i fornitori di servizi quando si verificano eventi che richiedono assistenza su dispositivi specifici e visualizzare lo stato del ticket di assistenza e le informazioni sulla garanzia. È possibile contattare Supporto Lenovo per ottenere indicazioni e assistenza tecnica quando si riscontrano problemi.

Invio di dati periodici a Lenovo

Facoltativamente è possibile consentire a Lenovo XClarity Orchestrator di raccogliere informazioni sull'ambiente hardware e di inviare i dati a Lenovo su base periodica. Lenovo utilizza questi dati per migliorare l'esperienza dei clienti con i prodotti e con il supporto Lenovo.

Prima di iniziare

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

Attenzione: È necessario accettare l'[Informativa sulla privacy di Lenovo](#) prima di poter trasferire i dati al supporto Lenovo.

Informazioni su questa attività

Analizzando i dati hardware di più utenti, Lenovo può acquisire informazioni sulle modifiche hardware regolari. Questi dati possono quindi essere utilizzati per migliorare le analisi predittive e l'esperienza di assistenza e supporto, approvvigionando le parti di ricambio nelle aree geografiche appropriate.

Quando si accetta di inviare i dati hardware a Lenovo, i seguenti dati vengono raccolti e inviati periodicamente.

- **Dati hardware quotidiani.** Solo le modifiche ai dati di inventario e ai dati di analisi dell'unità (se la raccolta dati è abilitata) per ogni dispositivo gestito
- **Dati hardware settimanali.** Tutti i dati di inventario per i dispositivi gestiti e le informazioni sugli strumenti di gestione delle risorse connessi

Attenzione: Questi dati *non sono anonimi*.

- I dati raccolti *includono* UUID, WWN, ID dispositivo e numeri di serie. XClarity Orchestrator modifica l'inventario eseguendo l'hashing di UUID, WWN e ID dispositivo mediante SHA512.
- I dati raccolti *non includono* informazioni di rete (indirizzi IP, nomi di dominio o nome host) o informazioni utente.

Quando i dati vengono inviati a Lenovo vengono trasmessi dall'istanza XClarity Orchestrator alla funzione Caricamento Lenovo mediante HTTPS. Le API REST vengono richiamate su questa connessione HTTPS per inviare i dati. Per l'autenticazione viene utilizzato un certificato precaricato su XClarity Orchestrator. Se un'istanza XClarity Orchestrator non ha accesso diretto a Internet ed è presente un proxy configurato in XClarity Orchestrator, i dati vengono trasmessi tramite questo proxy.

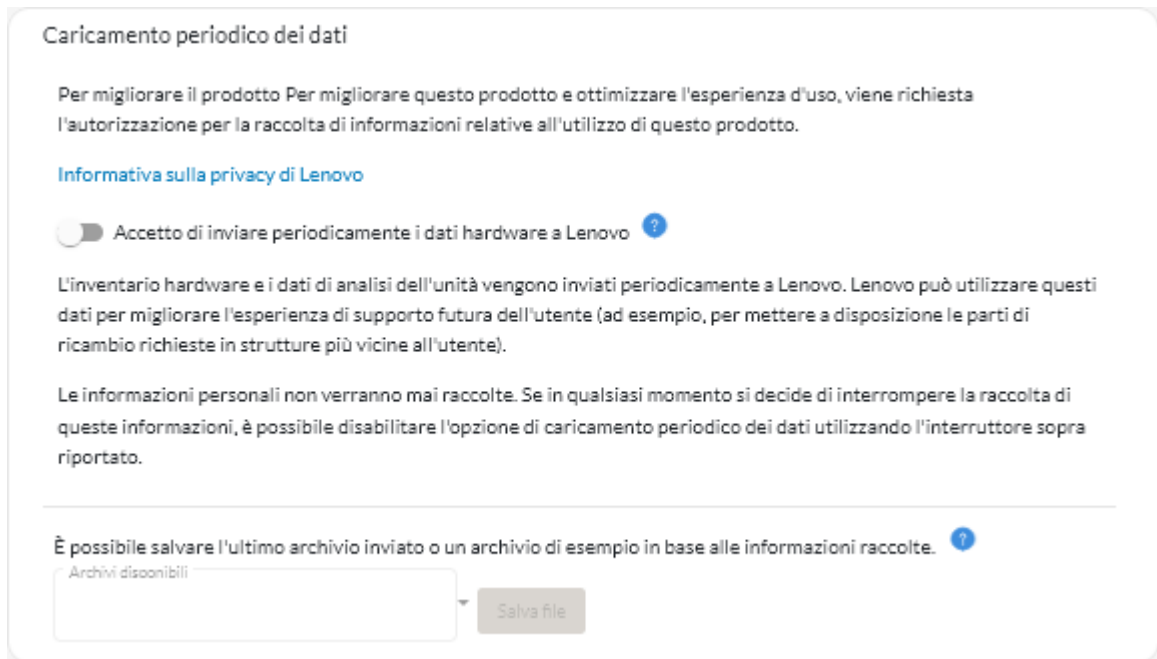
I dati vengono quindi spostati nel repository Lenovo Customer Care, dove vengono memorizzati per un massimo di 5 anni. Questo repository è una posizione sicura utilizzata anche quando i dati di debug vengono inviati a Lenovo per risolvere i problemi. Viene utilizzato dalla maggior parte dei prodotti server, storage e switch Lenovo.

Dal repository Lenovo Customer Care, le query vengono eseguite su tutti i dati forniti e i grafici vengono resi disponibili per l'analisi da parte del team del prodotto Lenovo.

Procedura

Completare le seguenti operazioni per consentire a XClarity Orchestrator di raccogliere e inviare i dati dei clienti a Lenovo.

Passo 1. Dalla barra dei menu di XClarity Orchestrator fare clic su **Amministrazione** (⚙️) → **Assistenza e supporto** e selezionare **Caricamento dati periodico** nel riquadro di navigazione sinistro per visualizzare la scheda Caricamento dati periodico.



Caricamento periodico dei dati

Per migliorare il prodotto Per migliorare questo prodotto e ottimizzare l'esperienza d'uso, viene richiesta l'autorizzazione per la raccolta di informazioni relative all'utilizzo di questo prodotto.

[Informativa sulla privacy di Lenovo](#)

Accetto di inviare periodicamente i dati hardware a Lenovo ⓘ

L'inventario hardware e i dati di analisi dell'unità vengono inviati periodicamente a Lenovo. Lenovo può utilizzare questi dati per migliorare l'esperienza di supporto futura dell'utente (ad esempio, per mettere a disposizione le parti di ricambio richieste in strutture più vicine all'utente).

Le informazioni personali non verranno mai raccolte. Se in qualsiasi momento si decide di interrompere la raccolta di queste informazioni, è possibile disabilitare l'opzione di caricamento periodico dei dati utilizzando l'interruttore sopra riportato.

È possibile salvare l'ultimo archivio inviato o un archivio di esempio in base alle informazioni raccolte. ⓘ

Archivi disonibili

Salva file

Passo 2. Facoltativamente accettare l'invio dei dati hardware a Lenovo.

Passo 3. Accettare l'[Informativa sulla privacy di Lenovo](#).

Al termine

Se si accetta di inviare i dati, da questa pagina è possibile eseguire le seguenti azioni.

- È possibile salvare gli ultimi archivi di dati giornalieri e settimanali inviati a Lenovo nel sistema locale selezionando l'archivio che si desidera scaricare e facendo quindi clic su **Salva file**.

Raccolta dei dati di servizio per XClarity Orchestrator

È possibile raccogliere manualmente i dati di servizio per Lenovo XClarity Orchestrator, quindi salvare le informazioni come archivio in formato tar.gz nel sistema locale. È possibile quindi inviare i file di servizio al fornitore di servizi preferito per ottenere assistenza nella risoluzione dei problemi in tempo reale.

Prima di iniziare

Ulteriori informazioni:  [Come raccogliere i dati di servizio](#)

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

Verificare che il browser Web non blocchi le finestre di dialogo a comparsa per il sito Web di XClarity Orchestrator quando si scaricano i dati del servizio

Procedura

Per raccogliere i dati di servizio per XClarity Orchestrator, effettuare le operazioni che seguono.

Passo 1. Sulla barra dei menu di XClarity Orchestrator fare clic su **Amministrazione** (🔑) → **Assistenza e supporto**, quindi su **Dati di servizio** nel riquadro di navigazione sinistro per visualizzare la scheda Dati del servizio di gestione.



Passo 2. Fare clic su **Salva con nome** per raccogliere dati di servizio e salvare l'archivio nel sistema locale.

Viene creato un processo per la raccolta dei dati di servizio. 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).

Al termine

È inoltre possibile eseguire le azioni correlate.

- Aprire manualmente un ticket di assistenza per un dispositivo specifico nella scheda Ticket di assistenza nella pagina di assistenza specifica del dispositivo facendo clic sull'icona **Apri ticket di assistenza** (🎫) (vedere [Apertura manuale di un ticket di assistenza nel centro di supporto Lenovo](#)).
- Allegare un archivio dei dati di servizio a un ticket di assistenza attivo selezionato dalla scheda Ticket di assistenza nella pagina di assistenza specifica del dispositivo facendo clic sull'icona **Allega file di servizio** (📎). È possibile allegare un file da XClarity Orchestrator dal sistema locale.

Nota:

- È possibile allegare un singolo file di archivio che non sia superiore a 2 GB. Il nome del file può avere una lunghezza massima di 200 caratteri. Per informazioni sulla creazione di archivi dei dati di servizio, vedere [Raccolta dei dati di servizio per dispositivi](#).
- Il ticket di assistenza deve essere in stato di apertura, avanzamento o di attesa. Non è possibile allegare un archivio a un ticket di assistenza che si trova in stato di chiusura o in uno stato di altro tipo.
- Non è possibile allegare un archivio a un ticket di assistenza *software* aperto per uno strumento di gestione delle risorse.
- Salvare uno o più archivi di dati di servizio selezionati nel sistema locale dalla scheda Dati del servizio di gestione facendo clic sull'icona **Salva** (↓). In caso di selezione multipla, i file vengono compressi in un unico file .tar.gz prima di essere scaricati.
- Eliminare uno o più archivi di dati di servizio selezionati che non sono più necessari dalla scheda Dati del servizio di gestione facendo clic sull'icona **Elimina** (🗑️) oppure eliminare tutti gli archivi facendo clic sull'icona **Elimina tutto** (⊖).

Raccolta dei dati di servizio per dispositivi

Se si verifica un problema con un dispositivo che richiede l'assistenza di un fornitore di servizi, come il centro di supporto Lenovo, per risolverlo, è possibile raccogliere manualmente i dati di servizio (inclusi informazioni sull'assistenza, inventario e log) per il dispositivo come file di archivio in formato tar.gz, al fine di identificare la causa del problema. È possibile salvare il file di archivio nel sistema locale, quindi inviare l'archivio al fornitore di servizi preferito.

Prima di iniziare

È necessario accettare l'[Informativa sulla privacy di Lenovo](#) prima di poter raccogliere i dati di servizio. È possibile accettare l'informativa sulla privacy facendo clic su **Amministrazione** (🔧) → **Assistenza e supporto** e selezionando **Configurazione Call Home** nel riquadro di navigazione sinistro e quindi facendo clic su **Accetto l'Informativa sulla privacy di Lenovo**.

Per informazioni sul salvataggio dei dati di servizio per XClarity Orchestrator nel sistema locale, vedere "[Raccolta dei dati di servizio per XClarity Orchestrator](#)" a pagina 202.

Per informazioni sull'apertura manuale di un ticket di assistenza e sull'invio di dati di servizio al centro di supporto Lenovo, vedere "[Apertura manuale di un ticket di assistenza nel centro di supporto Lenovo](#)" a pagina 212.

Per informazioni sulla configurazione della funzione Call Home per aprire automaticamente un ticket di assistenza nel centro di supporto Lenovo e inviare l'archivio dei dati di servizio quando si verifica un evento che richiede assistenza su un dispositivo, vedere "[Apertura automatica dei ticket di assistenza mediante Call Home](#)" a pagina 208.

Informazioni su questa attività

Quando si raccolgono i dati di servizio tramite Lenovo XClarity Orchestrator, il server Orchestrator invia la richiesta allo strumento di gestione delle risorse (ad esempio Lenovo XClarity Administrator). Lo strumento di gestione delle risorse raccoglie e salva i dati come file di archivio nel repository locale, quindi trasferisce il file di archivio in XClarity Orchestrator.

È possibile raccogliere i dati di inventario per un massimo di **50** dispositivi alla volta.

Procedura

Per raccogliere dati di servizio per un dispositivo specifico, effettuare le operazioni che seguono.

Passo 1. Sulla barra dei menu di XClarity Orchestrator fare clic su **Amministrazione** (🔧) → **Assistenza e supporto**, quindi su **Azioni dispositivo** nel riquadro di navigazione sinistro per visualizzare la scheda Azioni dispositivo.

- Aprire manualmente un ticket di assistenza per un dispositivo specifico nella scheda Ticket di assistenza nella pagina di assistenza specifica del dispositivo facendo clic sull'icona **Apri ticket di assistenza** (📄⊕) (vedere [Apertura manuale di un ticket di assistenza nel centro di supporto Lenovo](#)).
- Allegare un archivio dei dati di servizio a un ticket di assistenza attivo selezionato dalla scheda Ticket di assistenza nella pagina di assistenza specifica del dispositivo facendo clic sull'icona **Allega file di servizio** (📄⊕). È possibile allegare un file da XClarity Orchestrator dal sistema locale.

Nota:

- È possibile allegare un singolo file di archivio che non sia superiore a 2 GB. Il nome del file può avere una lunghezza massima di 200 caratteri. Per informazioni sulla creazione di archivi dei dati di servizio, vedere [Raccolta dei dati di servizio per dispositivi](#).
- Il ticket di assistenza deve essere in stato di apertura, avanzamento o di attesa. Non è possibile allegare un archivio a un ticket di assistenza che si trova in stato di chiusura o in uno stato di altro tipo.
- Non è possibile allegare un archivio a un ticket di assistenza *software* aperto per uno strumento di gestione delle risorse.
- Salvare uno o più archivi di dati di servizio selezionati nel sistema locale dalla scheda Dati di servizio facendo clic sull'icona **Salva** (↓). In caso di selezione multipla, i file vengono salvati come un unico file .tar.gz.

Nota: È possibile salvare un massimo di **50** archivi di dati di servizio nel sistema locale alla volta.

- Eliminare uno o più archivi di dati di servizio selezionati che non sono più necessari dalla scheda Dati di servizio facendo clic sull'icona **Elimina** (🗑️) oppure eliminare tutti gli archivi facendo clic sull'icona **Elimina tutto** (☹️).

Nota: Per eliminare tutti gli archivi è necessario essere membri del gruppo **SupervisorGroup**.

Importazione dei dati di servizio per i dispositivi

È possibile importare l'archivio dei dati di servizio per un dispositivo specifico. L'archivio può essere recuperato da uno strumento di gestione delle risorse di Lenovo XClarity Administrator o direttamente dal controller di gestione della scheda di base.

Informazioni su questa attività

È possibile importare fino a 10 file alla volta con un totale combinato di massimo 2 GB.

Se si importano più volte i dati di servizio per il dispositivo di salvataggio, i dati di inventario vengono sovrascritti dai dati di servizio importati per ultimi.

Procedura

Per importare un archivio dei dati di servizio, completare le seguenti operazioni.

- Passo 1. Sulla barra dei menu di XClarity Orchestrator fare clic su **Amministrazione** (⚙️) → **Assistenza e supporto**, quindi su **Dati di servizio** nel riquadro di navigazione sinistro per visualizzare la scheda Dati di servizio dispositivo.
- Passo 2. Fare clic sull'icona **Importa** (📄➡️) per importare gli archivi dei dati di servizio.
- Passo 3. Trascinare e rilasciare uno o più archivi dei dati di servizio (in formato .tar.gz, tzz o tgz) nella finestra di dialogo Importa oppure fare clic su **Sfoggia** per individuare l'archivio.
- Passo 4. Selezionare **Aggiungi il server nei dati del servizio all'inventario solo per la revisione** se l'archivio è per un dispositivo che attualmente non è gestito da XClarity Orchestrator

Passo 5. Fare clic su **Importa** per importare e analizzare l'archivio e gestire facoltativamente il dispositivo offline.

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).

Creazione e assegnazione di contatti per assistenza e supporto

Quando le risorse richiedono assistenza dal supporto Lenovo, Lenovo deve sapere chi contattare. È possibile definire le Informazioni sul contatto in un unico luogo e quindi assegnare tali contatti come contatti primari e secondari predefiniti per risorse specifiche.

Prima di iniziare

Assicurarsi che [Informativa sulla privacy di Lenovo](#) sia accettato. È possibile esaminare e accettare l'informativa sulla privacy dalla pagina **Amministrazione** → **Assistenza e supporto** → **Configurazione Call Home**.

Informazioni su questa attività

È possibile assegnare contatti primari e secondari ai gruppi di risorse. Quando si assegnano i contatti a un gruppo di risorse, i contatti vengono assegnati a tutte le risorse di tale gruppo.

L'assegnazione di contatti primari e secondari è facoltativa. Tuttavia, se si desidera assegnare un contatto secondario, è necessario assegnare anche un contatto primario.

Se un dispositivo è membro di più gruppi, è possibile che a ciascun gruppo sia assegnato un contatto primario differente. È possibile scegliere di utilizzare l'assegnazione del contatto principale per il primo gruppo o l'ultimo gruppo a cui è stato assegnato il dispositivo (vedere [Apertura manuale di un ticket di assistenza nel centro di supporto Lenovo](#)).

Se un dispositivo non è membro di un gruppo con un contatto primario assegnato, il contatto Call Home viene assegnato per impostazione predefinita. Il contatto Call Home viene utilizzato quando i ticket di assistenza vengono aperti automaticamente mediante Call Home (vedere [Apertura automatica dei ticket di assistenza mediante Call Home](#)). I contatti assegnati a risorse e gruppi hanno precedenza sul contatto Call Home predefinito.

Quando si apre manualmente un ticket di assistenza, è possibile scegliere di utilizzare i contatti assegnati alla risorsa del problema oppure un altro contatto (vedere [Apertura manuale di un ticket di assistenza nel centro di supporto Lenovo](#)).

Procedura

- **Definire un contatto**

1. Sulla barra dei menu di Lenovo XClarity Orchestrator fare clic su **Amministrazione** (⚙️) → **Assistenza e supporto**, quindi su **Informazioni sul contatto** nel riquadro di navigazione sinistro per visualizzare la scheda Informazioni sul contatto.
2. Fare clic sull'icona **Crea** (+) per visualizzare la finestra di dialogo Aggiungi contatto.
3. Compilare il nome del contatto, l'e-mail, il numero di telefono e la posizione.
4. Selezionare il metodo di contatto preferito.
5. Fare clic su **Salva** per creare il contatto.

- **Assegnare contatti ai gruppi di risorse**

1. Sulla barra dei menu di Lenovo XClarity Orchestrator fare clic su **Risorse** (🔊) → **Gruppi** per visualizzare la scheda Gruppi.
2. Selezionare il gruppo e fare clic sull'icona **Modifica** (✎) per visualizzare la finestra di dialogo Modifica gruppo.
3. Selezionare il gruppo di risorse.
4. Fare clic sulla scheda **Informazioni sul contatto**.
5. Selezionare il contatto del supporto primario e uno o più contatti del supporto secondario da assegnare a tutti i dispositivi del gruppo.
6. Fare clic su **Salva**.

Al termine

Nella scheda Informazioni sul contatto è possibile effettuare le operazioni che seguono.

- Modificare un contatto selezionato facendo clic sull'icona **Modifica** (✎).
- Eliminare un contatto selezionato facendo clic sull'icona **Rimuovi** (🗑).

Apertura automatica dei ticket di assistenza mediante Call Home

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

Prima di iniziare

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

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

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

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

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

Quando i contatti si trovano nei seguenti paesi, Call Home richiede un contratto Lenovo Premier Support. Per ulteriori informazioni, contattare un rappresentante Lenovo o un business partner autorizzato.

- Qatar
- Arabia Saudita
- Emirati Arabi Uniti

Informazioni su questa attività

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


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

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

Per informazioni sulla visualizzazione dei ticket di assistenza aperti automaticamente da Call Home, vedere .

Procedura

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

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

Configurazione Call Home

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

[Informativa sulla privacy di Lenovo](#)

Accetto l'informativa sulla privacy Lenovo

Dettagli cliente

Numero cliente

Contatto primario da utilizzare da più assegnazioni di gruppi ?

Assegnazione del primo gruppo

Assegnazione dell'ultimo gruppo

Contatto predefinito

Stato Call Home: Abilitato Disabilitato

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

Posizione del sistema ?

Applica Reimposta configurazione Test della connessione Call Home

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

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

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

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

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

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

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

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

Passo 7. Compilare le informazioni sulla posizione.

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

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

Al termine

È possibile effettuare le operazioni che seguono, che sono correlate ai dati di servizio.

- Ripristinare i valori predefiniti di Call Home facendo clic su **Reimposta configurazione**.
- Visualizzare le informazioni su *tutti* i ticket di assistenza inviati al centro di assistenza Lenovo, automaticamente o manualmente, mediante Call Home facendo clic su **Ticket di assistenza** nel riquadro di navigazione sinistro. Per ulteriori informazioni, vedere [Visualizzazione di ticket di assistenza e stato](#).
- Raccogliere i dati di servizio per un dispositivo selezionato dalla scheda Azioni dispositivo facendo clic sull'icona **Raccogli dati di servizio** (📄). Per ulteriori informazioni, vedere [Raccolta dei dati di servizio per dispositivi](#).
- Allegare un archivio dei dati di servizio a un ticket di assistenza attivo selezionato dalla scheda Ticket di assistenza nella pagina di assistenza specifica del dispositivo facendo clic sull'icona **Allega file di servizio** (📎). È possibile allegare un file da XClarity Orchestrator dal sistema locale.

Nota:

- È possibile allegare un singolo file di archivio che non sia superiore a 2 GB. Il nome del file può avere una lunghezza massima di 200 caratteri. Per informazioni sulla creazione di archivi dei dati di servizio, vedere [Raccolta dei dati di servizio per dispositivi](#).
- Il ticket di assistenza deve essere in stato di apertura, avanzamento o di attesa. Non è possibile allegare un archivio a un ticket di assistenza che si trova in stato di chiusura o in uno stato di altro tipo.
- Non è possibile allegare un archivio a un ticket di assistenza *software* aperto per uno strumento di gestione delle risorse.
- Aprire manualmente un ticket di assistenza nel centro di supporto Lenovo, raccogliere i dati di servizio per un dispositivo specifico e inviare tali file al centro di supporto Lenovo dalla scheda Azioni dispositivo, selezionando il dispositivo, quindi facendo clic sull'icona **Apri ticket di assistenza** (📄). Per ulteriori informazioni, vedere [Apertura manuale di un ticket di assistenza nel centro di supporto Lenovo](#). Se il centro di supporto Lenovo richiede dati aggiuntivi, potrebbe richiedere di raccogliere nuovamente i dati di servizio per il dispositivo specifico o un altro.

Apertura manuale di un ticket di assistenza nel centro di supporto Lenovo

Se la funzione Call Home è abilitata mediante un server d'inoltro di servizio e si verifica un evento che richiede assistenza su un dispositivo gestito, Lenovo XClarity Orchestrator apre automaticamente un ticket di assistenza, raccoglie i file di servizio per il dispositivo gestito e invia i file al centro di supporto Lenovo. È inoltre possibile raccogliere manualmente in un archivio i file di servizio per un dispositivo gestito, salvare l'archivio nel sistema locale e inviare i file al centro di supporto Lenovo in qualsiasi momento. L'apertura di un ticket di assistenza avvia il processo di determinazione di una soluzione dei problemi hardware, mettendo a disposizione del supporto Lenovo le informazioni pertinenti in modo rapido ed efficiente. Una volta completato e aperto un ticket di assistenza, i tecnici dell'assistenza Lenovo potranno iniziare a lavorare alla risoluzione del problema.

Prima di iniziare

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

- Accertarsi che le informazioni di contatto di call Home siano configurate e abilitate ([Apertura automatica dei ticket di assistenza mediante Call Home](#)).
- Accertarsi che XClarity Orchestrator sia in grado di comunicare con il centro di supporto Lenovo facendo clic su **Amministrazione** (🔑) → **Assistenza e supporto** dalla barra dei menu XClarity Orchestrator e facendo clic su **Configurazione Call Home** nel riquadro di navigazione sinistro per visualizzare la pagina Configurazione Call Home. Fare quindi clic su **Test di configurazione Call Home** per generare un evento di test e verificare che XClarity Orchestrator possa comunicare con il centro di supporto Lenovo.
- Accertarsi che tutte le porte richieste da XClarity Orchestrator (incluse le porte richieste per Call Home) siano disponibili prima di abilitare la funzione Call Home. Per ulteriori informazioni sulle porte, vedere [Disponibilità della porta](#) nella documentazione online di XClarity Orchestrator.
- Accertarsi che sia stata stabilita una connessione agli indirizzi Internet richiesti da Call Home. Per informazioni sui firewall, vedere [Firewall e server proxy](#) nella documentazione online di XClarity Orchestrator.
- Se XClarity Orchestrator accede a Internet con un proxy HTTP, accertarsi che il server proxy sia configurato per l'utilizzo dell'autenticazione di base e come proxy non ricevitore. Per ulteriori informazioni sulla configurazione del proxy, vedere [Configurazione delle impostazioni di rete](#).

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

Informazioni su questa attività

Quando si apre manualmente un ticket di assistenza, è possibile scegliere di utilizzare i contatti assegnati alla risorsa del problema oppure un altro contatto.



Quando i contatti primario e secondario vengono assegnati a un gruppo, questi contatti vengono assegnati a ciascun dispositivo di tale gruppo. A ciascun dispositivo può essere assegnato un contatto primario e uno o più contatti secondari. Se un dispositivo è membro di più gruppi, tutti i contatti secondari assegnati a tutti i gruppi di cui il dispositivo è membro vengono assegnati al dispositivo. Se un dispositivo è membro di più gruppi, è possibile che a ciascun gruppo sia assegnato un contatto primario differente. È possibile scegliere

di utilizzare l'assegnazione del contatto principale per il primo gruppo o l'ultimo gruppo a cui è stato assegnato il dispositivo (vedere [Apertura automatica dei ticket di assistenza mediante Call Home](#)).

Se un dispositivo non è membro di un gruppo con un contatto primario assegnato, il contatto Call Home viene assegnato per impostazione predefinita. Il contatto Call Home viene utilizzato quando i ticket di assistenza vengono aperti automaticamente mediante Call Home (vedere [Apertura automatica dei ticket di assistenza mediante Call Home](#)). I contatti assegnati a risorse e gruppi hanno precedenza sul contatto Call Home predefinito.


Procedura

Per aprire manualmente un ticket di assistenza, completare le seguenti operazioni.

- Se la funzione Call Home è configurata e abilitata, effettuare i passaggi riportati di seguito per aprire un ticket di assistenza, raccogliere i dati di servizio e inviare i file al centro di supporto Lenovo.
 1. Sulla barra dei menu di XClarity Orchestrator fare clic su **Risorse** , quindi sul tipo di dispositivo per visualizzare una scheda con una vista tabulare di tutti i dispositivi gestiti simili.
 2. Fare clic sulla riga relativa al dispositivo per visualizzare le schede di riepilogo per quel dispositivo.
 3. Fare clic su **Servizio** nel riquadro di navigazione sinistro per visualizzare la scheda Ticket di assistenza.
 4. Fare clic sull'icona **Apri ticket di assistenza**  per visualizzare la finestra di dialogo Aggiungi nuovo ticket.
 5. Fornire una descrizione del problema che si desidera segnalare, includendo i codici degli eventi rilevanti.
 6. Facoltativamente, scegliere la gravità del problema. È possibile selezionare uno dei seguenti valori.
 - **Urgente**
 - **Alta**
 - **Media** (impostazione predefinita)
 - **Bassa**
 7. Fare clic su **Invia**.
- Quando la funzione Call Home è configurata e abilitata e si verifica un evento che richiede assistenza su un dispositivo specifico, XClarity Orchestrator apre *automaticamente* un ticket di assistenza e trasferisce i dati di servizio relativi a quel dispositivo al centro di assistenza Lenovo.

Al termine

Nella pagina di assistenza specifica del dispositivo è possibile effettuare le operazioni che seguono.

- Visualizzare le informazioni su *tutti* i ticket di assistenza aperti facendo clic su **Assistenza e supporto** → **Ticket di assistenza** dalla barra dei menu di XClarity Orchestrator.
- Aggiungere una nota a un ticket di assistenza selezionato facendo clic sull'icona **Aggiungi nota al ticket di assistenza** .

Nota:

- Il ticket di assistenza deve essere in stato di apertura, avanzamento o di attesa. Non è possibile aggiungere una nota a un ticket di assistenza che si trova in stato di chiusura o in uno stato di altro tipo.
- È possibile aggiungere una nota solo ai ticket di assistenza Lenovo. Non è possibile aggiungere una nota ai ticket di assistenza IBM, Service Now o Cherwill.
- Non è possibile aggiungere una nota a un ticket di assistenza *software* aperto per uno strumento di gestione delle risorse.

- Allegare un archivio dei dati di servizio a un ticket di assistenza attivo selezionato dalla scheda Ticket di assistenza nella pagina di assistenza specifica del dispositivo facendo clic sull'icona **Allega file di servizio** (+). È possibile allegare un file da XClarity Orchestrator dal sistema locale.

Nota:

- È possibile allegare un singolo file di archivio che non sia superiore a 2 GB. Il nome del file può avere una lunghezza massima di 200 caratteri. Per informazioni sulla creazione di archivi dei dati di servizio, vedere [Raccolta dei dati di servizio per dispositivi](#).
- Il ticket di assistenza deve essere in stato di apertura, avanzamento o di attesa. Non è possibile allegare un archivio a un ticket di assistenza che si trova in stato di chiusura o in uno stato di altro tipo.
- Non è possibile allegare un archivio a un ticket di assistenza *software* aperto per uno strumento di gestione delle risorse.

Visualizzazione di ticket di assistenza e stato

È possibile visualizzare le informazioni sui ticket di assistenza creati manualmente o inviati automaticamente al centro di supporto Lenovo mediante Call Home e i ticket di assistenza generati da servizi di supporto diversi da Call Home.

Informazioni su questa attività

Lo stato dei ticket di assistenza viene sincronizzato con il centro di supporto Lenovo ogni 24 ore.

La colonna **Stato** identifica lo stato dei ticket di assistenza. Un ticket di assistenza può trovarsi in uno dei seguenti stati.

- **Attivo**
- **Risposto**
- **Annullato**
- **Annullati**
- **Creato**
- **Annullato dal cliente**
- **Chiuso**
- **Parte negata**
- **Duplica**
- **Errore**
- **Stato di errore**
- **In corso**
- **Inizializzato**
- **Unito**
- **Monitoraggio - soluzione distribuita**
- **Crea nuovo**
- **In attesa**
- **In sospeso**
- **Inizializzazione del problema.**
- **Problema risolto**
- **Elaborazione**
- **Rifiutato**
- **Ricerca in corso**
- **Risolto**
- **Soluzione fornita**
- **Inviato**
- **Sconosciuto**
- **In attesa**

- In attesa di dettagli
- In attesa di supporto interno Lenovo.
- In attesa della parte di supporto esterna
- In attesa del feedback del cliente sulla soluzione
- In attesa della distribuzione della soluzione
- Trasferito ai servizi gestiti
- Trasferimento a caldo
- Operazione in corso

La colonna **Tipo** identifica il tipo di ticket di assistenza elencato nella colonna Numero ticket di assistenza. Il tipo di ticket di assistenza può essere uno dei valori indicati di seguito.

- Ticket Cherwill
- Ticket Call Home di IBM
- Ticket Call Home Lenovo
- Ticket del pass-through di Lenovo Call Home
- Ticket Call Home del software di Lenovo
- ServiceNow

Procedura

- **Visualizzare lo stato di tutti i ticket di assistenza** Fare clic su **Amministrazione** (⚙️) → **Assistenza e supporto**, quindi su **Ticket di assistenza** nel riquadro di navigazione sinistro per visualizzare la scheda Ticket di assistenza.

Suggerimento: fare clic sull'ID evento per visualizzare un riepilogo dell'evento che ha generato il ticket di assistenza, incluso l'eventuale intervento dell'utente.






<input type="checkbox"/>	Numero tick	Stato	ID evento	Descrizione	Nome prod	Numero di s	Data creazi
<input type="checkbox"/>	100103...	In ese...	FQXXOSSl	test_ticket	Abyss-S...	ABYSSR...	11/09/2...
<input type="checkbox"/>	100103...	In ese...	806F010C	Uncorre...	Abyss-S...	ABYSSR...	11/09/2...

0 selezionato / 2 Totale Righe per pagina: 15

- **Visualizzare lo stato dei ticket di servizio per un dispositivo specifico**
 1. Sulla barra dei menu di XClarity Orchestrator fare clic su **Risorse** (📁), quindi sul tipo di dispositivo per visualizzare una scheda con una vista tabulare di tutti i dispositivi gestiti simili.
 2. Fare clic sulla riga relativa al dispositivo per visualizzare le schede di riepilogo per quel dispositivo.
 3. Fare clic su **Servizio** nel riquadro di navigazione sinistro per visualizzare la scheda Ticket di assistenza con un elenco di ticket di assistenza per il dispositivo.

Suggerimento: fare clic sull'ID evento per visualizzare un riepilogo dell'evento che ha generato il ticket di assistenza, incluso l'eventuale intervento dell'utente.

Ticket di assistenza









Tutte le azioni ▾ Filtri ▾ Cerca X

<input type="checkbox"/>	Numero ticket d	Stato :	ID evento :	Descrizione :	Numero di serie	Data creazione :
<input type="checkbox"/>	1001032647	In ese...	FQXXOSS00	test_ticket	ABYSSR093	11/09/23, ...
<input type="checkbox"/>	1001032643	In ese...	806F010C2C	Uncorrecta...	ABYSSR093	11/09/23, ...


0 selezionato / 2 Totale Righe per pagina: 15 ▾

Al termine


È possibile effettuare le operazioni che seguono, che sono correlate ai ticket di assistenza.

- Configurare XClarity Orchestrator per aprire automaticamente un ticket di assistenza quando si verifica un evento che richiede assistenza (vedere "[Apertura automatica dei ticket di assistenza mediante Call Home](#)" a pagina 208).
- Sincronizzare i dati con il centro di assistenza Lenovo e aggiornare lo stato di tutti i ticket di servizio attivi facendo clic sull'icona **Aggiorna stato ticket di assistenza** .
- Aprire manualmente un ticket di assistenza per un dispositivo specifico dalla scheda Ticket di assistenza nella pagina di assistenza specifica del dispositivo facendo clic sull'icona **Apri ticket di assistenza** .
- Aggiungere una nota a un ticket di assistenza selezionato facendo clic sull'icona **Aggiungi nota al ticket di assistenza** .

Nota:

- Il ticket di assistenza deve essere in stato di apertura, avanzamento o di attesa. Non è possibile aggiungere una nota a un ticket di assistenza che si trova in stato di chiusura o in uno stato di altro tipo.
- È possibile aggiungere una nota solo ai ticket di assistenza Lenovo. Non è possibile aggiungere una nota ai ticket di assistenza IBM, Service Now o Cherwill.
- Non è possibile aggiungere una nota a un ticket di assistenza *software* aperto per uno strumento di gestione delle risorse.
- Allegare un archivio dei dati di servizio a un ticket di assistenza attivo selezionato dalla scheda Ticket di assistenza nella pagina di assistenza specifica del dispositivo facendo clic sull'icona **Allega file di servizio** . È possibile allegare un file da XClarity Orchestrator dal sistema locale.

Nota:

- È possibile allegare un singolo file di archivio che non sia superiore a 2 GB. Il nome del file può avere una lunghezza massima di 200 caratteri. Per informazioni sulla creazione di archivi dei dati di servizio, vedere [Raccolta dei dati di servizio per dispositivi](#).
- Il ticket di assistenza deve essere in stato di apertura, avanzamento o di attesa. Non è possibile allegare un archivio a un ticket di assistenza che si trova in stato di chiusura o in uno stato di altro tipo.
- Non è possibile allegare un archivio a un ticket di assistenza *software* aperto per uno strumento di gestione delle risorse.
- Inoltrare report sui ticket di assistenza attivi periodicamente a uno o più indirizzi e-mail facendo clic sull'icona **Crea server d'inoltro dei report** . Il report viene inviato utilizzando i filtri dati attualmente applicati alla tabella. Tutte le colonne della tabella visibili e nascoste sono incluse nel report. Per ulteriori informazioni, vedere .

- Aggiungere un report sui ticket di assistenza attivi a un server d'inoltro dei report specifico utilizzando i filtri dati attualmente applicati alla tabella facendo clic sull'icona **Aggiungi al server d'inoltro dei report** (↗). Se il server d'inoltro dei report include già un report sui ticket di assistenza attivi, il report viene aggiornato per utilizzare i filtri dati correnti.

Visualizzazione delle informazioni sulla garanzia

È possibile determinare lo stato di garanzia (incluse le garanzie estese) dei dispositivi gestiti.

Prima di iniziare

Lenovo XClarity Orchestrator deve disporre dell'accesso ai seguenti URL per raccogliere le informazioni di garanzia per i dispositivi gestiti. Verificare che l'accesso a questi URL non sia bloccato da firewall. Per ulteriori informazioni, vedere [Firewall e server proxy](#) nella documentazione online di XClarity Orchestrator.

- Database Lenovo Warranty (tutti i paesi) - <https://ibase.lenovo.com/POIRequest.aspx>
- Servizio Web Lenovo Warranty - <http://supportapi.lenovo.com/warranty/> o <https://supportapi.lenovo.com/warranty/>

Nota:

- Il supporto in garanzia non è attualmente previsto per gli utenti in Cina.
- Le garanzie sono elencate per lo chassis ma non per i corrispondenti Chassis Management Module (CMM).

Informazioni su questa attività

Le informazioni sulla garanzia vengono recuperate settimanalmente per i dispositivi che dispongono di garanzie e quotidianamente per i dispositivi che non sono in garanzia.

Procedura

Per visualizzare informazioni sulla garanzia, fare clic su **Amministrazione** (⚙️) → **Assistenza e supporto**, quindi su **Garanzia** nel riquadro di navigazione sinistro per visualizzare la scheda Garanzia.

Garanzia								
Tutte le azioni				Cerca				
Dispositivo	Stato	Nome prod	Tipo/model	Numero gar	Numero di	Data di iniz	Data di sca	Gruppi
*node02_	Non di...	IBM Flex	7916/...	Non disp	SLOT002	Non disp	Non disp	Non disp
*node02_	Non di...	IBM Flex	7916/...	Non disp	SLOT002	Non disp	Non disp	Non disp
*node03_	Non di...	IBM Flex	7916/...	Non disp	SLOT003	Non disp	Non disp	Non disp
*node03_	Non di...	IBM Flex	7916/...	Non disp	SLOT003	Non disp	Non disp	Non disp
*node06_	Non di...	IBM Flex	7916/...	Non disp	SLOT006	Non disp	Non disp	Non disp
*node06_	Non di...	IBM Flex	7916/...	Non disp	SLOT006	Non disp	Non disp	Non disp
*node09_	Non di...	IBM Flex	7916/...	Non disp	SLOT009	Non disp	Non disp	Non disp
*node09_	Non di...	IBM Flex	7916/...	Non disp	SLOT009	Non disp	Non disp	Non disp
*node11_	Non di...	IBM Flex	7916/...	Non disp	SLOT011	Non disp	Non disp	Non disp
*node11_	Non di...	IBM Flex	7916/...	Non disp	SLOT011	Non disp	Non disp	Non disp
10.243.1	Non di...	Lenovo F	9532/...	Non disp	06DGCV	Non disp	Non disp	Non disp
10.243.1	Non di...	IBM Flex	8731/...	Non disp	23LAR6E	Non disp	Non disp	Non disp
10.243.1	Non di...	IBM Flex	7916/...	Non disp	CAR206:	Non disp	Non disp	Non disp
10.243.1	Non di...	IBM Flex	7917/...	Non disp	06EKZB:	Non disp	Non disp	Non disp
10.243.2	Non di...	IBM Flex	8737/...	Non disp	06PGVA:	Non disp	Non disp	Non disp

211 Totale Righe per pagina: 15

1 2 3 4 5

Al termine

È possibile completare le seguenti azioni nella scheda Garanzia.

- Configurare quando si desidera ricevere una notifica sulle scadenze della garanzia per i dispositivi gestiti facendo clic sull'icona **Configura impostazioni garanzia** (⚙️). È possibile configurare le seguenti impostazioni.
 - Abilitare la generazione di avvisi alla scadenza della garanzia del dispositivo.
 - Impostare il numero di giorni prima della scadenza delle garanzie per cui si desidera generare un avviso.
- Consultare le informazioni sulla garanzia (se disponibili) per un dispositivo specifico sul sito Web del supporto Lenovo facendo clic sul collegamento nella colonna **Stato**.
- Inoltrare report sulle garanzie periodicamente a uno o più indirizzi e-mail facendo clic su **Tutte le azioni** → **+** **Aggiungi server d'inoltro dei report**. Il report viene inviato utilizzando i filtri dati attualmente applicati alla tabella. Tutte le colonne della tabella visibili e nascoste sono incluse nel report.
- Aggiungere un report sulle garanzie a un server d'inoltro dei report specifico utilizzando i filtri dati attualmente applicati alla tabella facendo clic sull'icona **Aggiungi al server d'inoltro dei report** (➡️). Se il

server d'oltro dei report include già un report sulle garanzie, il report viene aggiornato per utilizzare i filtri dati correnti.

Lenovo