Lenovo

XClarity Controller 3
Guida per l'utente

Nota: Prima di utilizzare queste informazioni, consultare le informazioni generali in Appendice B "Informazioni particolari" a pagina 183.

Prima edizione (Ottobre 2024)

Contenuto

Capitolo 1. Introduzione

Lenovo XClarity Controller 3 (XCC3) è il controller di gestione di nuova generazione per i server Lenovo ThinkSystem.

Il controller consolida le funzionalità del processore di servizio, il Super I/O, il controller video e le funzioni di presenza remota in un unico chip sulla scheda di sistema del server. Fornisce, ad esempio, le seguenti funzionalità:

- Scelta di una connessione Ethernet condivisa o dedicata per la gestione dei sistemi
- Supporto per HTML5
- Supporto per l'accesso tramite XClarity Mobile
- XClarity Provisioning Manager
- Configurazione remota tramite XClarity Essentials o la CLI di XClarity Controller.
- Funzionalità di accesso locale o remoto a XClarity Controller per applicazioni e strumenti
- Funzioni avanzate di presenza remota.
- Supporto dell'API REST (schema Redfish) per le applicazioni software e i servizi aggiuntivi relativi al Web.

Nota:

- XClarity Controller attualmente supporta le specifiche 1.16.0 dell'API Redfish Scalable Platforms Management e lo schema 2022.2
- Nell'interfaccia Web di XClarity Controller, BMC viene utilizzato in riferimento a XCC.
- È possibile che una porta di rete per la gestione dei sistemi dedicata non sia disponibile su alcuni server ThinkSystem; questi server possono accedere a XClarity Controller solo tramite una porta di rete condivisa con il sistema operativo del server.

In questo documento viene descritto come utilizzare le funzioni di XClarity Controller su un server ThinkSystem. XClarity Controller si integra con XClarity Provisioning Manager e UEFI per fornire la funzione di gestione dei sistemi per i server ThinkSystem.

Per controllare la presenza di aggiornamenti firmware, effettuare le operazioni riportate di seguito.

Nota: La prima volta che si accede a Support Portal, è necessario scegliere la categoria del prodotto, la famiglia del prodotto e i numeri di modello per il server. La volta successiva che si accede a Support Portal, i prodotti selezionati vengono inizialmente precaricati dal sito Web e sono visualizzati solo i collegamenti per i propri prodotti. Per modificare o aggiungere un prodotto al proprio elenco di prodotti, fare clic sul collegamento **Gestisci elenchi prodotti**. Vengono effettuate periodicamente delle modifiche sul sito Web. Le procedure per individuare il firmware e la documentazione possono variare leggermente da quanto descritto in questo documento.

1. Accedere a http://datacentersupport.lenovo.com.
2. In **Support (Supporto)** selezionare **Data Center**.
3. Una volta caricato il contenuto, selezionare **Servers (Server)**.
4. In **Select Series (Scegli una serie)** selezionare innanzitutto la serie hardware specifica del server, quindi in **Select SubSeries (Seleziona sottoserie)** selezionare le sottoserie specifiche del prodotto server e infine in **Select Machine Type (Scegli il tipo di macchina)** selezionare il tipo specifico di macchina.

Funzioni dei livelli Standard e Premier di XClarity Controller

XClarity Controller include funzionalità di livello Standard e Premier. Fare riferimento alla documentazione relativa al proprio server per ulteriori informazioni sul livello di XClarity Controller installato sul proprio server. Tutti i livelli forniscono:

- Accesso remoto e gestione del server 24 ore al giorno, 7 giorni su 7
- Gestione remota indipendente dallo stato del server gestito
- Controllo remoto di hardware e sistemi operativi

Funzioni del livello Standard di XClarity Controller

Di seguito è riportato un elenco delle funzioni di livello Standard di XClarity Controller:

Interfacce di gestione standard del settore

- Interfaccia IPMI 2.0
- Redfish
- DCMI 1.5
- SNMPv3

Altre interfacce di gestione

- Web
- SSH CLI
- Pannello anteriore USB - Pannello dell'operatore virtuale tramite dispositivo mobile

Controllo accensione/reimpostazione del server

- Accensione
- Arresto forzato/normale
- Controllo dell'alimentazione pianificato
- Reimpostazione sistema
- Controllo dell'ordine di avvio

Log eventi

- IPMI SEL
- Log leggibile dall'operatore
- Log di controllo
- Mini-log

Monitoraggio ambientale

- Monitoraggio agentless
- Monitoraggio dei sensori
- Controllo delle ventole
- Controllo LED
- Errori di chipset (Caterr, IERR e così via)
- Indicazione delle condizioni del sistema

- Monitoraggio delle prestazioni di OOB per adattatori I/O
- Visualizzazione ed esportazione dell'inventario

RAS

- NMI virtuale
- Ripristino automatico del firmware
- Promozione automatica del firmware di backup
- Watchdog POST
- Watchdog del programma di caricamento del sistema operativo
- Watchdog sistema operativo
- Cattura della schermata blu (guasto del sistema operativo, in FFDC)
- Strumenti di diagnostica incorporati
- Call Home

Configurazione di rete

- IPv4
- IPv6
- Indirizzo IP, maschera di sottorete, gateway
- Modalità di assegnazione degli indirizzi IP
- Nome host
- Indirizzo MAC programmabile
- Doppia selezione MAC (se supportata dall'hardware del server)
- Riassegnazioni delle porte di rete
- Etichettatura VLAN

Protocolli di rete

- DHCP
- DNS
- DDNS
- HTTP/HTTPS
- SNMPv3
- SSL
- SSH
- SMTP
- Client LDAP
- NTP
- SSDP
- LLDP

Avvisi

- Trap PET
- Trap SNMP v1, v2c e v3

- E-mail
- Sottoscrizioni di notifiche Redfish

Presenza remota

- Disco remoto su scheda (RDOC)

Reindirizzamento seriale

- SOL IPMI
- Configurazione della porta seriale che include autorizzazione e velocità
- Buffer della console seriale (120 s)

Protezione

- CRTM processore non host
- Aggiornamenti firmware con firma digitale
- Role Based Access Control (RBAC)
- Account utente locale
- Account utente LDAP/AD
- Rollback sicuro del firmware
- NIST SP 800-131a
- Rilevamento intrusione dello chassis (se supportato dall'hardware del server)
- Solo protocolli sicuri e crittografati abilitati
- Registrazione di controllo delle modifiche della configurazione e delle azioni del server
- Autenticazione chiave pubblica
- Ritiro/reimpiego del sistema (RTD/ERTD)
- Supporto PFR
- FIPS 140-3
- Modalità di sicurezza e dashboard di sicurezza
- Archiviazione sicura delle password

Gestione dell'alimentazione

- Misuratore di alimentazione in tempo reale

Features on Demand

- Repository delle chiavi di attivazione

Distribuzione e configurazione

- Configurazione remota
- Pass-through del sistema operativo
- Distribuzione incorporata, strumenti di configurazione e pacchetti di driver
- Backup e ripristino della configurazione
- Dimensioni RDOC estese (con scheda MicroSD)
- Profili termici configurabili

Aggiornamenti firmware

- Aggiornamento agentless
- Aggiornamento remoto

Funzioni del livello Premier di XClarity Controller

Di seguito è riportato un elenco delle funzioni del livello Premier di XClarity Controller:

Tutte le "Funzioni del livello Standard di XClarity Controller" a pagina 2.

Log eventi

- Log di sostituzione dei componenti

RAS

- Acquisizione di avvio
- Acquisizione dei video sull'arresto anomalo

Avvisi

- Syslog

Presenza remota

- KVM remoto
- Montaggio dei file ISO/IMG client locali
- Controllo di qualità/larghezza di banda
- Montaggio di supporti virtuali di file http, Samba, NFS e ISO/IMG remoti

Reindirizzamento seriale

- Reindirizzamento seriale tramite SSH-CLI

Protezione

- Single Sign-On
- Security Key Lifecycle Manager (SKLM/KMIP)
- Blocco degli indirizzi IP
- Modalità di sicurezza rigorosa aziendale (conforme allo standard CNSA)
- Controllo del sistema

Gestione dell'alimentazione

- Limite alimentazione
- Monitoraggio delle prestazioni di OOB - Metriche delle prestazioni del sistema
- Grafico dell'alimentazione in tempo reale
- Grafici della temperatura

Distribuzione e configurazione

- Distribuzione del sistema operativo da remoto

Aggiornamenti firmware

- Sincronizzazione con il repository

- Aggiornamento del bundle firmware del System Pack
- Rollback del firmware dal repository locale nella scheda MicroSD

Aggiornamento di XClarity Controller

Se il server è dotato del livello Standard delle funzionalità del firmware di XClarity Controller, potrebbe essere necessario aggiornare le funzionalità di XClarity Controller sul server. Per ulteriori informazioni sui livelli di aggiornamento disponibili e su come ordinarli, fare riferimento a Capitolo 9 "Gestione licenza" a pagina 87.

Requisiti del browser Web e del sistema operativo

Utilizzare le informazioni in questo argomento per visualizzare l'elenco dei browser supportati, delle suite di crittografia e dei sistemi operativi per il server.

L'interfaccia Web di XClarity Controller richiede uno dei seguenti browser Web:

- Chrome 64.0 o versioni successive (64.0 o versioni successive per la console remota)
- Firefox ESR 78.0 o versione successiva
- Microsoft Edge 79.0 o versione successiva
- Safari 12.0 o versione superiore (iOS 7 o successiva e OS X)

Nota: Il supporto per la funzione di console remota non è disponibile tramite il browser sui sistemi operativi per dispositivi mobili.

I browser sopra elencati sono quelli attualmente supportati dal firmware di XClarity Controller. Il firmware di XClarity Controller viene migliorato periodicamente per includere il supporto di altri browser.

In base alla versione del firmware di XClarity Controller, il supporto del browser Web può differire da quello riportato in questa sezione. Per consultare l'elenco dei browser supportati dal firmware attuale di XClarity Controller, fare clic sull'elenco del menu **Browser supportati** dalla pagina di login di XClarity Controller.

Per una maggiore sicurezza, sono attualmente supportate soltanto cifrature avanzate in caso di utilizzo di HTTPS. Quando si utilizza HTTPS, la combinazione di browser e sistema operativo client deve supportare una delle seguenti suite di cifratura:

- TLS_AES_256_GCM_SHA384
- TLS_CHACHA20_POLY1305_SHA256
- TLS_AES_128_GCM_SHA256
- TLS_AES_128_CCM_8_SHA256
- TLS_AES_128_CCM_SHA256
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_DHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305
- TLS_DHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384

- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
- TLS_DHE_RSA_WITH_AES_256_CBC_SHA256
- TLS_DHE_RSA_WITH_AES_128_CBC_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384
- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256

Nota: Il browser Internet memorizza nella cache le informazioni relative alle pagine Web visitate, in modo da caricarle più rapidamente in futuro. Dopo un aggiornamento flash del firmware di XClarity Controller, il browser può continuare a utilizzare le informazioni nella cache invece di recuperarle da XClarity Controller. Una volta aggiornato il firmware di XClarity Controller, si consiglia di cancellare la cache del browser per accertarsi che le pagine Web gestite da XClarity Controller vengano visualizzate correttamente.

Supporto multilingua

Utilizzare le informazioni in questo argomento per visualizzare l'elenco delle lingue supportate da XClarity Controller.

Per impostazione predefinita, la lingua scelta per l'interfaccia Web di XClarity Controller è l'inglese. L'interfaccia è in grado di visualizzare più lingue. Alcune delle lingue supportate sono:

- Francese
- Tedesco
- Italiano
- Giapponese
- Coreano
- Portoghese (Brasile)
- Russo
- Cinese semplificato
- Spagnolo (internazionale)
- Cinese tradizionale

Per scegliere la lingua preferita, fare clic sulla freccia accanto alla lingua attualmente selezionata. Verrà visualizzato un menu a discesa che consente di scegliere la lingua preferita.

Le stringhe di testo generate dal firmware di XClarity Controller vengono visualizzate nella lingua indicata dal browser. Se nel browser è specificata una lingua diversa da una di quelle supportate elencate sopra, il testo viene visualizzato in inglese. Inoltre, eventuali stringhe di testo visualizzate dal firmware di XClarity Controller, ma non generate da XClarity Controller (ad esempio messaggi generati da adattatori PCIe, UEFI e così via), vengono visualizzate in inglese.

L'immissione di testo specifico di una lingua diversa dall'inglese, ad esempio un **Messaggio di sconfinamento** non è attualmente supportata. È supportato solo testo digitato in inglese.

Introduzione agli oggetti MIB

Utilizzare le informazioni in questo argomento per accedere agli oggetti MIB.

I MIB SNMP possono essere scaricati dall'indirizzo https://support.lenovo.com/ (ricerca per tipo di macchina sul portale). Sono inclusi i seguenti quattro MIB:

- **MIB SMI** descrive la struttura delle informazioni di gestione per il Lenovo Data Center Group.

- **MIB del prodotto** descrive l'identificatore di oggetto per i prodotti Lenovo.
- **MIB XCC** fornisce le informazioni sull'inventario e il monitoraggio per Lenovo XClarity Controller.
- **MIB degli avvisi XCC** definisce i trap per le condizioni di avviso rilevate da Lenovo XClarity Controller.

Nota: L'ordine di importazione per i quattro MIB è **MIB SMI** → **MIB del prodotto** → **MIB XCC** → **MIB degli avvisi XCC**.

Informazioni particolari in questo documento

Utilizzare queste informazioni per comprendere gli avvisi utilizzati in questo documento.

Le seguenti informazioni sono utilizzate nella documentazione:

- **Nota:** questo tipo di informazioni fornisce consigli utili, suggerimenti o indicazioni di guida.
- **Importante:** tali informazioni forniscono informazioni o consigli che potrebbero aiutare l'utente a evitare inconvenienti o problemi.
- **Attenzione:** questo tipo di informazioni segnala possibili danni ai programmi, ai dispositivi o ai dati. Un avviso di avvertenza è stato posto immediatamente prima dell'istruzione o della situazione in cui potrebbe verificarsi un danno.

Capitolo 2. Avvio e utilizzo dell'interfaccia Web di XClarity Controller

In questo argomento sono descritte le procedure di login e le operazioni che possono essere effettuate dall'interfaccia Web di XClarity Controller.

XClarity Controller unisce funzioni di processore di servizio, controller video e presenza remota in un unico chip. Per accedere a XClarity Controller da remoto, è in primo luogo necessario eseguire il login mediante l'interfaccia Web di XClarity Controller. In questo capitolo sono descritte le procedure di login e le operazioni che possono essere effettuate dall'interfaccia Web di XClarity Controller.

Accesso all'interfaccia Web di XClarity Controller

Le informazioni in questo argomento descrivono come accedere all'interfaccia Web di XClarity Controller.

XClarity Controller supporta l'indirizzamento IPv4 statico e DHCP (Dynamic Host Configuration Protocol). L'indirizzo IPv4 statico predefinito assegnato a XClarity Controller è 192.168.70.125. XClarity Controller è inizialmente configurato per provare a ottenere un indirizzo da un server DHCP. Se ciò non fosse possibile, viene utilizzato l'indirizzo IPv4 statico.

XClarity Controller supporta anche IPv6, ma non dispone di un indirizzo IP IPv6 statico fisso predefinito. Per l'accesso iniziale a XClarity Controller in un ambiente IPv6, è possibile utilizzare l'indirizzo IP IPv4 o l'indirizzo locale del collegamento a IPv6. XClarity Controller genera un indirizzo IPv6 locale del collegamento univoco, utilizzando l'indirizzo MAC IEEE 802 per inserire due ottetti, con i valori esadecimali 0xFF e 0xFE al centro dell'indirizzo MAC a 48 bit, come descritto in RFC4291 e invertendo il secondo bit a partire dalla destra del primo ottetto dell'indirizzo MAC. Ad esempio se l'indirizzo MAC è 08-94-ef-2f-28-af, l'indirizzo locale del collegamento sarà:
`fe80::0a94:efff:fe2f:28af`

Quando si accede a XClarity Controller, sono impostate le seguenti condizioni IPv6 predefinite:

- La configurazione automatica dell'indirizzo IPv6 è abilitata.
- La configurazione dell'indirizzo IP statico IPv6 è disabilitata.
- DHCPv6 è abilitato.
- La configurazione automatica senza stato è abilitata.

XClarity Controller consente di scegliere una connessione di rete per la gestione dei sistemi **dedicata** (se disponibile) o una **condivisa** con il server. La connessione predefinita per i server montati in rack e tower è quella **dedicata**.

La connessione di rete per la gestione dei sistemi dedicata sulla maggior parte dei server viene fornita mediante un controller separato per l'interfaccia di rete a 1 Gbit. Tuttavia, su alcuni sistemi la connessione di rete per la gestione dei sistemi dedicata può essere fornita utilizzando l'interfaccia NCSI (Network Controller Sideband Interface) su una delle porte di rete di un controller dell'interfaccia di rete a più porte. In questo caso, la connessione di rete per la gestione dei sistemi dedicata è limitata alla velocità 10/100 dell'interfaccia NCSI. Per maggiori informazioni e per conoscere tutte le limitazioni relative all'implementazione della porta di gestione sul sistema, consultare la documentazione del sistema.

Nota: Sul server è possibile che la porta di rete per la gestione dei sistemi **dedicata** non sia disponibile. Se l'hardware non dispone di una porta di rete **dedicata**, l'impostazione **condivisa** sarà l'unica impostazione di XClarity Controller disponibile.

Configurazione della connessione di rete di XClarity Controller mediante XClarity Provisioning Manager

Utilizzare le informazioni in questo argomento per configurare una connessione di rete di XClarity Controller mediante XClarity Provisioning Manager.

Una volta avviato il server, è possibile utilizzare XClarity Provisioning Manager per configurare la connessione di rete di XClarity Controller. Il server con XClarity Controller deve essere connesso a un server DHCP oppure la rete del server dovrà essere configurata per l'uso dell'indirizzo IP statico di XClarity Controller. Per configurare la connessione di rete di XClarity Controller mediante Setup Utility, effettuare le seguenti operazioni:

Passo 1. Accendere il server. Verrà visualizzata la schermata di benvenuto di ThinkSystem.

Nota: Dopo che il server è stato collegato all'alimentazione CA, possono essere necessari fino a 40 secondi affinché il pulsante di controllo dell'alimentazione diventi attivo.

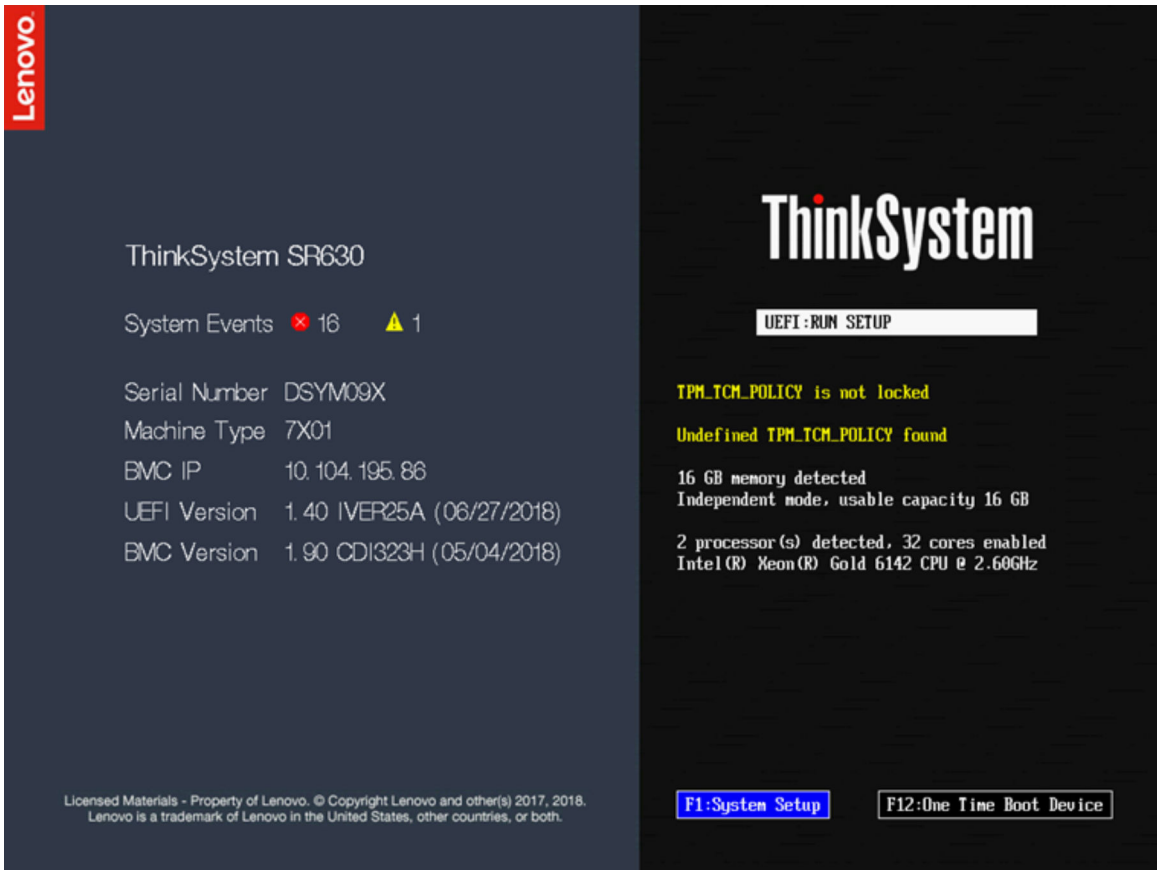


Figura 1. Schermata di benvenuto di ThinkSystem

Passo 2. Quando viene visualizzato il prompt `<F1> System Setup`, premere F1. Se sono stati impostati entrambi i livelli di password (accensione e amministratore), è necessario immettere la password amministratore per accedere a XClarity Provisioning Manager.

Passo 3. Dal menu principale di XClarity Provisioning Manager, selezionare **Configurazione UEFI**.

Passo 4. Nella schermata successiva, selezionare **Impostazioni BMC** e fare clic su **Impostazioni di rete**.

Passo 5. Sono disponibili tre opzioni di connessione alla rete di XClarity Controller nel campo **Controllo DHCP**:

- IP statico
- Abilitato per DHCP
- DHCP con fallback

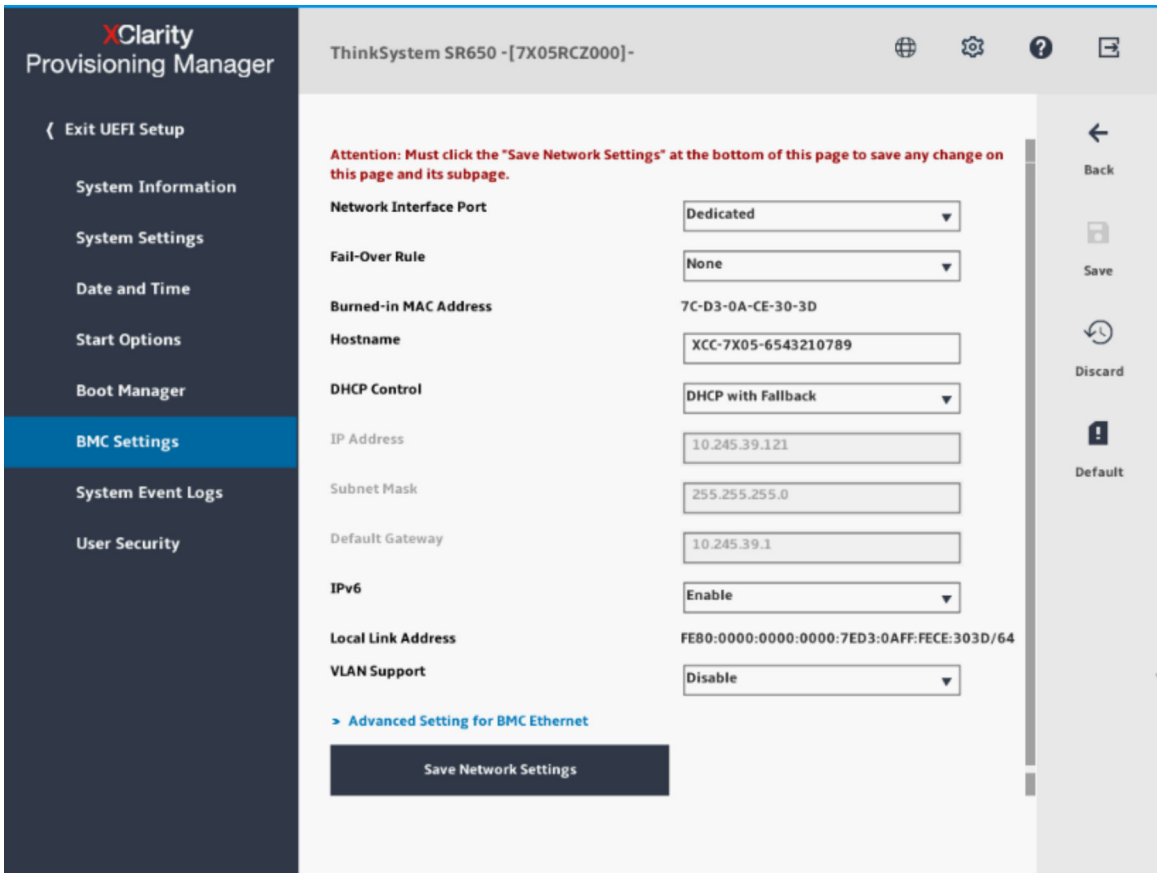


Figura 2. Impostazioni di connessione di rete

Passo 6. Selezionare una opzione per la connessione di rete.

Passo 7. Se si sceglie di utilizzare un indirizzo IP statico, è necessario specificare l'indirizzo IP, la maschera di sottorete e il gateway predefinito.

Passo 8. È inoltre possibile utilizzare Lenovo XClarity Controller Manager per selezionare una connessione di rete dedicata (se il server dispone di una porta di rete dedicata) o una connessione di rete XClarity Controller condivisa.

Nota:

- Sul server è possibile che la porta di rete per la gestione dei sistemi dedicata non sia disponibile. Se l'hardware non dispone di una porta di rete dedicata, l'impostazione **condivisa** sarà l'unica impostazione di XClarity Controller disponibile. Nella schermata **Configurazione di rete**, selezionare **Dedicata** (se disponibile) o **Condivisa** nel campo **Porta di interfaccia di rete**.
- Per trovare le posizioni dei connettori Ethernet sul server utilizzati da XClarity Controller, fare riferimento alla documentazione fornita con il server.

Passo 9. Fare clic su **Salva**.

Passo 10. Uscire da XClarity Provisioning Manager.

Nota:

- Perché le modifiche abbiano effetto e prima che il firmware del server sia di nuovo operativo sarà necessario attendere circa 1 minuto.
- È inoltre possibile configurare la connessione di rete di XClarity Controller mediante l'interfaccia Web di XClarity Controller o l'interfaccia della riga di comando (CLI, command-line interface). Nell'interfaccia Web di XClarity Controller, è possibile configurare le connessioni di rete facendo clic su **Configurazione BMC** nel pannello di navigazione sinistro, quindi selezionando **Rete**. Nella CLI di XClarity Controller, le connessioni di rete sono configurate utilizzando diversi comandi che dipendono dalla configurazione della propria installazione.

Login a XClarity Controller

Utilizzare le informazioni in questo argomento per accedere a XClarity Controller mediante l'interfaccia Web di XClarity Controller.

Importante: XClarity Controller è impostato inizialmente con il nome utente `USERID` e la password `PASSWORD` (con uno zero, non la lettera O). Questa impostazione utente predefinita assicura l'accesso da supervisore. Per una maggiore sicurezza, modificare questo nome utente e la password durante la configurazione iniziale. Dopo avere apportato la modifica, non è possibile impostare nuovamente `PASSWORD` come password di login.

Per accedere a XClarity Controller mediante l'interfaccia Web di XClarity Controller, completare le seguenti operazioni:

Passo 1. Aprire un browser Web. Nel campo dell'indirizzo o dell'URL, digitare `https://` seguito dall'indirizzo IP o dal nome host di XClarity Controller a cui si desidera collegarsi.

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

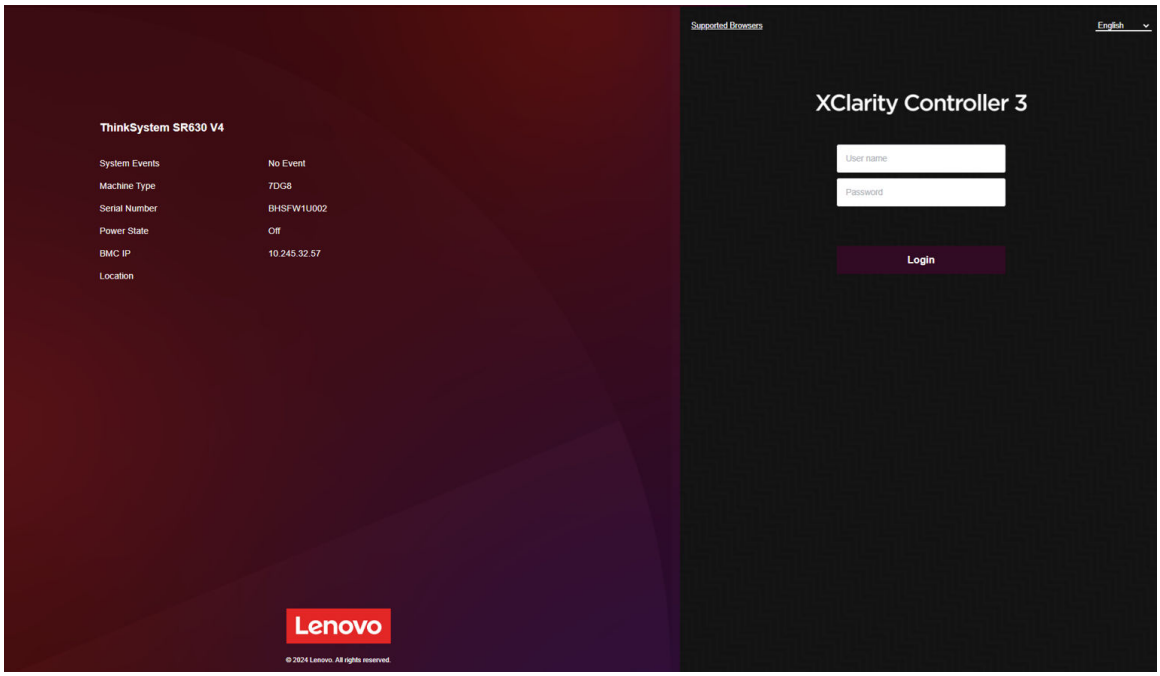


Figura 3. Pagina di login

Passo 3. Immettere il nome utente e la password nella finestra di login di XClarity Controller. Se si utilizza XClarity Controller per la prima volta, è possibile acquisire il nome utente e la password dall'amministratore di sistema. Tutti i tentativi di accesso sono documentati nel log di eventi. A

seconda della modalità in cui l'amministratore del sistema ha configurato l'ID utente, una volta eseguito il login potrebbe essere necessario immettere una nuova password.

Passo 4. Fare clic su **Login** per avviare la sessione. Il browser visualizzerà la home page di XClarity Controller, come mostrato nella seguente figura. Nella home page sono visualizzate le informazioni sul sistema gestito da XClarity Controller, oltre alle icone che indicano quanti errori critici 1 e avvisi 1 sono presenti attualmente nel sistema.

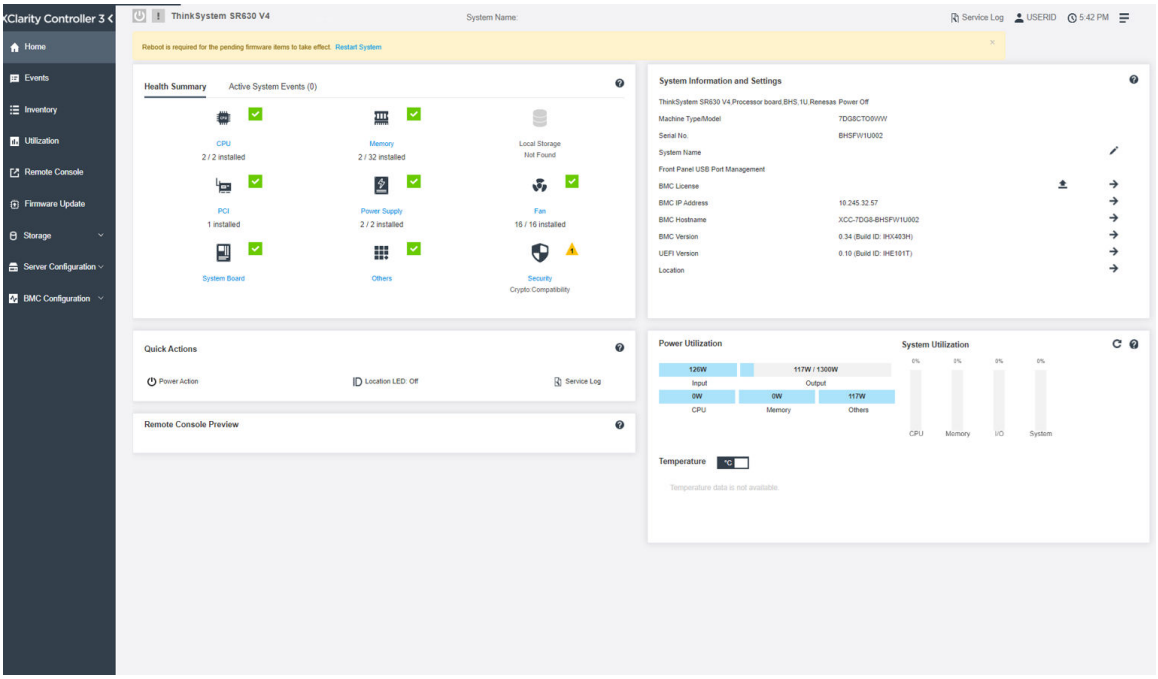


Figura 4. Home page

La home page è divisa in due sezioni principali. La prima sezione è il riquadro di navigazione sinistro, che riporta una serie di argomenti per eseguire le seguenti azioni:

- Monitoraggio dello stato del server
- Configurazione del server
- Configurazione di XClarity Controller o di BMC
- Aggiornamento del firmware

La seconda sezione include le informazioni grafiche fornite a destra del riquadro di navigazione. Il formato modulare fornisce una vista rapida dello stato del server e alcune azioni rapide disponibili.

Descrizione delle funzioni di XClarity Controller sull'interfaccia Web

Le informazioni contenute in questo argomento illustrano le funzioni di XClarity Controller sull'interfaccia Web.

Di seguito è riportata una tabella che descrive le funzioni di XClarity Controller nel riquadro di navigazione sinistro.

Nota: Quando si utilizza l'interfaccia Web, è inoltre possibile fare clic sull'icona del punto interrogativo per visualizzare la guida online.

Scheda	Selezione	Descrizione
Home page	Riepilogo integrità/Eventi di sistema attivi	Mostra lo stato corrente dei componenti hardware principali nel sistema.
	Informazioni sul sistema e impostazioni	Fornisce un riepilogo delle informazioni di sistema comuni.
	Azioni rapide	Fornisce un collegamento rapido per controllare il LED di posizione e alimentazione del server e un pulsante per scaricare i dati di servizio.
	Utilizzo dell'alimentazione	Fornisce una rapida panoramica dell'utilizzo dell'alimentazione corrente.
	Anteprima console remota	Controlla il server a livello di sistema operativo. È possibile visualizzare e utilizzare la console del server dal proprio computer. La sezione relativa alla console remota nella home page di XClarity Controller contiene un'immagine della schermata con un pulsante di avvio.
Eventi	Log eventi	Fornisce un elenco cronologico di tutti gli eventi di gestione e hardware.
	Log di controllo	Fornisce un record cronologico degli interventi dell'utente.
	Cronologia manutenzione	Visualizza tutta la cronologia di aggiornamento firmware, configurazione e sostituzione hardware.
	Destinatari avvisi **Nota:** Questa funzione sarà supportata in un aggiornamento futuro.	Gestisce chi riceverà una notifica degli eventi di sistema. Consente di configurare ogni destinatario e di gestire le impostazioni che si applicano a tutti i destinatari degli eventi. È inoltre possibile generare un evento di prova per verificare le impostazioni di configurazione delle notifiche.
Inventario		Visualizza tutti i componenti nel sistema, con il relativo stato e le informazioni principali. È possibile fare clic su un dispositivo per visualizzare le informazioni aggiuntive. **Nota:** Fare riferimento all'interfaccia Web di SMM3 per ulteriori dettagli sullo stato di alimentazione della soluzione.
Utilizzo		Visualizza la temperatura ambiente/componente, l'utilizzo dell'alimentazione, i livelli di tensione e le informazioni sulla velocità della ventola del server e dei relativi componenti in formato grafico o tabulare.
Console remota		Fornisce l'accesso alla funzionalità di console remota. È possibile utilizzare la funzione dei supporti virtuali per montare i file ISO o IMG che si trovano sul sistema o su un percorso di rete accessibile dal BMC mediante CIFS, NFS, HTTPS o SFTP. Il disco montato viene visualizzato come un'unità disco USB o un DVD ROM collegata al server.
Aggiornamento firmware		• Visualizza i livelli di firmware. • Aggiorna il firmware di XClarity Controller e il firmware del server. • Aggiorna il firmware di XClarity Controller da Repository.
Storage	Dettaglio	Visualizza la struttura fisica e la configurazione dello storage dei dispositivi di storage.
	Configurazione RAID	Visualizza o modifica la configurazione RAID corrente, incluse le informazioni di dischi virtuali e dispositivi di storage fisici.

Scheda	Selezione	Descrizione
Configurazione del server	Adattatori	Visualizza le informazioni degli adattatori di rete installati e le impostazioni configurabili tramite XClarity Controller.
	Opzioni di avvio	• Seleziona il dispositivo di avvio per l'avvio singolo al prossimo riavvio del server. • Modifica la modalità di avvio e le impostazioni dell'ordine di avvio.
	Criteri di alimentazione	• Configura la ridondanza dell'alimentazione durante un evento di errore dell'alimentatore. • Configura il criterio di limite alimentazione. • Configura i criteri di ripristino dell'alimentazione. **Nota:** Fare riferimento all'interfaccia Web SMM3 per ulteriori dettagli sullo stato dell'alimentazione della soluzione.
	Proprietà del server	• Monitora varie proprietà, condizioni di stato e impostazioni del server. • Gestisce i ritardi di spegnimento del server. • Crea il messaggio di sconfinamento. È possibile creare questo tipo di messaggio per consentire agli utenti di visualizzare quando viene eseguito il login a XClarity Controller.
	Chassis **Nota:** Questo elemento è disponibile solo sui nodi compatibili con lo chassis D3 V2.	• Visualizza le informazioni sullo chassis. • Riavviare il nodo o simulare un riposizionamento del nodo fisico. • Visualizza le preferenze di selezione del care-taker dello chassis. • Visualizza la cronologia di manutenzione dello chassis.
Configurazione BMC	Backup e ripristino	Reimposta la configurazione di XClarity Controller ai valori predefiniti iniziali, la configurazione corrente di backup o il ripristino della configurazione da un file.
	Licenza	Gestisce le chiavi di attivazione per le funzioni facoltative di XClarity Controller.
	Rete	Configura le proprietà, lo stato e le impostazioni di rete di XClarity Controller.
	Protezione	Configura le proprietà, lo stato e le impostazioni di sicurezza di XClarity Controller.
	Utente/LDAP	• Configura i profili di login e le impostazioni di login globali di XClarity Controller. • Visualizza gli account utente correntemente collegati a XClarity Controller. • La scheda LDAP configura l'autenticazione utente da utilizzare con uno o più server LDAP. Consente anche di abilitare o disabilitare la sicurezza LDAP e di gestirne i certificati.

Scheda	Selezione	Descrizione
	Call Home **Nota:** Questa funzione sarà supportata in un aggiornamento futuro.	Configurare l'opzione Call Home per raccogliere le informazioni sul sistema e inviarle a Lenovo per i servizi.

Capitolo 3. Configurazione di XClarity Controller

Utilizzare le informazioni in questo capitolo per comprendere le opzioni disponibili per le configurazioni di XClarity Controller.

Quando si configura XClarity Controller, sono disponibili le seguenti opzioni principali:

- Backup e ripristino
- Licenza
- Rete
- Protezione
- Utente/LDAP

Configurazione dell'account utente/di LDAP

Utilizzare le informazioni in questo argomento per comprendere come gestire gli account utente.

Fare clic su **Utente/LDAP** in **Configurazione BMC** per creare, modificare e visualizzare account utente e per configurare le impostazioni LDAP.

La scheda **Utente locale** mostra gli account utente configurati in XClarity Controller e quali di questi hanno attualmente eseguito il login a XClarity Controller.

La scheda **LDAP** mostra la configurazione LDAP per l'accesso agli account utente conservati su un server LDAP.

Metodo di autenticazione utente

Utilizzare le informazioni in questo argomento per comprendere le modalità utilizzate da XClarity Controller per autenticare i tentativi di login.

Fare clic sul menu a discesa accanto a **Consenti accesso da** per selezionare la modalità di autenticazione dei tentativi di accesso dell'utente. Selezionare uno dei seguenti metodi di autenticazione:

- **Solo locale:** gli utenti sono autenticati mediante una ricerca dell'account utente locale configurato in XClarity Controller. Se non sono trovati un ID utente e una password corrispondenti, l'accesso viene negato.
- **Solo LDAP:** XClarity Controller prova ad autenticare l'utente con le credenziali conservate su un server LDAP. Gli account utente locali in XClarity Controller **non** vengono ricercati con questo metodo di autenticazione.
- **Prima locale, poi LDAP:** viene provata prima l'autenticazione locale. Se questa non riesce, viene provata l'autenticazione LDAP.
- **Prima LDAP, poi utente locale:** viene provata prima l'autenticazione LDAP. Se l'autenticazione LDAP non riesce, viene provata quella locale.

Nota:

- Solo gli account gestiti in locale sono condivisi con le interfacce IPMI e SNMP. Queste interfacce non supportano l'autenticazione LDAP.
- Gli utenti IPMI e SNMP possono effettuare il login utilizzando gli account amministrati localmente solo se il campo **Consenti accesso da** è impostato su **Solo LDAP**.

Creazione di un nuovo ruolo

Utilizzare le informazioni in questo argomento per creare un nuovo ruolo.

Creazione di un ruolo

Fare clic sulla scheda **Ruoli** e su **Crea** per creare un ruolo personalizzato.

Completare i seguenti campi: **Nome ruolo** e **Livello di autorizzazione**. Per ulteriori dettagli sul livello di autorizzazione, fare riferimento alla seguente sezione.

Il ruolo creato viene fornito all'utente nel menu a discesa dei ruoli nella sezione utente.

Nota: Il ruolo utilizzato in Utente e LDAP non può modificare ed eliminare il nome del ruolo, ma può accedere alla modifica dell'autorizzazione personalizzata corrispondente.

Livello di autorizzazione

Un ruolo personalizzato è consentito per abilitare qualsiasi combinazione dei seguenti privilegi:

Configurazione - Rete e sicurezza del BMC
Un utente può modificare i parametri di configurazione nelle pagine Sicurezza BMC e Rete.

Gestione account utente
Un utente può aggiungere, modificare o eliminare utenti e modificare le impostazioni di login globali nella finestra Profili di login.

Accesso alla console remota
Un utente può accedere alla console remota.

Accesso alla console remota e al disco remoto
Un utente può accedere alla console remota e alla funzione per i supporti virtuali.

Alimentazione/riavvio server remoto
Un utente può eseguire funzioni di accensione e riavvio per il server.

Configurazione - Base
Un utente può modificare i parametri di configurazione nelle pagine Proprietà del server ed Eventi.

Possibilità di cancellare i log eventi
Un utente può cancellare il log di eventi. Chiunque può visualizzare i log di eventi, ma è richiesto questo livello di autorizzazione per cancellarli.

Configurazione - Avanzate (aggiornamento firmware, riavvio BMC, ripristino configurazione)
Un utente non ha limitazioni per la configurazione di XClarity Controller. Inoltre, l'utente avrà accesso amministrativo a XClarity Controller. L'accesso amministrativo include le seguenti funzioni avanzate: aggiornamenti firmware, avvio di rete PXE, ripristino dei valori predefiniti originali di XClarity Controller, modifica e ripristino delle impostazioni di XClarity Controller da un file di configurazione, riavvio e reimpostazione di XClarity Controller.

Configurazione - Sicurezza UEFI
Un utente può modificare le impostazioni di sicurezza UEFI.

Ruoli predefiniti

I seguenti ruoli sono predefiniti e non possono essere modificati o eliminati:

Amministratore
Il ruolo di amministratore non ha limitazioni e può eseguire tutte le operazioni.

Sola lettura

Il ruolo Sola lettura può visualizzare le informazioni sul server ma non può eseguire operazioni che incidono sullo stato del sistema, come salvataggio, modifica, cancellazione, riavvio e aggiornamento firmware.

Operatore
L'utente con il ruolo di operatore dispone dei seguenti privilegi:

- Configurazione - Rete e sicurezza del BMC
- Alimentazione/riavvio server remoto
- Configurazione - Base
- Possibilità di cancellare i log eventi
- Configurazione - Avanzate (aggiornamento firmware, riavvio BMC, ripristino configurazione)

Creazione di un nuovo account utente

Utilizzare le informazioni in questo argomento per creare un nuovo utente locale.

Creazione di un utente

Fare clic sulla scheda **utenti locali**, quindi su **Crea** per creare un nuovo account utente.

Completare i seguenti campi: **Nome utente**, **Password**, **Conferma password** e selezionare un **Ruolo** dal menu a discesa. Per ulteriori dettagli sul **Ruolo**, fare riferimento alla seguente sezione.

Ruolo

I seguenti ruoli sono predefiniti mentre il nuovo ruolo personalizzato può essere creato in base alle esigenze dell'utente:

Amministratore
Il ruolo di amministratore non ha limitazioni e può eseguire tutte le operazioni.

Sola lettura
Il ruolo Sola lettura può visualizzare le informazioni sul server ma non può eseguire operazioni che incidono sullo stato del sistema, come salvataggio, modifica, cancellazione, riavvio e aggiornamento firmware.

Operatore
L'utente con il ruolo di operatore dispone dei seguenti privilegi:

- Configurazione - Rete e sicurezza del BMC
- Alimentazione/riavvio server remoto
- Configurazione - Base
- Possibilità di cancellare i log eventi
- Configurazione - Avanzate (aggiornamento firmware, riavvio BMC, ripristino configurazione)

Impostazioni SNMPv3

Per abilitare l'accesso SNMPv3 per un utente, fare clic sul pulsante **Modifica** accanto all'utente corrispondente, quindi selezionare **SNMP** nell'elenco a discesa **Interfaccia accessibile all'utente**. Di seguito sono illustrate le varie opzioni di accesso utente:

Tipo di accesso
Sono supportate solo le operazioni di tipo **GET**. XClarity Controller non supporta le operazioni SNMPv3 **SET**. SNMP3 può eseguire solo le operazioni di tipo query.

Protocollo di autenticazione
Questo algoritmo è utilizzato dal modello di sicurezza SNMPv3 per l'autenticazione. Sono supportati i seguenti protocolli:

- Nessuno
- HMAC-SHA (predefinito)
- HMAC-SHA224
- HMAC-SHA256
- HMAC-SHA384
- HMAC-SHA512

Protocollo privacy
Il trasferimento di dati tra il client SNMP e l'agent può essere protetto utilizzando la crittografia. Sono supportati i seguenti metodi:

- Nessuno
- CBC-DES
- AES (predefinito)
- AES192
- AES256
- AES192C
- AES256C

Nota: Anche se un utente SNMPv3 utilizza stringhe ripetitive per una password, l'accesso a XClarity Controller è comunque consentito. Di seguito sono riportati due esempi come riferimento.

- Se la password è impostata su "**11111111**" (numero di otto cifre contenente otto 1), l'utente può comunque accedere a XClarity Controller se la password viene immessa accidentalmente con più di otto 1. Ad esempio, se la password immessa è "**1111111111**" (numero di dieci cifre contenente dieci 1), l'accesso verrà concesso. La stringa ripetitiva viene considerata una stessa chiave.
- Se la password è impostata su "**bertbert**", l'utente può comunque accedere a XClarity Controller se accidentalmente viene immessa la password "**bertbertbert**". Entrambe le password sono considerate la stessa chiave.

Per ulteriori dettagli, consultare **Considerazioni sulla sicurezza** nel documento Internet Standard of RFC 3414 (https://tools.ietf.org/html/rfc3414).

Chiave SSH

XClarity Controller supporta l'autenticazione della chiave pubblica SSH (tipo di chiave RSA). Per aggiungere una chiave SSH all'account utente locale, fare clic sul pulsante **Modifica** accanto all'utente corrispondente, quindi selezionare **Chiave SSH** nell'elenco a discesa **Interfaccia accessibile all'utente**. Sono disponibili le seguenti due opzioni:

Selezionare il file di chiavi
Selezionare il file della chiave SSH da importare in XClarity Controller dal server.

Immettere la chiave in un campo di testo
Incollare o digitare i dati dalla chiave SSH nel campo di testo.

Nota:

- È possibile che per alcuni strumenti di Lenovo, se eseguiti sul sistema operativo del server, venga creato un account utente temporaneo per accedere a XClarity Controller. Tale account temporaneo non è

visualizzabile e non utilizza nessuna delle 12 posizioni di account utente locale. L'account viene creato con un nome utente casuale (ad esempio, "20luN4SB") e una password. L'account può essere utilizzato solo per accedere a XClarity Controller sull'interfaccia interna Ethernet-over-USB e solo per le interfacce Redfish e SFTP. La creazione e la rimozione di questo account temporaneo sono registrate nel log di controllo, così come tutte le azioni eseguite dallo strumento con queste credenziali.

- Per l'ID del motore SNMPv3, XClarity Controller utilizza una stringa ESADECIMALE per indicare l'ID. Questa stringa ESADECIMALE viene convertita dal nome host predefinito di XClarity Controller. Fare riferimento al seguente esempio:

  Il nome host "XCC-7X06-S4AHJ300" viene prima convertito nel formato ASCII: 88 67 67 45 55 88 48 54 45 83 52 65 72 74 51 48 48

  La stringa ESADECIMALE viene integrata utilizzando il formato ASCII (ignorare gli spazi): 58 43 43 2d 37 58 30 36 2d 53 34 41 48 4a 33 30 30

Eliminazione di un account utente

Utilizzare le informazioni in questo argomento per rimuovere un account utente locale.

Per eliminare un account utente locale, fare clic sull'icona del cestino sulla riga dell'account che si desidera rimuovere. Se si è autorizzati, è possibile rimuovere il proprio account o l'account di altri utenti, purché non sia l'unico account rimanente con privilegi di **gestione account utente**.

Utilizzo delle password con hash per l'autenticazione

Utilizzare le informazioni in questa sezione per comprendere come utilizzare le password con hash per l'autenticazione.

Oltre all'utilizzo della password e degli account utente LDAP/AD, XClarity Controller supporta le password con hash di terze parti per l'autenticazione. La password speciale utilizza un formato con hash unidirezionale (SHA256) ed è supportata dalle interfacce di CLI, OneCLI e Web di XClarity Controller. Tuttavia, tenere presente che l'autenticazione delle interfacce XCC SNMP, IPMI e CIM non supporta le password con hash di terze parti. Solo lo strumento OneCLI e l'interfaccia CLI di XCC possono creare un nuovo account con una password con hash o eseguire un aggiornamento di una password con hash. XClarity Controller consente inoltre allo strumento OneCLI e all'interfaccia CLI di XClarity Controller di recuperare le password con hash, se la funzione di lettura delle password con hash è abilitata.

Impostazione della password con hash mediante l'interfaccia Web di XClarity Controller

Fare clic su **Sicurezza** in **Configurazione BMC** e scorrere fino alla sezione **Security Password Manager** per abilitare o disabilitare la funzione **Password di terze parti**. Se abilitata, una password con hash di terze parti viene utilizzata per l'autenticazione di accesso. Il recupero della password con hash di terze parti da XClarity Controller può essere abilitato o disabilitato.

Nota: Per impostazione predefinita, le funzioni **Password di terze parti** e **Consenti recupero password di terze parti** sono disabilitate.

Per verificare se la password utente è **Nativa** o è una **Password di terze parti**, fare clic su **Utente/LDAP** in **Configurazione BMC** per maggiori dettagli. Le informazioni verranno riportato sotto la colonna **Attributo avanzato**.

Nota:

- Se una password è di terze parti, gli utenti non possono modificarla e i campi **Password** e **Conferma password** sono disattivati.

- Se la password di terze parti è scaduta, verrà visualizzato un messaggio di avvertenza durante il processo di login dell'utente.

Impostazione della password con hash mediante la funzione OneCLI

- Abilitazione della funzione.

  ```
  $ sudo OneCli config set IMM.ThirdPartyPassword Enabled
  ```

- Creazione di password con hash (senza Salt). Di seguito è riportato un esempio di login a XClarity Controller mediante la password **password123**.

  ```
  $ pwhash = `echo -n password123 | openssl dgst -sha256 | awk '{print $NF}'`

  $ echo $pwhash 5e884898da28047151d0e56f8dc6292773603d0d6aabbdd62a11ef721d1542d8

  $ sudo OneCli config set IMM.Loginid.2 admin

  $ sudo OneCli config set IMM.SHA256Password.2 $pwhash

  $ sudo OneCli config set IMM.SHA256PasswordSalt.2 ""
  ```

- Creazione di un utente con password con hash (con Salt). Di seguito è riportato un esempio di login a XClarity Controller mediante la password **password123**. Salt = abc.

  ```
  $ pwhash = `echo -n password123abc | openssl dgst -sha256 | awk '{print $NF}'`

  $ echo $pwhash 292bcbc41bb078cf5bd258db60b63a4b337c8c954409442cfad7148bc6428fee

  $ sudo OneCli config set IMM.Loginid.3 Admin

  $ sudo OneCli config set IMM.SHA256Password.3 $pwhash

  $ sudo OneCli config set IMM.SHA256PasswordSalt.3 'abc'
  ```

- Recupero della password con hash e salt.

  ```
  $ sudo OneCli config set IMM.ThirdPartyPasswordReadable Enabled

  $ sudo OneCli config show IMM.SHA256Password.3

  $ sudo OneCli config show IMM.SHA256PasswordSalt.3
  ```

- Eliminazione della password con hash e salt.

  ```
  $ sudo OneCli config set IMM.SHA256Password.3 ""

  $ sudo OneCli config set IMM.SHA256PasswordSalt.3 ""
  ```

- Impostazione della password con hash in un account esistente.

  ```
  $ sudo OneCli config set IMM.Loginid.2 admin

  $ sudo OneCli config set IMM.Password.2 Passw0rd123abc

  $ sudo OneCli config set IMM.SHA256Password.2 $pwhash

  $ sudo OneCli config set IMM.SHA256PasswordSalt.2 ""
  ```

  Nota: Una volta impostata, la password con hash è subito effettiva. La password standard originale non sarà più valida. In questo esempio, la password standard originale **Passw0rd123abc** non può essere più utilizzata finché la password con hash non viene eliminata.

Impostazione della password con hash mediante la funzione CLI

- Abilitazione della funzione.

  ```
  > hashpw -sw enabled
  ```

- Creazione di password con hash (senza Salt). Di seguito è riportato un esempio di login a XClarity Controller mediante la password **password123**.

  ```
  $ pwhash = `echo -n password123 | openssl dgst -sha256 | awk '{print $NF}'`

  5e884898da28047151d0e56f8dc6292773603d0d6aabbdd62a11ef721d1542d8

  > users -2 -n admin -shp 5e884898da28047151d0e56f8dc6292773603d0d6aabbdd62a11ef721d1542d8 -a
  super
  ```

- Creazione di un utente con password con hash (con Salt). Di seguito è riportato un esempio di login a XClarity Controller mediante la password **password123**. Salt = abc.

  ```
  $ pwhash = `echo -n password123abc | openssl dgst -sha256 | awk '{print $NF}'`

  $ echo $pwhash 292bcbc41bb078cf5bd258db60b63a4b337c8c954409442cfad7148bc6428fee

  > users -3 -n Admin -shp 292bcbc41bb078cf5bd258db60b63a4b337c8c954409442cfad7148bc6428fee
  -ssalt 'abc' -a super
  ```

- Recupero della password con hash e salt.

  ```
  > hashpw -re enabled

  > users -3 -ghp -gsalt
  ```

- Eliminazione della password con hash e salt.

  ```
  > users -3 -shp "" -ssalt ""
  ```

- Impostazione della password con hash in un account esistente.

  ```
  > users -2 -n admin -p Passw0rd123abc -shp
  5e884898da28047151d0e56f8dc6292773603d0d6aabbdd62a11ef721d1542d8 -a super
  ```

  Nota: Una volta impostata, la password con hash è subito effettiva. La password standard originale non sarà più valida. In questo esempio, la password standard originale **Passw0rd123abc** non può essere più utilizzata finché la password con hash non viene eliminata.

Una volta impostata la password con hash, non utilizzarla per eseguire il login a XClarity Controller. Quando si esegue il login, sarà necessario utilizzare la password in testo normale. Nel seguente esempio, la password in testo normale è "password123".

```
$ pwhash = ‘echo –n password123 | openssl dgst –sha256 | awk '{print $NF}'’

5e884898da28047151d0e56f8dc6292773603d0d6aabbdd62a11ef721d1542d8

> users -2 -n admin -shp 5e884898da28047151d0e56f8dc6292773603d0d6aabbdd62a11ef721d1542d8 -a super
```

Configurazione delle impostazioni di login globali

Utilizzare le informazioni in questo argomento per configurare le impostazioni dei criteri di login e password applicabili a tutti gli utenti.

Timeout sessione di inattività Web

Utilizzare le informazioni in questo argomento per impostare l'opzione Timeout sessione di inattività Web.

Nel campo **Timeout sessione di inattività Web** è possibile specificare quanto tempo, in minuti, XClarity Controller attende prima di disconnettere una sessione Web inattiva. Il tempo di attesa massimo è 1.440 minuti. Se impostato su 0, la sessione Web non ha scadenza.

Il firmware XClarity Controller supporta un massimo di sei sessioni Web simultanee. Per liberare sessioni per altri utenti, è consigliabile effettuare il logout dalla sessione Web una volta terminato anziché attendere che la sessione venga chiusa automaticamente in seguito al timeout di inattività.

Nota: Se si lascia aperto il browser su una pagina Web di XClarity Controller che viene aggiornata automaticamente, la sessione Web non verrà terminata automaticamente a causa di inattività.

Impostazioni dei criteri di sicurezza dell'account

Utilizzare queste informazioni per comprendere e impostare i criteri di sicurezza dell'account per il server.

Di seguito è riportata una descrizione dei campi per le impostazioni di sicurezza.

Forza utente a modificare la password al primo accesso
Dopo l'impostazione di un nuovo utente con una password predefinita, la selezione di questa casella di controllo forzerà l'utente a modificare la propria password in occasione del primo login. Il valore predefinito per questo campo è rappresentato dalla casella di controllo abilitata.

Password complessa richiesta
La casella di opzione è selezionata per impostazione predefinita e la password complessa deve rispettare le seguenti regole:

- Può contenere solo i seguenti caratteri (nessuno spazio consentito): A-Z, a-z, 0-9, ~`!@#$%^&*()-+={}[]|:;"'<>,?/._
- Deve contenere almeno una lettera
- Deve contenere almeno un numero
- Deve contenere almeno due delle seguenti combinazioni:
  - Almeno una lettera maiuscola
  - Almeno una lettera minuscola
  - Almeno un carattere speciale
- Non sono consentiti altri caratteri (in particolare, spazi o spazi vuoti)
- Le password non possono avere più di due istanze consecutive dello stesso carattere (ad esempio, "aaa")
- La password non può essere una riproduzione letterale del nome utente, ad esempio non è possibile ripetere il nome utente una o più volte oppure invertire l'ordine dei caratteri del nome utente.
- Le password devono contenere un minimo di 8 e un massimo di 255 caratteri.

Se la casella dell'opzione non è selezionata, il numero di caratteri specificato per la lunghezza minima della password può essere compreso tra 0 e 255. Se la lunghezza minima della password è impostata su 0, è possibile che la password dell'account non venga richiesta.

Periodo di scadenza password (giorni)
Questo campo indica la durata massima consentita della password prima che sia necessario modificarla.

Periodo di avviso scadenza password (giorni)
Questo campo indica con quanti giorni di anticipo l'utente viene avvisato della scadenza della password.

Lunghezza minima della password (caratteri)
Questo campo contiene la lunghezza minima della password.

Ciclo minimo di riutilizzo password (volte)
Questo campo indica il numero di password precedenti che non possono essere riutilizzate.

Intervallo minimo di modifica password (ore)
Questo campo indica quanto tempo deve attendere un utente prima di poter modificare la propria password.

Numero massimo di errori di login (volte)
Questo campo indica il numero di tentativi di login non riusciti consentiti prima che l'utente venga bloccato per un periodo di tempo.

Periodo di blocco in seguito al numero massimo di errori di login (minuti)
Questo campo indica per quanto tempo (in minuti) il sottosistema XClarity Controller disabiliterà i tentativi di login remoto una volta raggiunto il numero massimo di errori di login.

Configurazione di LDAP

Utilizzare le informazioni in questo argomento per visualizzare o modificare le impostazioni LDAP di XClarity Controller.

Il supporto LDAP include:

- Supporto della versione 3 del protocollo LDAP (RFC-2251)
- Supporto delle API del client LDAP standard (RFC-1823)
- Supporto della sintassi del filtro di ricerca LDAP standard (RFC-2254)
- Supporto dell'estensione Lightweight Directory Access Protocol (v3) per Transport Layer Security (RFC-2830)

L'implementazione LDAP supporta i seguenti server LDAP:

- Microsoft Active Directory (Windows 2003, Windows 2008, Windows 2012, Windows 2016, Windows 2019)
- Microsoft Active Directory Application Mode (Windows 2003, Windows 2008)
- Microsoft Lightweight Directory Service (Windows 2008, Windows 2012, Windows 2016, Windows 2019)
- Novell eDirectory Server, versione 8.7 e 8.8
- OpenLDAP Server 2.1, 2.2, 2.3, 2.4, 2.5 e 2.6

Selezionare la scheda **LDAP** per visualizzare o modificare le impostazioni LDAP di XClarity Controller.

XClarity Controller permette di autenticare da remoto l'accesso di un utente tramite un server LDAP centrale, in sostituzione o in aggiunta agli account degli utenti locali memorizzati in XClarity Controller. I privilegi possono essere definiti per ogni account utente utilizzando il valore di "Attributo di autorizzazione di login". È inoltre possibile utilizzare il server LDAP per assegnare gli utenti ai gruppi ed eseguire l'autenticazione del gruppo, oltre alla normale autenticazione utente (controllo della password). Ad esempio, un XClarity Controller può essere associato a uno o più gruppi, l'utente supererà l'autenticazione del gruppo solo se appartiene almeno a un gruppo associato a XClarity Controller.

Per configurare un server LDAP, effettuare le seguenti operazioni:

1. In **Informazioni sul server LDAP**, sono disponibili le seguenti opzioni all'elenco degli elementi:
   - **Utilizza il server LDAP solo per l'autenticazione (con autorizzazione locale)**: se si seleziona questa opzione, XClarity Controller utilizzerà le credenziali soltanto per l'autenticazione presso il server LDAP e per recuperare informazioni sull'appartenenza ai gruppi. I nomi dei gruppi e i ruoli possono essere configurati nella sezione **Gruppi per autorizzazione locale**.
   - **Utilizza il server LDAP per autenticazione e autorizzazione**: se si seleziona questa opzione, XClarity Controller utilizzerà le credenziali sia per l'autenticazione presso il server LDAP che per identificare l'autorizzazione di un utente.

Nota: I server LDAP da utilizzare per l'autenticazione possono essere configurati manualmente o rilevati in modo dinamico tramite i record SRV del DNS.

- **Utilizza server preconfigurati**: è possibile configurare fino a tre server LDAP immettendo l'indirizzo IP o il nome host di ciascun server, se DNS è abilitato. Il numero di porta per ciascun server è facoltativo. Se questo campo è lasciato vuoto, per le connessioni LDAP non sicure sarà utilizzato il valore predefinito 389. Per le connessioni sicure, il valore predefinito della porta è 636. È necessario configurare almeno un server LDAP.
- **Usa DNS per trovare i server**: è possibile scegliere di rilevare i server LDAP in modo dinamico. I meccanismi descritti in RFC2782 (A DNS RR per specificare l'ubicazione dei servizi) vengono utilizzati per localizzare i server LDAP. Questo metodo è noto come DNS SRV. È necessario specificare un FQDN (Fully Qualified Domain Name, nome di dominio completo) da utilizzare come nome di dominio nella richiesta SRV del DNS.
  - **Foresta di AD**: in un ambiente con gruppi universali in domini incrociati, il nome della foresta (set di domini) deve essere configurato per rilevare i cataloghi globali richiesti (GC). In un ambiente in cui l'appartenenza al gruppo tra domini non si applica, questo campo può essere lasciato vuoto.
  - **Dominio di AD**: sarà necessario specificare un FQDN (Fully Qualified Domain Name, nome di dominio completo) da utilizzare come nome di dominio nella richiesta SRV del DNS.

Se si desidera abilitare il protocollo LDAP sicuro, selezionare la casella di controllo **Abilita LDAP sicuro**. Per supportare il protocollo LDAP sicuro, è necessario disporre di un certificato SSL valido e aver importato almeno un certificato attendibile del client SSL in XClarity Controller. Il server LDAP deve supportare la versione 1.2 di Transport Layer Security (TLS) per essere compatibile con il client LDAP sicuro XClarity Controller. Per ulteriori informazioni sulla gestione dei certificati, fare riferimento a "Gestione dei certificati SSL" a pagina 43.

2. Immettere le informazioni in **Parametri aggiuntivi**. Di seguito sono riportate le spiegazioni dei parametri.

Tipo di LDAP

Selezionare il tipo di server LDAP per l'autenticazione basata su LDAP. Sono disponibili i seguenti tipi di server:

- **OpenLDAP**

  OpenLDAP
- **Active Directory**

  Directory: Windows Active Directory
- **Altro**

  Directory: Apache Directory, eDirectory e così via.

Metodo di collegamento

Prima di poter ricercare o interrogare il server LDAP è necessario inviare una richiesta di collegamento. Questo campo controlla il modo in cui viene eseguito il collegamento iniziale al server LDAP. Sono disponibili i seguenti metodi di collegamento:

- **Usa credenziali configurate**

  Utilizzare questo metodo per collegarsi con il DN e la password del client configurati.
- **Usa credenziali di login**

  Utilizzare questo metodo per collegarsi con le credenziali fornite durante il processo di login. L'ID utente può essere fornito mediante un nome distinto (DN, Distinguished Name), un DN parziale, un nome di dominio completo o tramite un ID utente che corrisponde all'attributo di ricerca UID configurato su XClarity Controller. Se le credenziali presentate assomigliano a un DN parziale (ad esempio cn=joe), questo DN parziale verrà presentato al DN radice configurato nel tentativo di

creare un DN che corrisponda al record dell'utente. Se il tentativo di collegamento non riesce, verrà effettuato un ultimo tentativo anteponendo cn= alle credenziali di login e la stringa risultante al DN radice configurato.

Se il collegamento iniziale riesce correttamente, verrà eseguita una ricerca per trovare una voce sul server LDAP appartenente all'utente che si sta collegando. Se necessario, verrà effettuato un secondo tentativo di collegamento, questa volta con il DN recuperato dal record LDAP dell'utente e con la password immessa durante il processo di login. Se il secondo tentativo di collegamento non riesce, l'accesso dell'utente verrà negato. Il secondo collegamento viene eseguito solo se vengono utilizzati i metodi di collegamento **Utilizza credenziali configurate**.

Nome distinto client
Nome distinto (DN) client da utilizzare per il collegamento iniziale. Può essere costituito da un massimo di 300 caratteri.

Password client
Password per il client distinto.

DN radice
Questo è il nome distinto (DN) della voce root della struttura di directory sul server LDAP (ad esempio, dn=società,dc=com). Questo DN viene utilizzato come oggetto di base per tutte le richieste di ricerca.

Attributo di ricerca del nome di login dell'utente
Quando il metodo di collegamento è impostato su **Utilizza credenziali configurate**, il collegamento iniziale al server LDAP è seguito da una richiesta di ricerca che recupera informazioni specifiche sull'utente, compreso il DN utente, le autorizzazioni di login e l'appartenenza al gruppo. Questa richiesta di ricerca deve specificare il nome dell'attributo che rappresenta gli ID utente su tale server. Il nome attributo è configurato in questo campo. Nei server Active Directory il nome dell'attributo è in genere **CN** o **sAMAccountName**. Su server Novell eDirectory e OpenLDAP, il nome dell'attributo è uid. Se questo campo viene lasciato vuoto, il valore predefinito è **sAMAccountName**.

Filtro di gruppi
Il campo **Filtro di gruppi** è utilizzato per l'autenticazione dei gruppi. L'autenticazione dei gruppi viene tentata una volta verificate le credenziali dell'utente. Se l'autenticazione di un gruppo non riesce, l'accesso dell'utente verrà negato. Se si configura il filtro di un gruppo, questo sarà utilizzato per specificare a quali gruppi appartiene XClarity Controller. Ciò significa che, affinché l'autenticazione del gruppo riesca correttamente, l'utente deve appartenere almeno a uno dei gruppi configurati. Se il campo **Filtro di gruppo** viene lasciato vuoto, l'autenticazione del gruppo riuscirà automaticamente. Se il filtro di gruppo è configurato, verrà effettuato un tentativo di corrispondenza di almeno un gruppo nell'elenco a un gruppo a cui appartiene l'utente. Se non c'è alcuna corrispondenza, l'autenticazione dell'utente non riesce e viene negato l'accesso. Se invece esiste almeno una corrispondenza, l'autenticazione del gruppo riesce correttamente.
I confronti sono sensibili al maiuscolo/minuscolo. Il filtro è limitato a 511 caratteri e può essere costituito da uno o più nomi di gruppo. Per delimitare più nomi di gruppi, utilizzare i due punti (:). Gli spazi iniziali e finali vengono ignorati, ma qualsiasi altro spazio viene considerato come parte del nome del gruppo.

Nota: Il carattere jolly (*) non è più considerato come tale. Il concetto di carattere jolly non è più supportato per evitare rischi per la sicurezza. Il nome di un gruppo può essere specificato come DN completo oppure utilizzando solo la parte **cn** . Ad esempio, un gruppo con un DN uguale a cn= adminGroup, dc=mycompany, dc=com può essere specificato utilizzando il DN effettivo o con adminGroup.

Attributo di ricerca gruppi

Il campo **Attributo di ricerca gruppi** specifica il nome dell'attributo utilizzato per identificare i gruppi a cui appartiene un utente. Nei server Active Directory il nome dell'attributo è in genere **memberOf**. Nei server Novell eDirectory il nome dell'attributo è **groupMembership**. Nei server OpenLDAP gli utenti sono solitamente assegnati a gruppi il cui objectClass è uguale a PosixGroup. In questo contesto, questo campo specifica il nome dell'attributo utilizzato per identificare i membri di un determinato PosixGroup. Il nome di questo attributo è **memberUid**. Se questo campo è lasciato vuoto, il nome dell'attributo nel filtro sarà **memberOf**.

Attributo di autorizzazione di login

Quando un utente viene correttamente autenticato mediante un server LDAP, dovranno essere recuperate le autorizzazioni di login per l'utente. Per recuperare le autorizzazioni di login, il filtro di ricerca inviato al server dovrà specificare il nome dell'attributo associato alle autorizzazioni stesse. Il campo **Attributo di autorizzazione di login** specifica il nome attributo. Se si utilizza il server LDAP per l'autenticazione e l'autorizzazione, ma questo campo viene lasciato vuoto, all'utente verrà rifiutato l'accesso.

Il valore dell'attributo restituito dalle ricerche del server LDAP deve essere una stringa di bit immessa come 13 0 o 1 consecutivi oppure una stringa di bit come 13 0 o 1 consecutivi in totale. Ogni bit rappresenta una serie di funzioni. I bit sono numerati in base alle loro posizioni. Il bit più a sinistra è la posizione del bit 0 e il bit più a destra è la posizione del bit 12. Un valore pari a 1 in una posizione di bit abilita la funzione associata a tale posizione di bit. Un valore 0 alla posizione di bit disabilita la funzione associata a tale posizione.

La stringa 0100000000000 è un esempio valido, che viene utilizzato per consentirne l'inserimento in qualsiasi campo. L'attributo che viene utilizzato può consentire una stringa senza formattazione. Quando l'attributo viene recuperato correttamente, il valore restituito dal server LDAP viene interpretato in base alle informazioni riportate nella seguente tabella.

Tabella 1. Bit di autorizzazione

Una tabella con tre colonne contenente le spiegazioni delle posizioni di bit.

Posizione di bit	Funzione	Spiegazione
0	Nega sempre	Un utente non verrà mai autenticato. Questa funzione può essere utilizzata per bloccare un determinato utente associato a un determinato gruppo.
1	Accesso supervisore	All'utente viene assegnato il privilegio da amministratore. L'utente avrà accesso in lettura e scrittura per ogni funzione. Se si imposta questo bit, non sarà necessario impostare singolarmente gli altri bit.
2	Accesso in sola lettura	Un utente ha accesso in sola lettura e non potrà eseguire procedure di manutenzione (ad esempio riavvio, azioni remote o aggiornamenti firmware), né potrà apportare modifiche (ad esempio funzioni di salvataggio, cancellazione o ripristino). La posizione di bit 2 e tutti gli altri bit si escludono a vicenda, ma la posizione di bit 2 ha una precedenza più bassa. Se è impostato un qualsiasi altro bit, questo bit sarà ignorato.
3	Configurazione - Rete e sicurezza del BMC	Un utente può modificare le configurazioni della sicurezza, dei protocolli di rete, dell'interfaccia di rete, delle assegnazioni delle porte e della porta seriale.
4	Gestione account utente	Un utente può aggiungere, modificare o eliminare utenti e modificare le impostazioni globali di login nella finestra Profili di login.
5	Accesso alla console remota	Un utente può accedere alla console del server remoto.

Tabella 1. Bit di autorizzazione (continua)

Posizione di bit	Funzione	Spiegazione
6	Accesso alla console remota e al disco remoto	Un utente può accedere alla console del server remoto e alle funzioni del disco remoto per il server remoto.
7	Accesso accensione/ riavvio del server remoto	Un utente può accedere alle funzioni di accensione e riavvio per il server remoto.
8	Configurazione - Base	Un utente può modificare i parametri di configurazione nelle finestre Impostazioni del sistema e Avvisi.
9	Possibilità di cancellare i log eventi	Un utente può cancellare il log di eventi. **Nota:** Tutti gli utenti possono visualizzare i log di eventi, ma solo l'utente con questo livello di autorizzazione potrà cancellarli.
10	Configurazione - Avanzate (aggiornamento firmware, riavvio BMC, ripristino configurazione)	Un utente non ha limitazioni per la configurazione di XClarity Controller. Inoltre, l'utente avrà accesso in gestione a XClarity Controller. L'utente può eseguire queste funzioni avanzate: aggiornamenti del firmware, avvio della rete PXE, ripristino delle impostazioni predefinite originali dell'adattatore, modifica e ripristino della configurazione dell'adattatore da un file di configurazione e riavvio/reimpostazione dell'adattatore.
11	Configurazione - Sicurezza UEFI	Un utente può configurare le impostazioni correlate alla sicurezza UEFI. Tale operazione può anche essere eseguita nella pagina di configurazione della sicurezza UEFI F1.
12	Riservato	Riservato per un uso futuro e attualmente ignorato.

Se nessuno dei bit è impostato, all'utente verrà rifiutato l'accesso

Nota: Questa priorità è data alle autorizzazioni di accesso richiamate direttamente dal record utente. Se l'utente non dispone di un attributo di autorizzazione al login nel relativo record, verrà eseguito un tentativo di recupero delle autorizzazioni dai gruppi a cui appartiene l'utente e, se configurato, a cui corrisponde il filtro del gruppo. In questo caso, all'utente verrà assegnato l'operatore OR inclusivo di tutti i bit per tutti i gruppi. Allo stesso modo, il bit **Accesso in sola lettura** verrà impostato solo se tutti gli altri bit sono zero. Inoltre, se per uno dei gruppi è impostato il bit **Nega sempre**, all'utente verrà negato l'accesso. Il bit **Nega sempre** ha la precedenza su tutti gli altri bit.

Importante: Se si permette all'utente di modificare le impostazioni di base, di rete e/o di sicurezza correlate ai parametri di configurazione dell'adattatore, si dovrebbe prendere in considerazione la possibilità di consentire allo stesso utente di riavviare XClarity Controller (posizione di bit 10). In caso contrario, senza questa possibilità, un utente potrebbe essere in grado di modificare i parametri (ad esempio, l'indirizzo IP dell'adattatore), ma non di rendere effettive tali modifiche.

3. Se è utilizzata la modalità **Utilizza il server LDAP solo per l'autenticazione (con autorizzazione locale)**, configurare **Gruppi per autorizzazione locale**. Il nome del gruppo, il dominio del gruppo e il ruolo sono configurati per fornire l'autorizzazione locale per i gruppi di utenti. A ogni gruppo può essere assegnato un ruolo (autorizzazioni) identico a quello configurato nei ruoli in Utente locale. Gli account utente vengono assegnati a gruppi diversi sul server LDAP. A un utente viene assegnato il ruolo (autorizzazioni) del gruppo a cui appartiene l'account utente dopo il login a BMC. Il dominio del gruppo deve avere lo stesso formato del nome distinto. Ad esempio, dc=mycompany,dc=com verrà utilizzato come oggetto di base per le ricerche del gruppo. Se il campo viene lasciato vuoto, verrà utilizzato lo stesso valore del campo "DN radice". Altri gruppi possono essere aggiunti facendo clic sull'icona "+". Per eliminare i gruppi, fare invece clic sull'icona "x".
4. Selezionare l'attributo utilizzato per la visualizzazione del nome utente nel menu a discesa **Specifica attributo utilizzato per visualizzare il nome utente**.

Configurazione dei protocolli di rete

Utilizzare le informazioni in questo argomento per visualizzare o configurare le impostazioni di rete per XClarity Controller.

Configurazione delle impostazioni Ethernet

Utilizzare le informazioni in questo argomento per visualizzare o modificare la modalità di comunicazione di XClarity Controller tramite una connessione Ethernet.

Nota: I server AMD non supportano la funzione di failover Ethernet.

XClarity Controller utilizza due controller di rete, Collegati rispettivamente alla porta di gestione dedicata e alla porta condivisa. A ciascuno dei controller di rete è assegnato un indirizzo MAC integrato. Se viene utilizzato DHCP per assegnare un indirizzo IP a XClarity Controller, quando un utente passa tra le porte di rete o quando si verifica un failover dalla porta di rete dedicata alla porta di rete condivisa, è possibile che il server DHCP assegni a XClarity Controller un indirizzo IP differente. Quando si utilizza un server DHCP, è consigliabile che gli utenti si servano del nome host per accedere a XClarity Controller anziché di un indirizzo IP. Anche se le porte di rete di XClarity Controller non vengono modificate, è possibile che il server DHCP assegni un indirizzo IP diverso a XClarity Controller alla scadenza del lease DHCP o al riavvio di XClarity Controller. Se un utente deve accedere a XClarity Controller utilizzando un indirizzo IP che non verrà modificato, è necessario che XClarity Controller sia configurato per un indirizzo IP statico anziché DHCP.

Fare clic su **Rete** in **Configurazione BMC** per modificare le impostazioni Ethernet di XClarity Controller.

Configurazione del nome host di XClarity Controller

Il nome host predefinito di XClarity Controller viene generato tramite la combinazione della stringa "XCC -" seguita dal tipo di macchina server e dal numero di serie del server (ad esempio, "XCC-7X03-1234567890"). È possibile modificare il nome host di XClarity Controller immettendo un massimo di 63 caratteri in questo campo. Il nome host non deve includere punti (.) e può contenere solo caratteri alfabetici, numerici, trattini e caratteri di sottolineatura.

Porte Ethernet

Questa impostazione controlla l'abilitazione delle porte Ethernet utilizzate dal controller di gestione, incluse le porte condivise e dedicate.

Una volta **disabilitata** questa opzione, a tutte le porte Ethernet non verranno assegnati indirizzi IPv4 o IPv6 e verrà impedita qualsiasi ulteriore modifica a qualsiasi configurazione Ethernet.

Nota: Questa impostazione non influisce sull'interfaccia LAN USB o sulla porta di gestione USB nella parte anteriore del server. Tali interfacce dispongono di impostazioni di abilitazione dedicate.

Configurazione delle impostazioni di rete IPv4

Per utilizzare una connessione Ethernet IPv4, effettuare le seguenti operazioni:

1. Abilitare l'opzione **IPv4**.

   Nota: La disabilitazione dell'interfaccia Ethernet impedisce l'accesso a XClarity Controller dalla rete esterna.

2. Nel campo **Metodo**, selezionare una delle seguenti opzioni:
   - **Ottieni indirizzo IP da DHCP**: XClarity Controller otterrà il proprio indirizzo IPv4 da un server DHCP.
   - **Utilizza indirizzo IP statico**: XClarity Controller utilizzerà il valore specificato dall'utente per il proprio indirizzo IPv4.

- **Prima DHCP, quindi indirizzo IP statico**: XClarity Controller tenterà di ottenere il proprio indirizzo IPv4 da un server DHCP, ma nel caso il tentativo non abbia esito positivo utilizzerà il valore specificato dall'utente per il proprio indirizzo IPv4.

3. Nel campo **Indirizzo IPv4 statico** digitare l'indirizzo IP che si desidera assegnare a XClarity Controller.

   Nota: L'indirizzo IP deve contenere quattro numeri interi compresi tra 0 e 255 senza spazi e separati da punti. Questo campo non è configurabile se il metodo è impostato su **Ottieni indirizzo IP da DHCP**.

4. Nel campo **Maschera di rete**, immettere la maschera di sottorete utilizzata da XClarity Controller.

   Nota: La maschera di sottorete deve contenere quattro numeri interi compresi tra 0 e 255 senza spazi o punti consecutivi e separati da punti. L'impostazione predefinita è 255.255.255.0. Questo campo non è configurabile se il metodo è impostato su **Ottieni indirizzo IP da DHCP**.

5. Nel campo **Gateway predefinito**, immettere il router del gateway di rete.

   Nota: L'indirizzo gateway deve contenere quattro numeri interi compresi tra 0 e 255 senza spazi o punti consecutivi e separati da punti. Questo campo non è configurabile se il metodo è impostato su **Ottieni indirizzo IP da DHCP**.

Configurazione delle impostazioni Ethernet avanzata

Selezionare la scheda **Ethernet avanzata** per definire altre impostazioni Ethernet.

Per abilitare l'etichettatura VLAN (Virtual LAN), selezionare la casella di controllo **Abilita VLAN**. Quando la VLAN è abilitata ed è configurato un ID VLAN, XClarity Controller accetta solo i pacchetti con gli ID VLAN specificati. L'ID VLAN può essere configurato con valori numerici compresi tra 1 e 4094.

Nell'elenco **Indirizzo MAC** scegliere una delle seguenti opzioni:

- **Utilizza indirizzo MAC integrato**

  L'indirizzo MAC integrato è un indirizzo fisico univoco assegnato a questo XClarity Controller dal produttore. L'indirizzo è un campo di sola lettura.

- **Utilizzo dell'indirizzo MAC personalizzato**

  Se viene specificato un valore, l'indirizzo gestito in locale sovrascrive l'indirizzo MAC integrato. L'indirizzo gestito in locale deve essere un valore esadecimale compreso tra `00000000000` e `FFFFFFFFFFFF`. Questo valore deve essere in formato **xx:xx:xx:xx:xx:xx**, dove **x** è un numero esadecimale da 0 a 9 oppure un carattere da "a" a "f". XClarity Controller non supporta l'uso di indirizzi multicast. Il primo byte di un indirizzo multicast è un numero dispari (il bit meno significativo è impostato su 1), pertanto il primo byte deve essere un numero pari.

Nel campo **Velocità di trasferimento dati e rete duplex** selezionare **Negoziazione automatica** o **Personalizzata** per specificare la velocità di trasferimento dati e la rete duplex.

Nel campo **MTU (Maximum Transmission Unit)** specificare l'unità di trasmissione massima di un pacchetto (in byte) per la propria interfaccia di rete. La gamma massima dell'unità di trasmissione è compresa tra 1.000 e 1.500. Il valore predefinito per questo campo è 1.500.

Configurazione delle impostazioni di rete IPv6

1. Abilitare l'opzione **IPv6**.
2. Assegnare un indirizzo IPv6 all'interfaccia mediante uno dei seguenti metodi di assegnazione:
   - Utilizzare la configurazione automatica dell'indirizzo senza stato
   - Utilizzare la configurazione dell'indirizzo con stato (DHCPv6)
   - Utilizzare l'indirizzo IP assegnato staticamente

Nota: Quando si sceglie l'opzione **Utilizza indirizzo IP assegnato in modo statico**, verrà chiesto di immettere le seguenti informazioni:

- Indirizzo IPv6
- Lunghezza del prefisso
- Gateway

Configurazione di DNS

Utilizzare le informazioni in questo argomento per visualizzare o modificare le impostazioni DNS (Domain Name System) XClarity Controller.

Fare clic su **Rete** in **Configurazione BMC** per visualizzare o modificare le impostazioni DNS di XClarity Controller.

Se si seleziona la casella di controllo **Utilizza server per indirizzo DNS aggiuntivo**, specificare gli indirizzi IP di un massimo di tre server DNS (Domain Name System) sulla rete. Ogni indirizzo IP deve contenere quattro numeri interi compresi tra 0 e 255 separati da punti. Questi indirizzi dei server DNS vengono aggiunti in cima all'elenco di ricerca, in modo che la ricerca del nome host venga eseguita su questi server prima che il nome venga assegnato automaticamente da un server DHCP.

Se si fa clic sulla casella di controllo **Utilizza DNS per rilevare Lenovo XClarity Administrator**, XClarity Manager deve essere selezionato.

Configurazione di DDNS

Utilizzare le informazioni in questo argomento per abilitare o disabilitare il protocollo DDNS (Dynamic Domain Name System) su XClarity Controller.

Fare clic su **Rete** in **Configurazione BMC** per visualizzare o modificare le impostazioni DDNS di XClarity Controller.

Selezionare la casella di controllo **Abilita DDNS** per abilitare DDNS. Quando DDNS è abilitato, XClarity Controller notifica a un server di nomi di dominio la modifica, in tempo reale, della configurazione server di nomi di dominio attivo dei relativi nomi host configurati, degli indirizzi o di altre informazioni memorizzate sul server stesso.

Scegliere un'opzione dall'elenco di voci per scegliere come si desidera che venga selezionato il nome di dominio di XClarity Controller.

- **Utilizza nome di dominio personalizzato**: è possibile specificare il nome di dominio al quale appartiene XClarity Controller.
- **Utilizza il nome di dominio ottenuto dal server DHCP**: il nome di dominio al quale appartiene XClarity Controller è specificato dal server DHCP.

Configurazione di Ethernet-over-USB

Utilizzare le informazioni in questo argomento per controllare l'interfaccia Ethernet-over-USB utilizzata per la comunicazione in banda tra il server e XClarity Controller.

Fare clic su **Rete** in **Configurazione BMC** per visualizzare o modificare le impostazioni Ethernet-over-USB di XClarity Controller.

Il protocollo Ethernet-over-USB viene utilizzato per le comunicazioni in banda a XClarity Controller. Selezionare la casella di controllo per abilitare o disabilitare l'interfaccia Ethernet-over-USB.

Importante:

- Se si disabilita **Ethernet-over-USB**, non sarà possibile eseguire un aggiornamento in banda del firmware di XClarity Controller o del server utilizzando l'utility di aggiornamento in banda di XClarity Essentials. Utilizzare l'opzione Aggiornamento firmware nell'interfaccia Web di XClarity Controller o l'utility di aggiornamento fuori banda di XClarity Essentials per aggiornare il firmware.
- È importante disabilitare i timeout del Watchdog per evitare che il server si riavvii in modo imprevisto quando l'interfaccia USB in banda è disabilitata.
- Per utilizzare questa interfaccia, è necessario installare i driver del sistema operativo che supportano questa funzione (RNDIS per Windows, cdc_ether e usbnet per Linux). XClarity Controller fornisce un file INF per Windows che consente a Windows di riconoscere il dispositivo USB di XClarity Controller come dispositivo RNDIS.

Selezionare il metodo utilizzato da XClarity Controller per assegnare gli indirizzi agli endpoint dell'interfaccia Ethernet-over-USB.

- **Utilizza l'indirizzo locale del collegamento IPv6 per Ethernet-over-USB**: Questo metodo utilizza gli indirizzi IPv6 basati sull'indirizzo MAC assegnati agli endpoint dell'interfaccia Ethernet-over-USB. In genere, l'indirizzo locale del collegamento IPv6 viene generato utilizzando l'indirizzo MAC (RFC 4862), ma Windows 2008 e i nuovi sistemi operativi 2016 non supportano un indirizzo IPv6 locale del collegamento statico sul lato host dell'interfaccia. Il funzionamento predefinito di Windows prevede invece la rigenerazione causale di indirizzi locali del collegamento durante l'esecuzione. Se l'interfaccia Ethernet-over-USB di XClarity Controller è configurata in modo da utilizzare la modalità dell'indirizzo locale del collegamento IPv6, diverse funzioni che utilizzano questa interfaccia non funzioneranno perché XClarity Controller non conosce l'indirizzo assegnato da Windows all'interfaccia. Se sul server è in esecuzione Windows, utilizzare uno degli altri metodi di configurazione dell'indirizzo Ethernet-over-USB oppure disabilitare il comportamento predefinito di Windows mediante questo comando:
  ```
  netsh interface ipv6 set global randomizeidentifiers=disabled
  ```
- **Configura impostazione IPv4 per Ethernet-over-USB**: Con questo metodo, vengono specificati gli indirizzi IP e la maschera di rete assegnati a XClarity Controller e al lato server dell'interfaccia Ethernet-over-USB.

  Nota:

  – È necessario configurare manualmente l'indirizzo IP dell'interfaccia Ethernet-over-USB nel sistema operativo locale dopo aver configurato l'indirizzo IP di XClarity Controller, l'indirizzo IP del sistema operativo e la maschera di rete.

  – L'impostazione dell'indirizzo IP del sistema operativo viene utilizzata per consentire a XClarity Controller di riconoscere l'estremità opposta della rete Ethernet-over-USB (sistema operativo) ai fini della comunicazione, ad esempio il monitoraggio dello stato Watchdog o l'aggiornamento del firmware in banda.

L'associazione dei numeri di porta Ethernet esterne ai numeri di porta Ethernet-over-USB viene controllata selezionando la casella di controllo **Abilita inoltro porta da Ethernet esterna a Ethernet-over-USB** e completando le informazioni sulla mappatura per le porte da inoltrare dall'interfaccia di rete di gestione sul server.

Configurazione di SNMP

Utilizzare le informazioni in questo argomento per configurare gli agent SNMP.

Completare le seguenti operazioni per configurare le impostazioni degli avvisi SNMP di XClarity Controller.

1. Fare clic su **Rete** in **Configurazione BMC**.
2. Selezionare la casella di controllo corrispondente per abilitare **Agent SNMPv3**, **Trap SNMPv1**, **Trap SNMPv2** e/o **Trap SNMPv3**.

Nota:

- Per abilitare **Agent SNMPv3**, è necessario specificare un contatto e una posizione del BMC.
- Dopo aver abilitato **Agent SNMPv3**, è possibile configurare SNMPv3 per ciascun account utente di XClarity Controller.
- Per ricevere i trap, devono essere abilitati sia i trap SNMP sia l'agent SNMPv3.

3. Se si abilita il **Trap SNMPv1** o il **Trap SNMPv2**, completare i seguenti campi:
   a. Nel campo **Nome della comunità** immettere il nome della comunità. Il campo Nome della comunità non può essere vuoto.
   b. Nel campo **Host**, immettere l'indirizzo dell'host.
4. Se si abilita il **Trap SNMPv3**, completare i seguenti campi:
   a. Nel campo **ID motore**, immettere l'ID del motore. L'ID del motore non può essere vuoto.
   b. Nel campo **Porta di ricezione trap** immettere il numero di porta. Il numero di porta predefinito è 162.
5. Se si abilitano i trap SNMP, selezionare i seguenti tipi di evento per i quali si desidera ricevere un avviso:
   - **Critico**
   - **Attenzione**
   - **Sistema**

   Nota: Fare clic su ciascuna categoria principale per selezionare ulteriormente i tipi di eventi della sotto categoria di cui si desidera visualizzare gli avvisi.
6. Se si abilita **Agent SNMPv3**, completare le seguenti operazioni:
   a. Fare clic su **Utente/LDAP** in **Configurazione BMC**.
   b. Fare clic sul pulsante **Modifica** accanto all'utente corrispondente, quindi selezionare **SNMP** nell'elenco a discesa **Interfaccia accessibile all'utente**.

Nota: Fare clic sul pulsante **Invia** accanto a **Invia trap di verifica** per verificare le impostazioni SNMP.

Abilitazione dell'accesso di rete IPMI

Utilizzare le informazioni in questo argomento per controllare l'accesso di rete IPMI a XClarity Controller.

Completare le seguenti operazioni per abilitare l'accesso IPMI-over-LAN.

1. Fare clic su **Rete** in **Configurazione BMC** per visualizzare o modificare le impostazioni IPMI di XClarity Controller.
2. Fare clic sullo switch **IPMI-over-LAN** in **Abilitazione del servizio e assegnazione delle porte** per abilitare l'accesso di rete IPMI a XClarity Controller.
3. Fare clic su **Utente/LDAP** in **Configurazione BMC**.
4. Fare clic sul pulsante **Modifica** accanto all'utente corrispondente, quindi selezionare **IPMI-over-LAN** nell'elenco a discesa **Interfaccia accessibile all'utente**.

Importante:

- Se non si stanno utilizzando strumenti o applicazioni che accedono a XClarity Controller da rete mediante il protocollo IPMI, si consiglia di disabilitare l'accesso IPMI per una maggiore sicurezza.
- L'accesso IPMI-over-LAN a XClarity Controller è disabilitato per impostazione predefinita.

Configurazione delle impostazioni di rete con i comandi IPMI

Utilizzare le informazioni in questo argomento per configurare le impostazioni di rete tramite i comandi IPMI.

Poiché ciascuna impostazione di rete di BMC è configurata tramite richieste IPMI separate e senza un ordine specifico, BMC avrà una visualizzazione completa di tutte le impostazioni di rete solo dopo che ne viene eseguito il riavvio ai fini dell'applicazione delle modifiche di rete in sospeso. La richiesta di modifica di un'impostazione di rete può avere esito positivo quando viene emessa, ma può essere successivamente considerata non valida, qualora vengano richieste ulteriori modifiche. Se le impostazioni di rete in sospeso risultano incompatibili al riavvio di BMC, le nuove impostazioni non verranno applicate. Al riavvio del BMC, tentare di eseguire l'accesso utilizzando le nuove impostazioni per garantire che siano applicate come previsto.

Abilitazione del servizio e assegnazione delle porte

Utilizzare le informazioni in questo argomento per visualizzare o modificare i numeri di porta utilizzati da alcuni servizi su XClarity Controller.

Fare clic su **Rete** in **Configurazione BMC** per visualizzare o modificare le assegnazioni delle porte di XClarity Controller. Completare i seguenti campi per visualizzare o modificare le assegnazioni delle porte:

HTTPS (Web/Redfish)
Questo elemento è sempre abilitato. In questo campo, specificare il numero di porta per Web-over-HTTPS. Il valore predefinito è 443.

Presenza remota
Questo elemento è sempre abilitato. Il numero di porta è 443.

IPMI-over-LAN
Il numero di porta è 623. Questo campo non è configurabile dall'utente.

Nota: Verificare che **IPMI-over-LAN** sia selezionato e applicato nel campo **Interfaccia accessibile all'utente** per l'utente corrispondente nella pagina Utente/LDAP.

SSDP
Il numero di porta è 1900. Questo campo non è configurabile dall'utente.

SSH
In questo campo specificare il numero di porta configurato per accedere all'interfaccia della riga di comando tramite il protocollo SSH. Il valore predefinito è 22.

Agent SNMP
In questo campo specificare il numero di porta per l'agent SNMP che viene eseguito su XClarity Controller. Il valore predefinito è 161. I numeri di porta validi sono 1-65535.

Nota: Verificare che **SNMP** sia selezionato e applicato nel campo **Interfaccia accessibile all'utente** per l'utente corrispondente nella pagina Utente/LDAP.

Configurazione della restrizione dell'accesso

Utilizzare le informazioni in questo argomento per visualizzare o modificare le impostazioni che permettono di bloccare l'accesso a XClarity Controller dagli indirizzi IP o MAC.

Fare clic su **Rete** in **Configurazione BMC** per visualizzare o modificare le impostazioni di controllo dell'accesso a XClarity Controller.

Elementi bloccati e restrizione di orario

Queste opzioni consentono di bloccare indirizzi IP/Mac specifici per un determinato periodo di tempo.

- **Elenco degli indirizzi IP bloccati**

  - È possibile immettere fino a tre indirizzi o intervalli IPv4 e tre indirizzi o intervalli IPv6 separati da virgole cui non sarà consentito l'accesso a XClarity Controller. Fare riferimento agli esempi IPv4 riportati di seguito:
  - Esempio di indirizzo IPv4 singolo: 192.168.1.1
  - Esempio di indirizzo IPv4 della super-rete: 192.168.1.0/24
  - Esempio di intervallo IPv4: 192.168.1.1 - 192.168.1.5
- **Elenco di indirizzi MAC bloccati**
  - È possibile immettere fino a tre indirizzi MAC separati da virgole cui non sarà consentito l'accesso a XClarity Controller Ad esempio: 11:22:33:44:55:66.
- **Accesso limitato (uso singolo)**
  - È possibile pianificare un intervallo di tempo singolo durante il quale non sarà possibile accedere a XClarity Controller. Per l'intervallo di tempo specificato:
  - La data e l'ora di inizio devono essere successive all'ora XCC corrente.
  - La data e l'ora di fine devono essere successive alla data e all'ora di inizio.
- **Accesso limitato (quotidiano)**
  - È possibile pianificare un o più intervalli di tempo giornalieri durante i quali non sarà possibile accedere a XClarity Controller. Per ogni intervallo di tempo specificato:
  - La data e l'ora di fine devono essere successive alla data e all'ora di inizio.

Elenco di blocchi attivati esternamente

Queste opzioni consentono di configurare il blocco automatico di indirizzi IP (IPv4 e IPv6) specifici da cui il client ha successivamente tentato di eseguire il login a XClarity Controller con nome utente o password non corretta.

Il blocco automatico determina dinamicamente quando eccessivi errori di login provengono da un determinato indirizzo IP e impedisce a tale indirizzo di accedere a XClarity Controller per un periodo di tempo prestabilito.

- **Numero massimo di errori di login da un determinato IP**
  - Il numero massimo di volte indica il numero di errori di login consentiti a un utente con una password errata da un indirizzo IP specifico prima che tale indirizzo venga bloccato.
  - Se l'opzione è impostata su 0, l'indirizzo IP non verrà mai bloccato a causa di errori di login.
  - Il contatore degli errori di login per l'indirizzo IP specifico verrà reimpostato su zero dopo un login riuscito da tale indirizzo IP.
- **Periodo di blocco per il blocco di un IP**
  - Periodo di tempo minimo (in minuti) che deve trascorrere prima che un utente possa tentare di eseguire nuovamente il login da un indirizzo IP bloccato.
  - Se l'opzione è impostata su 0, l'accesso dall'indirizzo IP bloccato resta bloccato finché l'amministratore non lo sblocca in modo esplicito.
- **Elenco blocchi**
  - Nella tabella Elenco blocchi vengono visualizzati tutti gli indirizzi IP bloccati. È possibile sbloccare uno o tutti gli indirizzi IP nell'Elenco blocchi.

Configurazione della porta USB di gestione del pannello anteriore

Utilizzare le informazioni in questo argomento per configurare la porta USB di gestione del pannello anteriore di XClarity Controller.

Il collegamento a XClarity Controller è destinato principalmente a supportare l'uso di un dispositivo mobile su cui è in esecuzione l'app Lenovo XClarity Mobile. Quando si collega un cavo USB tra il dispositivo mobile e il pannello anteriore del server, viene stabilita una connessione Ethernet-over-USB tra l'app mobile in esecuzione sul dispositivo e XClarity Controller.

Su alcuni server la porta USB del pannello anteriore può essere commutata in modo da essere collegata al server o a XClarity Controller.

Nota: Questa funzione sarà supportata in un aggiornamento futuro.

Configurazione delle impostazioni di sicurezza

Utilizzare le informazioni in questo argomento per configurare i protocolli di sicurezza.

Nota: L'impostazione predefinita per la versione minima di TSL è TLS 1.2, ma è possibile configurare XClarity Controller in modo da utilizzare altre versioni di TLS se richiesto dal browser o dalle applicazioni di gestione. Per ulteriori informazioni, consultare "comando tls" a pagina 134.

Fare clic su **Protezione** in **Configurazione BMC** per accedere e configurare le proprietà di sicurezza, lo stato e le impostazioni per XClarity Controller.

Dashboard di sicurezza

Questo argomento è una panoramica del dashboard di sicurezza.

Il dashboard di sicurezza fornisce una valutazione generale sulla sicurezza e lo stato del sistema.

- **Eventi di sicurezza BMC**: segnala eventi di asserzione dei problemi di sicurezza, quali intrusione dello chassis, rilevamento di PFR danneggiati, incongruenza hardware rilevata dal controllo del sistema, ponticello di sicurezza aperto sul planare e così via.
- **Modalità di sicurezza BMC**: fornisce uno stato globale di conformità della modalità di sicurezza.
- **Servizi e porte BMC**: enumerano tutti i servizi/porte non sicuri abilitati ma non conformi alla modalità di sicurezza corrente.
- **Certificati BMC**: elencano tutti i certificati non conformi utilizzati da XCC.
- **Account utente BMC**: forniscono suggerimenti generali su come rendere più sicura la gestione di account e password.

Nota: Il dashboard mostra un'icona di avvertenza se esiste un rischio in queste aree di sicurezza rilevato da XCC. Il collegamento **Dettagli** in ogni categoria porta inoltre l'utente alla pagina di configurazione per risolvere i problemi.

Modalità di sicurezza

Questo argomento è una panoramica della modalità di sicurezza.

La licenza XCC Standard consente agli utenti di configurare i server in una delle due modalità di sicurezza: modalità standard e modalità di compatibilità. Queste opzioni sono disponibili in tutti i server V4.

La licenza di aggiornamento Lenovo XClarity Controller 3 Premier viene fornita con una terza modalità di sicurezza: modalità rigorosa aziendale. Questa modalità è più idonea per requisiti di sicurezza di alto livello.

Nota: Per impostazione predefinita, XCC utilizza un certificato autofirmato ECDSA e sono disponibili solo algoritmi basati su ECDSA. Per utilizzare il certificato basato su RSA, generare una CSR e firmarla con una CA interna o esterna, quindi importare il certificato firmato in XCC.

Modalità di sicurezza rigorosa aziendale

- La modalità di sicurezza rigorosa aziendale è la modalità più sicura.
- Tutti gli algoritmi di crittografia utilizzati da BMC sono conformi a CNSA 1.0.
- BMC opera in modalità di convalida FIPS 140-3.
- Richiede certificati di livello rigoroso aziendale.
- È possibile abilitare solo i servizi che supportano la crittografia CNSA 1.0.
- Richiede l'abilitazione della chiave Feature on Demand.

Modalità di sicurezza standard

- La modalità standard è la modalità di sicurezza predefinita.
- Tutti gli algoritmi di crittografia utilizzati da BMC sono conformi a FIPS 140-3.
- BMC opera in modalità di convalida FIPS 140-3 quando tutti i servizi abilitati utilizzano la crittografia conforme a FIPS 140-3.
- Richiede certificati di livello standard.
- I servizi che richiedono la crittografia e che non supportano la crittografia conforme a FIPS 140-3 sono disabilitati per impostazione predefinita.

Modalità di compatibilità

- La modalità di compatibilità è la modalità da utilizzare quando servizi e client richiedono crittografia non conforme alle modalità rigorosa aziendale/standard.
- È supportata un'ampia gamma di algoritmi di crittografia.
- Quando questa modalità è abilitata, BMC **NON** funziona in modalità di convalida standard.
- Consente di abilitare tutti i servizi.

Suite di crittografia TLS supportate

L'impostazione di crittografia TLS è quella di limitare le suite di crittografia TLS supportate rispetto ai servizi BMC.

Suite di crittografia TLS	Modalità di sicurezza	Versione TLS
TLS_AES_256_GCM_SHA384	• Rigorosa aziendale • Standard* • Compatibilità*	TLS 1.3
TLS_CHACHA20_POLY1305_SHA256	• Compatibilità	TLS 1.3
TLS_AES_128_GCM_SHA256	• Standard • Compatibilità	TLS 1.3
TLS_AES_128_CCM_SHA256	• Standard • Compatibilità	TLS 1.3
TLS_AES_128_CCM_8_SHA256	• Standard • Compatibilità	TLS 1.3

Suite di crittografia TLS	Modalità di sicurezza	Versione TLS
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	• Rigorosa aziendale • Standard* • Compatibilità*	TLS 1.2
TLS_DHE_RSA_WITH_AES_256_GCM_SHA384	• Rigorosa aziendale • Compatibilità*	TLS 1.2
TLS_ECDHE_ECDSA_WITH_AES_256_GCM_ SHA384	• Rigorosa aziendale	TLS 1.2
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	• Standard • Compatibilità	TLS 1.2
TLS_DHE_RSA_WITH_AES_128_GCM_SHA256	• Standard • Compatibilità	TLS 1.2
TLS_ECDHE_ECDSA_WITH_AES_128_GCM_ SHA256	• Standard • Compatibilità	TLS 1.2
TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305	• Compatibilità	TLS 1.2
TLS_ECDHE_ECDSA_WITH_CHACHA20_ POLY1305	• Compatibilità	TLS 1.2
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	• Standard • Compatibilità	TLS 1.2
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256	• Standard • Compatibilità	TLS 1.2
TLS_DHE_RSA_WITH_AES_256_CBC_SHA256	• Standard • Compatibilità	TLS 1.2
TLS_DHE_RSA_WITH_AES_128_CBC_SHA256	• Standard • Compatibilità	TLS 1.2
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_ SHA384	• Standard • Compatibilità	TLS 1.2
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_ SHA256	• Standard • Compatibilità	TLS 1.2
TLS_RSA_WITH_AES_256_GCM_SHA384	• Standard • Compatibilità	TLS 1.2
TLS_RSA_WITH_AES_128_GCM_SHA256	• Standard • Compatibilità	TLS 1.2
TLS_DHE_RSA_LATH_AES_256_GCM_SHA384	• Standard	TLS 1.2

Suite di crittografia TLS	Modalità di sicurezza	Versione TLS
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA3U	• Standard	TLS 1.2
TLS_RSA_WITH_AES_256_CBC_SHA256	• Standard	TLS 1.2
TLS_RSA_WITH_AES_128_CBC_SHA256	• Standard	TLS 1.2

Nota: Le modalità di sicurezza con un asterisco (*) elencate nella tabella richiedono la licenza di aggiornamento Lenovo XClarity Controller 3 Premier.

Matrice di servizio in tre modalità di sicurezza

Funzione/ Servizio	Utilizza la critto-grafia	Stato predefini-to	Supportato in modalità rigorosa	Supportato in modalità standard	Supportato in modalità di compatibilità
IPMI-over-KCS	No	Abilitato	Sì	Sì	Sì
IPMI-over-LAN	Sì	Disabilita-ta	No	Sì	Sì
Trap SNMPv1	No	Non configura-to	No	Sì	Sì
Trap SNMPv3	Sì	Non configura-to	No	Sì Se abilitato, verrà visualizzato un avviso per l'utilizzo della crittografia non FIPS	Sì
Agent SNMPv3	Sì	Non configura-to	No	Sì Se abilitato, verrà visualizzato un avviso per l'utilizzo della crittografia non FIPS	Sì
Avvisi e-mail	Sì	Non configura-to	Sì NON può essere abilitato con autenticazione CRAM-MD5	Sì Se è richiesta l'autenticazione CRAM-MD5, verrà visualizzato un avviso per l'utilizzo della crittografia non FIPS.	Sì
Avvisi Syslog	No	Non configura-to	No	Sì	Sì
TLS 1.2	Sì	Abilitato	Sì	Sì	Sì
TLS 1.3	Sì	Abilitato	Sì	Sì	Sì
Web-over-HTTPS	Sì	Abilitato	Sì	Sì	Sì
Redfish su HTTPS	Sì	Abilitato	Sì	Sì	Sì

Funzione/ Servizio	Utilizza la critto-grafia	Stato predefini-to	Supportato in modalità rigorosa	Supportato in modalità standard	Supportato in modalità di compatibilità
SSDP	No	Abilitato	Sì	Sì	Sì
SSH-CLI	Sì	Abilitato	Sì	Sì	Sì
SFTP	Sì	Disabilita-ta	Sì	Sì	Sì
LDAP	No	Non configura-to	No	Sì	Sì
LDAP sicuro	Sì	Non configura-to	Sì	Sì	Sì
Gestione della chiave di sicurezza	Sì	Non configura-to	Sì	Sì	Sì
Console remota	Sì	Abilitato	Sì	Sì	Sì
Supporti virtuali - CIFS	Sì	Non configura-to	No	Sì	Sì
Supporti virtuali - NFS	No	Non configura-to	No	Sì	Sì
Supporti virtuali - HTTPTF	Sì	Non configura-to	Sì	Sì	Sì
RDOC - Locale	Sì	Non configura-to	Sì	Sì	Sì
RDOC - CIFS	Sì	Non configura-to	No	Sì	Sì
RDOC - HTTP	No	Non configura-to	No	Sì	Sì
RDOC - HTTPS	Sì	Non configura-to	Sì	Sì	Sì
RDOC - FTP	No	Non configura-to	No	Sì	Sì
RDOC - SFTP	Sì	Non configura-to	Sì	Sì	Sì
Caricamento FFDC (SFTP)	Sì	Abilitato	Sì	Sì	Sì
Caricamento FFDC (TFTP)	No	Abilitato	No	Sì	Sì

Funzione/ Servizio	Utilizza la crittografia	Stato predefinito	Supportato in modalità rigorosa	Supportato in modalità standard	Supportato in modalità di compatibilità
Aggiornamento da repository - CIFS	Sì	Non configurato	No	Sì	Sì
Aggiornamento da repository - NFS	No	Non configurato	No	Sì	Sì
Aggiornamento da repository - HTTP	No	Non configurato	No	Sì	Sì
Aggiornamento da repository - HTTPS	Sì	Non configurato	Sì	Sì	Sì
Call Home	Sì	Disabilitata	Sì	Sì	Sì
Password di terze parti	Sì	Non configurato	No	Sì	Sì
Inoltro porta	N/D	Disabilitata	Sì	Sì	Sì

Commutazione della modalità di sicurezza

Utilizzare le informazioni in questa sezione per commutare e convalidare la modalità di sicurezza.

La modalità standard è la modalità di sicurezza predefinita.

In generale, se XCC rileva impostazioni non conformi alla modalità standard, XCC visualizza una notifica ma non richiede all'utente di modificare la modalità. In questo caso, XCC attiverà la modalità di sicurezza standard con sovrascrittura (mancata conformità).

L'utente può aprire il menu a discesa per selezionare la modalità differente e utilizzare la funzione **Convalida** per determinare il numero di elementi non conformi rilevati da XCC.

Quando l'utente fa clic su **Applica**, XCC convalida anche gli elementi conformi.

Panoramica di SSL

Questo argomento è una panoramica del protocollo di sicurezza SSL.

SSL è un protocollo di sicurezza che fornisce privacy nelle comunicazioni. SSL consente alle applicazioni client/server di comunicare in modo da evitare gli accessi non autorizzati, la manomissione e di dati e la contraffazione dei messaggi. È possibile configurare XClarity Controller in modo da utilizzare il supporto SSL per diversi tipi di connessioni, quali server Web sicuro (HTTPS), LDAP sicuro (LDAPS), CIM-over-HTTPS e server SSH, e per gestire i certificati necessari per SSL.

Gestione dei certificati SSL

Questo argomento fornisce informazioni sull'amministrazione dei certificati che possono essere utilizzati con il protocollo di sicurezza SSL.

I client WEB, Redfish e LDAP utilizzano la stessa configurazione del certificato. La connessione SSL deve essere ristabilita ogni volta che si desidera modificare la configurazione del certificato SSL. SSL può essere utilizzato con un certificato autofirmato o con un certificato firmato da un'autorità di certificazione di terze parti. L'utilizzo di un certificato autofirmato è il metodo più semplice per l'utilizzo di SSL, ma al costo di un piccolo rischio per la sicurezza, Dovuto al fatto che il client SSL non ha modo di convalidare l'identità del server SSL per il primo tentativo di connessione tra il client e il server. È possibile che una terza parte malintenzionata possa impersonare il server e intercettare i dati che vengono trasferiti tra XClarity Controller e il browser. Se al momento della connessione iniziale tra il browser e XClarity Controller il certificato autofirmato viene importato nell'archivio certificati del browser, tutte le comunicazioni future saranno sicure per il browser,presumendo che la connessione iniziale non sia stata compromessa da un attacco. Dopo aver utilizzato la pagina Gestione dei certificati SSL per generare una coppia di chiavi e un certificato autofirmato, SSL può essere abilitato.

Per una sicurezza più completa, utilizzare un certificato che viene firmato da un'autorità di certificazione o CA (Certificate Authority). Per ottenere un certificato firmato:

- Selezionare **Genera CSR (richiesta di firma del certificato)** dall'icona **Genera** in **Gestione certificati SSL**.
- Compila i campi obbligatori e seleziona **Genera**.
- Una volta generato, un certificato autofirmato verrà mostrato in **Gestione dei certificati SSL**.
- Selezionare **Scarica CSR (Certificate Signing Request)** dall'icona **Download** per scaricare il certificato firmato.
- Una volta scaricato il certificato firmato, selezionare l'icona **Importa certificato firmato** in **Gestione dei certificati CA** per eseguire l'importazione in XClarity Controller.

La funzione della CA è verificare l'identità di XClarity Controller. Un certificato contiene le firme digitali per la CA e il BMC. Se una CA nota emette il certificato o se il certificato della CA è già stato importato nel browser Web, il browser potrà convalidare il certificato e identificare correttamente il server Web BMC.

SSL confronta il nome host di XClarity Controller (o nome comune) nel certificato con il nome host visualizzato dal browser Web.

Gestione dei certificati SSL

Questo argomento fornisce informazioni su alcune delle azioni selezionabili per la gestione dei certificati con il protocollo di sicurezza SSL.

Fare clic su **Sicurezza** in **Configurazione BMC** per configurare la gestione dei certificati SSL.

Durante la gestione dei certificati di XClarity Controller, viene visualizzato il seguente elenco di azioni:

Scarica certificato firmato

Utilizzare questo collegamento per scaricare una copia del certificato correntemente installato. Il certificato può essere scaricato in formato PEM o DER. Il contenuto del certificato può essere visualizzato utilizzando uno strumento di terze parti come OpenSSL (http://www.openssl.org). La riga di comando per la visualizzazione del contenuto del certificato mediante OpenSSL è simile a quanto riportato nell'esempio di seguito:

```
openssl x509 -in cert.der -inform DER -text
```

Scarica CSR (Certificate Signing Request)

Utilizzare questo collegamento per scaricare una copia della richiesta di firma del certificato. La CSR (Certificate Signing Request, richiesta di firma del certificato) può essere scaricata in formato PEM o DER.

Genera certificato firmato
Genera un certificato autofirmato. Al termine dell'operazione, SSL può essere abilitato utilizzando il nuovo certificato.

Nota: Quando si esegue l'azione **Genera certificato firmato**, viene visualizzata una finestra Genera certificato autofirmato per HTTPS. Verrà richiesto di completare i campi obbligatori e facoltativi. È **necessario** completare i campi obbligatori. Una volta immesse le informazioni, fare clic su **Genera** per completare l'attività.

Genera CSR (Certificate Signing Request)
Genera una CSR (Certificate Signing Request). Al termine dell'operazione è possibile scaricare il file CSR e inviarlo a un'autorità di certificazione (CA) per la firma.

Nota: Quando si esegue l'azione **Genera CSR (Certificate Signing Request)**, viene visualizzata una finestra Genera CSR (Certificate Signing Request) per HTTPS. Verrà richiesto di completare i campi obbligatori e facoltativi. È **necessario** completare i campi obbligatori. Una volta immesse le informazioni, fare clic su **Genera** per completare l'attività.

Importa un certificato firmato
Utilizzare questa opzione per importare un certificato firmato. Per ottenere un certificato firmato, è necessario prima generare una richiesta di firma del certificato (CSR) e inviarla a un'autorità di certificazione.

Configurazione del server Secure Shell

Utilizzare le informazioni in questo argomento per comprendere e abilitare il protocollo di sicurezza SSH.

Fare clic su **Rete** in **Configurazione BMC** per configurare il server Secure Shell.

Per utilizzare il protocollo SSH, è necessario prima generare una chiave per abilitare il server SSH.

Nota:

- Per utilizzare questa opzione non è necessario la gestione dei certificati.
- XClarity Controller creerà inizialmente una chiave server SSH. Se si desidera generare una nuova chiave server SSH, fare clic su **Rete** in **Configurazione BMC**, quindi fare clic su **Genera chiave** in **Server SSH**.
- Dopo aver completato questa azione, è necessario riavviare XClarity Controller per rendere effettive le modifiche.

Accesso IPMI-over-KCS (Keyboard Controller Style)

Utilizzare le informazioni in questo argomento per controllare l'accesso IPMI-over-KCS (Keyboard Controller Style) a XClarity Controller.

XClarity Controller fornisce un'interfaccia IPMI tramite il canale KCS che non richiede alcuna autenticazione.

Fare clic su **Sicurezza** in **Configurazione BMC** per abilitare o disabilitare **Accesso IPMI-over-KCS**.

Nota:

- Dopo aver modificato le impostazioni, sarà necessario riavviare XClarity Controller per renderle effettive.

- **Disabilitato (abilitazione on demand)** disabilita il canale KCS per la maggior parte del tempo, ma consente ad alcuni strumenti Lenovo di scambiare informazioni con XClarity Controller durante la finestra di aggiornamento del firmware di sistema. In questo caso, il canale KCS viene abilitato per alcuni minuti e quindi disabilitato al completamento o al timeout.

Importante: Se non si stanno eseguendo strumenti o applicazioni sul server che accedono a XClarity Controller tramite il protocollo IPMI, si consiglia di disabilitare l'accesso KCS IPMI per una maggiore sicurezza. XClarity Essentials utilizza l'interfaccia IPMI-over-KCS a XClarity Controller. Se l'interfaccia IPMI-over-KCS è stata disabilitata, abilitarla nuovamente prima di eseguire XClarity Essentials su server. Quindi, disabilitare l'interfaccia al termine delle operazioni.

Come impedire il downgrade del firmware di sistema

Utilizzare le informazioni in questo argomento per evitare il downgrade del firmware di sistema.

Questa funzione consente di decidere se permettere o meno l'installazione di un firmware di sistema di livello inferiore rispetto a quello attuale.

Fare clic su **Rete** in **Configurazione BMC** per abilitare o disabilitare **Impedisci il downgrade del firmware di sistema**.

Tutte le modifiche apportate avranno effetto immediato, senza dover attendere il riavvio di XClarity Controller.

Configurazione della gestione delle chiavi di sicurezza (SKM)

Utilizzare le informazioni in questa sezione per creare e gestire le chiavi di sicurezza.

Questa funzione utilizza il server di gestione delle chiavi centralizzato per fornire chiavi che sbloccano l'hardware di storage e per accedere ai dati memorizzati sui SED in un server ThinkSystem. Il server di gestione delle chiavi include SKLM, il server di gestione delle chiavi IBM SED e KMIP, i server di gestione delle chiavi Thales/Gemalto SED (KeySecure e CipherTrust).

Nota: Questa funzione sarà supportata in un aggiornamento futuro.

Security Password Manager

Utilizzare le informazioni in questo argomento per consentire la password di terze parti.

Questa funzione consente all'utente di decidere se consentire o meno l'utilizzo di password di terze parti.

- **Password di terze parti**: una volta abilitata questa funzione, BMC potrà utilizzare un hash della password fornito dall'utente per l'autenticazione.
- **Consenti recupero password di terze parti**: l'utente può inoltre abilitare o disabilitare il recupero dell'hash della password di terze parti dal BMC.

Log di controllo esteso

Utilizzare le informazioni in questo argomento per gestire il log di controllo esteso.

Questa funzione consente di decidere se includere o meno le voci del log del comando IPMI set (dati grezzi) dai canali LAN e KCS nel log di controllo.

Fare clic su **Sicurezza** in **Configurazione BMC** sull'interfaccia utente Web di XCC per abilitare/disabilitare il log di controllo esteso.

Nota: Se il comando IPMI set proviene dal canale LAN, il nome utente e l'indirizzo IP di origine verranno inclusi nel messaggio del log. Tutti i comandi IPMI con dati sensibili per la sicurezza (ad esempio, password) sono invece esclusi.

Limite di login simultanei per l'account utente

Utilizzare le informazioni in questo argomento per limitare le sessioni simultanee per l'account utente.

Questa funzione consente all'utente di decidere il numero di sessioni simultanee consentite per l'account utente.

- **Numero di sessioni simultanee Web**: è possibile impostare da 1 a 10 sessioni.
- **Numero di sessioni simultanee della riga di comando**: è possibile impostare 1 o 2 sessioni.
- **Numero di sessioni simultanee Redfish**: è possibile impostare da 1 a 16 sessioni.

Nota: Se il numero totale di sessioni supera il numero impostato, l'utente non può più creare una nuova sessione.

Controllo del sistema

Questo argomento è una panoramica di Controllo del sistema.

La funzione Controllo del sistema crea un'istantanea dell'inventario dei componenti hardware come riferimento attendibile, quindi monitora le differenze con l'istantanea di riferimento. Quando si verifica un errore, questa funzione può segnalare un evento all'utente e può facoltativamente anche impedire l'avvio del server nel sistema operativo e richiedere una risposta all'utente.

L'utente può creare un'istantanea in qualsiasi momento anche se la funzione è disabilitata. La generazione di istantanee richiede circa un minuto. L'utente può selezionare un sottoinsieme di componenti hardware da applicare e scegliere un'azione corrispondente da intraprendere quando vengono rilevate delle differenze.

Nota: Il rilevamento di differenze viene eseguito all'accensione del server (POST) o al riavvio del sistema. Ad esempio, mentre il sistema operativo è ancora in esecuzione, se un'unità disco viene estratta e quindi ricollegata successivamente, Controllo del sistema non registra l'evento o non esegue alcuna azione. Se l'unità disco estratta non viene rilevata fino al successivo riavvio, la funzione Controllo del sistema interviene.

Nota: Durante il ripristino CA seguito dal primo avvio, XCC non può avvisare UEFI di impedire l'avvio del sistema operativo se vengono soddisfatte le seguenti condizioni:

- Controllo del sistema abilitato con:
  - Hardware di **CPU** o **DIMM** selezionato
  - Opzione **Impedisci avvio del sistema operativo** selezionata
- Una modifica della configurazione hardware non corrispondente a un'istantanea attendibile.

XCC segnala una mancata corrispondenza della configurazione dopo il POST; questa limitazione non persisterà al successivo riavvio del sistema operativo.

Abilitazione del controllo del sistema

Utilizzare le informazioni in questo argomento per abilitare il controllo del sistema.

La funzione Controllo del sistema è disabilitata per impostazione predefinita. È abilitata prima della spedizione in base al requisito dell'utente finale.

L'opzione di reimpostazione dei valori predefiniti di XCC disabilita inoltre la funzione Controllo del sistema e cancella le impostazioni, tranne la cronologia delle istantanee.

Durante l'abilitazione della funzione Controllo del sistema, all'utente viene chiesto di confermare le impostazioni, di utilizzare l'istantanea attendibile esistenti o di acquisire l'inventario come nuova istantanea attendibile prima di attivare la funzione Controllo del sistema. Una volta attivata l'opzione:

- Se il sistema è spento, Controllo del sistema inizia subito a raccogliere l'inventario hardware.
- Se il sistema è acceso, Controllo del sistema confronta i dati di inventario dei componenti con l'istantanea attendibile.

Se il risultato del confronto indica una variazione rispetto all'istantanea attendibile, XCC visualizza un'avvertenza di **Mancata conformità causata dall'errata corrispondenza della configurazione hardware**. I dettagli dell'elenco delle mancate corrispondenze elencano i singoli componenti hardware mancanti/modificati/nuovi con gli attributi di posizione/identificativo/descrizione, confrontati con l'istantanea attendibile.

L'utente può configurare l'ambito e l'azione di Controllo del sistema e decidere quale azione intraprendere in caso di mancata conformità del sistema tramite il pannello Ambito e azione.

Supporto della versione TLS

Utilizzare le informazioni in questo argomento per comprendere le diverse versioni TLS supportate.

Sono supportate le seguenti versioni TLS:

- TLS 1.2 e versioni successive
- TLS 1.3

Per un elenco completo delle suite di crittografia TLS supportate, vedere "Suite di crittografia TLS supportate" a pagina 38.

Backup e ripristino della configurazione BMC

Le informazioni in questo argomento descrivono come ripristinare o modificare la configurazione BMC.

Selezionare **Backup e ripristino** in **Configurazione BMC** per eseguire le seguenti azioni:

- Visualizzare il riepilogo della configurazione del controller di gestione
- Eseguire il backup e il ripristino della configurazione del controller di gestione
- Visualizzare lo stato del backup o del ripristino
- Ripristinare le impostazioni predefinite originali per la configurazione del controller di gestione
- Accedere alla procedura guidata di configurazione iniziale del controller di gestione

Backup della configurazione BMC

Le informazioni in questo argomento descrivono come eseguire il backup della configurazione BMC.

Selezionare **Backup e ripristino** in **Configurazione BMC**. Nella parte superiore si trova la sezione **Backup configurazione BMC**.

Se in precedenza era stato eseguito un backup, i relativi dettagli saranno visualizzati nel campo **Ultimo backup**.

Per eseguire la configurazione BMC di backup corrente, attenersi alla procedura illustrata di seguito:

1. Specificare la password per il file di backup di BMC.
2. Selezionare se si desidera crittografare l'intero file oppure solo i dati sensibili.
3. Iniziare il processo di backup facendo clic su **Avvia backup**. Durante il processo, non è consentito eseguire azioni di ripristino/reimpostazione di alcun tipo.
4. Una volta completato il processo, verrà visualizzato un pulsante che consente di scaricare e salvare il file.

Nota: Quando l'utente imposta un nuovo utente/password di XClarity Controller ed esegue un backup della configurazione vengono inclusi anche account/password predefiniti (`USERID/PASSWORD`). Se si eliminano in un secondo momento account/password predefiniti dalla copia di backup, il sistema visualizzerà un messaggio di notifica per avvisare l'utente che si è verificato un errore di ripristino di account/password di XClarity Controller. Gli utenti possono ignorare questo messaggio.

Ripristino della configurazione BMC

Le informazioni in questo argomento descrivono come ripristinare la configurazione BMC.

Selezionare **Backup e ripristino** in **Configurazione BMC**. Sotto **Configurazione BMC di backup** è presente la sezione **Ripristina BMC dal file di configurazione**.

Per ripristinare una configurazione precedentemente salvata di BMC, attenersi alla procedura riportate di seguito:

1. Selezionare il file di backup e immettere la password quando richiesto, quindi fare clic su **Avanti >**.
2. Verificare il file facendo clic su **Visualizza dettagli**.
3. Dopo aver verificato il contenuto, fare clic su **Avvia ripristino**.

Ripristino dei valori predefiniti originali di BMC

Le informazioni in questo argomento descrivono come ripristinare le impostazioni predefinite originali del BMC.

Selezionare **Backup e ripristino** in **Configurazione BMC**. In **Ripristina BMC dal file di configurazione** è presente la sezione **Ripristino valori predefiniti originali BMC**.

Per eseguire il ripristino di BMC alle impostazioni predefinite, attenersi alla procedura illustrata di seguito:

1. Fare clic su **Avvia per reimpostare BMC ai valori predefiniti**.

   Nota:

   - Solo gli utenti con autorizzazione da supervisore possono eseguire questa azione.
   - La connessione Ethernet viene temporaneamente interrotta. Una volta completata l'operazione di ripristino, è necessario effettuare nuovamente il login dall'interfaccia Web di XClarity Controller.
   - Quando si fa clic su **Avvia per reimpostare BMC ai valori predefiniti**, viene visualizzata una finestra di conferma che permette di selezionare le caselle di controllo per conservare le seguenti impostazioni:
     - **Mantieni impostazioni utente locali**: verrà eseguito il backup di Utente/Ruolo/Impostazione globale corrente. Ripristina il contenuto del comando CLI "users"/"roles"/"accesscfg". Ad esempio: Nome utente/Nome ruolo/Periodo di tempo avviso scadenza password/Regole di complessità password abilitate e così via.

  - **Mantieni impostazioni di rete**: verrà eseguito il backup dell'impostazione di rete corrente. Viene ripristinato l'output di rete del comando CLI "ifconfig". Ad esempio: Nome host/Indirizzo IPv4/ Indirizzo IPv6/Gateway e così via.
- Quando si fa clic su **OK**, tutte le modifiche della configurazione precedenti andranno perse, tranne quelle che si sceglie di conservare.
- Se si desidera abilitare LDAP quando si ripristina la configurazione BMC, è necessario innanzitutto importare un certificato di sicurezza attendibile.
- Di conseguenza, se si sta utilizzando il sistema locale BMC, la connessione TCP/IP andrà persa. Per ripristinare la connettività, sarà necessario riconfigurare l'interfaccia di rete di BMC.
- Una volta che il processo è stato completato, XClarity Controller verrà riavviato.
- Il ripristino delle impostazioni predefinite originali di BMC non avrà impatto sulle impostazioni UEFI e sulla modalità di accesso (utente singolo/multiutente) della console remota (salvata nei cookie del browser).

Riavvio di XClarity Controller

Le informazioni in questo argomento descrivono come riavviare XClarity Controller.

Per dettagli su come riavviare XClarity Controller, vedere "Azioni di alimentazione" a pagina 62.

Capitolo 4. Monitoraggio dello stato del server

Utilizzare le informazioni in questo capitolo per comprendere come visualizzare e monitorare le informazioni per il server a cui si accede.

Una volta eseguito il login a XClarity Controller verrà visualizzata una pagina con lo stato del sistema. In questa pagina, è possibile visualizzare lo stato dell'hardware del server, i log di controllo e i log di eventi, lo stato del sistema, la cronologia di manutenzione e i destinatari degli avvisi.

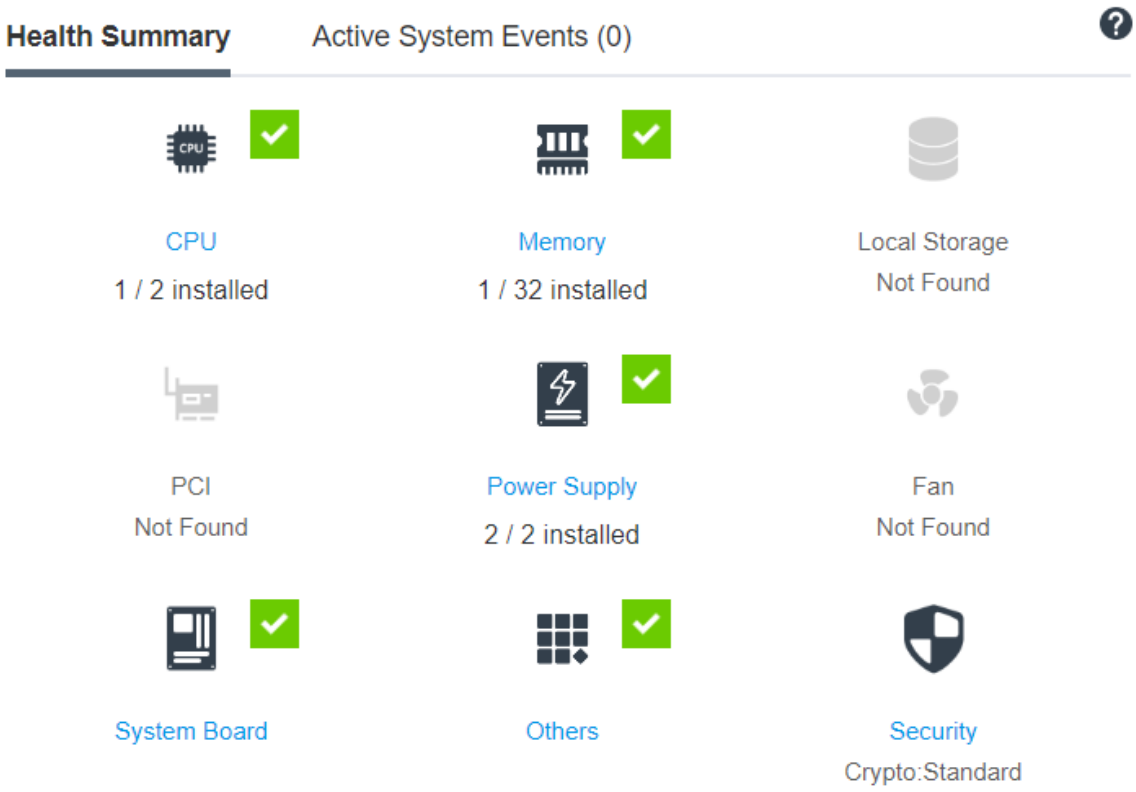
Visualizzazione di Riepilogo integrità/Eventi di sistema attivi

Utilizzare le informazioni in questo argomento per comprendere come visualizzare Riepilogo integrità/Eventi di sistema attivi.

Quando si accede alla home page di XClarity Controller, per impostazione predefinita viene visualizzata la finestra **Riepilogo integrità**. Viene fornita una rappresentazione grafica che mostra il numero di componenti hardware installati e rispettivo stato. I componenti hardware monitorati includono i seguenti:

- CPU (processore)
- Memoria
- Storage locale
- Adattatori PCI
- Alimentatore
- Ventola
- Scheda di sistema
- Altri
- Protezione

Nota: Storage locale potrebbe mostrare **non disponibile** sull'icona di stato sui sistemi con una configurazione del backplane simple-swap.



Se uno dei componenti hardware non funziona normalmente, verrà contrassegnato da un'icona di avvertenza o di condizione critica. Una condizione critica è indicata da un'icona con un cerchio rosso, mentre una condizione di avviso è indicata da un'icona con un triangolo giallo. Quando si posiziona il mouse sull'icona di avviso o di condizione critica, vengono visualizzati fino a tre eventi attualmente attivi per tale componente.

Per visualizzare gli altri eventi, fare clic sulla scheda **Eventi di sistema attivi**. Viene visualizzata una finestra in cui sono riportati gli eventi attualmente attivi nel sistema. Fare clic su **Visualizza tutti i log eventi** per visualizzare l'intera cronologia eventi.

Se il componente hardware è contrassegnato da un segno di spunta verde, funziona normalmente e non esistono eventi attivi.

Il testo al di sotto di un componente hardware indica il numero di componenti installati. Se si fa clic sul testo (collegamento), si verrà indirizzati alla pagina **Inventario**.

Nota: Nei nodi compatibili con lo chassis D3 V2 il collegamento **Alimentazione** è disponibile solo sul nodo care-taker.

Visualizzazione delle informazioni sul sistema

Questo argomento spiega come ottenere un riepilogo delle informazioni comuni sul server.

Il pannello **Informazioni sul sistema e impostazioni** situato a destra della home page fornisce un riepilogo delle informazioni comuni sul server, incluso quanto segue:

- Nome macchina, stato alimentazione e sistema operativo
- Tipo/modello di macchina
- Numero di serie
- Nome di sistema
- Gestione porta USB del pannello anteriore

  Nota: Questa funzione sarà supportata in un aggiornamento futuro.
- Licenza BMC
- Indirizzo IP BMC
- Nome host BMC
- Care-taker chassis attivo

  Nota: Questo elemento è disponibile solo sui nodi compatibili con lo chassis D3 V2.
- Versione BMC
- Versione UEFI
- Posizione

Il server può trovarsi in uno degli stati del sistema riportati nella tabella seguente.

Tabella 2. Descrizioni dello stato del sistema

Tabella a due colonne con intestazioni che documenta gli stati di sistema del server.

Stato	Descrizione
Spegnimento sistema/stato sconosciuto	Il server è spento.
Sistema acceso/UEFI in fase di avvio	Il server è acceso, ma UEFI non è in esecuzione.
Sistema in esecuzione in UEFI	Il server è acceso e UEFI è in esecuzione.
Sistema operativo in fase di avvio o sistema operativo non supportato (il sistema potrebbe trovarsi in questo stato se il sistema operativo non risponde ai ping)	Il server potrebbe trovarsi in questo stato per uno dei seguenti motivi: • Il programma di caricamento del sistema operativo è stato avviato, ma il sistema operativo non è in esecuzione. • L'interfaccia Ethernet-over-USB di BMC è disabilitata. • Il sistema operativo non ha caricato i driver che supportano l'interfaccia Ethernet-over-USB.
Sistema operativo avviato	Il sistema operativo del server è in esecuzione.
Sistema in esecuzione nel test di memoria	Il server è acceso e in esso sono in esecuzione gli strumenti di diagnostica della memoria.

Tabella 2. Descrizioni dello stato del sistema (continua)

Stato	Descrizione
Esecuzione del sistema in modalità di configurazione	Il server è acceso e il sistema è avviato nel menu di configurazione UEFI (F1) o nel menu di LXPM.
Il sistema è in esecuzione in modalità di manutenzione LXPM	Il server è acceso e il sistema si è avviato in modalità di manutenzione di LXPM, che non consente agli utenti di spostarsi nel menu di LXPM.

Se si desidera modificare il nome del sistema, fare clic sull'icona della matita. Digitare il nome del sistema che si desidera utilizzare, quindi fare clic sul segno di spunta verde.

Se il server dispone di una licenza diversa dalla licenza di livello Premier di XClarity Controller, è possibile acquistare un aggiornamento della licenza per abilitare le funzionalità avanzate. Per installare la licenza di upgrade dopo aver ottenuto una licenza di upgrade, fare clic sull'icona della freccia verso l'alto.

Per aggiungere, eliminare o esportare una licenza, fare clic sull'icona della freccia verso destra.

Per modificare le impostazioni pertinenti per le voci per indirizzo IP BMC, nome host BMC, versione UEFI, versione BMC e posizione, fare clic sull'icona della freccia verso destra.

- Per l'indirizzo IP e il nome host, si verrà indirizzati alla sezione **Configurazione Ethernet** in **Rete**.
- Per le voci relative alla versione UEFI e BMC, si verrà indirizzati alla pagina **Aggiornamento firmware**.
- Per la voce relativa alla posizione, si verrà indirizzati alla sezione **Proprietà del server** nella pagina **Configurazione server**.

Visualizzazione dell'utilizzo del sistema

Facendo clic su **Utilizzo** nel riquadro sinistro, viene fornito un riepilogo delle informazioni sull'utilizzo dei server comuni.

L'utilizzo del sistema è una metrica composita basata sull'utilizzo in tempo reale del processore, della memoria e dei sottosistemi I/O. I dati sull'utilizzo possono essere visualizzati nella vista grafica o nella vista tabella, che include le seguenti informazioni:

- **Temperatura**
  - Visualizza la temperatura ambiente in tempo reale e le temperature principali dei componenti.
  - Posizionando il cursore del mouse su un modulo di memoria, viene mostrata la temperatura corrente.
- **Utilizzo dell'alimentazione**
  - Visualizza il grafico a torta del consumo energetico corrente.

  - Posizionando il cursore del mouse sul grafico a torta viene visualizzato il consumo energetico corrente.
  - Il grafico a torta del consumo energetico è costituito da quattro categorie: CPU, memoria, altro e riserva. "Altro" indica il consumo energetico totale del sistema meno il consumo energetico della CPU e della memoria. Per "Riserva" si intende l'alimentazione totale allocata disponibile, meno il consumo energetico totale del sistema.
  - Nella scheda Tensione sono visualizzate le letture della tensione corrente e lo stato su tutti i sensori di tensione supportati dall'hardware.
- **Utilizzo del sistema**
  - Rappresenta l'istantanea di utilizzo corrente dei sottosistemi di sistema, processore, memoria e I/O.

    Nota: Questa funzione sarà supportata in un aggiornamento futuro.
- **Velocità ventola (RPM)**
  - La sezione sulla velocità della ventola mostra la velocità della ventola come percentuale della velocità massima.
  - L'utente può fare clic sull'icona a forma di ingranaggio per accedere alle opzioni **Incremento velocità della ventola**.
    - Questa impostazione consente un ulteriore raffreddamento del server in base alla temperatura ambiente. Può incrementare la ventola normale della velocità mediante l'algoritmo termico controllato. Non ci saranno modifiche se le ventole funzionano già alla massima velocità.

Visualizzazione dei log eventi

Il **log di eventi** fornisce un elenco cronologico di tutti gli eventi di gestione e hardware.

Selezionare la scheda **Log di eventi** in **Eventi** per visualizzare la pagina **Log di eventi**. Tutti gli eventi nel log hanno un formato orario basato sulle impostazioni di data e ora di XClarity Controller. Alcuni eventi generano anche degli avvisi, se configurati in tal senso nella pagina **Destinatari degli avvisi**. È possibile ordinare e filtrare gli eventi nel log di eventi.

Di seguito è riportata una descrizione delle azioni che possono essere eseguite nella pagina **Log di eventi**.

- **Personalizza tabella**: selezionare questa azione per scegliere il tipo di informazioni che si desidera visualizzare nella tabella. Quando data e ora sono identiche per più di un evento è possibile visualizzare un numero sequenziale per determinare più facilmente l'ordine degli eventi.

  Nota: Alcuni numeri sequenziali sono utilizzati dai processi interni del modulo BMC, pertanto è normale che siano presenti intervalli nei numeri sequenziali, quando gli eventi sono ordinati per numero di sequenza.
- **Cancella log**: selezionare questa azione per eliminare i log di eventi.
- **Aggiorna**: selezionare questa azione per visualizzare le voci del log di eventi aggiornate rispetto all'ultima visualizzazione della pagina.
- **Tipo**: selezionare i tipi di eventi da mostrare. Tra i tipi di eventi vi sono:
  -  Mostra voci di errore nel log
  -  Mostra voci di avviso nel log

–  Mostra voci informative nel log

Fare clic su ciascuna icona per attivare o disattivare gli errori da visualizzare. Se si fa clic in modo ciclico sull'icona è possibile attivare e disattivare la visualizzazione degli eventi. Una casella nera che circonda l'icona indica che verrà visualizzato il tipo di evento.

- **Filtro tipo origine**: selezionare una voce dal menu a discesa per visualizzare solo il tipo di voci del log di eventi che si desidera mostrare.
- **Filtro temporale**: selezionare questa azione per specificare l'intervallo degli eventi che si desidera visualizzare.
- **Cerca**: per cercare tipi specifici di eventi o parole chiave, fare clic sull'icona della lente d'ingrandimento e immettere una parola da cercare nella casella **Cerca**. Tenere presente la distinzione tra maiuscole e minuscole per questo campo.

Nota: Il numero massimo di record del log eventi è 1.024. Quando i log eventi sono pieni, la nuova voce del log sovrascriverà automaticamente la voce meno recente.

Visualizzazione dei log di controllo

Il **log di controllo** fornisce un record cronologico degli interventi dell'utente, ad esempio il login a XClarity Controller, la creazione di un nuovo utente e la modifica di una password utente.

È possibile utilizzare il log di controllo per tenere traccia e documentare l'autenticazione, le modifiche e le azioni del sistema.

Sia il log di eventi che il log di controllo supportano azioni simili di manutenzione e visualizzazione. Per visualizzare la descrizione delle azioni di visualizzazione e filtro eseguibili nella pagina Log di controllo, vedere "Visualizzazione dei log eventi" a pagina 55.

Nota:

- Dopo l'esecuzione degli strumenti Lenovo sul sistema operativo del server, è possibile che nel log di controllo siano contenuti record che mostrano le azioni eseguite in base a un nome utente (ad esempio, l'utente "20luN4SB") che potrebbe non essere riconosciuto dall'utente. È possibile che per alcuni strumenti, se eseguiti sul sistema operativo del server, venga creato un account utente temporaneo per accedere a XClarity Controller. L'account viene creato con un nome utente e una password casuali e può essere utilizzato solo per accedere a XClarity Controller sull'interfaccia Ethernet-over-USB interna. L'account può essere utilizzato solo per accedere alle interfacce Redfish e SFTP di XClarity Controller. La creazione e la rimozione di questo account temporaneo sono registrate nel log di controllo, così come tutte le azioni eseguite dallo strumento con queste credenziali.
- Il numero massimo di record del log di controllo è 1.024. Quando i log di controllo sono pieni, la nuova voce del log sovrascriverà automaticamente la voce meno recente.

Visualizzazione della cronologia manutenzione

La pagina **Cronologia manutenzione** include le informazioni sulla cronologia di aggiornamento firmware, configurazione e sostituzione hardware.

Il contenuto della cronologia di manutenzione può essere filtrato per visualizzare determinati tipi di eventi o di intervalli di tempo.

Nota: Il numero massimo di record della cronologia di manutenzione è 250. Quando i log della cronologia di manutenzione sono pieni, la nuova voce del log sovrascriverà automaticamente la voce meno recente.

Configurazione dei destinatari degli avvisi

Utilizzare le informazioni in questo argomento per aggiungere e modificare le notifiche e-mail e syslog o i destinatari trap SNMP.

Nota: Questa funzione sarà supportata in un aggiornamento futuro.

Capitolo 5. Configurazione del server

Utilizzare le informazioni in questo capitolo per comprendere le opzioni disponibili per le configurazioni del server.

Quando si configura il server, sono disponibili le seguenti opzioni principali:

- Adattatori
- Opzioni di avvio
- Criteri di alimentazione
- Proprietà del server
- Chassis

  Nota: Questo elemento è disponibile solo sui nodi compatibili con lo chassis D3 V2.

Visualizzazione delle informazioni sull'adattatore e delle impostazioni di configurazione

Utilizzare le informazioni in questo argomento per visualizzare le informazioni sugli adattatori installati nel server.

Fare clic su **Adattatori** in **Configurazione server** per visualizzare informazioni sugli adattatori installati nel server.

Nota: Se l'adattatore non supporta il monitoraggio dello stato, non sarà visibile per il monitoraggio o la configurazione. Per informazioni relative all'inventario di tutti gli adattatori PCI installati, fare riferimento alla pagina **Inventario**.

Configurazione di modalità e ordine di avvio del sistema

Per configurare la modalità e l'ordine di avvio del sistema, utilizzare le informazioni in questo argomento.

Quando si seleziona **Opzioni di avvio** in **Configurazione server**, è possibile configurare l'ordine di avvio del sistema.

Nota: Non è consentito utilizzare alcun metodo in banda non autenticato per cambiare le impostazioni di sistema correlate alla sicurezza. Ad esempio, Avvio sicuro NON deve essere in grado di configurare su API in banda non autenticate nel sistema operativo o nella shell UEFI. OneCLI non può pertanto essere in esecuzione in banda né acquisire credenziali temporanee mediante IPMI o qualsiasi strumento e API per configurare le impostazioni relative ad Avvio sicuro, al TPM e alla password di configurazione UEFI. Tutte le impostazioni relative alla sicurezza devono richiedere l'autenticazione appropriata con un privilegio sufficiente.

Per configurare l'ordine di avvio del sistema, selezionare un dispositivo dall'elenco **Dispositivi disponibili** e fare clic sulla freccia a destra per aggiungere il dispositivo all'ordine di avvio. Per rimuovere un dispositivo dall'ordine di avvio, selezionarlo dall'elenco dell'ordine di avvio e fare clic sulla freccia a sinistra per spostare di nuovo il dispositivo nell'elenco dei dispositivi disponibili. Per modificare l'ordine di avvio, selezionare un dispositivo e fare clic sulla freccia su o giù per spostare il dispositivo in alto o in basso in base alla priorità desiderata.

Quando si apporta una modifica all'ordine di avvio, prima di applicarla è necessario selezionare un'opzione di riavvio. Sono disponibili le seguenti opzioni:

- **Riavvia il server immediatamente**: le modifiche dell'ordine di avvio vengono salvate e il server viene riavviato immediatamente senza l'arresto del sistema operativo.
- **Riavvia server normalmente**: le modifiche dell'ordine di avvio vengono salvate e il sistema operativo viene arrestato prima del riavvio del server.
- **Riavvia manualmente in un secondo momento**: le modifiche dell'ordine di avvio vengono salvate, ma avranno effetto solo al successivo riavvio del server.

Configurazione dell'avvio singolo

Per ignorare temporaneamente l'avvio configurato ed eseguire l'avvio singolo su un dispositivo specificato, utilizzare le informazioni riportate in questo argomento.

Fare clic su **Opzioni di avvio** in **Configurazione server** e selezionare un dispositivo dal menu a discesa per configurare il dispositivo per cui il sistema eseguirà l'avvio singolo al successivo riavvio del server. Sono disponibili le seguenti opzioni:

Rete PXE
Configura il server per l'esecuzione di un tentativo di avvio di rete PXE (Preboot Execution Environment).

Supporti rimovibili primari
Il server viene avviato dal dispositivo USB predefinito.

CD/DVD predefinito
Il server viene avviato dall'unità CD/DVD predefinita.

Configurazione del sistema F1
Il server viene avviato in Lenovo XClarity Provisioning Manager.

Partizione di diagnostica
Il server viene avviato nella sezione Diagnostica di Lenovo XClarity Provisioning Manager.

Unità disco fisso predefinita
Il server viene avviato dall'unità disco predefinita.

Supporti remoti primari
Il server è stato avviato dai supporti virtuali montati.

Montato
Viene utilizzato l'ordine di avvio configurato. L'avvio singolo non sostituisce l'ordine di avvio di configurato.

Nessun avvio singolo
Viene utilizzato l'ordine di avvio configurato. L'avvio singolo non sostituisce l'ordine di avvio di configurato.

Quando si seleziona una modifica singola all'ordine di avvio, è necessario selezionare un'opzione di riavvio prima di applicare la modifica.

- **Riavvia il server immediatamente**: la modifica dell'ordine di avvio viene salvata e il server viene riavviato immediatamente senza l'arresto del sistema operativo.
- **Riavvia server normalmente**: la modifica dell'ordine di avvio viene salvata e il sistema operativo viene arrestato prima del riavvio del server.
- **Riavvia manualmente in un secondo momento**: la modifica dell'ordine di avvio viene salvata, ma avrà effetto solo al successivo riavvio del server.

Gestione dell'alimentazione del server

Utilizzare le informazioni in questo argomento per visualizzare informazioni sull'alimentazione ed eseguire funzioni di gestione dell'alimentazione.

Selezionare **Criteri alimentazione** in **Configurazione server** per visualizzare le informazioni sulla gestione dell'alimentazione ed eseguire funzioni di gestione dell'alimentazione.

Nota: In un enclosure contenente nodi server ad alta densità, il raffreddamento e l'alimentazione dello chassis sono controllati da SMM anziché da XClarity Controller. Fare riferimento all'interfaccia Web SMM3 per ulteriori dettagli sullo stato dell'alimentazione della soluzione.

Configurazione della ridondanza dell'alimentazione

Per configurare la ridondanza dell'alimentazione, utilizzare le informazioni in questo argomento.

Nota:

- I server AMD non supportano la configurazione della funzione dei criteri per il risparmio di energia.
- Quando sono installate 2 alimentatori, la modalità di ridondanza è impostata su Ridondante (N+N). Con questa configurazione di 2 alimentatori, se uno è in stato di errore, è in condizione di CA persa o è stato rimosso, nel log eventi XCC verrà visualizzato un evento di perdita ridondante.
- Quando dopo la spedizione viene installato solo 1 alimentatore, la modalità di ridondanza verrà automaticamente impostata su Non ridondante.

I campi disponibili nella sezione di ridondanza alimentazione includono quanto segue:

- **Ridondante (N+N)**: sono disponibili due o più fonti di alimentazione indipendenti in grado di fornire alimentazione al sistema contemporaneamente. Ciò significa che se una o più fonti di alimentazione non funzionano, le altre fonti possono continuare a fornire alimentazione al sistema senza interruzioni. La ridondanza N+N fornisce un elevato livello di tolleranza di errore e garantisce che il sistema resti operativo anche in caso di più guasti.
  - **Modalità di output zero**: se questa opzione viene abilitata in Configurazione ridondante, alcuni PSU entreranno automaticamente in stato di standby in condizioni di carico leggero. In questo modo l'alimentatore rimasto fornisce l'intero carico di alimentazione per aumentare l'efficienza.
- **Non ridondante**: in questa modalità l'operatività del server non è garantita in caso di perdita di un alimentatore. L'operatività del server risulterà limitata se un alimentatore non riesce a rimanere in funzione.

Fare clic su **Applica** dopo aver apportato le modifiche alla configurazione.

Configurazione dei criteri di limite alimentazione

Utilizzare le informazioni in questo argomento per configurare i criteri di limite alimentazione.

Nota:

- I server AMD non supportano la configurazione della funzione dei criteri per i limiti alimentazione.
- In un enclosure contenente nodi server ad alta densità, il raffreddamento e l'alimentazione dello chassis sono controllati da SMM anziché da XClarity Controller. Fare riferimento all'interfaccia Web SMM3 per ulteriori dettagli sullo stato dell'alimentazione della soluzione.

È possibile scegliere di abilitare o disabilitare la funzione del limite alimentazione. Se il limite alimentazione è abilitato, è possibile effettuare una selezione per limitare la quantità di alimentazione utilizzata dal server. Se il limite alimentazione è disabilitato, l'alimentazione massima usata dal server è determinata dai criteri di

ridondanza dell'alimentazione. Per modificare l'impostazione, fare in primo luogo clic su **Reimposta**. Scegliere l'impostazione preferita, quindi fare clic su **Applica**.

La capacità di alimentazione totale viene calcolata in base alla modalità di ridondanza dell'alimentazione e al numero di PSU installate nel sistema. L'impostazione manuale del limite di alimentazione massimo può essere superiore alla capacità di alimentazione effettiva.

Quando il limite di alimentazione è abilitato, è possibile che il sistema venga limitato per mantenere il limite di alimentazione.

Nota: Anche con il limite di alimentazione disabilitato, il sistema può essere limitato in determinate condizioni di errore, ad esempio nel caso di un errore di alimentazione, un problema di raffreddamento e così via.

Il limite di alimentazione può essere abilitato utilizzando misurazioni di **Input** o di **Output**. Nel menu a discesa selezionare il tipo di misurazioni che saranno utilizzate per determinare il limite alimentazione. Quando si passa da una misurazione all'altra, il numero sul cursore cambierà di conseguenza.

Esistono due modi di modificare il valore del limite alimentazione:

- **Metodo 1**: spostare il contrassegno del dispositivo di scorrimento verso il wattaggio desiderato per impostare il limite di alimentazione globale del server.
- **Metodo 2**: immettere il valore nella casella di input. Il contrassegno del dispositivo di scorrimento si sposterà automaticamente nella posizione corrispondente.

Fare clic su **Applica** dopo aver apportato le modifiche alla configurazione. Le modifiche avranno effetto immediato.

Configurazione dei criteri di ripristino dell'alimentazione

Per configurare la reazione del sistema in caso di ripristino dell'alimentazione dopo un'interruzione, utilizzare le informazioni riportate in questo argomento.

Quando si configurano i criteri di ripristino dell'alimentazione, sono disponibili le seguenti tre opzioni:

Sempre inattivo
Il server rimarrà spento anche quando viene ripristinata l'alimentazione.

Ripristina
Se il server era acceso nel momento in cui si è verificato il problema di alimentazione, verrà automaticamente acceso al ripristino dell'alimentazione. Altrimenti, il server rimarrà spento quando viene ripristinata l'alimentazione.

Nota: Selezionare la casella di controllo sottostante per impostare un ritardo casuale compreso tra 1 e 15 secondi per Accensione se il server era acceso prima che si verificasse l'interruzione dell'alimentazione.

Sempre attivo
Il server verrà acceso automaticamente una volta ripristinata l'alimentazione.

Fare clic su **Applica** dopo aver apportato le modifiche alla configurazione.

Azioni di alimentazione

Consultare le informazioni in questo argomento per comprendere le azioni di alimentazione che è possibile eseguire sul server.

Fare clic su **Azione di alimentazione** nella sezione **Azione rapida** della home page di XClarity Controller.

La seguente tabella contiene una descrizione delle azioni di alimentazione e riavvio che possono essere eseguite sul server.

Tabella 3. Azioni di alimentazione e descrizioni

Tabella a due colonne contenente le descrizioni delle azioni di alimentazione e riavvio del server.

Azione di alimentazione	Descrizione
Accendi il server	Selezionare questa azione per accendere il server e avviare il sistema operativo.
Spegni il server normalmente	Selezionare questa azione per arrestare il sistema operativo e spegnere il server.
Spegni il server immediatamente	Selezionare questa azione per spegnere il server senza prima arrestare il sistema operativo.
Riavvia il server normalmente	Selezionare questa azione per arrestare il sistema operativo ed eseguire un ciclo di alimentazione del server.
Riavvia il server immediatamente	Selezionare questa azione per eseguire immediatamente un ciclo di alimentazione del server senza prima arrestare il sistema operativo.
Avvia il server con la configurazione del sistema	Selezionare questa azione per accendere o riavviare il server visualizzando automaticamente la configurazione del sistema senza premere F1 durante l'avvio.
Attiva NMI (non-maskable interrupt)	Selezionare questa azione per forzare l'uso di NMI (non-maskable interrupt) su un sistema bloccato. La selezione di questa azione consente al sistema operativo di eseguire un dump di memoria che possa essere utilizzato a scopo di debug della condizione del blocco del sistema. Il riavvio automatico in base all'impostazione di NMI dal menu di configurazione del sistema F1 determina se XClarity Controller riavvierà o meno il server dopo l'uso di NMI.
Pianifica azioni di alimentazione	Selezionare questa azione per pianificare le azioni di accensione e di riavvio del server giornaliere e settimanali.
Riavvia controller di gestione	Selezionare questa azione per riavviare XClarity Controller
Avvio di un ciclo di alimentazione CA sul server	Selezionare questa azione per avviare il ciclo di alimentazione del server.

Nota:

- Se il sistema operativo è in modalità screen saver o bloccato quando viene eseguito un tentativo di arresto, XClarity Controller potrebbe non essere in grado di avviare un arresto normale. XClarity Controller eseguirà quindi un arresto o un ripristino forzato al raggiungimento dell'intervallo di ritardo spegnimento, mentre il sistema operativo potrebbe essere ancora in esecuzione.
- Se il LED di alimentazione sul pannello anteriore lampeggia rapidamente, XClarity Controller potrebbe non essere in grado di avviare una normale sequenza di accensione. XClarity Controller può accendere il sistema quando il LED di alimentazione inizia a lampeggiare lentamente.

Gestione e monitoraggio del consumo dell'alimentazione con i comandi IPMI

Utilizzare le informazioni in questo argomento per gestire e monitorare il consumo dell'alimentazione mediante i comandi IPMI.

Questo argomento descrive come utilizzare Intel Intelligent Power Node Manager e l'interfaccia DCMI (Data Center Manageability Interface) per offrire funzioni di monitoraggio delle specifiche di alimentazione e termiche e di gestione dell'alimentazione basata su criteri per un server che utilizza i comandi di gestione dell'alimentazione IPMI (Intelligent Platform Management Interface).

Per i server che utilizzano Intel Node Manager SPS 3.0, gli utenti di XClarity Controller possono utilizzare i comandi di gestione dell'alimentazione IPMI forniti da Intel Management Engine (ME) per controllare le funzioni di Node Manager e monitorare il consumo energetico del server. La gestione dell'alimentazione del server può anche essere eseguita tramite i comandi di gestione dell'alimentazione di DCMI. Esempi di comandi di gestione dell'alimentazione di DCMI e Node Manager sono forniti in questo argomento.

Gestione dell'alimentazione del server mediante i comandi Node Manager

Utilizzare le informazioni in questo argomento per gestire l'alimentazione del server mediante Node Manager.

Il firmware Intel Node Manager non ha un'interfaccia esterna, pertanto i comandi di Node Manager devono in primo luogo essere ricevuti da XClarity Controller, quindi inviati a Intel Node Manager. XClarity Controller agisce come un dispositivo di trasporto e di inoltro per i comandi IPMI che utilizzano il bridging IPMI standard.

Nota: Se si modificano i criteri del gestore nodi tramite i comandi IPMI di Node Manager è possibile che si creino conflitti con la funzionalità di gestione dell'alimentazione di XClarity Controller. Per impostazione predefinita, il bridging dei comandi di Node Manager è disabilitato per evitare conflitti.

Per gli utenti che desiderano gestire l'alimentazione del server tramite Node Manager anziché XClarity Controller, è disponibile un comando IPMI OEM composto da (funzione di rete: **0x3A**) e (comando: **0xC7**).

Per abilitare i comandi IPMI di Node Manager nativi:`ipmitool -H` **<$XClarity_Controller_IP>** `-U` **<USERID>** `-P` **<PASSW0RD>** `raw` **0x3a 0xc7 0x01**

Per disabilitare i comandi IPMI di Node Manager nativi:`ipmitool -H` **<$XClarity_Controller_IP>** `-U` **<USERID>** `-P` **<PASSW0RD>** `raw` **0x3a 0xc7 0x00**

Le seguenti informazioni sono esempi di comandi di gestione dell'alimentazione di Node Manager.

Nota:

- Specificando IPMI **canale 0** e un indirizzo di destinazione **0x2c**, è possibile utilizzare IPMITOOL per inviare a Intel Node Manager comandi per l'elaborazione. Per avviare un'azione viene utilizzato un messaggio di richiesta e un messaggio di risposta viene restituito al richiedente.
- I comandi vengono visualizzati nel seguente formato a causa di limitazioni di spazio.

Monitoraggio alimentazione tramite Ottieni statistiche alimentazione sistema globali, (codice comando 0xC8): Richiesta:`ipmitool -H` **<$XClarity_Controller_IP>** `-U` **<USERID>** `-P` **<PASSW0RD>** `-b` **0x00** `-t` **0x2c** `raw` **0x2E 0xC8 0x57 0x01 0x00 0x01 0x00 0x00** Risposta:57 01 00 38 00 04 00 41 00 39 00 ec 56 f7 53 5a 86 00 00 50

Limite alimentazione tramite Imposta criteri Intel Node Manager, (codice comando 0xC1): Richiesta: `ipmitool -H` **<$XClarity_Controller_IP>** `-U` **<USERID>** `-P` **<PASSW0RD>** `-b` **0x00** `-t` **0x2c** `raw` **0x2e 0xC1**

0x57 0x01 0x00 0x10 0x01 0xA0 0x00 0x00 0x00 0x60 0xea 0x00 0x00 0x00 0x00 0x1e 0x00 Risposta:57 01 00

Risparmio energetico tramite Imposta criteri Intel Node Manager, (codice comando 0xC1): Richiesta: `ipmitool -H` **<$XClarity_Controller_IP>** `-U` **<USERID>** `-P` **<PASSW0RD>** `-b` **0x00** `-t` **0x2c** `raw` **0x2e 0xC1 0x57 0x01 0x00 0x10 0x01 0x00 0x00 0x00 0x00 0x60 0xea 0x00 0x00 0x00 0x00 0x1e 0x00**

Recupero ID dispositivo tramite Recupera ID dispositivo Intel Management Engine : Richiesta:`ipmitool -H` **<$XClarity_Controller_IP>** `-U` **<USERID>** `-P` **<PASSW0RD>** `-b` **0x00** `-t` **0x2c** `raw` **0x06 0x01**Risposta:50 01 03 05 02 21 57 01 00 05 0b 03 40 20 01

Per ulteriori comandi di Intel Node Manager, consultare l'ultima versione di **Intel Intelligent Power Node Manager, specifiche dell'interfaccia esterna mediante IPMI** all'indirizzo https://businessportal.intel.com.

Gestione dell'alimentazione del server mediante i comandi DCMI

Utilizzare le informazioni in questo argomento per gestire l'alimentazione del server mediante i comandi DCMI.

DCMI offre funzioni di monitoraggio e controllo che possono essere esposte attraverso le interfacce software di gestione standard. Le funzioni di gestione dell'alimentazione server possono anche essere eseguite tramite comandi DCMI.

Le seguenti informazioni rappresentano esempi di comandi e funzioni di gestione dell'alimentazione di DCMI comunemente utilizzati. Per avviare un'azione viene utilizzato un messaggio di richiesta e un messaggio di risposta viene restituito al richiedente.

Nota: I comandi vengono visualizzati nei seguenti formati a causa di limitazioni di spazio.

Ottieni lettura alimentazione: Richiesta:`ipmitool -H` **<$XClarity_Controller_IP>** `-U` **<USERID>** `-P` **<PASSW0RD>** `raw` **0x2c 0x02 0xdc 0x01 0x00 0x00** Risposta:`dc 39 00 38 00 3b 00 39 00 e3 6f 0a 39 e8 03 00 00 40`

Imposta limite alimentazione: Richiesta:`ipmitool -H` **<$XClarity_Controller_IP>** `-U` **<USERID>** `-P` **PASSW0RD** `raw` **0x2c 0x04 0xdc 0x00 0x00 0x00 0x00 0xA0 0x00 0xe8 0x03 0x00 0x00 0x00 0x00 0xe8 0x03** Risposta:`dc`

Ottieni limite alimentazione: Richiesta:`ipmitool -H` **<$XClarity_Controller_IP>** `-U` **<USERID>** `-P` **<PASSW0RD>** `raw` **0x2c 0x03 0xdc 0x00 0x00** Risposta:`dc 00 00 00 a0 00 e8 03 00 00 00 00 01 00`

Attiva limite alimentazione: Richiesta:`ipmitool -H` **<$XClarity_Controller_IP>** `-U` **<USERID>** `-P` **<PASSW0RD>** `raw` **0x2c 0x05 0xdc 0x01 0x00 0x00** Risposta:`dc`

Disattiva limite alimentazione: Richiesta:`ipmitool -H` **<$XClarity_Controller_IP>** `-U` **<USERID>** `-P` **<PASSW0RD>** `raw` **0x2c 0x05 0xdc 0x00 0x00 0x00** Risposta:`dc`

Nota: È possibile che le azioni di eccezione per il comando **Imposta limite alimentazione** non siano supportate su alcuni server. Ad esempio, il parametro per **spegnimento forzato del sistema e registrazione degli eventi nel log eventi di sistema (SEL)** potrebbe non essere supportato.

Per l'elenco completo dei comandi supportati dalla specifica DCMI, consultare l'ultima versione del documento **Specifiche dell'interfaccia di gestione del data center** all'indirizzo https://www.intel.com/content/dam/www/public/us/en/documents/technical-specifications/dcmi-v1-5-rev-spec.pdf.

Download del log dei dati di servizio

Utilizzare le informazioni in questo argomento per raccogliere informazioni sull'assistenza per il server. Questo processo viene in genere effettuato solo su richiesta del personale di assistenza, al fine di risolvere un problema del server.

Nella home page di XClarity Controller fare clic sull'opzione **Log di servizio** nella sezione **Azione rapida** , quindi selezionare **Scarica log dei dati di servizio**.

Per impostazione predefinita, il log di servizio conterrà i seguenti dati: informazioni di sistema, inventario del sistema, utilizzo del sistema, tabella SMBIOS, lettura dei sensori, log eventi, chiave FOD, chiave SLP, configurazione UEFI e configurazione XClarity Controller 3.

Sposta il mouse sull'opzione Informazioni di base e fai clic sulla finestra mobile per visualizzare alcuni dei dati effettivi che verranno esportati.

Sebbene le informazioni di base siano obbligatorie, è possibile esportare anche le seguenti informazioni:

- Informazioni di rete (IP, nome host)
- Telemetria (dati di 24 ore)
- Log di controllo (contiene il nome utente)
- Schermata ultimo errore

Fare clic su **Esporta** per scaricare il log dei dati di servizio.

Il completamento del processo di raccolta dei dati di assistenza e supporto potrebbe richiedere alcuni minuti. Il file verrà salvato nella cartella di download predefinita. La convenzione di denominazione per il file di dati di servizio è la seguente:`<machine type and model>_<serial number>_xcc3_ServiceData_<date>-<time>.zip`

Ad esempio: 7X2106Z01A_2345678_xcc3_ServiceData_240517-112857.zip.

Oltre ai dati di servizio in formato .zip, è anche possibile scaricare il log di debug in formato file .tar.zst tramite **Sfoglia cronologia...** La convenzione di denominazione per il file lodf di debug è la seguente: `<machine type and model>_<serial number>_xcc3_DebugLog_<date>-<time>.tar.zst`

Ad esempio: 7X2106Z01A_2345678_xcc3_DebugLog_240517-112857.zip.

Nota:

- **Sfoglia cronologia...** conserverà inoltre i log di servizio esportati di recente.
- Il formato file .tar.zst utilizza un algoritmo di compressione diverso e può essere estratto con il pacchetto "zstd". Ad esempio:
  `tar --use-compress-program=unzstd -xvf <machine type and model>_<serial number>_xcc3_DebugLog_<date>-<time>.tar.zst`

Proprietà del server

Utilizzare le informazioni in questo argomento per modificare o visualizzare le proprietà relative al server.

Impostazione di posizione e contatto

Utilizzare le informazioni in questo argomento per impostare i vari parametri che permettono di identificare il sistema per le varie operazioni e per il personale di supporto.

Selezionare **Proprietà del server** in **Configurazione server** per configurare le informazioni di **Posizione e contatto**.

Contatto
Consente di specificare il nome e il numero di telefono della persona da contattare qualora si verifichi un problema con il sistema.

Nota: Questo campo è identico al campo Contatto nella configurazione SNMPv3 ed è necessario per abilitare SNMPv3.

Nome rack
Consente di individuare il server più facilmente specificando il rack in cui si trova.

Numero stanza
Consente di individuare il server più facilmente specificando la stanza in cui si trova.

Edificio
Consente di individuare il server più facilmente specificando l'edificio in cui si trova.

U minima
Consente di individuare il server più facilmente specificando la posizione nel rack.

Indirizzo
Consente di specificare l'indirizzo postale completo in cui si trova il server.

Nota: Una volta immesse, le informazioni rilevanti verranno visualizzate su una singola riga nel campo **Posizione** della sezione SNMPv3 e nella home page di XClarity Controller.

Impostazione dei timeout del server

Utilizzare le informazioni in questo argomento per impostare i timeout per il server.

Questi timeout sono utilizzati per ripristinare l'operazione in un server bloccato.

Selezionare **Proprietà del server** in **Configurazione server**, per configurare i timeout del server. Sono disponibili le selezioni di timeout del server seguenti:

Abilita ritardo spegnimento

Utilizzare questo campo per specificare il numero di minuti che il sottosistema BMC deve attendere prima di spegnere il sistema dopo l'arresto del sistema operativo.

Per impostare il valore di timeout per il ritardo spegnimento, selezionare l'intervallo di tempo dal menu a discesa e fare clic su **Applica**. Per disabilitare lo spegnimento forzato in XClarity Controller, selezionare **Nessuno** dal menu a discesa.

Messaggio di sconfinamento

Per creare un messaggio visualizzato quando un utente esegue il login a XClarity Controller, utilizzare le informazioni in questo argomento.

Selezionare **Proprietà del server** in **Configurazione server**. Utilizzare l'opzione **Messaggio di sconfinamento** per configurare un messaggio che si desidera venga visualizzato all'utente. Al termine, fare clic su **Applica**.

Il testo del messaggio verrà visualizzato nell'area Messaggio della pagina di login di XClarity Controller quando un utente esegue il login.

Servizio della soluzione

Utilizzare le informazioni in questo argomento per abilitare o disabilitare il servizio della soluzione.

Nota: Questa funzione sarà supportata in un aggiornamento futuro.

Impostazione di data e ora di XClarity Controller

Utilizzare le informazioni in questo argomento per comprendere le impostazioni di data e ora di XClarity Controller. Vengono fornite istruzioni per configurare la data e ora di XClarity Controller. La data e l'ora di XClarity Controller sono utilizzate per contrassegnare tutti gli eventi registrati nel log eventi e gli avvisi inviati.

Nella home page di XClarity Controller fare clic sull'icona dell'orologio nell'angolo superiore destro per visualizzare o modificare la data e l'ora di XClarity Controller. XClarity Controller non dispone di un proprio orologio in tempo reale. È possibile configurare XClarity Controller in modo da sincronizzare la data e l'ora con un server NTP (Network Time Protocol) o con l'hardware dell'orologio in tempo reale del server.

Sincronizzazione con NTP

Completare le seguenti operazioni per sincronizzare l'orologio di XClarity Controller con il server NTP:

- Selezionare **Sincronizza ora con NTP** e specificare l'indirizzo del server NTP.
- È possibile specificare server NTP aggiuntivi facendo clic sull'icona del segno più ("+").
- Specificare la frequenza in base alla quale si desidera che avvenga la sincronizzazione tra XClarity Controller e il server NTP.
- L'ora restituita dal server NTP è in formato UTC (Coordinated Universal Time).
  - Se si desidera che l'ora e la data di XClarity Controller vengano regolate in base all'area locale, selezionare la differenza di fuso orario per le impostazioni locali dal menu a discesa.
  - Se nella posizione in cui ci si trova è prevista l'ora legale, selezionare la casella di controllo **Imposta automaticamente l'ora legale**.
- Una volta completate le modifiche della configurazione, fare clic su **Applica**.

Sincronizzazione con l'host

È possibile che l'ora nell'hardware dell'orologio in tempo reale del server sia in formato UTC (Coordinated Universal Time) o che sia già regolata e memorizzata nel formato dell'ora locale. Alcuni sistemi operativi memorizzano l'orologio in tempo reale in formato UTC mentre altri memorizzano l'ora nel formato locale. L'orologio in tempo reale del server non indica il formato dell'ora impostato. Pertanto quando XClarity Controller è configurato per la sincronizzazione con l'orologio in tempo reale dell'host, l'utente può scegliere il modo in cui XClarity Controller dovrà utilizzare l'ora e la data ottenute dall'orologio in tempo reale.

- Locale (esempio, Windows): In questa modalità, XClarity Controller considera che l'ora e la data ottenute dall'orologio in tempo reale siano in formato locale, con tutte le differenze di fuso orario e DST già applicate. Se nella posizione in cui ci si trova è prevista l'ora legale, è anche possibile selezionare la casella di controllo **Imposta automaticamente l'ora legale**.
- UTC (esempio, Linux): In questa modalità, XClarity Controller considera che l'ora e la data ottenute dall'orologio in tempo reale siano in formato UTC (Coordinated Universal Time), senza differenze di fuso orario e DST già applicate. In questa modalità è possibile scegliere di regolare l'ora e la data in base all'area locale, selezionando la differenza di fuso orario per le impostazioni locali dal menu a discesa. Se nella posizione in cui ci si trova è prevista l'ora legale, è anche possibile selezionare la casella di controllo **Imposta automaticamente l'ora legale**.
- Una volta completate le modifiche della configurazione, fare clic su **Applica**.

Nota: In corrispondenza dell'ora legale, le azioni pianificate in XClarity Controller per l'intervallo di spostamento in avanti dell'ora non verranno eseguite. Se ad esempio l'inizio dell'ora legale negli Stati Uniti è previsto per le 2:00 del 12 marzo ed è prevista un'azione di alimentazione per le 2:10 del 12 marzo, questa azione non verrà eseguita. Allo scoccare delle ore 2:00, XClarity Controller passerà direttamente alle 3:00.

Configurazione dello chassis D3 V2

Utilizzare le informazioni in questo argomento per comprendere le impostazioni dello chassis D3 V2.

Fare clic su **Chassis** in **Configurazione server** per visualizzare informazioni sullo chassis D3 V2.

Informazioni sullo chassis

In questa sezione sono visualizzate le informazioni sullo chassis, quali UUID, numero di serie, tipo di macchina e versione firmware. Vengono inoltre mostrate le informazioni sui nodi, tra cui il fattore di forma, lo stato dell'alimentazione e l'indirizzo IP.

Nota:

- Fare clic sul pulsante **Reimposta/Riposiziona** accanto al nodo corrispondente per riavviare il nodo o simulare un riposizionamento del nodo fisico.
- Solo il nodo care-taker può reimpostare o riposizionare gli altri nodi.

Ruolo di caretaker dello chassis

In questa sezione sono visualizzate le preferenze di selezione del care-taker dello chassis.

Nota:

- Selezionare **Partecipa al ruolo di care-taker dello chassis** per abilitare un nodo a partecipare al processo di creazione del care-taker. Se è presente un altro nodo indicato come care-taker permanente, non verrà eseguito alcun processo di verifica, tranne se tale nodo non è assente.
- Selezionare **Designa questo nodo come care-taker permanente dello chassis** se si desidera che solo un nodo sia il care-taker. In questo caso, non l'alta disponibilità per il ruolo di care-taker non è presente. Se il nodo care-taker è assente dallo chassis verrà eseguito il processo di creazione del nodo care-taker per selezionare il successivo care-taker adatto.

Cronologia di manutenzione dello chassis

La cronologia di manutenzione dello chassis registra un record dei nodi aggiunti o rimossi nello chassis, nonché il ruolo di care-taker che viene modificato da un nodo a un altro.

Capitolo 6. Funzionalità di console remota

Utilizzare le informazioni in questo argomento per comprendere in che modo visualizzare e interagire da remoto con la console del server.

È possibile utilizzare la funzione di console remota nell'interfaccia Web di XClarity Controller per visualizzare e interagire con la console del server. È possibile assegnare un'immagine del disco (file IMG o ISO) come unità virtuale sul server. La funzionalità di console remota è disponibile con le funzioni di livello Premier di XClarity Controller ed è disponibile solo mediante l'interfaccia Web. Per utilizzare le funzioni di console remota, è necessario eseguire il login a XClarity Controller con un ID utente che dispone dei privilegi di accesso da supervisore o dei privilegi di accesso alla console remota. Per ulteriori informazioni sull'aggiornamento dal livello Standard di XClarity Controller al livello Premier di XClarity Controller, vedere "Aggiornamento di XClarity Controller" a pagina 6.

Utilizzare le funzioni di console remota per:

- Visualizzare da remoto video con risoluzione grafica fino a 1.920 x 1.200, 32 bpp a 60 Hz, indipendentemente dallo stato del server.
- Accedere in remoto al server utilizzando la tastiera e il mouse da un client remoto.
- Montare i file IMG e ISO presenti sul sistema locale o su un sistema remoto come unità virtuali disponibili per l'uso con il server.
- Caricare un'immagine IMG o ISO sulla memoria di XClarity Controller e montarla sul server come unità virtuale. È possibile caricare sulla memoria di XClarity Controller fino a due file con una dimensione totale massima di 100 MB.

Nota:

- Quando la funzione di console remota viene avviata in modalità multiutente (XClarity Controller con il set di funzioni di livello Premier di XClarity Controller supporta fino a sei sessioni simultanee), la funzione del disco remoto può essere eseguita da una sola sessione alla volta.
- La console remota è in grado di visualizzare solo il video generato dal controller video sulla scheda di sistema. Se è installato un adattatore del controller video separato, che viene utilizzato al posto del controller video del sistema, la console remota di XClarity Controller non è in grado di visualizzare il contenuto video dall'adattatore aggiunto.
- Se si dispone di firewall nella rete, è necessario che sia aperta una porta di rete affinché sia supportata la funzione di console remota. Per visualizzare o modificare il numero di porta di rete utilizzato dalla funzione di console remota, vedere "Abilitazione del servizio e assegnazione delle porte" a pagina 35.
- La funzione di console remota utilizza HTML5 per la visualizzazione del video del server sulle pagine Web. Per utilizzare questa funzione, è necessario che il browser in uso supporti la visualizzazione di contenuti video con elementi HTML5.
- Se si utilizzano certificati autofirmati e un indirizzo IPv6 per accedere a BMC con il browser Internet Explorer, l'avvio della sessione di console remota potrebbe non riuscire a causa di un errore del certificato. Per evitare questo problema, è possibile aggiungere il certificato autofirmato alle Autorità di certificazione radice attendibili di Internet Explorer:
  - Selezionare **Sicurezza** in **Configurazione di BMC** e scaricare il certificato autofirmato.
  - Modificare l'estensione del file del certificato in *.crt e fare doppio clic sul file del certificato Web.
  - Cancellare la cache del browser IE11.
  - Fare clic su **Installa certificato** per installare il certificato in Archivio certificati in base ai passaggi dell'Importazione guidata certificati.

Abilitazione della funzionalità di console remota

Questo argomento fornisce informazioni sulla funzionalità di console remota.

La funzionalità della console remota di XClarity Controller è disponibile solo nelle funzioni del livello Premier di XClarity Controller. Se non si dispone dei privilegi per utilizzare la console remota, verrà visualizzata un'icona a forma di lucchetto.

Dopo aver acquistato e ottenuto la chiave di attivazione per l'aggiornamento al livello Premier di XClarity Controller, installarla in base alle istruzioni in "Installazione di una chiave di attivazione" a pagina 87.

Per utilizzare la funzionalità di console remota, fare clic sull'immagine con una freccia bianca in posizione diagonale nella sezione **Anteprima console remota** della home page di XClarity Controller o nella pagina Web **Console remota**.

Controllo di alimentazione remota

Questo argomento descrive come inviare comandi di alimentazione e riavvio del server dalla finestra della console remota.

È possibile inviare i comandi di alimentazione e riavvio del server dalla finestra della console remota senza dover tornare alla pagina Web principale. Per controllare l'alimentazione del server con la console remota, fare clic su **Alimentazione** e selezionare uno dei seguenti comandi:

Accendi il server
Selezionare questa azione per accendere il server e avviare il sistema operativo.

Spegni il server normalmente
Selezionare questa azione per arrestare il sistema operativo e spegnere il server.

Spegni il server immediatamente
Selezionare questa azione per spegnere il server senza prima arrestare il sistema operativo.

Riavvia il server normalmente
Selezionare questa azione per arrestare il sistema operativo ed eseguire un ciclo di alimentazione del server.

Riavvia il server immediatamente
Selezionare questa azione per eseguire immediatamente un ciclo di alimentazione del server senza prima arrestare il sistema operativo.

Avvia il server con la configurazione del sistema
Selezionare questa azione per accendere o riavviare il server visualizzando automaticamente la configurazione del sistema senza premere F1 durante l'avvio.

Cattura della schermata nella console remota

Utilizzare le informazioni in questo argomento per comprendere come utilizzare la funzione di cattura della schermata nella console remota.

La funzione di cattura della schermata nella finestra della console remota cattura i contenuti visualizzati a video del server. Per catturare e salvare una schermata, effettuare le seguenti operazioni:

Passo 1. Nella finestra della console remota fare clic su **Cattura schermata**.

Passo 2. Nella finestra popup fare clic su **Salva file** e premere **OK**. Il file sarà denominato rpviewer.png e sarà salvato nella cartella di download predefinita.

Nota: L'immagine della cattura della schermata viene salvata come tipo di file JPG.

Supporto della tastiera nella console remota

Nella finestra della console remota in **Tastiera** sono disponibili le seguenti opzioni:

- Fare clic su **Tastiera virtuale** per avviare la tastiera virtuale. Questa funzione è utile se si utilizza un dispositivo tablet che non dispone di una tastiera fisica. Le seguenti opzioni possono essere utilizzate per creare macro e combinazioni di tasti da inviare al server. È possibile che il sistema operativo sul sistema client in uso non consenta l'uso di alcune combinazioni di tasti (ad esempio Ctrl+Alt+Canc) e non le trasmetta al server. Altri tasti, come F1 o Esc, possono essere intercettati dal programma o dal browser in uso. Le macro forniscono un meccanismo per inviare al server le sequenze di tasti che l'utente potrebbe non essere in grado di inviare.
- Fare clic su **Macro server** per utilizzare le macro definite del server. Alcune macro del server sono predefinite nel firmware XClarity Controller.

Modalità schermo della console remota

Utilizzare le informazioni in questo argomento per configurare le modalità schermo della console remota.

Per configurare le modalità schermo della console remota, fare clic su **Modalità schermo**.

Sono disponibili le seguenti opzioni di menu:

Schermo intero
Questa modalità riempie il desktop del client con i contenuti visualizzati a video. Premere il tasto ESC in questa modalità per uscire dalla modalità schermo intero. Poiché il menu della console remota non è visibile in modalità schermo intero, sarà necessario uscire dalla modalità schermo intero per utilizzare le funzioni disponibili nel menu della console remota, ad esempio le macro da tastiera.

Adatta a schermo
Impostazione predefinita all'avvio della console remota. In questa impostazione, il desktop di destinazione è visualizzato completamente senza barre di scorrimento. Le proporzioni vengono mantenute.

Metodi di montaggio dei supporti

Utilizzare le informazioni in questo argomento per comprendere come eseguire il montaggio dei supporti.

Sono disponibili tre meccanismi per montare i file IMG e ISO come unità virtuali.

- Le unità virtuali possono essere aggiunte al server dalla sessione della console remota facendo clic su **Supporti**.
- Direttamente dalla pagina Web della console remota, senza stabilire una sessione della console remota.
- Strumento autonomo.

Per poter utilizzare le funzioni dei supporti virtuali, gli utenti devono disporre dei privilegi **Accesso alla console remota e al disco remoto**.

I file possono essere montati come supporti virtuali dal sistema locale o da un server remoto. È inoltre possibile accedervi sulla rete oppure possono essere caricati nella memoria di XClarity Controller tramite la funzione RDOC. Questi meccanismi sono descritti di seguito.

- I supporti locali sono file IMG o ISO situati sul sistema che si utilizza per accedere a XClarity Controller. Questo meccanismo è disponibile solo tramite la sessione della console remota, non direttamente dalla pagina Web della console remota ed è disponibile solo con le funzioni di livello Premier di XClarity Controller. Per montare i supporti locali, fare clic su **Monta tutti i supporti locali** nella sezione **Monta file dei supporti locali**. È possibile montare simultaneamente fino a quattro file sul server.
- I file situati su un sistema remoto possono anche essere montati come supporti virtuali. È possibile montare come unità virtuali fino a quattro file contemporaneamente. XClarity Controller supporta i seguenti protocolli di condivisione file:
  - **CIFS - Common Internet File System**:
    - Immettere l'URL che individua il file sul sistema remoto.
    - Se si desidera che il file venga presentato sul server come supporto virtuale di sola lettura, selezionare la casella di controllo.
    - Immettere le credenziali necessarie per l'accesso di XClarity Controller al file sul sistema remoto.

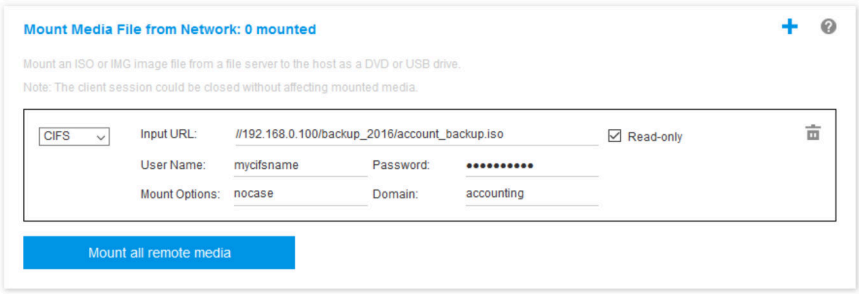
      Nota: XClarity Controller non supporta spazi nel nome utente, nella password o nell'URL. Assicurarsi che le credenziali di login del server CIFS non siano configurate con uno spazio nel nome utente o nella password e che l'URL non contenga uno spazio.
    - Le opzioni di montaggio sono facoltative e sono definite tramite il protocollo CIFS.
    - Se il server remoto appartiene a una raccolta di server, dove la sicurezza è gestita a livello centrale, immettere il nome di dominio a cui appartiene il server remoto.
  - **NFS - Network File System**:
    - Immettere l'URL che individua il file sul sistema remoto.
    - Se si desidera che il file venga presentato sul server come supporto virtuale di sola lettura, selezionare la casella di controllo.
    - Le opzioni di montaggio sono facoltative e sono definite tramite il protocollo NFS. Sono supportati sia NFSv3 che NFSv4. Ad esempio, per utilizzare NFSv3, è necessario specificare l'opzione "nfsvers=3". Se il server NFS utilizza la caratteristica di sicurezza AUTH_SYS per autenticare le operazioni NFS, è necessario specificare l'opzione "sec=sys".
  - **HTTPFS - HTTP Fuse-based File System**:
    - Immettere l'URL che individua il file sul sistema remoto.
    - Se si desidera che il file venga presentato sul server come supporto virtuale di sola lettura, selezionare la casella di controllo.

      Nota: Durante il processo di montaggio potrebbero verificarsi degli errori per i certificati di sicurezza generati da Microsoft IIS. In questo caso vedere "Errori di montaggio dei supporti" a pagina 77.

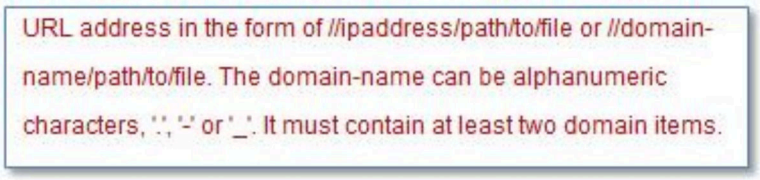
  Fare clic su **Monta tutti i supporti remoti** per montare il file come supporto virtuale. Per rimuovere i supporti virtuali, fare clic sull'icona del cestino a destra dei supporti montati.
- Nella memoria di XClarity Controller è possibile caricare fino a due file, i quali possono essere montati come supporti virtuali utilizzando la funzione RDOC di XClarity Controller. La dimensione totale di entrambi i file non deve superare 100 MB. Questi file rimarranno nella memoria di XClarity Controller finché non verranno rimossi, anche se la sessione della console remota è terminata. La funzione RDOC supporta i seguenti meccanismi durante il caricamento dei file:
  - **CIFS - Common Internet File System**: vedere la descrizione precedente per dettagli. **Esempio**:

    Per montare un file ISO denominato account_backup.iso che si trova nella directory backup_2016 di un server CIFS all'indirizzo IP 192.168.0.100 come un'unità virtuale di sola lettura sul server, è necessario compilare i campi come mostrato nella figura riportata di seguito. In questo esempio, il server all'indirizzo IP 192.168.0.100 è membro di una raccolta di server nel dominio "accounting". Il nome di dominio è opzionale. Se il server CIFS non fa parte di un dominio, lasciare vuoto il campo **Dominio**. In

questo esempio, nel campo **Opzioni di montaggio** viene specificata l'opzione di montaggio CIFS "nocase" per indicare al server CIFS di ignorare la verifica dei caratteri maiuscoli/minuscoli per il nome file. Il campo **Opzioni di montaggio** è facoltativo. Le informazioni immesse dall'utente in questo campo non vengono utilizzate da BMC, ma vengono semplicemente passate al server CIFS quando viene eseguita una richiesta di montaggio. Fare riferimento alla documentazione per l'implementazione del server CIFS per determinare quali opzioni sono supportate dal server CIFS.

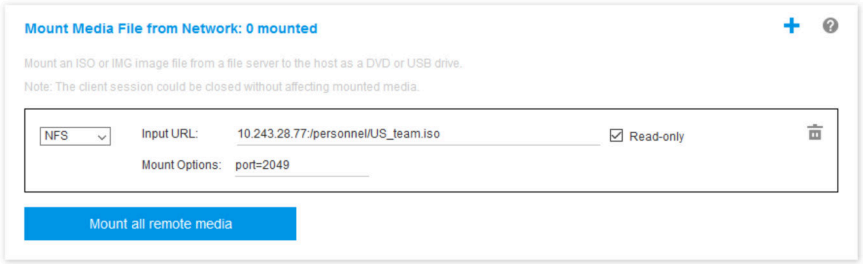


Il BMC fornisce linee guida quando si specifica l'URL. Se l'URL immesso non è valido, il pulsante di montaggio verrà disattivato e sotto il campo dell'URL verrà visualizzato del testo di colore rosso che mostra il formato previsto per l'URL.

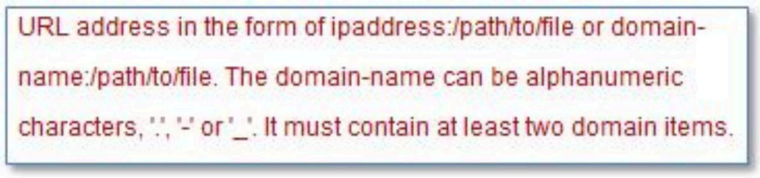


– **NFS - Network File System**: vedere la descrizione precedente per dettagli. **Esempio**:

Per montare un file ISO denominato US_team.iso che si trova nella directory "personnel" di un server NFS all'indirizzo IP 10.243.28.77 come un'unità virtuale di sola lettura sul server, è necessario compilare i campi come mostrato nella figura riportata di seguito. L'opzione di montaggio NTF "port= 2049" specifica che deve essere utilizzata la porta di rete 2049 per trasferire i dati. Il campo **Opzioni di montaggio** è facoltativo. Le informazioni immesse dall'utente in questo campo vengono passate al server NFS quando viene eseguita una richiesta di montaggio. Fare riferimento alla documentazione per l'implementazione del server NFS per determinare quali opzioni sono supportate dal server NFS.



Il BMC fornisce linee guida quando si specifica l'URL. Se l'URL immesso non è valido, il pulsante di montaggio verrà disattivato e sotto il campo dell'URL verrà visualizzato del testo di colore rosso che mostra il formato previsto per l'URL.

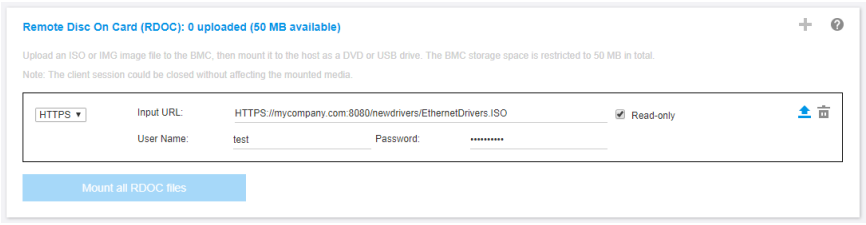


- **HTTPS - Hypertext Transfer Protocol Secure**:
  - Immettere l'URL che individua il file sul sistema remoto.
  - Se si desidera che il file venga presentato sul server come supporto virtuale di sola lettura, selezionare la casella di controllo.
  - Immettere le credenziali necessarie per l'accesso di XClarity Controller al file sul sistema remoto.

  Nota:

  - Durante il processo di montaggio potrebbero verificarsi degli errori per i certificati di sicurezza generati da Microsoft IIS. In questo caso vedere "Errori di montaggio dei supporti" a pagina 77.
  - XClarity Controller non supporta spazi nel nome utente, nella password o nell'URL. Assicurarsi che le credenziali di login del server CIFS non siano configurate con uno spazio nel nome utente o nella password e che l'URL non contenga uno spazio. **Esempio**:

    Per montare un file ISO denominato EthernetDrivers.ISO che si trova nella directory "newdrivers" di un server HTTPS con nome di dominio "mycompany.com" utilizzando la porta di rete 8080 come unità virtuale di sola lettura sul server, è necessario compilare i campi come mostrato nella figura riportata di seguito.



    Il BMC fornisce linee guida quando si specifica l'URL. Se l'URL immesso non è valido, il pulsante di montaggio verrà disattivato e sotto il campo dell'URL verrà visualizzato del testo di colore rosso che mostra il formato previsto per l'URL.

    URL address in the form of https://ipaddress[:port]/path/to/file or HTTPS://domain-name[:port]/path/to/file. The domain-name can be alphanumeric characters, '.', '-' or '_'. It must contain at least two domain items. The port number is optional

- **SFTP - SSH File Transfer Protocol**
  - Immettere l'URL che individua il file sul sistema remoto.
  - Se si desidera che il file venga presentato sul server come supporto virtuale di sola lettura, selezionare la casella di controllo.
  - Immettere le credenziali necessarie per l'accesso di XClarity Controller al file sul sistema remoto.

  Nota:

  - XClarity Controller non supporta spazi nel nome utente, nella password o nell'URL. Assicurarsi che le credenziali di login del server CIFS non siano configurate con uno spazio nel nome utente o nella password e che l'URL non contenga uno spazio.

  - Quando XClarity Controller si connette a un server HTTPS, viene visualizzata una finestra popup con le informazioni del certificato di sicurezza utilizzato dal server HTTPS. XClarity Controller non è in grado di verificare l'autenticità del certificato di sicurezza.
- **LOCALE - Common Internet File System**:
  - Cercare nel sistema il file ISO o IMG che si desidera montare.
  - Se si desidera che il file venga presentato sul server come supporto virtuale di sola lettura, selezionare la casella di controllo.

Fare clic su **Monta tutti i file RDOC** per montare il file sotto come supporto virtuale. Per rimuovere i supporti virtuali, fare clic sull'icona del cestino a destra dei supporti montati.

Strumento autonomo

Gli utenti che richiedono il montaggio di dispositivi o immagini (.iso/.img) mediante XClarity Controller possono utilizzare la parte di codice autonoma rdmount del pacchetto OneCLI. Nello specifico, il comando rdmount consente di aprire una connessione a XClarity Controller e di montare il dispositivo o le immagini sull'host.

rdmount ha la seguente sintassi:

```
rdmount -s ip_address -d <iso or device path> -l <userid> -p <password> -w port (443)
```

Esempio per il montaggio di un file iso:

```
$sudo ./rdmount -s 10.243.11.212 -d /home/user/temp/SLE-15-Installer-DVD-x86_64-RC2-DVD1.iso -l userid -p password -w 443
```

Errori di montaggio dei supporti

Utilizzare le informazioni in questo argomento per risolvere i problemi di montaggio dei supporti.

Durante il processo di montaggio potrebbero verificarsi degli errori se si utilizzano certificati di sicurezza generati da Microsoft IIS. In questo caso, sostituire il certificato di sicurezza con un nuovo certificato generato da openssl. In particolare, il file pfx appena generato viene caricato nel server Microsoft IIS.

Di seguito è riportato un esempio che mostra come viene generato il certificato di sicurezza tramite openssl nel sistema operativo Linux.

```
$ openssl
OpenSSL>

$ openssl genrsa 1024 > server.key
Generating RSA private key, 1024 bit long modulus
.....++++++
.....++++++
e is 65537 (0x10001)

$ openssl req -new -key server.key > server.csr
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:CN
State or Province Name (full name) [Some-State]:BJ
Locality Name (eg, city) []:HD
Organization Name (eg, company) [Internet Widgits Pty Ltd]:Lenovo
```

```
Organizational Unit Name (eg, section) []:Lenovo
Common Name (e.g. server FQDN or YOUR name) []:10.245.18.66
Email Address []:test@test.com

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:LNV

$ ls
server.csr  server.key

$ openssl req -x509 -days 3650 -key server.key -in server.csr > server.crt
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:CN
State or Province Name (full name) [Some-State]:BJ
Locality Name (eg, city) []:BJ
Organization Name (eg, company) [Internet Widgits Pty Ltd]:LNV
Organizational Unit Name (eg, section) []:LNV
Common Name (e.g. server FQDN or YOUR name) []:10.245.18.66
Email Address []:test@test.com

$ ls
server.crt  server.csr  server.key

$ openssl pkcs12 -export -out server.pfx -inkey server.key -in server.crt
Enter Export Password:
Verifying - Enter Export Password:

$ ls
server.crt  server.csr  server.key  server.pfx
```

Uscita dalla sessione della console remota

Questo argomento descrive come uscire dalla sessione della console remota.

Per uscire dalla sessione della console remota, chiudere le finestre delle sessioni dei supporti virtuali e della console remota.

Capitolo 7. Configurazione dello storage

Utilizzare le informazioni in questo capitolo per comprendere le opzioni disponibili per le configurazioni dello storage.

Quando si configura lo storage, sono disponibili le seguenti opzioni principali:

- Dettagli dello storage
- Configurazione RAID

Dettagli dello storage

Utilizzare le informazioni in questo argomento per eseguire la funzione Dettagli dello storage.

Questa funzione visualizza la struttura fisica e la configurazione dello storage dei dispositivi di storage corredate di dettagli come posizione, produttore, nome del prodotto, stato, capacità, interfaccia, supporto, fattore di forma e altre informazioni.

Un avviso o un evento critico verrà attivato quando il valore della durata residua dell'unità SSD raggiunge la soglia o è inferiore. Il valore di durata residua predefinito per l'avviso e l'evento critico è rispettivamente dell'8% e del 4%. Fare clic sull'icona a forma di ingranaggio accanto a **Dettagli dello storage** per impostare il valore di soglia.

Per configurare i backplane SAS/SATA/NVMe (AnyBay) che supportano la modalità **Corsia PCIe x1**, fare clic sull'icona a forma di ingranaggio accanto a **Backplane**, quindi selezionare il gruppo dei vani delle unità e fare clic sul pulsante **Applica** per salvare la configurazione.

Configurazione RAID

Utilizzare le informazioni in questo argomento per eseguire le funzioni di configurazione RAID.

Utilizzare le informazioni in questo argomento per visualizzare e configurare i pool di storage, i volumi associati e le unità dell'adattatore RAID. Se il sistema è spento, accenderlo per visualizzare le informazioni RAID.

Visualizzazione e configurazione delle unità virtuali

Utilizzare le informazioni in questo argomento per visualizzare e configurare le unità virtuali.

Quando si seleziona **Configura RAID** in **Configurazione server**, la scheda **Configurazione array** verrà selezionata e i dischi virtuali esistenti verranno visualizzati per impostazione predefinita. Le unità logiche vengono ordinate per controller e array disco. Vengono visualizzate le informazioni dettagliate sul disco virtuale, ad esempio la dimensione di striping del disco virtuale e le informazioni sul disco virtuale avviabile.

Per configurare le impostazioni RAID, fare clic su **Abilita modalità di modifica**.

Nella modalità di modifica è possibile fare clic sul menu di azione del controller, per visualizzare i dischi virtuali RAID correnti e creare nuovi dischi virtuali RAID.

Nel menu Azioni controller è possibile effettuare le seguenti operazioni:

Cancella configurazione RAID

Cancella la configurazione e i dati sul controller selezionato.

Importa unità esterne
Importa le unità esterne che sono state rilevate. Un'unità esterna è un'unità che è stata spostata da una configurazione RAID differente al controller RAID corrente

Nota: Se non vengono rilevate unità esterne, si riceverà una notifica.

Gestisci configurazione esterna
Importa le unità esterne che sono state rilevate. Un'unità esterna è un'unità che è stata spostata da una configurazione RAID differente al controller RAID corrente

Nota: Se non vengono rilevate unità esterne, si riceverà una notifica.

Le informazioni dei dischi virtuali RAID correnti per un controller specifico sono riportate nelle rispettive "Schede disco virtuali". In ogni scheda sono visualizzate informazioni come il nome, lo stato, la capacità e le azioni del disco virtuale. L'icona della matita consente di modificare le informazioni e l'icona del cestino consente di eliminare le "Schede disco virtuali".

Nota: La capacità e il livello RAID non possono essere modificati.

Se si fa clic sul nome del disco virtuale, verrà visualizzata una finestra delle proprietà del disco virtuale.

Creazione di un nuovo disco virtuale RAID

Per creare un nuovo disco virtuale RAID, attenersi alla procedura riportata di seguito:

Nota: Se la capacità di storage non è sufficiente, non sarà possibile creare un nuovo disco virtuale.

1. **Selezionare le unità o un array di dischi con capacità di storage disponibile**
   a. Quando si crea un disco virtuale in un nuovo array di dischi, è necessario specificare il livello RAID.

      Nota: Se non sono disponibili unità sufficienti da selezionare e si fa clic su **Avanti**, verrà visualizzato un messaggio di errore nel campo di livello RAID.

   b. Per alcuni livelli RAID, è richiesto un intervallo. È inoltre necessario che nell'intervallo sia presente una quantità minima di unità. Per tali situazioni, specificare il numero di intervallo nel campo **Numero intervallo**, selezionare **Membro** o **Hot-spare** dal menu a discesa accanto alle unità, quindi selezionare la casella di controllo accanto alle unità che verranno utilizzate per creare il disco virtuale.
   c. Per creare dischi virtuali in un array di dischi esistente, è necessario selezionare un array di dischi con capacità libera.
2. **Creare di un disco virtuale**
   a. Per impostazione predefinita, la creazione di un disco virtuale utilizzerà tutta la capacità di storage. L'icona **Aggiungi** è disabilitata se tutto lo storage è utilizzato. È possibile fare clic sull'icona della matita per modificare la capacità o altre proprietà.
   b. Quando si modifica il primo disco virtuale per utilizzare parte della capacità di storage, l'icona **Aggiungi** viene abilitata. Fare clic sull'icona per aprire la finestra **Aggiungi disco virtuale**.
   c. Fare clic sull'icona **Rimuovi** per rimuovere un disco virtuale. Questa icona non verrà visualizzata se è presente un solo disco virtuale. Quando si fa clic sull'icona **Rimuovi**, la riga selezionata verrà immediatamente eliminata. Non verrà visualizzata alcuna finestra di conferma poiché il disco virtuale non è stato ancora creato.
   d. Fare clic su **Avvia creazione** per avviare il processo.

Nota: Quando il controller non è supportato, verrà visualizzato un messaggio.

Visualizzazione e configurazione dell'inventario di storage

Utilizzare le informazioni in questo argomento per visualizzare e configurare l'inventario di storage.

Nella scheda **Inventario storage** è possibile visualizzare e configurare gli array di dischi, i dischi virtuali associati e le unità disco per il controller RAID.

- **Per i dispositivi di storage che supportano la configurazione RAID**:
  1. Se il controller include gli array di dischi configurati, verranno visualizzate le unità installate in base all'array di dischi. Di seguito sono descritti gli elementi visualizzati nella finestra.
     - **Titolo della tabella**: mostra ID dell'array di dischi, livello RAID e numero totale di unità.
     - **Contenuto della tabella**: elenca le proprietà di base, come nome dell'unità, stato dell'unità, tipo, prodotto, produttore, numero di serie e azioni. È possibile accedere alla pagina **Inventario** per visualizzare tutte le proprietà che possono essere rilevate da XClarity Controller.
     - **Azioni**: di seguito sono riportate le azioni che possono essere eseguite. Alcune azioni non saranno disponibili quando l'unità si trova in uno stato differente.
       - **Assegna hot-spare**: specifica l'unità come hot-spare globale o hot-spare dedicato.
       - **Rimuovi hot-spare**: rimuove l'unità dall'hot-spare.
       - **Imposta unità disco come offline**: imposta l'unità su offline.
       - **Imposta unità disco come online**: imposta l'unità su online.
       - **Avvia ricostruzione**: ricostruisce RAID.
       - **Imposta unità disco come riutilizzabile**: imposta l'unità come riutilizzabile.
       - **Imposta unità disco come mancante**: imposta l'unità come mancante.
       - **Imposta unità come valida su JBOD**: aggiunge l'unità a JBOD.
       - **Imposta unità non configurata come valida**: rende l'unità disponibile per essere configurata in un array o per l'utilizzo come hot-spare di emergenza.
       - **Imposta unità non configurata come non valida**: contrassegna l'unità non valida, impedendo che venga utilizzata in un array o come hot-spare di emergenza.
       - **Imposta unità disco come pronta per la rimozione**: imposta l'unità per la rimozione.
  2. Le eventuali unità che non sono state ancora configurate incluse nel controller verranno visualizzate nella tabella **Unità disco non RAID**. Se si fa clic sull'opzione **Converti JBOD in Pronto per la configurazione**, verrà visualizzata una finestra in cui sono riportate tutte le unità che supportano questa azione. È possibile selezionare una o più unità da convertire.

Per i dispositivi di storage che non supportano la configurazione RAID: XClarity Controller potrebbe non essere in grado di rilevare le proprietà di alcune unità.

Capitolo 8. Aggiornamento del firmware del server

Utilizzare le informazioni in questo argomento per aggiornare il firmware del server.

Panoramica dell'aggiornamento firmware

Informazioni generali sull'aggiornamento del firmware del server.

Facendo clic su **Aggiorna firmware** nel riquadro sinistro, viene fornita una panoramica delle informazioni sul firmware.

- **Aggiornamento da repository:** sincronizzazione del firmware del server con il repository remoto CIFS/NFS per l'aggiornamento batch. Vedere "Aggiornamento da repository" a pagina 84.
- **Firmware di sistema:** panoramica dello stato del firmware di sistema, della versione e dell'aggiornamento del firmware di sistema.

  Nota: Fare clic su **Sincronizzazione automatica** per abilitare o disabilitare **Promozione automatica BMC primario al backup**. Quando questa impostazione è abilitata, il firmware del banco di backup in sospeso verrà sincronizzato dal banco primario, dopo che il banco primario avrà superato la misurazione ISM (Image Stability Metric).
- **Firmware dell'adattatore:** panoramica del firmware dell'adattatore installato, dello stato, della versione e dell'aggiornamento del firmware dell'adattatore.
- **Firmware unità di alimentazione:** panoramica della versione del firmware dell'unità di alimentazione e dell'aggiornamento del firmware della PSU.
- **Firmware PSoC del backplane dell'unità:** panoramica della versione del firmware del backplane. E per eseguire l'aggiornamento firmware del sistema.

Vengono visualizzati lo stato e le versioni correnti del firmware per driver BMC, UEFI, LXPM, sistema operativo integrato, FPGA e adattatori, comprese la versione primaria e di backup di BMC. Sono disponibili tre categorie per lo stato del firmware:

- **Attivo:** il firmware è attivo.
- **Inattivo:** il firmware non è attivo.
- **In attesa di riavvio:** l'immagine del firmware è stata aggiornata e diventerà effettiva dopo il riavvio del server del BMC.
- **N/D:** nessun firmware è stato installato per questo componente.

Attenzione:

- XCC e IMM devono essere aggiornati alla versione più recente prima di aggiornare UEFI. L'aggiornamento in un ordine diverso potrebbe avere come risultato un comportamento non corretto.
- L'installazione dell'aggiornamento firmware non corretto potrebbe causare un malfunzionamento del server. Prima di installare un aggiornamento del firmware o del driver di dispositivo, leggere eventuali file readme e di cronologia delle modifiche forniti con l'aggiornamento scaricato. Questi file contengono informazioni importanti circa l'aggiornamento e la relativa procedura di installazione, inclusa qualsiasi procedura speciale per l'aggiornamento da una versione precedente del firmware o del driver di dispositivo all'ultima versione. Poiché il browser Web potrebbe contenere dati della cache di XCC, si consiglia di ricaricare la pagina Web dopo avere aggiornato il firmware di XCC.
- Ad eccezione dell'adattatore SATA M.2, i server con processori AMD non supportano l'aggiornamento firmware dell'adattatore fuori banda.

- Alcuni aggiornamenti firmware richiedono il riavvio del sistema, che esegue l'attivazione del firmware o l'aggiornamento interno. Questo processo nell'avvio del sistema è detto "modalità di manutenzione del sistema" e non consente temporaneamente azioni legate all'alimentazione da parte dell'utente. La modalità viene abilitata anche durante l'aggiornamento firmware. L'utente non scollega l'alimentazione CA quando il sistema entra in modalità di manutenzione.

Aggiornamento firmware del sistema, dell'adattatore e dell'alimentatore

Procedura per aggiornare il firmware di sistema, il firmware dell'adattatore e il firmware dell'alimentatore.

Per applicare manualmente l'aggiornamento per **Firmware del sistema**, **Firmware dell'adattatore** e **Firmware PSU**, completare le seguenti operazioni:

1. Fare clic su **Aggiorna firmware** all'interno di ogni funzione. Viene visualizzata la finestra Aggiorna firmware del server.
2. Fare clic su **Sfoglia...** per selezionare il file di aggiornamento firmware che si desidera utilizzare.
3. Passare al file che si desidera selezionare e fare clic su **Apri**. Verrà visualizzata di nuovo la finestra Aggiorna firmware del server con il file selezionato.
4. Fare clic su **Avanti** per iniziare il processo di caricamento e verifica del file selezionato. Un misuratore di avanzamento verrà visualizzato appena il file viene caricato e verificato. È possibile visualizzare questa finestra di stato per verificare che il file selezionato per l'aggiornamento sia il file corretto. Per **Firmware del sistema**, la finestra di stato contiene informazioni relative al tipo di file del firmware da aggiornare come BMC, UEFI o LXPM. Una volta caricato e verificato il file del firmware, fare clic su **Avanti** per selezionare il dispositivo che si desidera aggiornare.
5. Fare clic su **Aggiorna** per iniziare l'aggiornamento firmware. Viene visualizzato un misuratore di avanzamento che mostra lo stato dell'aggiornamento. Una volta completato l'aggiornamento firmware, fare clic su **Fine**. Se l'aggiornamento richiede il riavvio di XClarity Controller per l'applicazione, verrà visualizzato un messaggio di avvertenza. Per dettagli su come riavviare XClarity Controller, vedere "Azioni di alimentazione" a pagina 62.

Aggiornamento da repository

Aggiornamento del firmware del server da un repository remoto

Panoramica

Nota: La funzionalità CIFS/NFS/HTTPS/Cronologia firmware integrato richiede la licenza XCC Premier.

XCC supporta l'aggiornamento firmware su un server utilizzando il pacchetto bundle di aggiornamento (Service Packs). Questa funzione semplifica il processo mediante un singolo strumento client API o Redfish per aggiornare tutto il firmware nel sistema, inclusi i pacchetti di firmware OOB e IB. Il processo include l'identificazione dei pacchetti firmware applicabili, il download e l'estrazione da un server HTTP/HTTPS remoto oppure il caricamento su storage interno del BMC tramite un browser Web oppure il montaggio da una directory condivisa CIFS o NFS.

I file di metadati (formato JSON) devono essere inseriti nella directory radice del file system condiviso di rete se si utilizza il montaggio CIFS o NFS, con i payload del firmware specificati nei metadati. Il dispositivo microSD del server può memorizzare repository cronologici, consentendo agli utenti di ripristinare i livelli di firmware.

Se i pacchetti di firmware contengono payload che non supportano l'aggiornamento firmware fuori banda, BMC avvia il server e lo configura per l'avvio dall'immagine del sistema operativo integrato, installato nel BMC prima di eseguire l'aggiornamento.

Bundle di aggiornamento e metadati

Il bundle di aggiornamento (Service Packs) è un file compresso di un bundle firmware. Contiene uno o più pacchetti di firmware per i componenti in un sistema. La funzione Aggiornamento da repository di XCC utilizza il file del bundle di aggiornamento. Il file del bundle decompresso contiene file di metadati e binari payload. I file di metadati JSON forniscono informazioni a XCC sul tipo di immagini firmware contenute nel file del bundle, mentre i file binari payload forniscono le immagini del firmware.

Repository del firmware in XCC

Il bundle di aggiornamento può contenere più pacchetti firmware e XCC riserva 2 GB di spazio nella memoria flash per le nuove funzioni. Quando si riceve un nuovo bundle, XCC cancella i dati vecchi. Alcune piattaforme utilizzano una scheda MicroSD per fornire ulteriore storage e XCC sposta l'ultimo bundle aggiornato nel repository cronologico della scheda SD. Il repository della cronologia firmware può memorizzare un massimo di tre bundle e gli utenti possono utilizzare la funzione Rollback del firmware per ripristinare un bundle precedente.

Nota:

- Se il bundle di aggiornamento include solo il pacchetto firmware OOB disponibile per il sistema, XCC non modifica lo stato di alimentazione del sistema. Per aggiornare il firmware del dispositivo PCI, è necessario che il sistema sia acceso.
- Se il bundle di aggiornamento include il pacchetto firmware IB disponibile per il sistema, XCC memorizza lo stato di alimentazione del sistema prima di aggiornare e ripristinare lo stato di alimentazione una volta completato l'aggiornamento del bundle. Durante il processo di aggiornamento, XCC riavvia l'host nel sistema operativo integrato.
- Se il bundle di aggiornamento include un livello prerequisito del firmware UEFI e la versione UEFI installata corrente non soddisfa tale livello, XCC spegne il sistema per eseguire prima un aggiornamento firmware UEFI.
- Se il bundle di aggiornamento include un livello prerequisito del firmware XCC e la versione XCC attualmente installata non soddisfa tale livello, XCC viene riavviato dopo l'aggiornamento.

Aggiornamento con WebGUI

Con **Aggiornamento da repository**, l'utente può configurare XCC per sincronizzare il firmware del server con uno storage interno. Il repository del firmware deve contenere pacchetti, tra cui file binari e metadati o file JSON di metadati del bundle di aggiornamento e i corrispondenti file binari. XCC analizza i file JSON metadati per selezionare i pacchetti firmware che supportano l'aggiornamento OOB per questo hardware di sistema specifico, quindi avvia un aggiornamento batch.

Per aggiornare da repository, effettuare le seguenti operazioni:

1. Quando si utilizza lo storage interno, fare clic su **Importa pacchetto firmware** e cercare il pacchetto firmware (formato .tgz o zip).
2. Fare clic su **Aggiorna sistema** per iniziare l'aggiornamento batch.
3. Fare clic su **Visualizza dettagli** per visualizzare lo stato dell'aggiornamento.
   - **Segno di spunta verde** : l'aggiornamento del firmware è stato completato correttamente.
   - **Indicatore rosso X** : l'aggiornamento del firmware non è riuscito.
   - **Aggiornamento:** il firmware è in fase di aggiornamento.
   - **Annulla:** l'aggiornamento del firmware è stato annullato.
   - **Attesa:** l'aggiornamento del firmware è in attesa di essere distribuito.

   Nota: Fare clic su **Interrompi aggiornamento** per annullare gli aggiornamenti in coda dopo il completamento dell'aggiornamento del pacchetto di installazione corrente.

4. Quando si utilizza CIFS o NFS, fare clic su **Smonta** per disconnettersi dal repository remoto.
5. Se l'aggiornamento richiede il riavvio di XClarity Controller per l'applicazione, verrà visualizzato un messaggio di avvertenza. Per dettagli su come riavviare XClarity Controller, vedere "Azioni di alimentazione" a pagina 62.

Nota: Se nel sistema è installata una scheda MicroSD, è possibile visualizzare la cronologia degli aggiornamenti del bundle di aggiornamento e selezionare l'indice del bundle di aggiornamento per eseguire il rollback del firmware. Il processo è simile all'aggiornamento dal repository; l'unica differenza è che il bundle di aggiornamento cronologico viene salvato nella scheda MicroSD.

Capitolo 9. Gestione licenza

La gestione della licenza di Lenovo XClarity Controller consente di installare e gestire funzioni facoltative per la gestione di sistemi e server.

Esistono più livelli di funzionalità del firmware di XClarity Controller e funzionalità disponibili per il proprio server. Il livello delle funzioni del firmware installate sul server può variare in base al tipo di hardware.

È possibile aggiornare le funzionalità di XClarity Controller acquistando e installando una chiave di attivazione.

Per ordinare una chiave di attivazione, contattare un rappresentante di vendita o un business partner.

Utilizzare l'interfaccia Web di XClarity Controller o la CLI di XClarity Controller per installare manualmente una chiave di attivazione che consenta di utilizzare una funzione facoltativa appena acquistata. Prima di attivare una chiave:

- La chiave di attivazione deve trovarsi sul sistema utilizzato per eseguire il login a XClarity Controller.
- È necessario aver ordinato la chiave di licenza e aver ricevuto il relativo codice di autorizzazione via e-mail o posta ordinaria.

Per informazioni sulla gestione di una chiave di attivazione mediante l'interfaccia Web di XClarity Controller, vedere "Installazione di una chiave di attivazione" a pagina 87, "Rimozione di una chiave di attivazione" a pagina 87 o "Esportazione di una chiave di attivazione" a pagina 88. Per informazioni sulla gestione di una chiave di attivazione mediante la CLI di XClarity Controller, vedere "comando keycfg" a pagina 117.

Per registrare un ID per la gestione della licenza di XClarity Controller, fare clic sul seguente collegamento: https://fod.lenovo.com/lkms/angular/app/pages/index.htm#/welcome

Informazioni aggiuntive relative alla gestione della licenza per i server Lenovo sono disponibili sul seguente sito Web **Lenovo Press**:

https://lenovopress.com/redp4895-using-lenovo-features-on-demand

Installazione di una chiave di attivazione

Utilizzare le informazioni in questo argomento per aggiungere una funzione facoltativa al server.

Per installare una chiave di attivazione, effettuare le seguenti operazioni:

Passo 1. Fare clic su **Licenza** in **Configurazione BMC**.

Passo 2. Fare clic su **Aggiorna licenza**.

Passo 3. Nella finestra **Aggiungi una nuova licenza** fare clic su **Sfoglia**, quindi selezionare il file della chiave di attivazione da aggiungere nella finestra Caricamento file e fare clic su **Apri** per aggiungere il file. Per completare l'aggiunta della chiave, fare clic su **Importa** nella finestra Aggiungi chiave di attivazione.

Nota: Se la chiave di attivazione non è valida, verrà visualizzata una finestra di errore.

Rimozione di una chiave di attivazione

Utilizzare le informazioni in questo argomento per eliminare una funzione facoltativa dal server.

Per rimuovere una chiave di attivazione, effettuare le seguenti operazioni:

Passo 1. Fare clic su **Licenza** in **Configurazione BMC**.

Passo 2. Selezionare la chiave di attivazione da rimuovere, quindi fare clic su **Elimina**.

Passo 3. Nella finestra Conferma eliminazione chiave di attivazione fare clic su **OK** per confermare l'eliminazione della chiave di attivazione. La chiave di attivazione selezionata verrà rimossa dal server e non verrà più visualizzata nella pagina Gestione licenza.

Esportazione di una chiave di attivazione

Utilizzare le informazioni in questo argomento per esportare una funzione facoltativa dal server.

Per esportare una chiave di attivazione, effettuare le seguenti operazioni:

Passo 1. Fare clic su **Licenza** in **Configurazione BMC**.

Passo 2. Dalla pagina Gestione licenza, selezionare la chiave di attivazione da esportare, quindi fare clic su **Esporta**.

Passo 3. Nella finestra **Esporta la licenza selezionata** fare clic su **Esporta** per confermare la richiesta di esportazione della chiave di attivazione.

Passo 4. Selezionare la directory in cui salvare il file. La chiave di attivazione selezionata verrà esportata dal server.

Capitolo 10. Interfaccia della riga di comando

Utilizzare le informazioni in questo argomento per immettere i comandi che gestiscono e monitorano XClarity Controller senza l'utilizzo dell'interfaccia Web.

Utilizzare l'interfaccia della riga comandi (CLI, command-line interface) di XClarity Controller per accedere a XClarity Controller senza utilizzare l'interfaccia Web. La CLI fornisce una serie di funzioni di gestione che sono disponibili anche dall'interfaccia Web.

È possibile accedere alla CLI mediante una **sessione SSH**. È **necessario** autenticarsi a XClarity Controller prima di poter emettere qualsiasi comando CLI.

Accesso all'interfaccia della riga di comando

Utilizzare le informazioni in questo argomento per accedere alla CLI.

Per accedere alla CLI, avviare una sessione SSH all'indirizzo IP di XClarity Controller (per ulteriori informazioni, vedere "Configurazione del reindirizzamento da seriale a SSH" a pagina 89).

Accesso alla sessione della riga di comando

Utilizzare le informazioni in questo argomento per accedere alla sessione della riga di comando.

Per accedere alla riga di comando, effettuare le seguenti operazioni:

Passo 1. Stabilire una connessione con XClarity Controller.

Passo 2. Alla richiesta del nome utente, immettere l'ID utente.

Passo 3. Alla richiesta della password, immettere la password utilizzata per eseguire il login a XClarity Controller.

> **Nota:** Il prompt della riga di comando è `system>`. La sessione della riga di comando continuerà finché non si digita `exit`. L'utente sarà scollegato e la sessione sarà terminata.

Configurazione del reindirizzamento da seriale a SSH

Questo argomento fornisce informazioni relative all'utilizzo di XClarity Controller come server terminale seriale.

Il reindirizzamento da seriale a SSH consente a un amministratore di sistema di utilizzare XClarity Controller come server terminale seriale. Quando è abilitato il reindirizzamento seriale, una porta seriale del server può essere utilizzata per l'accesso da una connessione SSH.

Nota: Il comando **console 1** della CLI è utilizzato per avviare una sessione di reindirizzamento seriale con la porta COM.

Sessione di esempio

```
$ ssh USERID@10.240.1.12
Password:

system>
```

Tutto il traffico dalla sessione SSH è indirizzato a COM2.

```
ESC (
```

Immettere la sequenza di tasti di uscita per tornare alla CLI. In questo esempio, premere Esc e digitare una parentesi sinistra. Il prompt della CLI indicherà che si è tornati alla CLI IMM.

```
system>
```

Sintassi dei comandi

Esaminare le linee guida in questo argomento per comprendere come immettere i comandi nella CLI.

Prima di utilizzare i comandi, leggere le seguenti linee guida:

- Ogni comando ha il seguente formato:
  `command [`**`arguments`**`] [-`**`options`**`]`
- La sintassi del comando è sensibile al maiuscolo/minuscolo.
- Il nome del comando è tutto in minuscolo.
- Tutti gli argomenti devono seguire il comando. Le opzioni seguono gli argomenti.
- Ogni opzione è preceduta da un trattino (-). Un'opzione può essere breve (una singola lettera) o lunga (più lettere).
- Se un'opzione ha un argomento, l'argomento sarà obbligatorio, ad esempio:
  `ifconfig eth0 -i 192.168.70.34 -g 192.168.70.29 -s 255.255.255.0`
  Dove **ifconfig** è il comando, **eth0** è un argomento e -i, -g e -s sono le opzioni. In questo esempio, tutte e tre le opzioni hanno argomenti.
- Le parentesi indicano che un argomento o un'opzione sono facoltativi. Le parentesi non fanno parte del comando che viene digitato.

Funzioni e limitazioni

Questo argomento contiene informazioni sulle funzioni e le limitazioni della CLI.

La CLI ha le seguenti funzioni e limitazioni:

- Sono consentite più sessioni CLI contemporanee tramite SSH.
- È consentito un comando per riga (con un massimo di 1.024 caratteri, spazi inclusi).
- Non esiste alcun carattere di continuazione per comandi lunghi. L'unica funzione di modifica è il tasto Backspace per cancellare il carattere appena immesso.
- I tasti Freccia su e Freccia giù possono essere utilizzati per spostarsi tra gli ultimi otto comandi. Il comando **history** visualizza un elenco degli ultimi otto comandi, pertanto è possibile utilizzarlo come collegamento rapido per eseguire un comando, ad esempio:

```
system > history
 0 ifconfig eth0
 1 readlog
 2 readlog
 3 readlog
 4 history
system > !0
-state enabled
-c dthens
-i 192.168.70.125
-g 0.0.0.0
-s 255.255.255.0
```

```
-n XClarity ControllerA00096B9E003A
-r auto
-d auto
-m 1500
-b 00:09:6B:9E:00:3A
-l 00:00:00:00:00:00
system >
```

- Nella CLI, il limite del buffer di output è 2 KB. Non esiste alcun buffering. L'output di un singolo comando non può superare 2.048 caratteri. Questo limite non è valido per la modalità di reindirizzamento seriale (il buffer dei dati si verifica durante il reindirizzamento).
- I messaggi di testo semplice sono utilizzati per denotare lo stato di esecuzione del comando, ad esempio:
```
system> power on
ok
system> power state
Power: On
State: System power off/State unknown
system>
```
- La sintassi del comando è sensibile al maiuscolo/minuscolo.
- Deve essere presente almeno uno spazio tra un'opzione e il relativo argomento. Ad esempio, `ifconfig eth0 -i192.168.70.133` è una sintassi non corretta. La sintassi corretta è `ifconfig eth0 -i 192.168.70.133`.
- Tutti i comandi dispongono delle opzioni `-h`, `-help` e `?`, che forniscono una guida per la sintassi. I seguenti esempi danno tutti lo stesso risultato:
```
system> power -h
system> power -help
system> power ?
```
- Alcuni dei comandi descritti nelle seguenti sezioni potrebbero non essere disponibili per la configurazione del proprio sistema. Per visualizzare un elenco dei comandi supportati dalla propria configurazione, utilizzare l'opzione `help` o `?` come mostrato nei seguenti esempi:
```
system> help
system> ?
```

Elenco di comandi in ordine alfabetico

Questo argomento contiene un elenco di comandi CLI in ordine alfabetico. Sono forniti i collegamenti agli argomenti per ogni comando. Ogni argomento relativo ai comandi fornisce informazioni sul comando, la rispettiva funzione, la sintassi e l'uso.

Di seguito è riportato l'elenco completo di tutti i comandi CLI di XClarity Controller, in ordine alfabetico:

- "comando usbeth" a pagina 136
- "comando users" a pagina 136
- "comando volts" a pagina 101
- "comando vpd" a pagina 101

Comandi dei programmi di utilità

Questo argomento fornisce un elenco alfabetico dei comandi CLI dei programmi di utilità.

Attualmente esistono 3 comandi dei programmi di utilità:

comando exit

Utilizzare questo comando per scollegarsi dalla sessione CLI,

Utilizzare il comando **exit** per scollegarsi e terminare la sessione CLI.

comando help

Questo comando visualizza un elenco di tutti i comandi.

Utilizzare il comando **help** per visualizzare un elenco di tutti i comandi con una breve descrizione per ognuno di essi. È anche possibile digitare ? al prompt dei comandi.

comando history

Questo comando fornisce un elenco dei comandi emessi in precedenza.

Utilizzare il comando **history** per visualizzare un elenco cronologico indicizzato degli ultimi otto comandi emessi. Gli indici possono essere quindi utilizzati come collegamenti (preceduti da!) per riemettere i comandi da questo elenco cronologico.

Esempio:

```
system> history
 0 ifconfig eth0
 1 readlog
 2 readlog
 3 readlog
 4 history
system> ifconfig eth0
-state enabled
-c dthens
-i 192.168.70.125
HISTORY-g 0.0.0.0
-s 255.255.255.0
-n XCCA00096B9E003A
-r auto
-d auto
-m 1500
-b 00:09:6B:9E:00:3A
-l 00:00:00:00:00:00
system>
```

Comandi di monitoraggio

Questo argomento fornisce un elenco alfabetico dei comandi CLI di monitoraggio.

Attualmente esistono 11 comandi di monitoraggio:

comando clearlog

Questo comando viene utilizzato per cancellare il log eventi IMM.

Utilizzare il comando **clearlog** per cancellare il log eventi IMM. Per utilizzare questo comando, è necessario disporre dell'autorizzazione per cancellare i log di eventi.

Nota: Questo comando è destinato solo all'uso da parte di personale di supporto.

Sintassi:
```
clearlog [-options]
```

Tabella 4. opzioni di clearlog

Opzione	Descrizione	Valori
-t	Tipo di evento, scegliere il tipo di evento da cancellare. Se non specificato, verranno selezionati tutti i tipi di eventi.	all, platform, audit • all: tutti i tipi di eventi, inclusi gli eventi della piattaforma e di controllo. • platform: il tipo di evento della piattaforma. • audit: il tipo di evento di controllo.

Esempio:
```
system> clearlog
All event log cleared successfully
system>
system> clearlog -t all
All event log cleared successfully
system>
system> clearlog -t platform
Platform event log cleared successfully
system>
system> clearlog -t audit
Audit event log cleared successfully
system>
```

comando fans

Questo comando viene utilizzato per visualizzare la velocità delle ventole del server.

Utilizzare il comando **fans** per visualizzare la velocità delle singole ventole del server.

Esempio:
```
system> fans
fan1 75%
fan2 80%
fan3 90%
system>
```

comando mhlog

Utilizzare questo comando per visualizzare le voci di log delle attività della cronologia di manutenzione.

Sintassi:

```
mhlog [-options]
```

Tabella 5. opzioni di mhlog

Opzione	Descrizione	Valori
-c	Visualizza le voci relative al conteggio	Tra 1 e 250
-i	Visualizza le voci a partire dall'indice	Tra 1 e 250
-f	Nome file remoto del file di log	Nome file valido per il nome file del file di log
-ip	Indirizzo del server tftp/sftp	Indirizzo IP valido per il server TFTP/SFTP
-pn	Numero di porta del server tftp/sftp	Numero di porta valido per il server TFTP/SFTP (valore predefinito 69/22)
-u	Nome utente per il server sftp	Nome utente valido per il server SFTP
-pw	Password per il server sftp	Password valida per il server SFTP

Esempio:

```
system> mhlog
Type            Message                                                  Time
-------------   ------------                                             ----
Hardware        SAS Backplane1(SN: XXXX9CE009L) is added.               05/08/2020,04:23:18
Hardware        CPU 1(SKU NO: 50844440) is added.                        05/08/2020,04:23:22
Hardware        CPU 2(SKU NO: 50844440) is added.                        05/08/2020,04:23:22
Hardware        M2 Card(SN: R1SH9AJ0037) is added.                      05/08/2020,04:23:22
Firmware        Primary XCC firmware is updated to TGBT99T by XCC Web.  05/08/2020,06:40:37
Firmware        Primary XCC firmware is activated to TGBT99T.           05/08/2020,06:41:26
Hardware        PSU1(SN: D1DG94C0075) is added.                          05/08/2020,06:43:28
system>
```

comando led

Utilizzare questo comando per visualizzare e impostare gli stati dei LED.

Il comando **led** visualizza e imposta gli stati dei LED del server.

- L'esecuzione del comando **led** senza opzioni visualizza lo stato dei LED del pannello anteriore.
- L'opzione del comando **led -d** deve essere utilizzata con l'opzione del comando **led -identify on**.

La seguente tabella mostra gli argomenti per le opzioni.

Sintassi:

```
led [-options]
```

Tabella 6. opzioni di led

Opzione	Descrizione	Valori
-l	Ottiene lo stato di tutti i LED del sistema e dei relativi componenti secondari	
-identify	Modifica lo stato del LED di identificazione chiusura	off, on, blink
-d	Accende il LED di identificazione per il periodo di tempo specificato	Periodo di tempo (secondi)

Esempio:

```
system> led
Fault                   Off
Identify                On              Blue
Chklog                  Off
Power                   Off

system> led -l
Label                   Location                    State          Color
Battery                 Planar                      Off
BMC Heartbeat           Planar                      Blink          Green
BRD                     Lightpath Card              Off
Channel A               Planar                      Off
Channel B               Planar                      Off
Channel C               Planar                      Off
Channel D               Planar                      Off
Channel E               Planar                      Off
Chklog                  Front Panel                 Off
CNFG                    Lightpath Card              Off
CPU                     Lightpath Card              Off
CPU 1                   Planar                      Off
CPU 2                   Planar                      Off
DASD                    Lightpath Card              Off
DIMM                    Lightpath Card              Off
DIMM 1                  Planar                      Off
DIMM 10                 Planar                      Off
DIMM 11                 Planar                      Off
DIMM 12                 Planar                      Off
DIMM 13                 Planar                      Off
DIMM 14                 Planar                      Off
DIMM 15                 Planar                      Off
DIMM 16                 Planar                      Off
DIMM 2                  Planar                      Off
DIMM 3                  Planar                      Off
DIMM 4                  Planar                      Off
DIMM 5                  Planar                      Off
DIMM 6                  Planar                      Off
DIMM 7                  Planar                      Off
DIMM 8                  Planar                      Off
DIMM 9                  Planar                      Off
FAN                     Lightpath Card              Off
FAN 1                   Planar                      Off
FAN 2                   Planar                      Off
FAN 3                   Planar                      Off
Fault                   Front Panel (+)             Off
Identify                Front Panel (+)             On             Blue
LINK                    Lightpath Card              Off
LOG                     Lightpath Card              Off
NMI                     Lightpath Card              Off
OVER SPEC               Lightpath Card              Off
PCI 1                   FRU                         Off
PCI 2                   FRU                         Off
PCI 3                   FRU                         Off
PCI 4                   FRU                         Off
Planar                  Planar                      Off
Power                   Front Panel (+)             Off
PS                      Lightpath Card              Off
RAID                    Lightpath Card              Off
Riser 1                 Planar                      Off
Riser 2                 Planar                      Off
SAS ERR                 FRU                         Off
SAS MISSING             Planar                      Off
```

```
SP                    Lightpath Card            Off
TEMP                  Lightpath Card            Off
VRM                   Lightpath Card            Off
system>
```

comando readlog

Questo comando visualizza i log eventi di IMM.

Utilizzare il comando **readlog** per visualizzare le voci del log eventi IMM. Vengono visualizzati cinque log di eventi alla volta. Le voci sono visualizzate dalle più recenti alle più vecchie.

Nota:

- R - non valido
- I - informazioni
- W - avviso
- E - critico

Sintassi:
```
readlog [-options]
```

Tabella 7. opzioni di readlog

Opzione	Descrizione	Valori
-a	Visualizza tutte le voci del log eventi, a partire dalla più recente.	
-f	Reimposta il contatore e visualizza le prime 5 voci nel log eventi, a partire dalla più recente.	
-date	Visualizza le voci del log eventi per la data specificata	Utilizzare il seguente formato: mm/dd/yyyy
-sev	Visualizza le voci del log eventi in base per il livello di gravità specificato.	R, I, W, E
-i	Imposta l'indirizzo IP IPv4 o IPv6 del server TFTP o SFTP in cui viene salvato il log eventi. Le opzioni del comando **-i** e **-l** sono utilizzate insieme per specificare il percorso.	Indirizzo IP valido
-l	Imposta il nome del file del log eventi. Le opzioni del comando **-i** e **-l** sono utilizzate insieme per specificare il percorso.	Nome file valido
-pn	Visualizza o imposta il numero di porta del server TFTP o SFTP.	Numero di porta valido (valore predefinito 69/22)
-u	Specifica il nome utente per il server SFTP.	Nome utente valido
-pw	Specifica la password per il server SFTP.	Password valida
-di	Funzionalità del log di controllo estesa	nessuno, ipmi

Esempio:

```
system> readlog -f
1 I 2017-06-17T09:31:59.217  Remote Login Successful. Login ID: USERID
from SSH at IP address 10.134.78.180
2 I 2017-06-17T07:23:04.685  Remote Login Successful. Login ID: USERID
from webguis at IP address 10.134.78.180.
3 I 2017-06-16T11:00:35.581  Login ID: USERID from webguis at IP address 10.134.78.180 has logged off.
4 I 2017-06-16T11:00:15.174  Login ID: USERID from webguis at IP address 10.104.209.144 has logged off.
5  I 2017-06-16T10:40:14.352  Login ID: USERID from webguis at IP address 10.104.209.144 has logged off.
system> readlog
6 E SERVPROC 12/18/03 10:09:31 Fan 2 Fault. Multiple fan failures
7 E SERVPROC 12/18/03 10:09:31 Fan 1 Fault. Single fan failure
8 I SERVPROC 12/18/03 10:09:25 Ethernet[0] Link Established at 100Mb, Full Duplex.
9 I SERVPROC 12/18/03 10:09:24 Ethernet[0] configured to do Auto Speed/Auto Duplex.
10 I SERVPROC 12/18/03 10:09:24 Ethernet[0] MAC Address currently
being used: 0x00-09-6B-CA-0C-80
system>
```

comando servicelog

Questo comando viene utilizzato per generare un nuovo file di dati di servizio.

Nota: In precedenza questo comando era denominato **ffdc**.

Utilizzare il comando **servicelog** per generare e trasferire i dati di servizio all'assistenza.

L'elenco seguente è costituito dai comandi da utilizzare con il comando **servicelog**:

La seguente tabella mostra gli argomenti per le opzioni.

Sintassi:
```
servicelog [subset_command] [-options]
```

Tabella 8. comandi del subset servicelog

Opzione	Descrizione
generazione	Crea un nuovo file di dati di servizio
status	Controlla lo stato del file di dati di servizio
copy	Copia i dati di servizio esistenti
delete	Elimina i dati di servizio esistenti

Tabella 9. opzioni di servicelog

Opzione	Descrizione	Valori
-t	Tipo di log di servizio	1, 2, 3 • **1**: log di debug (FFDC, predefinito) • **2**: log dei dati di servizio • **3**: log di debug accoppiato al log dei dati di servizio; è valido solo quando si copiano i file di log
Opzioni aggiuntive per il comando di generazione		

Tabella 9. opzioni di servicelog (continua)

Opzione	Descrizione	Valori
-c	Selezione della categoria di dati di dump. La categoria di dati non sarà contenuta se non specificata con questa opzione.	• Per il tipo 1 (ffdc): corefile • Per il tipo 2 (log dei dati di servizio): network, audit, telemetry, osscreen
Opzioni aggiuntive per i comandi di generazione e copia		
-f	Nome file remoto o directory di destinazione sftp.	Per sftp, utilizzare il percorso completo o una / davanti al nome della directory (~/ o /tmp/). Il valore predefinito è il nome generato dal sistema.
-ip	Indirizzo del server tftp/sftp.	Indirizzo IP valido
-pn	Numero di porta del server tftp/sftp.	Numero di porta valido (valore predefinito 69/22)
-u	Nome utente per il server sftp.	Nome utente valido
-pw	Password per il server sftp.	Password valida
-timeout	Minuti per consentire la copia in primo piano.	Tra 1 e 5 (predefinito 1)

Esempio:

```
system> servicelog generate
Generating ffdc...
system> servicelog status
Type 1 ffdc: in progress
system> servicelog copy -t 1 -ip 192.168.70.230 -u User2 -pw Passw0rd -f /tmp/
Waiting for ffdc.....
Copying ffdc...
ok
system> servicelog status
Type 1 ffdc: completed
8737AC1_DSY0123_xcc_120317-153327.tgz


system> servicelog generate
Generating ffdc...
system> servicelog status
Type 1 ffdc: in progress
system> servicelog status
Type 1 ffdc: in progress
system> servicelog copy -ip 192.168.70.230
Copying ffdc...
ok
system> servicelog status
Type 1 ffdc: completed
8737AC1_DSY0123_xcc_120926-105320.tgz
system>
```

comando syshealth

Questo comando fornisce un riepilogo degli eventi di integrità o attivi.

Utilizzare il comando **syshealth** per visualizzare un riepilogo degli eventi di integrità o attivi del server. Vengono visualizzati lo stato di alimentazione, lo stato del sistema, lo stato dell'hardware (include ventola, alimentatore, storage, processore, memoria), il numero di riavvii e lo stato del software IMM.

Sintassi:
```
syshealth [arguments]
```

Tabella 10. argomenti d syshealth

Argomenti	Descrizione
summary	Visualizza il riepilogo dello stato del sistema.
activeevents	Visualizza gli eventi attivi.
cooling	Visualizza lo stato di integrità dei dispositivi di raffreddamento.
power	Visualizza lo stato di integrità dei moduli di alimentazione.
storage	Visualizza lo stato di integrità dello storage locale.
processors	Visualizza lo stato di integrità dei processori.
memory	Visualizza lo stato di integrità della memoria.

Esempio:
```
system> syshealth summary
Power    On
State    OS booted
Restarts 29

system> syshealth activeevents
No Active Event Available!
```

comando temps

Questo comando visualizza tutte le informazioni su temperatura e soglie di temperatura.

Utilizzare il comando **temps** per visualizzare tutte le temperature e le soglie di temperatura. La stessa serie di temperature è visualizzata come nell'interfaccia Web.

Sintassi:
```
temps
```

Esempio:
```
system> temps
Temperatures are displayed in degrees Fahrenheit/Celsius
              WR          W      T             SS             HS
-----------------------------------------------------------------------
Ambient Temp  109.40/43   N/A    78.80/26.00   109.40/43.00   122.00/50.00
Exhaust Temp  N/A          N/A    32.00/0 .00   116.60/47.00   N/A
system>
```

Nota:

1. L'output ha le seguenti intestazioni di colonna:

   WR: reimpostazione di avvertenza (valore di isteresi della soglia positivo)

   W: avvertenza (soglia massima non critica)

   T: temperatura (valore corrente)

SS: arresto normale (soglia critica massima)

HS: arresto forzato (soglia massima irreversibile)

2. Tutti i valori di temperatura sono espressi in gradi Fahrenheit/Celsius.
3. N/A sta per non applicabile.

comando volts

Utilizzare questo comando per visualizzare le informazioni sulla tensione del server.

Utilizzare il comando **volts** per visualizzare tutte le tensioni e le soglie di tensione. La stessa serie di tensioni è visualizzata come nell'interfaccia Web.

Sintassi:
```
volts
```

Esempio:
```
system> volts
              HSL  SSL   WL    WRL   V     WRH   WH   SSH   HSH
-------------------------------------------------------------------
CMOS Battery  N/A  2.25  2.39  0.03  3.12  0.03  N/A  N/A   N/A
system>
```

Nota: L'output ha le seguenti intestazioni di colonna:

HSL: arresto forzato minimo (soglia minima irreversibile)

SSL: arresto normale minimo (soglia critica minima)

WL: avvertenza minima (soglia minima non critica)

WRL: reimpostazione di avvertenza minima (valore di isteresi della soglia negativo)

V: tensione (valore corrente)

WRH: reimpostazione di avvertenza elevata (valore di isteresi della soglia positivo)

WH: avvertenza elevata (soglia massima non critica)

SSH: arresto normale elevato (soglia critica massima)

HSH: arresto forzato elevato (soglia massima irreversibile)

comando vpd

Questo comando visualizza i dati di configurazione e informativi (VPD, Vital Product Data) associati all'hardware e al software del server.

Utilizzare il comando **vpd** per visualizzare i dati VPD (Vital Product Data) del sistema (sys), di IMM (bmc), del BIOS del server (uefi), di Lenovo XClarity Provisioning Manager (lxpm), del firmware del server (fw), dei componenti del server (comp) e dei dispositivi PCIe (pcie). Le stesse informazioni sono riportate come nell'interfaccia Web.

Sintassi:
```
vpd [arguments]
```

Tabella 11. argomenti di vpd

Argomenti	Descrizione
vpd sys	Visualizza i dati VPD (Vital Product Data) per il sistema.
vpd bmc	Visualizza i dati VPD (Vital Product Data) per il controller di gestione.

Tabella 11. argomenti di vpd (continua)

Argomenti	Descrizione
vpd uefi	Visualizza i dati VPD (Vital Product Data) per il BIOS del sistema.
vpd lxpm	Visualizza i dati VPD (Vital Product Data) per LXPM del sistema.
vpd fw	Visualizza i dati VPD (Vital Product Data) per il firmware di sistema.
vpd comp	Visualizza i dati VPD (Vital Product Data) per i componenti del sistema.
vpd pcie	Visualizza i dati VPD (Vital Product Data) per i dispositivi PCIe.

Esempio:
```
system> vpd bmc
Type             Status       Version    Build       ReleaseDate
--------------   -------      -------    ------      ------------
BMC (Primary)   Active       0.00        DVI399T     2017/06/06
BMC (Backup)    Inactive     1.00        TEI305J     2017/04/13
system>
```

Comandi di controllo per l'accensione e il riavvio del server

Questo argomento fornisce un elenco alfabetico dei comandi CLI di accensione e riavvio.

Attualmente esistono 4 comandi di accensione e riavvio del server:

comando power

Questo comando descrive come controllare l'alimentazione del server.

Utilizzare il comando **power** per controllare l'alimentazione del server. Per emettere i comandi **power**, è necessario disporre del livello di autorizzazione di accesso Alimentazione/riavvio server remoto.

Sintassi:
```
power on [-options]
power off [-options]
power cycle [-options]
power uefi
power state
```

Tabella 12. comandi power

Comando	Descrizione
power on	Utilizzare questo comando per accendere il server.
power off	Utilizzare questo comando per spegnere il server.
power cycle	Utilizzare questo comando per spegnere e riaccendere il server.
power uefi	Utilizzare questo comando per avviare la configurazione F1 di UEFI.
power state	Utilizzare questo comando per visualizzare lo stato di alimentazione e lo stato corrente del server.

Tabella 13. opzioni di power

Opzione	Descrizione	Valori
-s	Utilizzare questa opzione per arrestare il sistema operativo prima che il server venga spento. **Nota:** L'opzione **-s** è implicita quando si utilizza l'opzione **-every** per i comandi **power off** e **power cycle**.	
-every	Utilizzare questa opzione con i comandi **power on**, **power off** e **power cycle** per controllare l'alimentazione del server. È possibile configurare la data, l'ora e la frequenza (giornaliera o settimanale) di accensione, spegnimento o esecuzione del ciclo di alimentazione del server.	Sun, Mon, Tue, Wed, Thu, Fri, Sat, Day, vuoto
-t	Utilizzare questa opzione per specificare l'orario (in ore e minuti) di accensione del server, arresto del sistema operativo e spegnimento o riavvio del server.	Utilizzare il seguente formato: hh: mm
-d	Utilizzare questa opzione per specificare la data di accensione del server. Questa è un'opzione aggiuntiva per il comando **power on**. **Nota:** Le opzioni **-d** e **-every** non possono essere utilizzate contemporaneamente per lo stesso comando.	Utilizzare il seguente formato: mm/dd/yyyy
-clear	Utilizzare questa opzione per cancellare la data di accensione pianificata. Questa è un'opzione aggiuntiva per il comando **power on**.	

Le seguenti informazioni costituiscono esempi del comando **power**.

Per arrestare il sistema operativo e spegnere il server ogni domenica alle 1:30, immettere il seguente comando:
```
system> power off -every Sun -t 01:30
```

Per arrestare il sistema operativo e riavviare il server ogni giorno alle 1:30, immettere il seguente comando:
```
system> power cycle -every Day -t 01:30
```

Per accendere il server ogni lunedì alle 1:30, immettere il seguente comando:
```
system> power on -every Mon -t 1:30
```

Per accendere il server il 31 dicembre 2013 alle 23:30, immettere il seguente comando:
```
system> power on -d 12/31/2013 -t 23:30
```

Per cancellare un ciclo di espansione settimanale, immettere il seguente comando:
```
system> power cycle -every clear
```

comando reset

Questo comando descrive come reimpostare il server.

Utilizzare il comando **reset** per riavviare il server. Per utilizzare questo comando, è necessario disporre dell'autorizzazione di accesso per l'accensione e il riavvio.

Sintassi:
```
reset [-options]
```

Tabella 14. opzioni di reset

Opzione	Descrizione	Valori
-s	Arresta il sistema operativo prima che il server venga reimpostato.	
-d	Ritarda la reimpostazione per il numero di secondi specificato.	0 - 120
-nmi	Genera NMI (non-maskable interrupt) sul server.	

comando fuelg

Questo comando visualizza le informazioni sull'alimentazione del server.

Utilizzare il comando **fuelg** per visualizzare informazioni sull'utilizzo dell'alimentazione del server e configurare la gestione dell'alimentazione del server. Questo comando consente inoltre di configurare i criteri per la perdita di ridondanza dell'alimentazione.

Sintassi:
```
fuelg [-options]
```

Tabella 15. opzioni di fuelg

Opzione	Descrizione	Valori
-pme	Abilita o disabilita la gestione e il limite dell'alimentazione sul server.	on, off
-pcapmode	Imposta la modalità di limite alimentazione per il server.	output, input
-pcap	Un valore numerico che rientra nell'intervallo dei valori di limite alimentazione visualizzato quando si esegue il comando fuelg sulla destinazione senza alcuna opzione.	valore numerico di wattaggio
-history	Visualizza il consumo energetico o la cronologia delle prestazioni.	pc, perf
-period	Valore numerico per visualizzare la cronologia.	1, 6, 12, 24 ore
-pm	Impostare la modalità dei criteri per la perdita di alimentazione ridondante.	• **bt** - base con limitazione • **rt** - ridondante con limitazione (predefinita)
-zm	Abilita o disabilita la modalità di output zero. Questa impostazione può essere specificata solo quando la modalità criteri è impostata su ridondante con limitazione.	on, off

Tabella 15. opzioni di fuelg (continua)

Opzione	Descrizione	Valori
-perf	Visualizza l'utilizzo corrente dell'elaborazione, inclusi sistema, processore, modulo di memoria e I/O.	
-pc	Visualizza il consumo di energia corrente	• **output**: visualizza il consumo energetico corrente in uscita del sistema, del processore, del modulo di memoria e di altri componenti. • **input** - visualizza il consumo corrente di energia in ingresso, incluso il consumo energetico del sistema. **Nota:** Per i server AMD, il consumo energetico corrente in uscita non verrà visualizzato per alcuni componenti.

comando pxeboot

Questo comando visualizza e imposta la condizione di Preboot eXecution Environment.

Sintassi:
```
pxeboot [-options]
```

Tabella 16. opzioni di pxeboot

Opzione	Descrizione	Valori
-en	Imposta la condizione di Preboot eXecution Environment per il successivo riavvio del sistema.	enabled, disabled

Comandi di configurazione

Questo argomento fornisce un elenco alfabetico dei comandi CLI di configurazione.

Attualmente esistono 41 comandi di configurazione:

comando accseccfg

Utilizzare questo comando per visualizzare e configurare le impostazioni di sicurezza dell'account.

Sintassi:
```
accseccfg [-options]
```

Tabella 17. opzioni di accseccfg

Opzione	Descrizione	Valori
-am	Imposta il metodo di autenticazione utente.	local, ldap, localldap, ldaplocal
-lp	Periodo di blocco in seguito al numero massimo di errori di login (minuti).	Tra 0 e 2.880, 0 = il periodo di blocco non scade

Tabella 17. opzioni di accseccfg (continua)

Opzione	Descrizione	Valori
-pe	Periodo di tempo per la scadenza della password (giorni).	Tra 0 e 365, 0 = nessuna scadenza
-pew	Periodo di tempo avviso scadenza password **Nota:** Il periodo di avviso di scadenza password deve essere inferiore al periodo di scadenza della password.	Tra 0 e 30, 0 = nessun avviso
-pc	Regole di complessità password abilitate.	on, off
-pl	Lunghezza della password.	Se le regole di complessità password sono abilitate, la lunghezza della password è compresa tra 8 e 32 caratteri. In caso contrario, è compresa tra 0 e 32.
-ci	Intervallo minimo di modifica password (ore).	Tra 0 e 240, 0 = modifica immediatamente
-lf	Numero massimo di errori di login.	Tra 0 e 10, 0 = nessun blocco
-chgnew	Modifica la nuova password utente dopo il primo login.	on, off
-rc	Ciclo di riutilizzo password.	Tra 0 e 10, 0 = riutilizza immediatamente
-wt	Timeout sessione di inattività Web e Secure Shell (minuti).	Tra 0 e 1.440

Esempio:
```
system> accseccfg
  -am: local
  -lp: 60
  -pe: none
  -pew: 0
  -pc: on
  -pl: 10
  -ci: 0
  -lf: 5
  -chgnew: on
  -rc: 5
  -wt: 20
system>
```

comando asu

Questo comando consente di configurare le impostazioni UEFI.

I comandi ASU (Advanced Settings Utility) consentono di configurare le impostazioni UEFI. Perché tali impostazioni UEFI abbiano effetto, il sistema host dovrà essere riavviato.

Sintassi:
```
asu [subset_command]
```

Tabella 18. comandi asu subset

Comando	Descrizione	Valore
help	Utilizzare questo comando per visualizzare le informazioni sulla guida per una o più impostazioni.	**setting_name**
set	Utilizzare questo comando per modificare il valore di un'impostazione. Impostare l'opzione UEFI sul valore di input. **Nota:** • Impostare una o più coppie impostazione/valore. • L'impostazione può contenere caratteri jolly se si espande per una singola impostazione. • Il valore deve essere racchiuso tra virgolette se contiene spazi. • I valori di elenchi ordinati sono separati dal simbolo uguale (=). Ad esempio, set B*.Bootorder "CD/DVD Rom=Hard Disk 0=PXE Network."	**setting_name=value**
show	Utilizzare questo comando per visualizzare il valore corrente di una o più impostazioni.	**setting_name**
showvalues	Utilizzare questo comando per visualizzare tutti i valori possibili per una o più impostazioni. **Nota:** • Questo comando visualizza le informazioni sui valori consentiti per l'impostazione. • È visualizzato il numero minimo e il numero massimo di istanze consentite per l'impostazione. • Sarà visualizzato il valore predefinito, se disponibile. • Il valore predefinito è racchiuso tra parentesi angolari (< e >). • I valori di testo mostrano la lunghezza minima e massima e l'espressione regolare.	**setting_name**
showgroups	Utilizzare questo comando per visualizzare i gruppi di impostazioni disponibili. Questo comando visualizza i nomi dei gruppi noti. I nomi dei gruppi possono variare in base ai dispositivi installati.	
Nota: • Nella sintassi del comando, **setting_name** è il nome di un'impostazione che si desidera visualizzare o modificare e **value** è il valore di tale impostazione. • **setting_name** può essere più di un nome, tranne nel caso in cui si utilizzi il comando **set**. • **setting_name** può contenere caratteri jolly, ad esempio un asterisco (*) o un punto interrogativo (?). • **setting_name** può essere un gruppo, il nome di un'impostazione o **all** (tutti).		

Esempi:

- Per visualizzare tutte le opzioni del comando asu, immettere `asu help`.
- Per visualizzare la guida di un comando, immettere `asu help setting_name`.
- Per modificare un valore, immettere `asu set setting_name=value`.
- Per visualizzare il valore corrente, immettere `asu show setting_name`.

- Per visualizzare tutti i valori possibili per un'impostazione, immettere `asu showvalues setting_name`. Esempio di comando show values:
```
system> asu showvalues S*.POST*
SystemRecovery.POSTWatchdogTimer==<Disable>=Enable
SystemRecovery.POSTWatchdogTimerValue=numeric min=5 max=20 step=1 default=5
system>
```
- Per visualizzare i gruppi di impostazioni disponibili, immettere `asu showgroups`.

La seguente tabella mostra gli argomenti per le opzioni.

Tabella 19. opzioni asu

La seguente tabella multiriga a tre colonne contiene le opzioni, le descrizioni delle opzioni e i valori associati per le opzioni.

Opzione	Descrizione	Valori
-b	Visualizza in formato batch.	
-help[1]	Visualizza l'uso e le opzioni del comando. L'opzione -help viene inserita prima del comando, ad esempio **asu -help show**.	
-l	Nome dell'impostazione in formato lungo (include la configurazione impostata).	
-m	Nome dell'impostazione in formato misto (utilizzare l'ID configurazione).	
-v[2]	Output dettagliato.	

1. L'opzione -help può essere utilizzata con qualsiasi comando.
2. L'opzione -v è utilizzata solo tra **asu** e il comando.

Sintassi:
```
asu [-options] command [cmdopts]
options:
   -v verbose output
   -help display main help
cmdopts:
   -help help for the command
```

Nota: Fare riferimento ai singoli comandi per altre opzioni.

Utilizzare i comandi delle transazioni asu per definire più impostazioni UEFI e creare ed eseguire comandi in modalità batch. Utilizzare i comandi **tropen** e **trset** per creare un file di transazioni contenente più impostazioni da applicare. Una transazione con un determinato ID viene aperta utilizzando il comando **tropen**. Le impostazioni sono aggiunte alla serie mediante il comando **trset**. La transazione completata viene confermata mediante il comando **trcommit**. Una volta completata la transazione è possibile eliminarla mediante il comando **trrm**.

Nota: L'operazione di ripristino delle impostazioni UEFI crea una transazione con un ID formato da tre numeri casuali.

La seguente tabella contiene i comandi delle transazioni che possono essere utilizzati con il comando **asu**.

Tabella 20. comandi transazioni asu

La seguente tabella multiriga a tre colonne contiene i comandi delle transazioni, le descrizioni dei comandi e i valori associati ai comandi.

Comando	Descrizione	Valore
tropen **ID**	Questo comando crea un nuovo file di transazioni contenente diverse impostazioni da definire.	**ID** è la stringa di identificazione, contenente da 1 a 3 caratteri alfanumerici.
trset **ID**	Questo comando aggiunge una o più impostazioni o coppie di valori a una transazione.	**ID** è la stringa di identificazione, contenente da 1 a 3 caratteri alfanumerici.
trlist **ID**	Questo comando visualizza prima il contenuto del file della transazione. Ciò può essere utile quando il file della transazione viene creato nella shell della CLI.	**ID** è la stringa di identificazione, contenente da 1 a 3 caratteri alfanumerici.
trcommit **ID**	Questo comando esegue il commit e il contenuto del file della transazione. Saranno visualizzati i risultati dell'operazione e gli eventuali errori.	**ID** è la stringa di identificazione, contenente da 1 a 3 caratteri alfanumerici.
trrm **ID**	Questo comando rimuove il file della transazione in seguito al commit.	**ID** è la stringa di identificazione, contenente da 1 a 3 caratteri alfanumerici.

Esempio di definizione di più impostazioni UEFI:

```
asu tropen TR1
asu trset TR1 UEFI.BootModes.SystemBootMode "UEFI and Legacy"
asu trset TR1 BootOrder.BootOrder "CD/DVD Rom=Hard Disk 0=PXE Network"
asu trset TR1 BootOrder.WolBootOrder "CD/DVD Rom=Hard Disk 0=PXE Network"
asu trset TR1 UEFI.DevicesandIOPorts.Com1BaudRate 115200
asu trset TR1 UEFI.DevicesandIOPorts.Com1DataBits 8
asu trset TR1 UEFI.DevicesandIOPorts.Com1FlowControl Disable
asu trset TR1 UEFI.DevicesandIOPorts.Com1Parity None
asu trset TR1 UEFI.DevicesandIOPorts.Com1StopBits 1
asu trset TR1 UEFI.DevicesandIOPorts.COMPort1 Enable
asu trcommit TR1
```

comando backup

Utilizzare questo comando backup per creare un file di backup contenente le impostazioni di sicurezza del sistema corrente.

Sintassi:

```
backup [-options]
```

Tabella 21. opzioni di backup

Opzione	Descrizione	Valori
-f	Nome del file di backup	Nome file valido
-pp	La password o la frase delimitata tra virgolette utilizzata per crittografare le password all'interno del file di backup	Password o pass-phrase valida racchiusa tra virgolette
-ip	Indirizzo IP del server TFTP/SFTP	Indirizzo IP valido
-pn	Numero di porta del server TFTP/SFTP	Numero di porta valido (valore predefinito 69/22)

Tabella 21. opzioni di backup (continua)

Opzione	Descrizione	Valori
-u	Nome utente per il server SFTP	Nome utente valido
-pw	Password per il server SFTP	Password valida
-fd	Nome file per la descrizione XML dei comandi CLI di backup	Nome file valido

Esempio:
```
system> backup -f xcc-back.cli -pp xxxxxx -ip 192.168.70.200
ok
system>
```

comando dhcpinfo

Utilizzare questo comando per visualizzare la configurazione IP assegnata dal server DHCP per eth0.

Utilizzare il comando **dhcpinfo** per visualizzare la configurazione IP assegnata dal server DHCP per eth0, se l'interfaccia è configurata automaticamente da un server DHCP. È possibile utilizzare il comando **ifconfig** per abilitare o disabilitare DHCP.

Sintassi:
```
dhcpinfo [ethernet_number]
```

Esempio:
```
dhcpinfo eth1
```

La seguente tabella descrive l'output dall'esempio.

Tabella 22. output di dhcpinfo

Campo	Descrizione
-server	Il server DHCP che ha assegnato la configurazione
-n	Nome host assegnato
-i	Indirizzo IPv4 assegnato
-i6	Indirizzo IPv6 assegnato
-g	Indirizzo gateway assegnato
-s	Maschera di sottorete assegnata
-d	Nome di dominio IPv4 assegnato
-d6	Nome di dominio IPv6 assegnato
-dns1	Indirizzo IP del server DNS IPv4 primario
-dns2	Indirizzo IP del server DNS IPv4 secondario
-dns3	Indirizzo IP del server DNS IPv4 terziario
-i6	Indirizzo IPv6
-d6	Nome di dominio IPv6
-dns61	Indirizzo IP del server DNS IPv6 primario

Tabella 22. output di dhcpinfo (continua)

Campo	Descrizione
-dns62	Indirizzo IP DNS IPv6 secondario
-dns63	Indirizzo IP del server DNS IPv6 terziario

comando dns

Utilizzare questo comando per visualizzare e impostare la configurazione DNS di IMM.

Sintassi:
```
dns [-options]
```

Tabella 23. opzioni di dns

Opzione	Descrizione	Valori
-state	Stato del DNS	on, off
-i1	Indirizzo IP del server DNS IPv4 primario	Indirizzo IP in formato decimale puntato.
-i2	Indirizzo IP del server DNS IPv4 secondario	Indirizzo IP in formato decimale puntato.
-i3	Indirizzo IP del server DNS IPv4 terziario	Indirizzo IP in formato decimale puntato.
-i61	Indirizzo IP del server DNS IPv6 primario	Indirizzo IP in formato IPv6.
-i62	Indirizzo IP DNS IPv6 secondario	Indirizzo IP in formato IPv6.
-i63	Indirizzo IP del server DNS IPv6 terziario	Indirizzo IP in formato IPv6.
-ddns	Stato del DDNS	enabled, disabled
-dnsrc	Nome di dominio DDNS preferito	dhcp, manual
-ddn	DDN specificato manualmente	
-ddncur	DDN corrente (sola lettura)	
-p	Server DNS preferiti (ipv4, ipv6)	ipv4, ipv6
-dscvry	Rilevamento degli indirizzi LXCA	enabled, disabled
-dsclist	Elenco LXCA di DNS SRV	
-dscxm	Configurazione di XClarity Manager	

Il seguente esempio mostra una configurazione di IMM con DNS disabilitato:
```
system> dns
   -state   :  disabled
   -i1      :  0.0.0.0
   -i2      :  0.0.0.0
   -i3      :  0.0.0.0
   -i61     :  ::
   -i62     :  ::
   -i63     :  ::
   -ddns    :  enabled
   -dnsrc   :  DHCP
   -ddn     :
   -ddncur  :  labs.lenovo.com
   -p       :  ipv6
   -dscvry  :  enabled
system>
```

comando encaps

Utilizzare questo comando per consentire a BMC di uscire dalla modalità di incapsulamento.

Sintassi:
```
encaps [arguments]
```

Tabella 24. argomenti di encaps

Argomenti	Descrizione
lite off	Consente a BMC di uscire dalla modalità di incapsulamento e aprire l'accesso globale a tutti gli utenti

comando ethtousb

Utilizzare il comando **ethtousb** per visualizzare e configurare un'associazione tra porte Ethernet-Ethernet-over-USB.

Il comando consente di associare un numero di porta Ethernet esterna a un numero di porta differente per Ethernet-over-USB.

Sintassi:
```
ethtousb [-options]
```

Tabella 25. comando ethtousb

Opzione	Descrizione	Valori
-en	Stato Ethernet-over-USB.	enabled, disabled **Nota:** Abilitare l'interfaccia Ethernet-over-USB tramite **<usbeth>** per rendere effettiva l'associazione della porta.
-m**[x] port1:port2**	Configura l'associazione della porta per l'indice **x**.	Dove: • Il numero di indice di porta, **x**, è specificato come numero intero compreso tra 1 e 10 nell'opzione del comando. • **porta1** della coppia di porte è il numero di porta Ethernet esterna. • **porta2** della coppia di porte è il numero di porta Ethernet-over-USB.
-rm **map_ index**	Rimuove l'associazione della porta per l'indice specificato.	Il numero di indice della porta, **map_index**, viene specificato come numero intero compreso tra 1 e 10 nell'opzione di comando. **Nota:** Gli indici di associazione della porta vengono visualizzati utilizzando il comando **ethtousb** senza opzioni.

Esempio:
```
system> ethtousb -en enabled -m1 100:200 -m2 101:201
system> ethtousb
        ethtousb : On
        ===============
         1:   100:  200
         2:   101:  201
system>
```

comando firewall

Utilizzare questo comando per configurare il firewall per limitare l'accesso a determinati indirizzi e, se lo si desidera, limitare l'intervallo di tempo per l'accesso. Se non viene specificata alcuna opzione, verranno visualizzate le impostazioni correnti.

Sintassi:
```
firewall [-options]
```

Tabella 26. opzioni di firewall

Opzione	Descrizione	Valori
La seguente opzione è per la whitelist degli indirizzi IP		
-wips	Mostra/configura gli indirizzi IP della whitelist.	<indirizzi IP validi>, clr • **Indirizzi IP validi**: da 1 a 3 indirizzi IP consentiti (separati da virgole, CIDR o intervallo) **Nota:** Gli indirizzi IPv4 e IPv6 possono utilizzare il formato CIDR per bloccare un intervallo di indirizzi. • **-clr**: cancella la whitelist
Le seguenti opzioni sono per gli elementi bloccati e la restrizione di orario		
-bips	Blocca gli indirizzi IP da 1 a 3 (separati da virgola, CIDR o intervallo)	Indirizzi IP validi **Nota:** Gli indirizzi IPv4 e IPv6 possono utilizzare il formato CIDR per bloccare un intervallo di indirizzi.
-bmacs	Blocca gli indirizzi MAC da 1 a 3 (separati da virgola)	Indirizzi MAC validi **Nota:** Il filtro degli indirizzi MAC funziona solo con indirizzi specifici.
-bbt	L'ora di inizio del blocco deve essere successiva all'ora corrente	Ora con formato <YYYY-MM-DD HH:MM>
-bet	L'ora di fine del blocco deve essere successiva all'ora di inizio	Ora con formato <YYYY-MM-DD HH:MM>
-bti	Blocca da 1 a 3 intervalli di tempo (separati da virgola) ad esempio, **firewall - bti 01:00–02:00,05:05–10:30** bloccherà l'accesso nel periodo 01:00-02:00 e 05:05-10:30 ogni giorno	Intervallo di tempo con formato <HH:MM-HH:MM>
-clr	Cancella la regola del firewall per un determinato tipo	ip, mac, datetime, interval, all
Le seguenti opzioni sono per il blocco dell'indirizzo IP		
-iplp	Periodo di blocco degli indirizzi IP in minuti.	Valore numerico compreso tra 0 e 2880, 0 = nessuna scadenza

Tabella 26. opzioni di firewall (continua)

Opzione	Descrizione	Valori
-iplf	Numero massimo di errori di login prima che l'indirizzo IP sia bloccato.	Valore numerico compreso tra 0 e 32, 0 = nessun blocco **Nota:** Se questo valore non è 0, deve essere maggiore di o uguale a **<Numero massimo di errori di login>** impostato da **<accseccfg -lf>**
-ipbl	Mostra/configura l'elenco degli indirizzi IP bloccati.	del, clrall, show • **-del**: elimina un indirizzo IPv4 o IPv6 dall'elenco dei blocchi • **-clrall**: cancella tutti gli IP di blocco • **-show**: mostra tutti gli IP di blocco

Nell'elenco seguente sono riportati esempi di sintassi per il comando **firewall**:

- Per visualizzare il valore di tutte le opzioni e l'elenco degli indirizzi IP bloccati, immettere `firewall`.
- Per bloccare l'accesso da parte di più IP immettere `firewall -bips 192.168.1.1,192.168.1.0/24,192.168.1.1-192.168.1.5`.
- Per bloccare ogni giorno tutti gli accessi nelle ore 01:00-02:00, 05:05-10:30, 14:15-20:00, immettere `firewall -bti 01:00-02:00,05:05-10:30,14:15-20:00`.
- Per cancellare tutte le regole per gli elementi bloccati e la restrizione di orario, immettere `firewall –clr all`.
- Per impostare il periodo di blocco dell'indirizzo IP su 60 minuti, immettere `firewall -iplp 60`.
- Per impostare il numero massimo di errori di login su 5, immettere `firewall -iplf 5`.
- Per eliminare 192.168.100.1 dall'elenco degli indirizzi IP bloccati, immettere `firewall -ipbl -del 192.168.100.1`.
- Per eliminare 3fcc:1234::2 dall'elenco degli indirizzi IP bloccati, immettere `firewall –ipbl -del 3fcc:1234::2`.
- Per eliminare tutti gli indirizzi IP bloccati, immettere `firewall –ipbl –clrall`.
- Per mostrare tutti gli indirizzi IP bloccati, immettere `firewall –ipbl –show`.

comando hashpw

Utilizzare questo comando con l'opzione -sw per abilitare/disabilitare la funzione di password di terze parti oppure con l'opzione -re per abilitare o disabilitare l'autorizzazione a recuperare la password di terze parti.

Sintassi:
```
hashpw [-options]
```

Tabella 27. opzioni di hashpw

Opzione	Descrizione	Valori
-sw	Stato dello switch della password di terze parti	enabled, disabled
-re	Stato di lettura della password di terze parti **Nota:** La lettura può essere impostata se lo switch è abilitato.	enabled, disabled

Esempio:
```
system> hashpw –sw enabled –re enabled
```

```
system> users -5 –n guest5 –shp ef92b778bafe771e89245b89ecbc08a44a4e166c06659911881f383d4473e94f – r Administrator
system> users -5 ghp
ef92b778bafe771e89245b89ecbc08a44a4e166c06659911881f383d4473e94f
system> users
Account      Login ID      Advanced Attribute            Role               Password Expires
-------      --------       ------------------            ------              ----------------
1            USERID        Native                         Administrator      Password doesn't expire
5            guest5        Third-party Password          Administrator      90 day(s)
```

comando ifconfig

Utilizzare questo comando per configurare l'interfaccia Ethernet.

Utilizzare il comando **ifconfig** per visualizzare la configurazione corrente dell'interfaccia Ethernet. Per modificare la configurazione dell'interfaccia Ethernet, immettere le opzioni seguite dai valori. Per modificare la configurazione dell'interfaccia, è necessario disporre almeno dell'autorizzazione Configurazione sicurezza e networking adattatore.

Sintassi:
```
ifconfig [ethernet_number] [-options]
```

Esempio:
```
dhcpinfo eth1 -b
```

Tabella 28. opzioni di ifconfig

Opzione	Descrizione	Valori
-state	Stato interfaccia	disabled, enabled
-c	Metodo di configurazione	dhcp, static, dthens (dthens corrisponde all'opzione **Prova server DHCP, se non riesce utilizza configurazione statica** sull'interfaccia Web)
-ghn	Consente di ottenere il nome host da DHCP	disabled, enabled
-i	Indirizzo IP statico	Indirizzo in formato valido.
-g	Indirizzo gateway	Indirizzo in formato valido.
-s	Maschera di sottorete	Indirizzo in formato valido.
-n	Nome host	Una stringa contenente fino a 63 caratteri. La stringa può includere lettere, cifre, punti, caratteri di sottolineatura e trattini.
-auto	L'impostazione di autonegoziazione, che determina se le impostazioni della velocità di trasferimento dati e della rete duplex possono essere configurate	true, false
-vlan	Abilita o disabilita l'etichettatura VLAN	enabled, disabled
-vlanid	ID VLAN	Valore numerico compreso tra 1 e 4.094.
-r	Velocità di trasferimento dati	10, 100, 1000
-d	Modalità duplex	full, half
-m	MTU	Valore numerico compreso tra 60 e 1.500.

Tabella 28. opzioni di ifconfig (continua)

Opzione	Descrizione	Valori
-l	LAA	Formato dell'indirizzo MAC. Gli indirizzi multicast non sono consentiti (il primo byte deve essere pari).
-b	Indirizzo MAC integrato (sola lettura)	
-dn	Nome di dominio (sola lettura)	
-ipv6	Stato IPv6	disabled, enabled
-ipv6static	Stato IPv6 statico	disabled, enabled
-i6	Indirizzo IP statico	Indirizzo IP statico per il canale 0 Ethernet in formato IPv6.
-p6	Lunghezza del prefisso dell'indirizzo	Valore numerico compreso tra 1 e 128.
-g6	Gateway o instradamento predefinito	Indirizzo IP per il gateway o instradamento predefinito per il canale 0 Ethernet in IPv6.
-dhcp6	Modalità DHCP IPv6	enabled, disabled
-sa6	Modalità IPv6 senza stato	enabled, disabled
-lla	Indirizzo locale del collegamento (sola lettura)	
-ncsi	Selezione della porta NIC NCSI	nic[x]:porta[y] **Nota:** Utilizzare la virgola come delimitatore se sono presenti due o più impostazioni.
-nic	Modalità NIC dello switch[1]	shared, dedicated, shared:nic[x][2]
-failover[2]	Modalità failover	none, shared, shared:nic[x]
-nssync[3]	Sincronizzazione delle impostazioni di rete	enabled, disabled
-address_table	Tabella degli indirizzi IPv6 generati automaticamente e relative lunghezze dei prefissi (sola lettura) **Nota:** L'opzione è visibile solo se sono abilitati IPv6 e la configurazione automatica senza stato.	

Nota:

1. -nic mostrerà anche lo stato di nic. [active] indica quale XCC di nic è in uso.

   Ad esempio:
   ```
   -nic: shared:nic3
   nic1: dedicate
   nic2: ext card slot #3
   nic3: ext card slot 5 [active]
   ```
   Indica che nic3 è in modalità condivisa sullo slot 5, nic2 è sullo slot 3, nic1 è la porta dedicata a XCC e XCC utilizza nic3.
2. Il valore shared:nic[x] è disponibile sui server che dispongono di una scheda di rete mezzanino facoltativa. La scheda di rete mezzanino può essere utilizzata da IMM.
3. Se IMM è configurato per utilizzare la porta di rete di gestione dedicata, l'opzione -failover indicherà a IMM di passare alla porta di rete condivisa (shared), se la porta dedicata (dedicated) viene disconnessa.
4. Se la modalità failover è abilitata, l'opzione -nssync indica al modulo IMM di utilizzare le stesse impostazioni di rete utilizzate sulla porta di rete di gestione dedicata per la porta di rete condivisa.

Esempio:

```
system> ifconfig eth0 -c static -i 192.168.70.133
These configuration changes will become active after the next reset of the IMM.
system>
```

comando keycfg

Utilizzare questo comando per visualizzare, aggiungere o eliminare le chiavi di attivazione.

Le chiavi di attivazione controllano l'accesso alle funzioni IMM opzionali.

Nota:

- Aggiungere nuove chiavi di attivazione mediante il trasferimento di file.
- Eliminare vecchie chiavi specificando il numero o il tipo di chiave. Quando si eliminano chiavi in base al tipo, sarà eliminata soltanto la prima chiave del tipo specificato.

Sintassi:

```
keycfg [-options]
```

Tabella 29. opzioni di keycfg

Opzione	Descrizione	Valori
-add	Aggiunge la chiave di attivazione	ip, pn, u, pw, f • **-ip**: indirizzo IP del server TFTP/SFTP con la chiave di attivazione da aggiungere • **-pn**: numero di porta per il server TFTP/SFTP con chiave di attivazione da aggiungere (predefinito 69/22) • **-u**: nome utente per il server SFTP con la chiave di attivazione da aggiungere • **-pw**: password per il server SFTP con la chiave di attivazione da aggiungere • **-f**: nome del file per la chiave di attivazione da aggiungere
-del	Elimina la chiave di attivazione per numero di indice	Il numero di indice della chiave di attivazione valido dall'elenco **keycfg**
-deltype	Elimina la chiave di attivazione per tipo di chiave	Valore del tipo di chiave valido

Quando il comando **keycfg** viene eseguito senza opzioni, sarà visualizzato l'elenco di chiavi di attivazione installate. Le informazioni sulle chiavi visualizzate includono un numero di indice per ciascuna chiave, il tipo di chiave di attivazione, la data fino alla quale è valida la chiave, il numero di utilizzi rimanenti, lo stato della chiave e una descrizione.

Esempio:

```
system> keycfg
ID  Type  Valid           Uses           Status    Description
1   4     10/10/2010      5               "valid"   "IMM remote presence"
2   3     10/20/2010      2               "valid"   "IMM feature
3   32796 NO CONSTRAINTS  NO CONSTRAINTS "valid"   "IBM Security Key Lifecycle Manager for SEDs FoD"
system>
```

Nota: Il campo **Descrizione** per l'ID numero 3 viene visualizzato su righe separate per limitazioni di spazio.

comando ldap

Utilizzare questo comando per visualizzare e configurare i parametri di configurazione del protocollo LDAP.

Sintassi:
```
ldap [-options]
```

Tabella 30. opzioni di ldap

Opzione	Descrizione	Valori
-aom	Modalità di sola autenticazione per gli utenti di Active Directory	enabled, disabled
-a	Metodo di autenticazione utente	• **loc**: solo locale • **ldap**: solo LDAP • **locld**: prima locale, quindi LDAP • **ldloc**: prima LDAP, quindi locale
-b	Metodo di collegamento	• **anon**: anonimo • **client**: collegamento con ClientDN e password • **login**: collegamento con le credenziali di login
-c	Nome distinto client	Stringa contenente un massimo di 127 caratteri per **client_dn**
-d	Dominio di ricerca	Stringa contenente un massimo di 63 caratteri per **search_domain**
-fn	Nome forest	Per ambienti di Active Directory. Stringa contenente un massimo di 127 caratteri.
-f	Filtro di gruppi	Stringa contenente un massimo di 127 caratteri per **group_filter**
-g	Attributo di ricerca gruppi	Stringa contenente un massimo di 63 caratteri per **group_search_attr**
-l	Attributo di autorizzazione di login	Stringa contenente un massimo di 63 caratteri per **string**
-p	Password client	Stringa contenente un massimo di 15 caratteri per **client_pw**
-pc	Conferma password client	Stringa contenente un massimo di 15 caratteri per **confirm_pw** La sintassi del comando è: **client_pw** -pc **confirm_pw** Questa opzione è richiesta quando si modifica la password del client. Essa confronta l'argomento **confirm_pw** con l'argomento **client_pw**. Il comando non riuscirà se gli argomenti non corrispondono.
-r	Nome distinto voce radice	Stringa contenente un massimo di 127 caratteri per **root_dn**
-s1ip	Indirizzo IP/nome host server 1	Stringa contenente un massimo di 127 caratteri o un indirizzo IP per **host name/ip_addr**
-s2ip	Indirizzo IP/nome host server 2	Stringa contenente un massimo di 127 caratteri o un indirizzo IP per **host name/ip_addr**
-s3ip	Indirizzo IP/nome host server 3	Stringa contenente un massimo di 127 caratteri o un indirizzo IP per **host name/ip_addr**
-s4ip	Indirizzo IP/nome host server 4	Stringa contenente un massimo di 127 caratteri o un indirizzo IP per **host name/ip_addr**

Tabella 30. opzioni di ldap (continua)

Opzione	Descrizione	Valori
-s1pn	Numero di porta server 1	Un valore numerico per la porta costituito da un massimo di 5 cifre per **port_number**
-s2pn	Numero di porta server 2	Un valore numerico per la porta costituito da un massimo di 5 cifre per **port_number**
-s3pn	Numero di porta server 3	Un valore numerico per la porta costituito da un massimo di 5 cifre per **port_number**
-s4pn	Numero di porta server 4	Un valore numerico per la porta costituito da un massimo di 5 cifre per **port_number**
-u	Attributo di ricerca del nome di login dell'utente	Stringa contenente un massimo di 63 caratteri per **search_attrib**
-v	Ottiene l'indirizzo del server LDAP mediante DNS	off, on
-h	Visualizza le opzioni e l'uso del comando	

Esempio:
```
system> ldap
   -aom enable
   -a   locld
   -b   client
   -c   cn=admin,dc=lenovo,dc=com
   -d
   -fn
   -f   example.com
   -g   cn
   -l   XCC3RBSPermissions
   -r
   -s1ip 10.241.99.94
   -s2ip
   -s3ip
   -s4ip
   -s1pn 389
   -s2pn 389
   -s3pn 389
   -s4pn 389
   -u uid
   -v off
system>
```

comando ntp

Utilizzare questo comando per visualizzare e configurare il protocollo NTP (Network Time Protocol).

Sintassi:
```
ntp [-options]
```

Tabella 31. comando ntp

Opzione	Descrizione	Valori
-en	Abilita o disabilita il protocollo NTP (Network Time Protocol).	enabled, disabled
-i**[x]**	Nome o indirizzo IP del server NTP (Network Time Protocol) per l'indice **x**.	Il nome del server NTP da utilizzare per la sincronizzazione dell'orologio. L'intervallo dei numeri di indice del server NTP è da -i1 a -i4. **Nota:** -i è uguale a i1.
-f	La frequenza (in minuti) con cui l'orologio IMM viene sincronizzato con il server NTP (Network Time Protocol).	Da 3 a 1.440 minuti.
-synch	Richiede una sincronizzazione immediata con il server NTP (Network Time Protocol).	Nessun valore è utilizzato con questo parametro.

Esempio:
```
system> ntp
-en: disabled
-f: 3 minutes
-i: not set
```

comando portcontrol

Utilizzare questo comando per attivare o disattivare una porta di servizio di rete.

Sintassi:
```
portcontrol [-options]
```

Tabella 32. opzioni di portcontrol

Opzione	Descrizione	Valori
-ipmi	Abilita o disabilita l'accesso ipmi tramite LAN	on, off
-ipmi-kcs	Abilita on demand, abilita o disabilita l'accesso ipmi dal server	auto, on, off
-rest	Abilita o disabilita il rilevamento REST	on, off
-snmp	Abilita o disabilita il rilevamento SNMP	on, off
-ssdp	Abilita o disabilita il rilevamento SSDP	on, off
-cli	Abilita o disabilita il rilevamento CLI	on, off
-web	Abilita o disabilita il rilevamento WEB	on, off
-all	Abilita o disabilita tutte le interfacce e i protocolli di rilevamento	on, off

Esempio:

```
system> portcontrol
ipmi : on
ipmi-kcs : on
rest : on
snmp : off
ssdp : on
cli : on
web : on
system>
```

comando ports

Utilizzare questo comando per visualizzare e configurare le porte di IMM.

Sintassi:

```
ports [-options]
```

Tabella 33. opzioni di ports

Opzione	Descrizione	Valori
-open	Visualizza le porte aperte (sola lettura)	
-reset	Ripristina impostazioni predefinite delle porte (sola lettura)	
-http	Numero di porta HTTP	Numero di porta predefinito: 80
-https	Numero di porta HTTPS	Numero di porta predefinito: 443
-ssh	Numero di porta della CLI legacy SSH	Numero di porta predefinito: 22
-snmpa	Numero di porta agent SNMP	Numero di porta predefinito: 161
-snmpt	Numero di porta trap SNMP	Numero di porta predefinito: 162
-rp	Numero di porta presenza remota	Numero di porta predefinito: 3900

Esempio:

```
system> ports
  -http 80
  -https 443
  -rp 3900
  -snmpa 161
  -snmpt 162
  -ssh 22
system>
```

comando rdmount

Utilizzare questo comando per montare immagini del disco remoto o condivisioni di rete

Nota:

- Nella memoria di XClarity Controller è possibile caricare fino a due file, i quali possono essere montati come supporti virtuali utilizzando la funzione RDOC di XClarity Controller. La dimensione totale di entrambi i file non deve superare 50 MB. Le immagini caricate sono in sola lettura, tranne se viene utilizzata l'opzione -rw.

- Quando si utilizzano i protocolli HTTP, SFTP o FTP per montare o associare le immagini, la dimensione totale di tutte le immagini può essere massimo di 50 MB. Se vengono utilizzati i protocolli NFS o SAMBA non vi è alcun limite di dimensione.

Sintassi:
```
rdmount [-options]
```

Tabella 34. opzioni di rdmount

Opzione	Descrizione
-r	operazione rdoc (se utilizzata, deve essere la prima opzione) -r -map: monta le immagini RDOC -r -unmap<filename>: smonta le immagini RDOC montate -r -maplist: mostra le immagini RDOC montate mediante il browser Web di XClarity Controller e l'interfaccia CLI
-map	-t <samba|nfs|http|sftp|ftp> tipo di file system -ro sola lettura -rw lettura-scrittura -u utente -p password -l percorso file (formato URL) -o opzione (stringa di opzione extra per montaggi samba e nfs) -d dominio (dominio per montaggio samba)
-maplist	Mostra le immagini associate
-unmap	<id|fname> utilizza l'ID con le immagini di rete, nome del file con rdoc
-mount	Monta le immagini associate
-unmount	Smonta le immagini montate

comando restore

Utilizzare questo comando per ripristinare le impostazioni del sistema da un file di backup.

Sintassi:
```
restore [-options]
```

Tabella 35. opzioni di restore

Opzione	Descrizione	Valori
-f	Nome file di backup	Nome file valido
-pp	La password o la pass-phrase utilizzata per crittografare le password all'interno del file di backup	Password o pass-phrase valida racchiusa tra virgolette
-ip	Indirizzo IP del server TFTP/SFTP	Indirizzo IP valido

Tabella 35. opzioni di restore (continua)

Opzione	Descrizione	Valori
-pn	Numero di porta del server TFTP/ SFTP	Numero di porta valido (valore predefinito 69/22)
-u	Nome utente per il server SFTP	Nome utente valido
-pw	Password per il server SFTP	Password valida

Esempio:
```
system> restore f xcc-back.cli pp xxxxxx ip 192.168.70.200
ok
system>
```

comando roles

Utilizzare questo comando per visualizzare o configurare i ruoli.

Sintassi:
```
roles role_account[3-31] [-options]
```

Tabella 36. opzioni di roles

Opzione	Descrizione	Valori
-n	Nome del ruolo	Limite di 32 caratteri
-p	Consente di impostare privilegi	custom:am, rca, rcvma, pr, cel, bc, nsc, ac, us • **am**: accesso alla gestione dell'account utente • **rca**: accesso alla console remota • **rcvma**: accesso alla console remota e al disco remoto (supporto virtuale) • **pr**: accesso all'accensione o al riavvio del server remoto • **cel**: possibilità di cancellare i log eventi • **bc**: configurazione adattatore (base) • **nsc**: configurazione adattatore (rete e sicurezza) • **ac**: configurazione adattatore (avanzata) • **us**: sicurezza UEFI **Nota:** I contrassegni di autorizzazione personalizzati di cui sopra possono essere utilizzati in qualsiasi combinazione
-d	Consente di eliminare una riga	

Esempio:
```
system> roles -3 -n test1 -p custom:am|rca|rcvma
ok


system> roles
Account              Role                              Privilege                    Assigned To
```

```
------- ---------------------------------   ------------------------     ------------------------------
    0                    Administrator                    all                          USERID
    1                        ReadOnly                       none
    2                        Operator           custom:pr|cel|bc|nsc
    3                           test1            custom:am|rca|rcvma
```

comando rtd

Utilizzare questo comando per ripristinare tutte le impostazioni BMC predefinite originali.

Nota: In precedenza questo comando era denominato **restoredefaults** e **clearcfg**.

Sintassi:
```
rtd [-options]
```

Tabella 37. opzioni rtd

Opzione	Descrizione
-all	Ripristina tutte le impostazioni BMC predefinite originali.
-eu	Ripristina tutte le impostazioni BMC predefinite originali, tranne le impostazioni utente.
-en	Ripristina tutte le impostazioni BMC predefinite originali, tranne le impostazioni di rete.
-eun	Ripristina tutte le impostazioni BMC predefinite originali, tranne le impostazioni di utente e di rete.

Esempio:
```
system> rtd -all

This action will cause all IMM settings to be set to factory defaults.

If this is the local system, you will lose your TCP/IP connection as a result.
You will need to reconfigure the IMM network interface to restore connectivity.
After the IMM configuration is cleared, the IMM will be restarted.

Proceed? (y/n)
Y
Restoring defaults
```

comando seccfg

Utilizzare questo comando eseguire il rollback del firmware.

Sintassi:
```
seccfg [-options]
```

Tabella 38. opzioni di seccfg

Opzione	Descrizione	Valore
-fwrb	Consente di eseguire il rollback del firmware alle versioni precedenti.	enabled, disabled
-aubp	Abilita o disabilita la funzione di backup automatico per la promozione primaria.	enabled, disabled

comando securityinfo

Questo comando viene utilizzato per visualizzare le informazioni relative alla sicurezza.

Sintassi:
```
securityinfo [-options]
```

Tabella 39. opzioni di securityinfo

Opzione	Descrizione
-event	Visualizza gli eventi di sicurezza.
-cryptomode	Visualizza lo stato della modalità di crittografia di sicurezza.
-service	Visualizza lo stato di sicurezza dei servizi e delle porte.
-cert	Visualizza lo stato di sicurezza del certificato.
-account	Visualizza lo stato di sicurezza degli account utente.

comando securitymode

Questo comando viene utilizzato per generare un nuovo file di dati di servizio.

Sintassi:
```
securitymode [-options]
```

Tabella 40. opzioni di securitymode

Opzione	Descrizione	Valori
-mode	Seleziona la modalità di sicurezza. • CNSA - Rigorosa aziendale • FIPS - Standard • COMPAT- Compatibilità	CNSA, FIPS, COMPAT • **CNSA**: sono consentiti solo i servizi che supportano la crittografia di livello rigoroso aziendale. Per l'abilitazione è richiesta la chiave Feature on Demand. • **FIPS**: i servizi che richiedono la crittografia e che non supportano la crittografia di livello standard sono disabilitati per impostazione predefinita. • **COMPAT**: quando questa modalità è abilitata, XCC NON funziona in modalità di convalida standard. Consente di abilitare tutti i servizi.
-h	Elenca l'utilizzo e le opzioni.	

comando set

Utilizzare questo comando per modificare alcune impostazioni IMM.

- Alcune impostazioni IMM possono essere modificate con un semplice comando **set**.
- Alcune di queste impostazioni, come le variabili d'ambiente, sono utilizzate dalla CLI.

La seguente tabella mostra gli argomenti per le opzioni.

Tabella 41. comando set

La seguente tabella a riga singola con tre colonne contiene la descrizione dei comandi e le informazioni associate.

Tabella 41. comando set (continua)

Opzione	Descrizione	Valori
value	Imposta il valore per il percorso o l'impostazione specificati	Valore appropriato per il percorso o l'impostazione specificati.

Sintassi:
```
set [-options]
option:
  value
```

comando snmp

Utilizzare questo comando per visualizzare e configurare le informazioni sull'interfaccia SNMP.

Sintassi:
```
snmp [-options]
```

Tabella 42. opzioni di snmp

Opzione	Descrizione	Valori
-a3	Agent SNMPv3	on, off **Nota:** Per abilitare l'agent SNMPv3, devono essere soddisfatti i seguenti criteri: • Contatto di IMM specificato mediante l'opzione del comando -cn. • Posizione di IMM specificata mediante l'opzione del comando -l.
-t	Trap SNMPv3	on, off
-tn	Nome utente del trap SNMPv3	Nome utente valido
-tauth	Protocollo di autenticazione del trap SNMPv3	nessuno, HMAC-SHA
-tapw	Password di autenticazione del trap SNMPv3	Password valida
-tpriv	Protocollo di privacy del trap SNMPv3	nessuno, CBC-DES, AES
-tppw	Password per la privacy del trap SNMPv3	Password valida
-tix	Nome host o indirizzo IP della comunità **x**	Indirizzo IP o nome host valido (limitato a 63 caratteri, **x** può variare da 1 a 3). **Nota:** • Un indirizzo IP o nome host può contenere solo punti, caratteri di sottolineatura, segni meno, lettere e cifre. Non sono consentiti spazi integrati o punti consecutivi. • Cancellare un indirizzo IP o un nome host della comunità non specificando alcun argomento.
-l	Posizione di IMM	Stringa (massimo 47 caratteri). **Nota:** • Gli argomenti contenenti spazi devono essere racchiusi tra virgolette. Non sono consentiti spazi iniziali o finali negli argomenti. • Cancellare la posizione di IMM non specificando alcun argomento o specificando una stringa vuota come argomento, ad esempio "".

Tabella 42. opzioni di snmp (continua)

Opzione	Descrizione	Valori
-cn	Nome contatto di IMM	Stringa (massimo 47 caratteri). **Nota:** • Gli argomenti contenenti spazi devono essere racchiusi tra virgolette. Non sono consentiti spazi iniziali o finali negli argomenti. • Cancellare il nome del contatto di IMM, non specificando alcun argomento o specificando una stringa vuota come argomento, ad esempio "".
-t1	Trap SNMPv1	on, off
-c	Nome della comunità SNMP	Stringa (massimo 15 caratteri). **Nota:** • Gli argomenti contenenti spazi devono essere racchiusi tra virgolette. Non sono consentiti spazi iniziali o finali negli argomenti. • Cancellare il nome della comunità SNMP specificando nessun argomento o specificando una stringa vuota come argomento, ad esempio "".
-ci	Nome host/indirizzo IP della comunità 1	Indirizzo IP o nome host valido (massimo 63 caratteri). **Nota:** • Un indirizzo IP o nome host può contenere solo punti, caratteri di sottolineatura, segni meno, lettere e cifre. Non sono consentiti spazi integrati o punti consecutivi. • Cancellare un indirizzo IP o un nome host della comunità non specificando alcun argomento.
-c1iy	Nome host/indirizzo IP della comunità **y**	Indirizzo IP o nome host valido (limitato a 63 caratteri, **y** può essere 2 o 3). **Nota:** • Un indirizzo IP o nome host può contenere solo punti, caratteri di sottolineatura, segni meno, lettere e cifre. Non sono consentiti spazi integrati o punti consecutivi. • Cancellare un indirizzo IP o un nome host della comunità non specificando alcun argomento.
-t2	Trap SNMPv2	on, off
-ct	Nome della comunità trap SNMPv2	Stringa (massimo 15 caratteri). **Nota:** • Gli argomenti contenenti spazi devono essere racchiusi tra virgolette. Non sono consentiti spazi iniziali o finali negli argomenti. • Cancellare il nome del contatto di IMM, non specificando alcun argomento o specificando una stringa vuota come argomento, ad esempio "".
-cti	Indirizzo IP/nome host della comunità del trap SNMPv2 1	Indirizzo IP o nome host valido (massimo 63 caratteri). **Nota:** • Un indirizzo IP o nome host può contenere solo punti, caratteri di sottolineatura, segni meno, lettere e cifre. Non sono consentiti spazi integrati o punti consecutivi. • Cancellare un indirizzo IP o un nome host della comunità SNMP non specificando alcun argomento.

Tabella 42. opzioni di snmp (continua)

Opzione	Descrizione	Valori
-eid	ID motore SNMP	Stringa (massimo 1-27 caratteri)
-send	Invia informazioni su un trap di verifica	

Esempio:
```
system> snmp
-t enabled
-a3 enabled
-l ZhangjiangMansion
-cn Kelvin
-t1 enabled
-c community1
-ci host1
-t2 enabled
-ct community2
-cti host2
-eid XCC-7Z70-DSYM09X
system>
```

comando snmpalerts

Utilizzare questo comando per gestire gli avvisi inviati via SNMP.

Sintassi:
```
snmpalerts [-options]
```

Tabella 43. opzioni di snmpalerts

Opzione	Descrizione	Valori
-status	Stato avviso SNMP	on, off
-crt	Imposta gli eventi critici che inviano gli avvisi	all, none, custom:te|vo|po|di|fa|cp|me|in|re|ot|pc Le impostazioni personalizzate degli avvisi gravi sono specificate mediante un elenco di valori separati da barre verticali nel formato **snmpalerts -crt custom:te|vo**, dove i valori personalizzati sono: • te: soglia di temperatura critica superata • vo: soglia di voltaggio critica superata • po: errore grave di alimentazione • di: errore dell'unità disco fisso • fa: errore della ventola • cp: errore del microprocessore • me: errore di memoria • in: incompatibilità hardware • re: errore di ridondanza alimentazione • ot: tutti gli altri eventi critici • pc: eventi critici PCIe

Tabella 43. opzioni di snmpalerts (continua)

Opzione	Descrizione	Valori
-wrn	Imposta gli eventi di avvertenza che inviano gli avvisi	all, none, custom:rp|te|vo|po|fa|cp|me|ot|pw Le impostazioni personalizzate degli avvisi di avvertenza sono specificate mediante un elenco di valori separati da barre verticali nel formato **snmpalerts -wrn custom:rp|te**, dove i valori personalizzati sono: • rp: avvertenza di ridondanza alimentazione • te: soglia di temperatura di avvertenza superata • vo: soglia di voltaggio di avvertenza superata • po: soglia di alimentazione di avvertenza superata • fa: evento della ventola non critico • cp: microprocessore in stato danneggiato • me: avvertenza di memoria • ot: tutti gli altri eventi di avvertenza • pw: eventi di avviso PCIe
-sys	Imposta gli eventi di routine che inviano gli avvisi	all, none, custom:lo|tio|ot|po|bf|til|pf|el|ne|nl|dh|oa Le impostazioni personalizzate degli avvisi di routine sono specificate mediante un elenco di valori separati da barre verticali nel formato **snmpalerts -sys custom:lo|tio**, dove i valori personalizzati sono: • lo: login remoto riuscito correttamente • tio: timeout del sistema operativo • ot: tutti gli altri eventi di sistema e informativi • po: sistema acceso/spento • bf: errore di avvio del sistema operativo • til: timeout watchdog del programma di caricamento del sistema operativo • pf: PFA (predicted failure) • el: log di eventi pieno al 75% • ne: modifica di rete • nl: collegamento NIC host inattivo/attivo • dh: hotplug dell'unità • oa: tutti gli altri eventi di controllo

comando sshcfg

Utilizzare questo comando per visualizzare e configurare i parametri SSH.

Sintassi:
```
sshcfg [-options]
```

Tabella 44. opzioni di sshcfg

Opzione	Descrizione	Valori
-cstatus	Lo stato della CLI di SSH	enabled, disabled
-hk	Chiave del server	gen, all • **gen**: genera la chiave privata del server SSH • **all**: visualizza la chiave pubblica del server

Esempio:
```
system> sshcfg
-cstatus enabled
CLI SSH port 22
ssh-rsa 2048 bit fingerprint: b4:a3:5d:df:0f:87:0a:95:f4:d4:7d:c1:8c:27:51:61
1 SSH public keys installed
system>
```

comando sslcfg

Utilizzare questo comando per visualizzare e configurare SSL per IMM e gestire i certificati.

Il comando **sslcfg** viene utilizzato per generare una nuova chiave di crittografia e un certificato autofirmato o una richiesta di firma del certificato (CSR).

Sintassi:
```
sslcfg [-options]
```

Tabella 45. opzioni di sslcfg

Opzione	Descrizione	Valori
-server	Stato Web-over-HTTPS	enabled, disabled **Nota:** • Web-over-HTTPS può essere abilitato solo se è presente un certificato. • Utilizzare **-rm** per disabilitare completamente il certificato.
-client	Stato LDAP sicuro	enabled, disabled **Nota:** Il client SSL può essere abilitato solo se è presente un certificato client o server valido.
-cert	Genera un certificato autofirmato	server, client, sysdir, storekey **Nota:** • I valori per le opzioni dei comandi **-c**, **-sp**, **-cl**, **-on** e **-hn** sono richiesti per la generazione di un certificato autofirmato. • I valori per le opzioni dei comandi **-cp**, **-ea**, **-ou**, **-s**, **-gn**, **-in** e **-dq** sono facoltativi quando si genera un certificato autofirmato.
-csr	Genera CSR	server, client, sysdir, storekey **Nota:** • I valori per le opzioni dei comandi **-c**, **-sp**, **-cl**, **-on** e **-hn** sono richiesti quando si genera una CSR. • I valori per le opzioni dei comandi **-cp**, **-ea**, **-ou**, **-s**, **-gn**, **-in**, **-dq**, **-cpwd** e **-un** sono facoltativi quando si genera una CSR.

Tabella 45. opzioni di sslcfg (continua)

Opzione	Descrizione	Valori
-form	Formato della CSR o del certificato di cui verrà eseguita l'esportazione.	der, pem (pem è il valore predefinito)
-algo	Algoritmo CSR	p256, p384, rsa2048, rsa3072, rsa4096 **Nota:** Verrà impostato un valore predefinito (p256) se non è presente un'opzione -algo.
-rm	Rimuove il certificato	server, storekey **Nota:** Un certificato autofirmato predefinito (server) verrà generato automaticamente dopo la rimozione di quello corrente.
-i	Indirizzo IP per il server TFTP/SFTP	Indirizzo IP valido **Nota:** Un indirizzo IP per il server TFTP o SFTP deve essere specificato quando si carica un certificato o quando si scarica un certificato o una CSR.
-pn	Numero di porta del server TFTP/SFTP	Numero di porta valido (valore predefinito 69/22)
-u	Nome utente per il server SFTP	Nome utente valido
-pw	Password per il server SFTP	Password valida
-l	Nome file certificato	Nome file valido **Nota:** Un nome file è necessario quando si scarica o si carica un certificato o una CSR. Se non viene specificato alcun nome file per il download, verrà utilizzato e visualizzato il nome predefinito.
-dnld	Esporta il file specificato nell'host remoto	Questa opzione non utilizza alcun argomento, ma deve essere utilizzata con le opzioni **-cert** o **-csr** e **-i** e **-l** del comando.
-upld	Importa il file del certificato	Questa opzione non utilizza alcun argomento ma è necessario specificare i valori anche per le opzioni dei comandi **-cert**, **-i** e **-l**.
-tc**x**	Certificato attendibile **x** per il client SSL	import, download, remove **Nota:** Il numero del certificato attendibile, **x**, è specificato come numero intero compreso tra 1 e 4 nell'opzione del comando.
Opzioni necessarie per la generazione di un certificato autofirmato o di una CSR **Nota:** Obbligatorio quando si genera un certificato autofirmato o una CSR.		
-c	Paese	Il codice paese (2 lettere)
-sp	Stato o provincia	Stringa racchiusa tra virgolette (massimo 60 caratteri)
-cl	Città o località	Stringa racchiusa tra virgolette (massimo 50 caratteri)
-on	Nome organizzazione	Stringa racchiusa tra virgolette (massimo 60 caratteri)
-hn	Nome host BMC	Stringa (massimo 60 caratteri)
Opzioni opzionali per la generazione di un certificato autofirmato o di una CSR **Nota:** Facoltativo quando si genera un certificato autofirmato o una CSR.		
-cp	Contatto	Stringa racchiusa tra virgolette (massimo 60 caratteri)
-ea	Indirizzo e-mail della persona di contatto	Indirizzo e-mail valido (massimo 60 caratteri)
-ou	Unità organizzativa	Stringa racchiusa tra virgolette (massimo 60 caratteri)
-s	Cognome	Stringa racchiusa tra virgolette (massimo 60 caratteri)

Tabella 45. opzioni di sslcfg (continua)

Opzione	Descrizione	Valori
-gn	Nome	Stringa racchiusa tra virgolette (massimo 60 caratteri)
-in	Iniziali	Stringa racchiusa tra virgolette (massimo 20 caratteri)
-dq	Qualificatore nome di dominio	Stringa racchiusa tra virgolette (massimo 60 caratteri)
Opzioni facoltative per la generazione di una CSR **Nota:** Facoltativo quando si genera una CSR.		
-cpwd	Invalida password	Stringa (minimo 6 caratteri, massimo 30 caratteri)
-un	Nome non strutturato	Stringa racchiusa tra virgolette (massimo 60 caratteri)

Esempi:

```
system> sslcfg
-server enabled
-client disabled
-sysdir enabled
SSL Server Certificate status:
 A self-signed certificate is installed
SSL Client Certificate status:
 A self-signed certificate is installed
SSL Client Trusted Certificate status:
 Trusted Certificate 1: Not available
 Trusted Certificate 2: Not available
 Trusted Certificate 3: Not available
 Trusted Certificate 4: Not available
```

Esempi di certificati dei client:

- Per generare una CSR per una chiave di storage, immettere il seguente comando:
  ```
  system> sslcfg -csr storekey -c US -sp NC -cl rtp -on LNV -hn XCC-5cf3fc -cp Contact -ea "" -ou""
  ok
  ```
- Per scaricare un certificato da IMM su un altro server, immettere il seguente comando:
  ```
  system> sslcfg -csr storekey -dnld -i 192.168.70.230 -l storekey.csr
  ok
  ```
- Per caricare il certificato elaborato dall'autorità di certificazione (CA), immettere il seguente comando:
  ```
  system> sslcfg -cert storekey -upld -i 192.168.70.230 -l tklm.der
  ```
- Per generare un certificato autofirmato, immettere il seguente comando:
  ```
  system> sslcfg -cert storekey -c US -sp NC -cl rtp -on LNV -hn XCC-5cf3fc -cp Contact -ea "" -ou "
  ok
  ```

Esempio di certificato server SKLM:

- Per importare il certificato server SKLM, immettere il seguente comando:
  ```
  system> storekeycfg -add -ip 192.168.70.200 -f tklm-server.der
  ok
  ```

comando syslock

Utilizzare questo comando per visualizzare e configurare le impostazioni di blocco del sistema.

Sintassi:
```
syslock [-options]
```

Tabella 46. opzioni di syslock

Opzione	Descrizione	Valori
-en	Abilita o disabilita la funzione di blocco della configurazione di sistema. **Nota:** L'abilitazione con l'opzione **-e** può promuovere l'inventario corrente come istantanea attendibile.	enabled, disabled
-e	Abilita le impostazioni di blocco della configurazione di sistema con o senza applicare l'inventario corrente in un'istantanea attendibile. **Nota:** Verrà impostato un valore predefinito se non è presente un'opzione **-e**.	enabled, disabled
-l **[x]**	Elenca l'inventario di un'istantanea specifica nell'indice **x**.	Il numero di indice, x, viene specificato come numero intero nell'opzione del comando.
-m	Crea un'istantanea manuale.	
-d	Descrizione dell'istantanea manuale.	Stringa contenente un massimo di 32 caratteri.
-c	Elenca le differenze dell'inventario rispetto all'istantanea attendibile.	
-po	Imposta i criteri di blocco. **Nota:** L'azione impedirà l'avvio del server se Controllo del sistema è in uno stato non conforme.	none, osboot, pperm
-cpu	Imposta il blocco CPU.	on, off
-dimm	Imposta il blocco DIMM.	on, off
-pci	Imposta il blocco PCI.	on, off
-drive	Imposta il blocco dell'unità.	on, off
-riser	Imposta il blocco della scheda verticale.	on, off
-bp	Imposta il blocco bp.	on, off

comando thermal

Utilizzare questo comando per visualizzare e configurare i criteri della modalità termica del sistema host.

L'esecuzione del comando **thermal** senza opzioni visualizza i criteri della modalità termica. La seguente tabella mostra gli argomenti per le opzioni.

Sintassi:
```
thermal [-options]
```

Tabella 47. opzioni di thermal

Opzione	Descrizione	Valori
-mode	Visualizza i criteri della modalità termica e configura la tabella termica dei sistemi host (sola lettura)	• Elaborazione generale - Efficienza energetica • Elaborazione generale - Frequenza di picco • Elaborazione generale - Prestazione massima • Virtualizzazione - Efficienza energetica • Virtualizzazione - Prestazione massima • Database - Elaborazione delle transazioni • Bassa latenza • High Performance Computing • Personalizzato • Sconosciuto
-table **table_number**	**table_number** specifica quale tabella termica alternativa utilizzare.	1 = Basso: incremento minimo della velocità della ventola 2 = Medio: incremento moderato della velocità della ventola 3 = Alto: incremento elevato della velocità della ventola 0 = Normale: nessun incremento della velocità della ventola

Esempio:
```
system> thermal
-mode normal
-table 80860126 1 10DE0DFA 3
system>
```

comando tls

Utilizzare questo comando per impostare il livello minimo di TLS.

Sintassi:
```
tls [-options]
```

Tabella 48. opzioni di tls

Opzione	Descrizione	Valori
-min	Seleziona il livello minimo di TLS	1.2, 1.3 **Nota:** Quando la crittografia è impostata in modalità di conformità NIST-800-131A, la versione di TLS deve essere impostata su 1.2.
-h	Elenca l'uso e le opzioni	
Nota: 1. Quando la crittografia è impostata in modalità di conformità NIST-800-131A, la versione di TLS deve essere impostata su 1.2.		

Esempi:

Per indicazioni sull'utilizzo del comando tls, eseguire questo comando:
```
system> tls
-h
system>
```

Per ottenere la versione corrente di tls, eseguire questo comando:
```
system> tls
-min 1.2
system>
```

Per modificare la versione corrente di tls in 1.2, eseguire questo comando:
```
system> tls -min 1.2
ok
system>
```

comando trespass

Utilizzare questo comando per configurare e visualizzare i messaggi di sconfinamento.

Il comando **trespass** può essere utilizzato per configurare e visualizzare i messaggi di sconfinamento. I messaggi di sconfinamento verranno visualizzati a qualsiasi utente che accederà tramite l'interfaccia WEB o CLI.

Sintassi:
```
trespass [-options]
```

Tabella 49. opzioni di trespass

Opzione	Descrizione
-s	Consente di configurare i messaggi di sconfinamento
-h	Elenca l'uso e le opzioni

Esempio:
```
system> trespass -s testingmessage
ok
system> trespass
testingmessage
system>
system> trespass -s "testing message"
ok
system> trespass
testing message
system>
```

comando uefipw

Utilizzare questo comando per configurare le password di amministratore UEFI. La password è di sola scrittura.

Il comando **uefipw** può essere utilizzato con l'opzione "-p" per configurare la password di amministratore UEFI per XCC o con l'opzione "-ep" affinché LXCA l'interfaccia CLI per configurare la password di amministratore UEFI. La password è di sola scrittura.

Sintassi:
```
uefipw [-options]
```

Tabella 50. opzioni di uefipw

Opzione	Descrizione
-cp	Password corrente (limite di 20 caratteri)
-p	Password nuova (limite di 20 caratteri)

comando usbeth

Utilizzare questo comando per abilitare o disabilitare l'interfaccia LAN su USB in banda.

Nota:

- Le impostazioni di configurazione IP del sistema operativo non vengono utilizzate per impostare l'indirizzo IP del sistema operativo dell'interfaccia Ethernet-over-USB, ma per avvisare BMC che tale indirizzo è stato modificato.
- Prima di configurare le tre impostazioni IP di Ethernet-over-USB, è necessario configurare manualmente l'indirizzo IP del sistema operativo dell'interfaccia Ethernet-over-USB nel sistema operativo locale.

Sintassi:
```
usbeth [-options]
```

Tabella 51. opzioni di usbeth

Opzione	Descrizione	Valori
-en	Abilita o disabilita l'interfaccia in banda (Ethernet-over-USB).	enabled, disabled
-am	Consente di selezionare la modalità indirizzo LLA IPv4 o IPv6.	ipv4, ipv6lla
Nota: Le opzioni -ip, -sn e -ipos sono valide solo quando è selezionata la modalità -am ipv4		
-ip	Indirizzo IP dell'interfaccia Ethernet-over-USB per BMC.	Indirizzo IP valido
-sn	Maschera di sottorete dell'interfaccia Ethernet-over-USB per BMC.	Indirizzo IP valido
-ipos	Indirizzo IP dell'interfaccia Ethernet-over-USB per il sistema operativo.	Indirizzo IP valido

Esempio:
```
system> usbeth
-en : disabled
system> usbeth -en enabled
ok
system> usbeth
-en : disabled
system>
```

comando users

Utilizzare questo comando per accedere a tutti gli account utente e ai relativi livelli di autorizzazione.

Il comando **users** è utilizzato anche per creare nuovi account utente o per modificarne di esistenti.
L'esecuzione del comando **users** senza opzioni visualizza un elenco di utenti e alcune informazioni di base.

Sintassi:
```
users [-user_index] [-options]
```

Tabella 52. opzioni di users

Opzione	Descrizione	Valori
-user_index	Numero di indice account utente.	Dove **user_index** è un numero da 1 a 12 (inclusi) o **all** per tutti gli utenti.
-l	Visualizza i giorni di scadenza della password	
-n	Nome account utente	Stringa univoca contenente solo numeri, lettere, punti e caratteri di sottolineatura. Minimo 4 caratteri e massimo 16.
-p	Password dell'account utente	Stringa che contiene almeno un carattere alfabetico e uno non alfabetico. Minimo 6 e massimo 255 caratteri. Un valore null crea un account senza una password che l'utente deve impostare durante il primo login.
-shp	Imposta la password con hash	64 caratteri in totale
-ssalt	Imposta salt	Limite di 64 caratteri
-ghp	Ottiene hashpassword	
-gsalt	Ottiene salt	
-ep	Password di crittografia (per backup/ripristino)	Password valida
-esalt	salt per password crittografata	Solo per il backup o il ripristino
-r	Nome del ruolo	Administrator, Operator, ReadOnly. Come elencato nel comando "comando roles" a pagina 123.
-clear	Cancella l'account utente specificato	Il numero di indice dell'account utente da cancellare deve essere specificato nel seguente formato: `users -clear -user_index` **Nota:** Se si è autorizzati, è possibile rimuovere il proprio account o l'account di altri utenti (anche se sono attualmente collegati), purché non sia l'unico account rimanente con privilegi di gestione account utente. Le sessioni già in corso al momento dell'eliminazione degli account utente non verranno terminate automaticamente.
-curr	Visualizza gli utenti correntemente collegati	
-ai	Interfaccia accessibile all'utente	web, ssh, redfish, ipmi, snmp, all **Nota:** Verrà impostato un valore predefinito (web|ssh|redfish) se l'opzione -ai non è presente.
-sauth	Protocollo di autenticazione SNMPv3	None, HMAC_MD5, HMAC_SHA96, HMAC128_SHA224, HMAC192_SHA256, HMAC256_SHA384, HMAC384_SHA512
-spriv	Protocollo privacy SNMPv3	None, CBC_DES, CFB128_AES128, AES192, AES256, AES192C, AES256C
-spw	Password della privacy SNMPv3	Password valida
-sepw	Password della privacy SNMPv3 (crittografata)	Password valida
-sacc	Tipo di accesso SNMPv3	get
-strap1	Nome host trap SNMPv3 1	Nome host valido

Tabella 52. opzioni di users (continua)

Opzione	Descrizione	Valori
-strap2	Nome host trap SNMPv3 2	Nome host valido
-strap3	Nome host trap SNMPv3 3	Nome host valido
-pk	Visualizza la chiave pubblica SSH per l'utente	Numero di indice account utente. **Nota:** • Ogni chiave SSH assegnata all'utente viene visualizzata con un numero di indice della chiave di identificazione. • Quando si utilizzano le opzioni delle chiavi pubbliche SSH, è necessario utilizzare l'opzione `-pk` dopo l'indice utente (opzione `-userindex`) nel formato: `users -2 -pk`. • Tutte le chiavi sono in formato OpenSSH.
Le seguenti opzioni vengono utilizzate insieme a -pk		
-e	Visualizza l'intera chiave SSH in formato OpenSSH **(opzione di chiave pubblica SSH)**	Questa opzione non utilizza alcun argomento e deve essere utilizzata senza le altre opzioni `users -pk`. **Nota:** Quando si utilizzano le opzioni delle chiavi pubbliche SSH, è necessario utilizzare l'opzione `-pk` dopo l'indice utente (opzione `-userindex`) nel formato: `users -2 -pk -e`.
-remove	Rimuove la chiave pubblica SSH dall'utente **(opzione di chiave pubblica SSH)**	Il numero di indice della chiave pubblica da rimuovere deve essere specificato come `-key_index` o `-all` per tutte le chiavi assegnate all'utente. **Nota:** Quando si utilizzano le opzioni delle chiavi pubbliche SSH, è necessario utilizzare l'opzione `-pk` dopo l'indice utente (opzione `-userindex`) nel formato: `users -2 -pk -remove -1`.
-add	Aggiunge la chiave pubblica SSH per l'utente **(opzione di chiave pubblica SSH)**	Chiave racchiusa tra virgolette in formato OpenSSH **Nota:** • L'opzione `-add` è utilizzata senza tutte le altre opzioni del comando `users -pk`. • Quando si utilizzano le opzioni delle chiavi pubbliche SSH, è necessario utilizzare l'opzione `-pk` dopo l'indice utente (opzione `-userindex`) nel formato: `users -2 -pk -add "AAAAB3NzC1yc2EAAAABIwAAA QEAvfnTUzRF7pdBuaBy4dO/aIFasa/ Gtc+o/wlZnuC4aD HMA1UmnMylOCiIaNOy4OOICEKCqjKEhrYymtAoVtfKApv Y39GpnSGRC/ qcLGWLM4cmirKL5kxHNOqIcwbT1NPceoKH j46X7E +mqlfWnAhhjDpcVFjagM3Ek2y7w/tBGrwGgN7DP HJU1tzcJy68mEAnIrzjUoR98Q3/B9cJD77ydGKe8rPdI2 hIEpXR5dNUiupA1Yd8PSSMgdukASKEd3eRRZTBl3SAtMu cUsTkYjlXcqex1OQz4+N5OR6MbNcwlsx+mTEAvvcpJhug a7OUNPGhLJMl6k7jeJiQ8Xd2p XbOZQ=="`
-upld	Carica una chiave pubblica SSH in formato OpenSSH o RFC4716 **(opzione di chiave pubblica SSH)**	Richiede le opzioni `-i` e `-l` per specificare la posizione della chiave. **Nota:** • L'opzione `-upld` è utilizzata senza tutte le altre opzioni del comando `users -pk` (tranne `-i` e `-l`). • Per sostituire una chiave con una nuova, è necessario specificare `-key_index`. Per aggiungere una chiave alla fine dell'elenco di chiavi corrente, non specificare un indice di chiave. • Quando si utilizzano le opzioni delle chiavi pubbliche SSH, è necessario utilizzare l'opzione `-pk` dopo l'indice utente (opzione `-userindex`) nel formato: `users -2 -pk -upld -i tftp://9.72.216.40/ -l file.key`.

Tabella 52. opzioni di users (continua)

Opzione	Descrizione	Valori
-dnld	Scarica la chiave pubblica SSH specificata in un server TFTP/SFTP **(opzione di chiave pubblica SSH)**	Richiede `-key_index` per specificare la chiave da scaricare e le opzioni `-i` e `-l` per specificare il percorso di download su un altro computer che esegue un server TFTP. **Nota:** • L'opzione `-dnld` è utilizzata senza tutte le altre opzioni del comando `users -pk` (tranne `-i`, `-l` e `-key_index`). • Quando si utilizzano le opzioni delle chiavi pubbliche SSH, è necessario utilizzare l'opzione `-pk` dopo l'indice utente (opzione `-userindex`) nel formato: `users -2 -pk -dnld -1 -i tftp://9.72.216.40/ -l file.key`.
-i	L'indirizzo IP del server TFTP/SFTP per il caricamento o il download di un file di chiavi **(opzione di chiave pubblica SSH)**	Indirizzo IP valido **Nota:** L'opzione `-i` è richiesta dalle opzioni dei comandi `users -pk -dnld` e `users -pk -upld`.
-pn	Numero di porta del server TFTP/SFTP **(opzione di chiave pubblica SSH)**	Numero di porta valido (valore predefinito 69/22) **Nota:** Un parametro facoltativo per le opzioni dei comandi `users -pk -upld` e `users -pk -dnld`.
-u	Nome utente per il server SFTP **(opzione di chiave pubblica SSH)**	Nome utente valido **Nota:** Un parametro facoltativo per le opzioni dei comandi `users -pk -upld` e `users -pk -dnld`.
-pw	Password per il server SFTP **(opzione di chiave pubblica SSH)**	Password valida **Nota:** Un parametro facoltativo per le opzioni dei comandi `users -pk -upld` e `users -pk -dnld`.
-l	Nome file per il caricamento o il download di un file di chiavi tramite TFTP o SFTP **(opzione di chiave pubblica SSH)**	Nome file valido **Nota:** L'opzione `-l` è richiesta dalle opzioni dei comandi `users -pk -dnld` e `users -pk -upld`.
-af	Accetta le connessioni dall'host **(opzione di chiave pubblica SSH)**	Un elenco separato da virgole di nomi host e indirizzi IP, limitati a 511 caratteri. I caratteri validi sono caratteri alfanumerici, virgole, asterischi, punti interrogativi, punti esclamativi, punti, trattini, due punti e simbolo percentuale.
-cm	Commento **(opzione di chiave pubblica SSH)**	Stringa racchiusa tra virgolette contenente fino a 255 caratteri. **Nota:** Quando si utilizzano le opzioni delle chiavi pubbliche SSH, è necessario utilizzare l'opzione `-pk` dopo l'indice utente (opzione `-userindex`) nel formato: `users -2 -pk -cm "This is my comment."`.

Esempio:

```
system> users
 Login ID     Name      Advanced Attribute     Role            Password Expires
 --------     ----      ------------------     ------           ----------------
    1         USERID                Native     Administrator          89 day(s)
system> users -2 -n sptest -p PasswOrd12 -r Administrator
The user is required to change the password when the user logs in to the management server for the first time
ok
```

```
system> users
 Login ID     Name      Advanced Attribute      Role              Password Expires
 --------     ----      ------------------      ------            ----------------
    1         USERID                Native      Administrator            90 day(s)
    2         sptest                Native      Administrator     Password expired
system> hashpw -sw enabled -re enabled
system> users -5 -n guest5 -shp 292bcbc41bb078cf5bd258db60b63a4b337c8c954409442cfad7148bc6428fee -ssalt abc -r  Administr
system> users -5 ghp
292bcbc41bb078cf5bd258db60b63a4b337c8c954409442cfad7148bc6428fee
system> users -5 gsalt
abc
system>
```

Comandi di controllo IMM

Questo argomento fornisce un elenco alfabetico dei comandi CLI di controllo IMM.

Attualmente esistono 7 comandi di controllo IMM:

comando batch

Utilizzare questo comando per eseguire uno o più comandi CLI contenuti in un file.

Nota:

- Le linee di commenti nel file batch iniziano con un carattere cancelletto (#).
- Quando si esegue un file batch, i comandi che non riescono vengono restituiti con un codice di ritorno di errore.
- I comandi del file batch che contengono opzioni di comando non riconosciute possono generare delle avvertenze.

Sintassi:
```
batch [-options]
```

Tabella 53. opzioni di batch

Opzione	Descrizione	Valori
-f	Nome file batch	Nome file valido
-ip	Indirizzo IP del server TFTP/SFTP	Indirizzo IP valido
-pn	Numero di porta del server TFTP/SFTP	Numero di porta valido (valore predefinito 69/22)
-u	Nome utente per il server SFTP	Nome utente valido
-pw	Password per il server SFTP	Password valida

Esempio:
```
system> batch -f sslcfg.cli -ip 192.168.70.200
1 : sslcfg client dnld ip 192.168.70.20
Command total/errors/warnings: 8 / 1 / 0
system>
```

comando clock

Utilizzare questo comando per visualizzare la data e l'ora correnti. È possibile configurare le impostazioni di offset UTC e ora legale.

Sintassi:
```
clock [-options]
```

Tabella 54. opzioni di clock

Opzione	Descrizione	Valori
-u	Offset UTC	Un offset UTC di +2, -7, -6, -5, -4 e -3 richiede impostazioni di ora legale speciali. • Per +2, le opzioni dell'ora legale sono: off, ee (Europa dell'Est), tky (Turchia), bei (Beirut), amm (Amman), jem (Gerusalemme). • Per -7, le impostazioni dell'ora legale sono: off, mtn (Mountain), maz (Mazatlan). • Per -6, le impostazioni dell'ora legale sono: off, mex (Messico), cna (Nord America Centrale). • Per -5, le impostazioni dell'ora legale sono: off, cub (Cuba), ena (Nord America Orientale). • Per -4, le impostazioni dell'ora legale sono: off, asu (Asuncion), cui (Cuiaba), san (Santiago), cat (Canada - Atlantico). • Per -3, le impostazioni dell'ora legale sono: off, gtb (Godthab), bre (Brasile - Est).
-dst	Ora legale	on, off, caso speciale
-host	Formato dell'ora ottenuta dall'host (default: utc)	local, utc **Nota:** I sistemi Windows usano local, mentre Linux usa utc

Nota:

- BMC ottiene l'ora dal server host o dal server NTP.
- L'ora ottenuta dall'host può essere l'ora locale o l'ora UTC. L'opzione dell'host deve essere impostata su UTC se NTP non è in uso e l'host utilizza il formato UTC.
- L'offset UTC può avere il formato +0200, +2:00, +2 o 2 per offset positivi e -0500 -5:00 o -5 per offset negativi.
- Offset UTC e ora legale sono utilizzati con NTP o quando la modalità host è UTC.

Esempio:
```
system> clock
12/12/2011 13:15:23 GMT-5:00 dst on
```

comando info

Utilizzare questo comando per visualizzare e configurare le informazioni sul BMC.

Sintassi:
```
info [-options]
```

Tabella 55. opzioni di info

Opzione	Descrizione	Valori
-name	Nome BMC	Stringa
-contact	Nome della persona di contatto del BMC	Stringa

Tabella 55. opzioni di info (continua)

Opzione	Descrizione	Valori
-location	Posizione del BMC	Stringa
-postal	Indirizzo postale completo del BMC	Stringa
-room	ID spazio del BMC	Stringa
-rack	ID rack del BMC	Stringa
-rup	Posizione del BMC nel rack	Stringa

Esempio:
```
system> info
  -name: BMCName
  -location: location
  -contact: contact
  -rack: rack
  -room: room
  -postal: postal
  -rup: 1
system>
```

comando spreset

Utilizzare questo comando per riavviare IMM.

Per emettere questo comando è necessario disporre almeno dell'autorizzazione per la configurazione avanzata dell'adattatore.

Sintassi:
```
spreset
```

Comandi senza agente

Questo argomento fornisce un elenco alfabetico dei comandi senza agente.

Attualmente esistono 3 comandi senza agente:

comando storage

Utilizzare questo comando per visualizzare e configurare (se supportato dalla piattaforma) le informazioni sui dispositivi di storage del server gestiti da IMM.

Sintassi:
```
storage [-options]
```

Tabella 56. opzioni di storage

Opzione	Descrizione	Valori
-list	Visualizza l'elenco delle destinazioni di storage gestite da IMM.	**controllers|pools|volumes|drives** • controllers: visualizza l'elenco dei controller RAID supportati[1] • pools: visualizza l'elenco dei pool di storage associati al controller RAID[1] • volumes: visualizza l'elenco dei volumi di storage associati al controller RAID[1] • drives: visualizza l'elenco delle unità di storage associate al controller RAID[1]
-list **storage targets** -target **target_id**	Visualizza l'elenco delle destinazioni (**targets**) di storage gestite da IMM in base a **target_id**.	**pools|volumes|drives** e **ctrl[x]|pool[x]** Dove **storage targets** e **target_id** sono: • **pools** e **ctrl[x]**: visualizzano l'elenco dei pool di storage associati al controller RAID, in base a target_id[1] • **volumes** e **ctrl[x]|pool[x]**: visualizzano l'elenco dei volumi di storage associati al controller RAID, in base a target_id[1] • **drives** e **ctrl[x]|pool[x]**: visualizzano l'elenco delle unità di storage associate al controller RAID, in base a target_id[1]
-list devices	Visualizza lo stato di tutti i dischi gestiti da IMM.	
-show **target_id**	Visualizza le informazioni per la destinazione selezionata gestita da IMM.	Dove **target_id** è **ctrl[x]|vol[x]|disk[x]|pool[x]**[3]
-show **target_id** info	Visualizza le informazioni dettagliate per la destinazione selezionata gestita da IMM.	Dove **target_id** è **ctrl[x]|vol[x]|disk[x]|pool[x]**[3]
-show **target_id** firmware[3]	Visualizza le informazioni sul firmware per la destinazione selezionata gestita da IMM.	Dove **target_id** è **ctrl[x]|disk[x]**[2]
-showinfo **nvme**	Visualizza le informazioni sul firmware del disco Nvme.	
-wthre show	Visualizza la soglia di usura critica e di avviso dell'unità SSD.	Valore soglia (da 1 a 99)
-wthre -ct **threshold value**	Imposta la soglia critica di usura dell'unità SSD.	Valore soglia (da 1 a 99)
-wthre -wt **threshold value**	Imposta la soglia di avviso di usura dell'unità SSD.	Valore soglia (da 1 a 99) **Nota:** Il valore di avviso deve essere maggiore di quello critico.
-config ctrl -scanforgn -target **target_id**[3]	Rileva la configurazione RAID esterna.	Dove **target_id** è **ctrl[x]**[5]
-config ctrl -imptforgn -target **target_id**[3]	Importa la configurazione RAID esterna.	Dove **target_id** è **ctrl[x]**[5]
-config ctrl -clrforgn -target **target_id**[3]	Cancella la configurazione RAID esterna.	Dove **target_id** è **ctrl[x]**[5]

Tabella 56. opzioni di storage (continua)

Opzione	Descrizione	Valori
-config ctrl -clrcfg -target **target_id**[3]	Cancella la configurazione RAID.	Dove **target_id** è **ctrl[x]**[5]
-config ctrl -bootdevice -vd **volume** -target **target_id**	Imposta il dispositivo di avvio in base al volume.	Dove **target_id** è **ctrl[x]** e **volume** è un valore nella prima colonna dell'output "list volumes".
-config ctrl -bootdevice -pd **drive** -target **target_id**	Imposta il dispositivo di avvio in base all'unità.	Dove **target_id** è **ctrl[x]** e **drive** è un valore nella prima colonna dell'output "list drives".
-config ctrl -bootdevice -index **index** -target **target_id**	Imposta il dispositivo di avvio in base all'indice.	Dove **target_id** è **ctrl[x]** e **index** è un valore in "[]" che è l'output dell'opzione "display".
-config ctrl -bootdevice -display -target **target_id**	Mostra il dispositivo avviabile.	
-config drv -mkoffline -target **target_id**[3]	Modifica lo stato dell'unità da online ad offline.	Dove **target_id** è **disk[x]**[5]
-config drv -mkonline -target **target_id**[3]	Modifica lo stato dell'unità da offline a online.	Dove **target_id** è **disk[x]**[5]
-config drv -mkmissing -target **target_id**[3]	Contrassegna l'unità offline come unità valida non configurata.	Dove **target_id** è **disk[x]**[5]
-config drv -prprm -target **target_id**[3]	Prepara un'unità valida non configurata per la rimozione.	Dove **target_id** è **disk[x]**[5]
-config drv -undoprprm -target **target_id**[3]	Annulla la preparazione di un'unità valida non configurata per l'operazione di rimozione.	Dove **target_id** è **disk[x]**[5]
-config drv -mkbad -target **target_id**[3]	Modifica l'unità valida non configurata in un'unità non valida non configurata.	Dove **target_id** è **disk[x]**[5]
-config drv -mkgood -target **target_id**[3]	Modifica un'unità non valida non configurata in un'unità valida non configurata. o Converte l'unità JBOD (Just a Bunch Of Disks) in un'unità valida non configurata.	Dove **target_id** è **disk[x]**[5]
-config drv -mkjbod -target **target_id**[3]	Imposta l'unità non configurata come valida su JBOD.	Dove **target_id** è **disk[x]**[5]
-config drv -rebuild -target **target_id**[3]	Avvia l'unità di ricostruzione.	Dove **target_id** è **disk[x]**[5]
-config drv -addhsp -target **target_id**[3]	Assegna l'unità selezionata come hot-spare caldo a un controller o ai pool di storage esistenti.	Dove **target_id** è **disk[x]**[5]
-config drv -dedicated pools -target **target_id**[3]	Assegna l'unità come hot-spare dedicato ai pool di storage selezionati.	Dove **target_id** è **disk[x]**[5]

Tabella 56. opzioni di storage (continua)

Opzione	Descrizione	Valori
-config drv -rmhsp -target **target_id**[3]	Rimuove l'unità hot-spare.	Dove **target_id** è **disk[x]**[5]
-config vol -remove -target**target_id**[3]	Rimuove un volume.	Dove **target_id** è **vol[x]**[5]
-config vol -set [-N] [-w] [-r] [-i] [-a] [-d] [-b] -target **target_id**[3]	Modifica le proprietà di un volume.	• [-N **volume_name**] è il nome del volume • [-w **<0|1|2|3>**] rappresenta i criteri di scrittura su cache: – Digitare **0** per i criteri Write Through – Digitare **1** per i criteri di scrittura protetta – Digitare **2** per i criteri di scrittura non protetta – Tipo **3** per nessun criterio • [-r **<0|1>**] rappresenta i criteri di lettura della cache: – Digitare **0** per i criteri No Read Ahead – Digitare **1** per i criteri Read Ahead • [-i **<0|1>**] sono i criteri di I/O della cache: – Digitare **0** per i criteri Direct I/O – Digitare **1** per i criteri Cached I/O • [-a **<0|2|3>**] sono i criteri di accesso: – Digitare **0** per i criteri Read Write – Digitare **2** per i criteri Read Only – Digitare **3** per i criteri Blocked • [-d **<0|1|2>**] sono i criteri di cache del disco: – Digitare **0** se i criteri sono immutati – Digitare **1** per abilitare i criteri[6] – Digitare **2** per disabilitare i criteri • [-b **<0|1>**] è l'inizializzazione in background: – Digitare **0** per abilitare l'inizializzazione – Digitare **1** per disabilitare l'inizializzazione • **-target_id** is **vol[x]**[5]

Tabella 56. opzioni di storage (continua)

Opzione	Descrizione	Valori
-config vol -add [-R] [-D disk] [-H disk] [-1 hole] [-N] [-w] [-r][3],[7]	Crea un volume per un nuovo pool di storage quando la destinazione è un controller. o Crea un volume con un pool di storage esistente quando la destinazione è un pool di storage.	• [-R **<0|1|5|1E|6|10|50|60|00>**] Questa opzione definisce il livello RAID e viene utilizzata soltanto con un nuovo pool di storage • [-D disk **[id11]:disk[id12]:..disk[id21]:disk [id22]:..**] Questa opzione definisce il gruppo di dispositivi (inclusi gli span) ed è utilizzata soltanto con un nuovo pool di storage • [-H disk **[id1]:disk[id2]:..**] Questa opzione definisce il gruppo di hot-spare ed è utilizzata soltanto con un nuovo pool di storage • [-1 hole] Questa opzione definisce il numero di indice dello spazio del foro libero per un pool di storage esistente • [-N **volume_name**] è il nome del volume • [-w **<0|1|2|3>**] rappresenta i criteri di scrittura su cache: – Digitare **0** per i criteri Write Through – Digitare **1** per i criteri di scrittura protetta – Digitare **2** per i criteri di scrittura non protetta – Tipo **3** per nessun criterio • [-r **<0|1>**] rappresenta i criteri di lettura della cache: – Digitare **0** per i criteri No Read Ahead – Digitare **1** per i criteri Read Ahead
-config vol -add[-i] [-a] [-d] [-f] [-S] [-P] -target **target_id**[3]	Crea un volume per un nuovo pool di storage quando la destinazione è un controller. o Crea un volume con un pool di storage esistente quando la destinazione è un pool di storage.	• [-i **<0|1>**] sono i criteri di I/O della cache: – Digitare **0** per i criteri Direct I/O – Digitare **1** per i criteri Cached I/O • [-a **<0|2|3>**] sono i criteri di accesso: – Digitare **0** per i criteri Read Write – Digitare **2** per i criteri Read Only – Digitare **3** per i criteri Blocked • [-d **<0|1|2>**] sono i criteri di cache del disco: – Digitare **0** se i criteri rimangono immutati – Digitare **1** per abilitare i criteri[6] – Digitare **2** per disabilitare i criteri • [-f **<0|1|2>**] è il tipo di inizializzazione: – Digitare **0** per nessuna inizializzazione – Digitare **1** per l'inizializzazione rapida – Digitare **2** per l'inizializzazione completa • [-S **volume_size**] è la dimensione del nuovo volume in MB • [-P **strip_size**] è la dimensione di striping del volume, ad esempio 512B, 4K, 128K, 1M e così via

Tabella 56. opzioni di storage (continua)

Opzione	Descrizione	Valori
		• -target **target_id** è: – **ctrl[x]** (nuovo pool di storage)[5] – **pool[x]** (pool di storage esistente)[5]
-config vol -getfreecap [-R] [-D disk] [-H disk] -target **target_id**[3]	Recupera la quantità di capacità libera per il gruppo di unità.	• [-R **<0|1|5|1E|6|10|50|60|00>**] Questa opzione definisce il livello RAID e viene utilizzata soltanto con un nuovo pool di storage • [-D disk **[id11]:[id12]:..[id21]:[id22]:..**] Questa opzione definisce il gruppo di dispositivi (inclusi gli span) ed è utilizzata soltanto con un nuovo pool di storage • [-H disk **[id1]:[id2]:..**]Questa opzione definisce il gruppo di hot-spare ed è utilizzata soltanto con un nuovo pool di storage • -target **target_id** è **ctrl[x]**[5]
-fgi **vol[idx]**	Esegue l'inizializzazione rapida dei volumi specificati	Dove **vol[idx]** è **vol[id1],vol[id2]:..**
-help	Visualizza le opzioni e l'uso del comando.	

Nota:
1. Questo comando è supportato solo su server in cui IMM può accedere al controller RAID.
2. Le informazioni sul firmware vengono visualizzate solo per i controller, i dischi e i DIMM flash associati. Le informazioni sul firmware per i pool e i volumi associati non vengono visualizzate.
3. Le informazioni vengono visualizzate su più righe per limitazioni di spazio.
4. Questo comando è supportato solo sui server che supportano i log RAID.
5. Questo comando è supportato solo sui server che supportano le configurazioni RAID.
6. Il valore **Enable** non supporta le configurazioni RAID livello 1.
7. Un elenco parziale delle opzioni disponibili è riportato qui. Le rimanenti opzioni per il comando **storage -config vol -add** sono elencate nella riga di seguito.

Esempi:

```
system> storage -config ctrl -clrcfg -target ctrl[0]
ok
system>
system> storage -config ctrl -clrforgn -target ctrl[0]
ok
system>
system> storage -config ctrl -imptforgn -target ctrl[0]
ok
system>
system> storage -config ctrl -scanforgn -target ctrl[0]
Detect 1 foreign configuration(s) on controller ctrl[0]
system>
system> storage -config drv -addhsp -dedicated pool[0-1] -target disk[0-0]
ok
system>
system> storage -config drv -addhsp -target disk[0-0]
ok
system>
system> storage -config drv -mkbad -target disk[0-0]
ok
system>
```

```
system> storage -config drv -mkgood -target disk[0-0]
ok
system>
system> storage -config drv -mkmissing -target disk[0-0]
ok
system>
system> storage -config drv -mkoffline -target disk[0-0]
ok
system>
system> storage -config drv -mkonline -target disk[0-0]
ok
system>
system> storage -config drv -prprm -target disk[0-0]
ok
system>
system> storage -config drv -rmhsp -target disk[0-0]
ok
system>
system> storage -config drv -undoprprm -target disk[0-0]
ok
system>
system> storage -config vol -add -1 1 -target pool[0-1]
ok
system>
system> storage -config vol -add -R 1 -D
disk[0-0]:disk[0-1] -w 1 -r 2 -i 0 -a 0 -d 0 -f 0
-N LD_volume -S 100000 -P 64K -H disk[0-2] -target ctrl[0]
ok
system>
system> storage -config vol -getfreecap -R 1 -D
disk[0-0]:disk[0-1] -H disk[0-2] -target ctrl[0]
The drive group configuration is good with free capacity 500000MB
system>
system> storage -config vol -remove -target vol[0-1]
ok
system>
system> storage -config vol -set -N LD_volume
-w 0 -target vol[0-0]
ok
system>
system> storage -list controllers
ctrl[0]    ServerRAID M5110e(Slot No. 0)
ctrl[1]    ServerRAID M5110f(Slot No. 1)
system>
system> storage -list drives
disk[0-0]    Drive 0
disk[0-1]    Drive 1
disk[0-2]    Drive 2
system>
system> storage -list pools
pool[0-0]    Storage Pool 0
pool[0-1]    Storage Pool 1
system>
system> storage -list volumes
vol[0-0]    Volume 0
vol[0-1]    Volume 1
Vol[0-2]    Volume 2
system>
system> storage -list drives -target ctrl[0]
disk[0-0]    Drive 0
disk[0-1]    Drive 1
```

```
disk[0-2]    Drive 2
system>
system> storage -list drives -target pool[0-0]
disk[0-0]    Drive 0
disk[0-1]    Drive 1
system>
system> storage -list pools -target ctrl[0]
pool[0-0]    Storage Pool 0
system>
system> storage -list volumes -target ctrl[0]
vol[0-0]    Volume 0
vol[0-1]    Volume 1
system>
system> storage -list volumes -target pool[0-0]
vol[0-0]    Volume 0
vol[0-1]    Volume 1
system>
system> storage -show ctrl[0] firmware
Total Firmware number: 2
Name: RAID Firmware1
Description: RAID Firmware
Manfacture: IBM
Version: 4.01(3)T
Release Date: 01/05/2013
Name: RAID Firmware2
Description: RAID Firmware
system>
system> storage -show ctrl[0] info
Product Name: ServerRAID M5110e
Firmware Package Version: 23.7.0.1.2
Battery Backup: Installed
Manufacture: IBM
UUID: 1234567890123456
Model Type / Model: 1234AHH
Serial No.: 1234567890
FRU No.: 5005076049CC4
Part No.: LSI2004
Cache Model Status: Unknown
Cache Model Memory Size: 300MB
Cache Model Serial No.: PBKUD0XTA0P04Y
PCI Slot Number: 0
PCI Bus Number: 2
PCI Device Number: 2
PCI Function Number: 10
PCI Device ID: 0x1000
PCI Subsystem Device ID: 0x1413
Ports: 2
Port 1: 12345678901234
Port 2: 12345678901235
Storage Pools: 2
pool[0-0]    Storage Pool 0
pool[0-1]    Storage Pool 1
Drives: 3
disk[0-0]    Drive 0
disk[0-1]    Drive 1
disk[0-2]    Drive 2
system>
system> storage -show disk[0-0] firmware
Total Firmware number: 1
Name: Drive
Description:
```

```
Manufacture:
Version: BE24
Release Date:
system>
system> storage -show disk[0-0] info
Product Name: ST98394893
State: Online
Slot No.: 0
Disk Type: SATA
Media Type: HHD
Health Status: Normal
Capacity: 100.000GB
Speed: 6.0Gb/s
Current Temperature: 33C
Manufacture: ATA
Device ID: 5
Enclusure ID: 0x00FC
Machine Type:
Model:
Serial No.: 9XKJKL
FRU No.:
Part No.:
system>
system> storage -show pool[0-0]
RAID State: RAID 0
RAID Capacity: 67.000GB (0.000GB free)
Drives: 2
disk[0-0]    Drive 0
disk[0-1]    Drive 1
Volumes: 2
vol[0-0]    Volume 0
vol[0-1]    Volume 1
system>
system> storage -show pool[0-1] info
RAID State: RAID 1
RAID Capacity: 231.898GB (200.000GB free)
Holes: 2
#1 Free Capacity: 100.000GB
#2 Free Capacity: 100.000GB

Drives: 2
disk[0-1]    Drive 1
disk[0-2]    Drive 2

Volume: 1
vol[0-1]    LD_volume
system>
system> storage -show vol[0-0]
Name: Volume 0
Stripe Size: 64KB
Status: Offline
Capacity: 100.000GB
system>
system> storage -show vol[0-0] info
Name: LD_volume
Status: Optimal
Stripe Size: 64KB
Bootable: Not Bootable
Capacity: 231.898GB
Read Policy: No Read Ahead
Write Policy: Write Through
```

```
I/O Policy: Direct I/O
Access Policy: Read Write
Disk Cache Policy: Unchanged
Background Initialization: Enable
system>
```

comando adapter

Questo comando permette di visualizzare le informazioni di inventario dell'adattatore PCIe.

Sintassi:
```
adapter [-options]
```

Tabella 57. opzioni di adapter

Opzione	Descrizione	Valori
-list	Visualizza un elenco di tutti gli adattatori PCIe nel server.	
-show **target_id**	Mostra informazioni dettagliate per l'adattatore PCIe di destinazione.	**target_id [info|firmware|ports]** Dove: • **info**: visualizza le informazioni sull'hardware per l'adattatore • **firmware**: visualizza tutte le informazioni sul firmware per l'adattatore • **ports**: visualizza tutte le informazioni sulla porta Ethernet per l'adattatore

Se il comando **adapter** non è supportato, il server risponde con il seguente messaggio quando viene eseguito il comando:
```
Your platform does not support this command.
```

Nota: Se si rimuove, si sostituisce o si configura un adattatore, è necessario riavviare il server (almeno una volta) per visualizzare le informazioni aggiornate sull'adattatore.

Esempi:
```
system> adapter -list
ob-1     Flex System CN4054 10Gbps Virtual Fabric Adapter
ob-2     GPU Card 1
slot-1   Raid Controller 1
slot-2   Adapter 01:02:03
system>
system> adapter -show ob-1 info
Product Name: Flex System CN4054 10Gbps Virtual Fabric Adapter
Card Interface: PCIe x 16
Function Count: 2
Function Name: xxx Emulx xx component1
Segment Number: 2348
Bus Number: 23949
Device Number: 1334
Function Number: 21
Vendor Id: 12
Device Id: 33
Revision Id: 1
Class Code: 2
Sub Vendor: 334
Sub Device: 223
Slot Description: a slot
```

```
Slot Type: 23
Slot Data Bus Width: 0
Hot Plug: 12
PCI Type: 11
Blade Slot Port: xxx
UUID: 39302938485
Manufacturer: IBM
Serial Number: 998AAGG
Part Number: ADB233
Model: 345
Function Sku: 221
Fod Uid: 2355
Required Daughter: 0
Max Data Width: 0
Connector Layout: pci x
Package Type: dici
Function Name: xxx nVidia xx component2
Segment Number: 2348
Bus Number: 23949
Device Number: 1334
Function Number: 21
Vendor Id: 12
Device Id: 33
Revision Id: 1
Class Code: 2
Sub Vendor: 334
Sub Device: 223
Slot Description: a slot
Slot Type: 23
Slot Data Bus Width: 0
Hot Plug: 12
PCI Type: 11
Blade Slot Port: xxx
UUID: 39302938485
Manufacturer: IBM
Serial Number: 998AAGG
Part Number: ADB233
Model: 345
Function Sku: 221
Fod Uid: 2355
Required Daughter: 0
Max Data Width: 0
Connector Layout: pci x
Package Type: dici
system>
```

Comandi di supporto

Questo argomento fornisce un elenco alfabetico di comandi di supporto.

Esiste solo un comando di supporto: "comando dbgshbmc" a pagina 152.

comando dbgshbmc

Utilizzare questo comando sbloccare l'accesso alla rete per la shell di debug sicura.

Nota: In precedenza questo comando era denominato **dbgshimm**.

Importante: Questo comando è destinato solo all'uso da parte di personale di supporto.

La seguente tabella mostra gli argomenti per le opzioni.

Sintassi:
```
dbgshbmc [subset_command]
```

Tabella 58. comandi del subset dbgshbmc

Opzione	Descrizione
status	Visualizza lo stato
enable	Abilita l'accesso del debug (predefinita se non è specificata alcuna opzione)
disabilita	Disabilita l'accesso del debug

Capitolo 11. Interfaccia IPMI

In questo capitolo viene descritta l'interfaccia IPMI supportata da XClarity Controller.

Per informazioni dettagliate sui comandi IPMI standard, consultare il documento delle specifiche IPMI (Intelligent Platform Management Interface) (versione 2.0 o successiva). In questo documento vengono fornite le descrizioni dei parametri OEM utilizzati con i comandi IPMI OEM e IPMI standard supportati dal firmware di XClarity Controller.

Gestione di XClarity Controller con IPMI

Utilizzare le informazioni in questo argomento per gestire XClarity Controller mediante l'interfaccia IPMI (Intelligent Platform Management Interface).

XClarity Controller viene fornito con un ID utente inizialmente impostato su nome utente USERID e password PASSW0RD (con uno zero al posto della lettera O). Questo utente ha accesso da supervisore.

Importante: Per una maggiore sicurezza, modificare questo nome utente e la password durante la configurazione iniziale.

In un sistema Flex System, un utente può configurare un modulo CMM Flex System per gestire centralmente gli account utente IPMI di XClarity Controller. In questo caso, potrebbe non essere possibile accedere a XClarity Controller mediante IPMI finché il modulo CMM non ha configurato gli ID utente IPMI.

Nota: Le credenziali ID utente configurate dal modulo CMM potrebbero essere differenti dalla combinazione USERID/PASSW0RD descritta in precedenza. Se tramite il modulo CMM non è stato configurato alcun ID utente IPMI, la porta di rete associata al protocollo IPMI risulterà chiusa.

XClarity Controller fornisce inoltre le seguenti funzionalità di gestione del server remoto IPMI:

Interfacce della riga di comando IPMI
L'interfaccia della riga di comando IPMI fornisce accesso diretto alle funzioni di gestione dei server mediante il protocollo IPMI 2.0. È possibile utilizzare IPMItool al fine di inviare i comandi per controllare l'accensione del server, visualizzare le informazioni sul server e identificare il server. Per ulteriori informazioni su IPMItool, vedere "Utilizzo di IPMItool" a pagina 155.

SOL (Serial over LAN)
Per gestire i server da una posizione remota, utilizzare IPMItool per stabilire una connessione Serial over LAN (SOL). Per ulteriori informazioni su IPMItool, vedere "Utilizzo di IPMItool" a pagina 155.

Utilizzo di IPMItool

Utilizzare le informazioni in questo argomento per accedere alle informazioni su IPMItool.

IPMItool fornisce diversi strumenti che possono essere utilizzati per gestire e configurare un sistema IPMI. È possibile utilizzare IPMItool in banda o fuori banda per gestire e configurare XClarity Controller.

Per ulteriori informazioni o per scaricare IPMItool, visitare il sito https://github.com/ipmitool/ipmitool.

Comandi IPMI con parametri OEM

Comando Get/Set dei parametri di configurazione LAN

Per riflettere le funzionalità fornite da XCC per alcune impostazioni di rete, i valori di alcuni dati dei parametri vengono definiti nel modo seguente.

DHCP

Oltre ai metodi tradizionali per ottenere un indirizzo IP, XCC fornisce una modalità per ottenere un indirizzo IP da un server DHCP per un determinato periodo di tempo e, in caso di esito negativo, permette di utilizzare un indirizzo IP statico.

La seguente tabella multiriga a tre colonne contiene le opzioni, le descrizioni delle opzioni e i valori associati per le opzioni.

Parametro	#	Dati dei parametri
Origine indirizzo IP	4	data1 [7:4] - riservato [3:0] - origine indirizzo 0h = non specificato 1h = indirizzo statico (configurato manualmente) 2h = indirizzo ottenuto da XCC con DHCP 3h = indirizzo ottenuto tramite BIOS o software di sistema 4h = indirizzo ottenuto da XCC con un altro protocollo di assegnazione degli indirizzi. XCC utilizza il valore 4h per indicare la modalità dell'indirizzo DHCP con failover statico.

Selezione dell'interfaccia Ethernet

XCC è dotato di due schede MAC Ethernet 10/100 con interfacce RMII. Inoltre, include anche due schede MAC Ethernet da 1 Gbps con interfacce RGMII. Una scheda MAC viene generalmente collegata al NIC del server condiviso mentre l'altra viene utilizzata come porta di gestione del sistema dedicata. È possibile attivare una sola porta Ethernet di un server alla volta. Non è possibile abilitare entrambe le porte contemporaneamente.

In alcuni server, i progettisti di sistema possono scegliere di collegare solo una delle due interfacce Ethernet sul planare del sistema. In questi sistemi, solo l'interfaccia Ethernet connessa al planare è supportata da XCC. Una richiesta di utilizzo della porta non collegata restituisce un codice di completamento CCh.

Gli ID dei pacchetti delle schede di rete facoltative sono numerati nel modo seguente:

- scheda facoltativa n. 1, ID pacchetto = 03h (eth2)
- scheda facoltativa n. 2, ID pacchetto = 04h (eth3)

La seguente tabella multiriga a tre colonne contiene le opzioni, le descrizioni delle opzioni e i valori associati per le opzioni.

Parametro	#	Dati dei parametri
Parametro OEM Questo numero di parametro viene utilizzato da XCC per indicare le porte Ethernet (pacchetti logici) da utilizzare. Questo parametro del comando Get/Set dei parametri di configurazione LAN non utilizza una selezione serie o una determinata selezione blocco. Pertanto, questi campi devono essere impostati su 00h. I dati della risposta restituiranno 3 byte o facoltativamente 4 byte, se il dispositivo si trova in un pacchetto NCSI. Byte 1 = codice di completamento Byte 2 = revisione Byte 3 = 00h per eth0, 01h per eth1 e così via Byte 4 = numero del canale (facoltativo), se il dispositivo è un pacchetto NCSI	C0h	data1 00h = eth0 01h = eth1 02h = eth2 e così via FFh = disabilita tutte le porte di rete esterne XCC supporta un secondo byte di dati facoltativo per specificare il canale da utilizzare in un pacchetto data2 00h = canale 0 01h = canale 1 e così via Se data2 non viene specificato nella richiesta, viene utilizzato il canale 0

Il byte data1 viene utilizzato per specificare il pacchetto logico. Potrebbe trattarsi di un NIC di gestione dei sistemi dedicato o di un'interfaccia NCSI nel NIC condiviso con il server.

Il byte data2 viene utilizzato per specificare il canale per il pacchetto logico, se il pacchetto è un dispositivo NCSI. Se data2 non viene specificato nella richiesta e il pacchetto logico è un dispositivo NCSI, viene utilizzato il canale 0. Se data2 non viene specificato nella richiesta ma il pacchetto logico non è un dispositivo NCSI, le informazioni del canale vengono ignorate.

Esempi:

Appendice A: se il canale 2 del NIC condiviso sul planare (ID pacchetto = 0, eth0) deve essere utilizzato come porta di gestione, i dati di input saranno: 0xC0 0x00 0x02

Appendice B: se è necessario utilizzare il primo canale della prima scheda mezzanine di rete, l'input sarà: 0xC0 0x02 0x0

Abilitazione/Disabilitazione Ethernet-over-USB

Il parametro seguente viene utilizzato per abilitare o disabilitare l'interfaccia in banda di XCC.

La seguente tabella multiriga a tre colonne contiene le opzioni, le descrizioni delle opzioni e i valori associati per le opzioni.

Parametro	#	Dati dei parametri
Parametro OEM Questo numero di parametro viene utilizzato da XCC per abilitare o disabilitare l'interfaccia Ethernet-over-USB. Questo parametro del comando Get dei parametri di configurazione LAN non utilizza una selezione serie o una determinata selezione blocco. Pertanto, questi campi devono essere impostati su 00h. I dati della risposta restituiranno 3 byte: Byte 1 = codice di completamento Byte 2 = revisione Byte 3 = 00h (disabilitato) o 01h (abilitato)	C1h	data1 0x00 = disabilitato 0x01 = abilitato

Il byte data1 viene utilizzato per specificare il pacchetto logico. Potrebbe trattarsi di un NIC di gestione dei sistemi dedicato o di un'interfaccia NCSI nel NIC condiviso con il server.

Il byte data2 viene utilizzato per specificare il canale per il pacchetto logico, se il pacchetto è un dispositivo NCSI. Se data2 non viene specificato nella richiesta e il pacchetto logico è un dispositivo NCSI, viene utilizzato il canale 0. Se data2 non viene specificato nella richiesta ma il pacchetto logico non è un dispositivo NCSI, le informazioni del canale vengono ignorate.

Esempi:

Appendice A: se il canale 2 del NIC condiviso sul planare (ID pacchetto = 0, eth0) deve essere utilizzato come porta di gestione, i dati di input saranno: 0xC0 0x00 0x02

Appendice B: se è necessario utilizzare il primo canale della prima scheda mezzanine di rete, l'input sarà: 0xC0 0x02 0x0

Opzione IPMI per ottenere il formato DUID-LLT

DUID è un valore aggiuntivo di sola lettura che deve essere esposto tramite IPMI. Secondo le specifiche RFC3315, questo formato DUID è basato su Link Layer Address Plus Time.

Parametro	#	Dati dei parametri
Parametro OEM Questo numero di parametro viene utilizzato da XCC per abilitare o disabilitare l'interfaccia Ethernet-over-USB. Questo parametro del comando Get dei parametri di configurazione LAN non utilizza una selezione serie o una determinata selezione blocco. Pertanto, questi campi devono essere impostati su 00h. I dati della risposta restituiranno 3 byte: Byte 1 = codice di completamento Byte 2 = revisione parametri (come da specifica IPMI) Byte 3 = lunghezza dei seguenti byte di dati (16 byte attualmente) Byte 4-n DUID_LLT	C2h	

Parametri di configurazione Ethernet

I parametri seguenti possono essere utilizzati per configurare specifiche impostazioni Ethernet.

Parametro	#	Dati dei parametri
Parametro OEM Questo numero di parametro viene utilizzato da XCC per abilitare o disabilitare l'impostazione di negoziazione automatica per l'interfaccia Ethernet. I dati della risposta restituiranno 3 byte: Byte 1 = codice di completamento Byte 2 = revisione Byte 3 = 00h (disabilitato) o 01h (abilitato)	C3h	data1 0x00 = disabilitato 0x01 = abilitato Nota: sui sistemi Enclosure Flex e ThinkSystem D2 (nodo di elaborazione ThinkSystem SD530) l'impostazione di negoziazione automatica non è modificabile perché potrebbe interrompere il percorso di comunicazione di rete tramite CMM e SMM.
Parametro OEM Questo numero di parametro viene utilizzato da XCC per ottenere o impostare la velocità di trasferimento dati dell'interfaccia Ethernet. I dati della risposta restituiranno 3 byte: Byte 1 = codice di completamento Byte 2 = revisione Byte 3 = 00h (10 Mb) o 01h (100 Mb)	C4h	data1 0x00 = 10 Mbit 0x01 = 100 Mbit
Parametro OEM Questo numero di parametro viene utilizzato da XCC per ottenere o configurare l'impostazione Duplex dell'interfaccia Ethernet. I dati della risposta restituiranno 3 byte: Byte 1 = codice di completamento Byte 2 = revisione Byte 3 = 00h (half-duplex) o 01h (full-duplex)	C5h	data1 0x00 = half-duplex 0x01 = full-duplex

Parametro	#	Dati dei parametri
Parametro OEM Questo numero di parametro viene utilizzato da XCC per ottenere o configurare l'impostazione MTU (Maximum Transmission Unit) dell'interfaccia Ethernet. I dati della risposta restituiranno 3 byte: Byte 1 = codice di completamento Byte 2 = revisione Byte 3-4 = dimensione MTU	C6h	data1 Dimensione MTU
Parametro OEM Questo numero di parametro viene utilizzato da XCC per ottenere o configurare l'indirizzo MAC gestito localmente. I dati della risposta restituiranno 3 byte: Byte 1 = codice di completamento Byte 2 = revisione Byte 3-8 = indirizzo MAC	C7h	data1-6 Indirizzo MAC

Opzione IPMI per ottenere l'indirizzo LLA (Link Local Address)

Parametro di sola lettura per recuperare l'indirizzo LLA (Link Local Address) IPv6.

Parametro	#	Dati dei parametri
Parametro OEM Questo parametro viene utilizzato per ottenere l'indirizzo LLA (Link Local Address) di XCC. I dati della risposta restituiranno quanto segue: Byte 1 = codice di completamento Byte 2 = revisione parametri (come da specifica IPMI) Byte 3 = lunghezza del prefisso dell'indirizzo IPv6 Byte 4-19 = indirizzo LLA (Link Local Address) in formato binario	C8h	

Opzione IPMI per abilitare/disabilitare IPv6

Parametro di lettura/scrittura per abilitare/disabilitare IPv6 in XCC.

Parametro	#	Dati dei parametri
Parametro OEM Questo parametro viene utilizzato per abilitare/disabilitare IPv6 in XCC I dati della risposta restituiranno quanto segue: Byte 1 = codice di completamento Byte 2 = revisione parametri (come da specifica IPMI) Byte 3 = 00h (disabilitato) o 01h (abilitato)	C9h	data1 0x00 = disabilitato 0x01 = abilitato

Pass-through Ethernet-over-USB alla rete esterna

Il parametro seguente viene utilizzato per configurare Ethernet-over-USB su pass-through Ethernet esterno.

Parametro	#	Dati dei parametri
Parametro OEM Questo parametro del comando Get/Set dei parametri di configurazione LAN non utilizza una selezione serie o una determinata selezione blocco. Pertanto, questi campi devono essere impostati su 00h. I dati della risposta Get restituiranno quanto segue: Byte 1 = codice di completamento Byte 2 = revisione Byte 3 = riservato (00h) Byte 4:5 = numero della porta Ethernet-over-USB (LSByte per primo) Byte 6:7 = numero della porta Ethernet esterna (LSByte per primo) Il numero di byte da seguire può variare (1, 4 o 16 byte) a seconda della modalità di indirizzamento: • Byte 8 = modalità predefinite: 00h = il pass-through è disabilitato 01h = viene utilizzato l'indirizzo IP del CMM Byte 8:11 = l'indirizzo IP di rete esterno IPv4 in formato binario Byte 8:23 = l'indirizzo IP di rete esterno IPv6 in formato binario Codici di completamento: 00h - operazione completata 80h - parametro non supportato C1h - comando non supportato C7h - lunghezza dei dati della richiesta non valida	CAh	Comando Set dei parametri di configurazione LAN: data1 riservato (= 00h) data2:3 Numero della porta Ethernet-over-USB, LSByte per primo data4:5 Numero della porta Ethernet esterna, LSByte per primo Il numero di byte da seguire può variare (1, 4 o 16 byte) a seconda della modalità di indirizzamento: data6 00h = disabilita il pass-through 01h = utilizza l'indirizzo IP del CMM data6:9 L'indirizzo IP di rete esterno IPv4 in formato binario data6:21 L'indirizzo IP di rete esterno IPv6 in formato binario
Parametro OEM Questo parametro viene utilizzato per impostare e ottenere l'indirizzo IP LAN-over-USB e la maschera di rete di XCC: I dati della risposta restituiranno quanto segue: Byte 1 = codice di completamento	CBh	Data1:4 Indirizzo IP dell'interfaccia LAN-over-USB lato XCC. Data5:8 Maschera di rete dell'interfaccia LAN-over-USB lato XCC.

Parametro	#	Dati dei parametri
Byte 2 = revisione parametri (come da specifica IPMI) Byte 3:10 = indirizzo IP e valore della maschera di rete (MS-byte) per primi		
Parametro OEM Questo parametro viene utilizzato per impostare e ottenere l'indirizzo IP LAN-over-USB del sistema operativo host. I dati della risposta restituiranno quanto segue: Byte 1 = codice di completamento Byte 2 = revisione parametri (come da specifica IPMI) Byte 3:6 = indirizzo IP (MS-byte) per primo	CCh	Data1:4 Indirizzo IP dell'interfaccia LAN-over-USB lato host.

Inventario del pacchetto logico della query

Il parametro seguente viene utilizzato per eseguire una query dell'inventario del pacchetto NCSI.

Parametro	#	Dati dei parametri
Parametro OEM Questo parametro del comando Get/Set dei parametri di configurazione LAN non utilizza una selezione serie o una determinata selezione blocco. Pertanto, questi campi devono essere impostati su 00h. Operazione di inventario del pacchetto della query L'operazione per le informazioni sul pacchetto della query viene eseguita inviando la richiesta con due byte di dati 0x00, oltre al numero del parametro D3h. Inventario del pacchetto della query: --> 0x0C 0x02 0x00 0xD3 0x00 0x00 La risposta di XCC include un byte di informazioni per ogni pacchetto presente: bit 7:4 = numero di canali NCSI nel pacchetto bit 3:0 = numero del pacchetto logico Risposta --> 0x00 0x00 0x40 0x01 0x32 indica che sono presenti 3 pacchetti logici: il pacchetto 0 ha 4 canali NCSI il pacchetto 1 non è un NIC NCSI, quindi non supporta i canali NCSI il pacchetto 2 ha 3 canali NCSI	D3h	Comando Get/Set dei parametri di configurazione LAN:

Dati del pacchetto logico Get/Set

Il parametro seguente viene utilizzato per leggere e impostare la priorità assegnata a ciascun pacchetto.

Parametro	#	Dati dei parametri
Parametro OEM Questo parametro del comando Get/Set dei parametri di configurazione LAN non utilizza una selezione serie o una determinata selezione blocco. Pertanto, questi campi devono essere impostati su 00h. Il comando supporta due operazioni: • Lettura della priorità del pacchetto • Impostazione della priorità del pacchetto Operazione di lettura della priorità del pacchetto L'operazione di lettura della priorità del pacchetto viene eseguita inviando la richiesta con due byte di dati 0x00, oltre al numero del parametro D4h. Lettura della priorità del pacchetto: --> 0x0C 0x02 0x01 0xD4 0x00 0x00 Risposta --> 0x00 0x00 0x00 0x12 0x23 pacchetto logico 0 = priorità 0 pacchetto logico 2 = priorità 1 pacchetto logico 3 = priorità 2 Operazione di impostazione della priorità del pacchetto L'operazione di impostazione della priorità del pacchetto viene eseguita inviando la richiesta con uno o più parametri, in aggiunta al numero del parametro D4h. Impostazione della priorità del pacchetto: --> 0x0C 0x01 0x01 0xD4 0x00 0x12 0x23	D4	Comando Get/Set dei parametri di configurazione LAN: Bit [7-4] = priorità del pacchetto logico (1 = massimo, 15 = minimo) Bit [3-0] = numero del pacchetto logico

Parametro	#	Dati dei parametri
impostazione pacchetto logico 0 = priorità 0 impostazione pacchetto logico 2 = priorità 1 impostazione pacchetto logico 3 = priorità 2 Risposta: solo codice di completamento, nessun dato aggiuntivo		

Comando Get/Set dello stato di sincronizzazione della rete XCC

Parametro	#	Dati dei parametri
Parametro OEM Il byte viene utilizzato per configurare l'impostazione di sincronizzazione della rete tra la modalità NIC dedicata e condivisa Questo parametro del comando Get dei parametri di configurazione LAN non utilizza una selezione serie o una determinata selezione blocco. Pertanto, questi campi devono essere impostati su 00h. I dati della risposta restituiranno 3 byte: Byte 1 = codice di completamento Byte 2 = revisione Byte 3 = 00h (abilitato) o 01h (disabilitato)	D5h	data1 0x00 = sincronizzazione 0x01 = indipendenza

Il byte viene utilizzato per configurare l'impostazione di sincronizzazione della rete tra la modalità NIC dedicata e condivisa. Il valore predefinito è 0h e indica che XCC aggiornerà automaticamente l'impostazione di rete tra la modifica della modalità e l'utilizzo del NIC condiviso (integrato) come riferimento principale. Se il valore viene configurato su 1h, ogni impostazione di rete sarà indipendente, ovvero sarà possibile configurare differenti modalità di rete, quali "Abilita VLAN su NIC dedicato" e "Disabilita VLAN su NIC condiviso".

Comando Get/Set della modalità di rete XCC

Parametro	#	Dati dei parametri
Parametro OEM Questo parametro viene utilizzato per ottenere/impostare la modalità di rete del NIC di gestione di XCC. I dati della risposta restituiranno 4 byte: Byte 1 = codice di completamento Byte 2 = revisione Byte 3 = modalità di rete applicata/specificata Byte 4 = ID pacchetto della modalità di rete applicata Byte 5 = ID canale della modalità di rete applicata	D6h	Comando Set dei parametri di configurazione LAN: data1 Modalità di rete da impostare Comando Get dei parametri di configurazione LAN: data1 Modalità di rete da ottenere. Questi dati sono facoltativi, per impostazione predefinita viene eseguita una query della modalità di rete corrente.

Comandi IPMI OEM

XCC supporta i seguenti comandi IPMI OEM. Ogni comando richiede un livello di privilegio differente, come elencato di seguito.

Codice	Comandi Netfn 0x2E	Privilegio
0xCC	Reimposta valori predefiniti XCC	PRIV_USR

Codice	Comandi Netfn 0x3A	Privilegio
0x00	Query versione firmware	PRIV_USR
0x0D	Informazioni scheda	PRIV_USR
0x1E	Opzioni di ritardo del ripristino dell'alimentazione dello chassis	PRIV_USR
0x38	NMI e reimpostazione	PRIV_USR
0x49	Avvia raccolta dei dati	PRIV_USR
0x4A	Esegui push del file	PRIV_USR
0x4D	Stato raccolta dei dati	PRIV_USR
0x50	Ottieni informazioni build	PRIV_USR
0x55	Ottieni/Imposta nome host	PRIV_USR
0x6B	Query del livello di revisione del firmware FPGA	PRIV_USR

Codice	Comandi Netfn 0x3A	Privilegio
0x6C	Query del livello di revisione hardware della scheda	PRIV_USR
0x6D	Query del livello di revisione del firmware PSoC	PRIV_USR
0x98	Controllo porta USB FP	PRIV_USR
0xC7	Switch IPMI NM nativo	PRIV_ADM

Reimposta comando predefinito di XCC

Questo comando reimposta i valori predefiniti dell'impostazione di configurazione di XCC.

Funzione di rete = 0x2E			
Codice	**Comando**	**Dati della richiesta/della risposta**	**Descrizione**
0xCC	Reimposta valori predefiniti XCC	**Richiesta:** Byte 1 - 0x5EByte 2 - 0x2B Byte 3 - 0x00 Byte 4 - 0x0AByte 5 - 0x01 Byte 6 - 0xFF Byte 7 - 0x00Byte 8 - 0x00 Byte 9 - 0x00 **Risposta:** Byte 1 - CodeByte di completamento 2 - 0x5EByte 3 - 0x2B Byte 4 - 0x00 Byte 5 - 0x0AByte 6 - 0x01 Byte 7 - Dati della risposta 0 = Operazione completata non zero = errore	Questo comando reimposta i valori predefiniti delle impostazioni di configurazione di XCC.

Comandi per informazioni scheda/firmware

In questa sezione sono elencati i comandi per eseguire una query delle informazioni sulla scheda e sul firmware.

Funzione netta = 0x3A			
Codice	**Comando**	**Dati della richiesta/della risposta**	**Descrizione**
0x00	Query versione firmware	**Richiesta**: Dati richiesta non presenti **Risposta**: Byte 1 - Codice di completamento Byte 2 - Versione principale Byte 3 - Versione minore	Questo comando restituisce i numeri delle versioni principale e secondaria del firmware. Se il comando viene eseguito con 1 byte facoltativo di dati della richiesta, la risposta di XCC include anche il terzo campo (revisione) della versione. (Principale.Minore.Revisione)
0x0D	Query informazioni scheda	**Richiesta**: N/A **Risposta**: Byte 1 - ID sistema Byte 2 - Revisione scheda	Questo comando restituisce l'ID della scheda e la revisione del planare.
0x50	Query informazioni build	**Richiesta**: N/A **Risposta**: Byte 1 - Codice di completamento Byte 2:10 - Nome build ASCIIZ Byte 11:23 - Data build ASCIIZ Byte 24:31 - Ora build ASCII	Questo comando restituisce il nome, la data e l'ora della build. Le stringhe del nome e della data della build hanno una terminazione zero. Il formato della data della build è YYYY-MM-DD. Ad esempio, "ZUBT99A" “2005-03-07” “23:59:59”

Funzione netta = 0x3A			
Codice	**Comando**	**Dati della richiesta/della risposta**	**Descrizione**
0x6B	Query del livello di revisione del firmware FPGA	**Richiesta**: Byte 1 - Tipo di dispositivo FPGA* Tipo di dispositivo FPGA 0 = locale (livello attivo) 1 = scheda CPU 1 (livello attivo) 2 = scheda CPU 2 (livello attivo) 3 = scheda CPU 3 (livello attivo) 4 = scheda CPU 4 (livello attivo) 5 = ROM primaria locale 6 = ROM di ripristino locale **Risposta**: Byte 1 - Codice di completamento Byte 2 - Livello revisione principale Byte 3 - Livello revisione minore Byte 4 - Livello revisione minore secondaria (Byte di test sulle piattaforme XCC)	Questo comando restituisce il livello di revisione del firmware FPGA. Se il byte 1 viene omesso, verrà selezionato il valore "Locale" (livello attivo)
0x6C	Query del livello di revisione hardware della scheda	**Richiesta**: Nessun dato. **Risposta**: Byte 1 - Codice di completamento Byte 2 - Livello revisione	Questo comando restituisce il livello di revisione dell'hardware della scheda in cui si trova FPGA.
0x6D	Query del livello di revisione del firmware PSoC	**Richiesta**: Nessuna **Risposta**: Byte 1 - Codice di completamento Byte 2 - bin# Byte 3 - APID Byte 4 - Rev Byte 5-6 - ID FRU	Questo comando restituisce il livello di revisione di tutti i dispositivi PSoC rilevati. Nota: bin# rappresenta una posizione fisica. Per ulteriori informazioni, consultare le specifiche di sistema.

Funzione netta = 0x3A			
Codice	**Comando**	**Dati della richiesta/della risposta**	**Descrizione**
		Byte 6:N - Ripetizione dei byte 2-6 per ogni PSoC rilevato	

Comandi di controllo del sistema

La specifica IPMI fornisce il controllo di reimpostazione e alimentazione di base. Lenovo aggiunge funzioni di controllo aggiuntive.

<table>
<tr><th colspan="4">Funzione di rete = 0x2E</th></tr>
<tr><th>Codice</th><th>Comando</th><th>Dati della richiesta/della risposta</th><th>Descrizione</th></tr>
<tr><td>0x1E</td><td>Opzioni di ritardo del ripristino dell'alimentazione dello chassis</td><td>Richiesta:<table><tr><td>Byte 1</td><td>Tipo di richiesta:

0x00 = Imposta opzioni di ritardo

0x01 = Query opzioni di ritardo</td></tr><tr><td>Byte 2</td><td>(se byte 1 = 0x00)

0x00 = Disabilitato (impostazione predefinita)

0x01 = Casuale

0x02 - 0xFF Riservati</td></tr></table>Risposta:

Byte 1 - Codice di completamento

Byte 2 - Opzioni di ritardo (solo per richiesta di tipo Query)</td><td>Questa impostazione viene utilizzata quando i criteri di ripristino dell'alimentazione dello chassis sono impostati su "Sempre acceso" o "Ripristina alimentazione" (se precedentemente acceso), dopo l'applicazione o il ripristino dell'alimentazione CA. Sono disponibili 2 opzioni: Disabilitato (impostazione predefinita, nessun ritardo quando acceso) e Casuale. L'impostazione di ritardo casuale fornisce un ritardo casuale compreso tra 1 e 15 secondi, dal momento in cui l'applicazione CA viene applicata/ripristinata e quando il server viene acceso automaticamente.

Il comando è supportato da XCC solo sui server rack.</td></tr>
<tr><td>0x38</td><td>NMI e reimpostazione</td><td>Richiesta:

Byte 1- Numero di secondi
0 = solo NMI

Byte 2 - Tipo di reimpostazione
0 = soft reset
1 = ciclo di alimentazione

Risposta:

Byte 1 - Codice di completamento</td><td>Questo comando viene utilizzato per eseguire un NMI di sistema. Facoltativamente, il sistema può essere reimpostato (riavviato) o spento e riacceso dopo il NMI.

Se il campo "Numero di secondi" non è impostato su 0, il sistema verrà reimpostato o spento e riacceso dopo il numero di secondi specificato.

Il byte 2 della richiesta è facoltativo. Se il byte 2 non viene fornito o se il valore è 0x00, viene eseguito un soft reset. Se il byte 2 è 0x01, il sistema viene spento e riacceso.</td></tr>
</table>

Comandi vari

Questa sezione include i comandi che non rientrano in altre sezioni.

<table>
<tr><th colspan="4">Funzione netta = 0x3A</th></tr>
<tr><th>Codice</th><th>Comando</th><th>Dati della richiesta/della risposta</th><th>Descrizione</th></tr>
<tr><td>0x55</td><td>Ottieni/ Imposta nome host</td><td>Lunghezza richiesta = 0:

Dati della richiesta vuoti

Risposta:

<table><tr><td>Byte 1</td><td>Codice di completamen-to</td></tr><tr><td>Byte 2-65</td><td>Nome host corrente.

ASCIIZ, stringa con terminazione Null.</td></tr></table>
Lunghezza richiesta 1-64:

<table><tr><td>Byte 1-64</td><td>Nome host DHCP

ASCIIZ termina con 00h</td></tr></table></td><td>Utilizzare questo comando per ottenere/impostare il nome host.

Quando si imposta il nome host, il valore desiderato deve terminare con 00h. Il nome host è limitato a 63 caratteri più il valore Null.</td></tr>
<tr><td>0x98</td><td>Controllo porta USB FP</td><td>Richiesta:

Byte 1

<table><tr><td>01h:</td><td>Ottieni proprietario attuale della porta USB del pannello anteriore</td></tr></table>
Risposta:

Byte 1 - Codice di completamento

Byte 2

<table><tr><td>00h:</td><td>Di proprietà dell'host</td></tr><tr><td>01h:</td><td>Di proprietà del BMC</td></tr></table>
Richiesta:

Byte 1

<table><tr><td>02h:</td><td>Ottieni la configurazione</td></tr></table></td><td>Questo comando viene utilizzato per eseguire una query di stato/ configurazione della porta USB FP, per configurare modalità/timeout della porta USB FP e per alternare il proprietario della porta USB tra host e BMC.

Nella configurazione, USB FP può disporre di 3 modalità: dedicato all'host, proprietà esclusiva del BMC o modalità condivisa che consente di alternare il proprietario tra host e BMC.

Se la modalità condivisa è abilitata, la porta USB è collegata al BMC quando il server è spento e al server quando l'alimentazione del server è attiva.

Quando la modalità condivisa è abilitata e l'alimentazione del server è attiva, il BMC restituisce la porta USB al server dopo il timeout di inattività della configurazione.

Se il server è dotato del pulsante di identificazione, gli utenti possono abilitare/disabilitare il pulsante ID</td></tr>
</table>

<table>
<tr><th colspan="4">Funzione netta = 0x3A</th></tr>
<tr><th>Codice</th><th>Comando</th><th>Dati della richiesta/della risposta</th><th>Descrizione</th></tr>
<tr><td></td><td></td><td>
<table>
<tr><td></td><td>della porta USB del pannello anteriore</td></tr>
</table>
Risposta:
Byte 1 - Codice di completamento
Byte 2
<table>
<tr><td>00h:</td><td>Dedicato all'host</td></tr>
<tr><td>01h:</td><td>Dedicato al BMC</td></tr>
<tr><td>02h:</td><td>Modalità condivisa</td></tr>
</table>
Byte 3:4 - Timeout di inattività in minuti (MSB per primo)
Byte 5 - Abilita pulsante ID
<table>
<tr><td>00h:</td><td>Disabilitata</td></tr>
<tr><td>01h:</td><td>Abilitato</td></tr>
</table>
Byte 6 - Isteresi (facoltativo) in secondi
Richiesta:
Byte 1
03h: imposta la configurazione della porta USB del pannello anteriore
Byte 2
<table>
<tr><td>00h:</td><td>Dedicato all'host</td></tr>
<tr><td>01h:</td><td>Dedicato al BMC</td></tr>
<tr><td>02h:</td><td>Modalità condivisa</td></tr>
</table>
Byte 3:4 - Timeout di inattività in minuti (MSB per primo)
Byte 5 - Abilita pulsante ID
<table>
<tr><td>00h:</td><td>Disabilitata</td></tr>
</table>
</td><td>per alternare il proprietario della porta USB FP, tenendo premuto il pulsante ID per più di 3 secondi.

L'isteresi in secondi verrà impostata quando si alterna automaticamente la porta durante il ciclo di alimentazione. Si tratta di un parametro facoltativo.

Server SD530

Sulla piattaforma SD530, la porta è facoltativa e, se presente, è cablata direttamente solo a XCC. La commutazione della porta all'host non è disponibile.
• Quando il comando viene inviato con byte 1 = 1, XCC risponderà sempre che la porta è di proprietà del controller BMC.
• Quando il comando viene inviato con byte 1 = 2, XCC risponderà sempre che la porta è dedicata al controller BMC.
• Quando il comando viene inviato con byte 1 = 3 o byte 1 = 4, XCC risponderà con il codice di completamento D6h.

Server non SD530

Sulla piattaforma non SD530, è possibile disabilitare l'uso della porta USB del pannello anteriore da parte di XCC, passando alla modalità "Solo host".

Quando il comando viene inviato con byte 1 = 5 o byte 1 = 6, XCC risponderà con il codice di completamento D6h.</td></tr>
</table>

<table>
<tr><th colspan="4">Funzione netta = 0x3A</th></tr>
<tr><th>Codice</th><th>Comando</th><th>Dati della richiesta/della risposta</th><th>Descrizione</th></tr>
<tr><td></td><td></td><td>
<table>
<tr><td>01h:</td><td>Abilitato</td></tr>
</table>
Byte 6 - Isteresi (facoltativo) in secondi

Risposta:

Byte 1 - CodeByte di completamento 2
<table>
<tr><td>00h:</td><td>Passa all'host</td></tr>
<tr><td>01h:</td><td>Passa al BMC</td></tr>
</table>
Risposta:

Byte 1 - Codice di completamento

Byte 1
<table>
<tr><td>05h:</td><td>Abilita/ Disabilita la porta USB del pannello anteriore</td></tr>
</table>
Byte 2
<table>
<tr><td>00h:</td><td>Disabilita</td></tr>
<tr><td>01h:</td><td>Abilita</td></tr>
</table>
Risposta:

Byte 1 - Codice di completamento

Richiesta:

Byte 1
<table>
<tr><td>06h:</td><td>Leggi lo stato Abilita/ Disabilita della porta USB del pannello anteriore</td></tr>
</table>
Risposta:

Byte 1 - Codice di completamento

Byte 2
</td><td></td></tr>
<tr><td>0xC7</td><td>Switch IPMI NM nativo</td><td>Lunghezza richiesta = 0:</td><td>Questo comando viene utilizzato per abilitare o disabilitare la</td></tr>
</table>

<table>
<tr><th colspan="4">Funzione netta = 0x3A</th></tr>
<tr><th>Codice</th><th>Comando</th><th>Dati della richiesta/della risposta</th><th>Descrizione</th></tr>
<tr><td></td><td></td><td>Dati della richiesta vuoti

Risposta:
<table><tr><td>Byte 1</td><td>Codice di completamento</td></tr><tr><td>Byte 2</td><td>Stato di abilitazione/disabilitazione corrente</td></tr></table>
Lunghezza richiesta= 1:
<table><tr><td>Byte 1</td><td>Attributo di abilitazione/disabilitazione dell'interfaccia IPMI NM nativa

00h - Disabilita

01h - Abilita</td></tr></table>
Risposta:
<table><tr><td>Byte 1</td><td>Codice di completamento</td></tr></table></td><td>funzione di bridging di XCC per i comandi IPMI Intel nativi.</td></tr>
</table>

Appendice A. Richiesta di supporto e assistenza tecnica

Se è necessaria assistenza tecnica o se si desidera ottenere maggiori informazioni sui prodotti Lenovo, è disponibile una vasta gamma di risorse Lenovo.

Informazioni aggiornate su sistemi, dispositivi opzionali, servizi e supporto forniti da Lenovo sono disponibili all'indirizzo Web seguente:

http://datacentersupport.lenovo.com

Nota: Questo argomento include riferimenti ai siti Web IBM e a informazioni relative all'assistenza. IBM è il fornitore di servizi preferito di Lenovo per ThinkSystem.

Prima di contattare l'assistenza

Prima di contattare l'assistenza, è possibile eseguire diversi passaggi per provare a risolvere il problema autonomamente. Se si decide che è necessario contattare l'assistenza, raccogliere le informazioni necessarie al tecnico per risolvere più rapidamente il problema.

Eseguire il tentativo di risolvere il problema autonomamente

È possibile risolvere molti problemi senza assistenza esterna seguendo le procedure di risoluzione dei problemi fornite da Lenovo nella guida online o nella documentazione del prodotto Lenovo. La documentazione del prodotto Lenovo descrive inoltre i test di diagnostica che è possibile effettuare. La documentazione della maggior parte dei sistemi, dei sistemi operativi e dei programmi contiene procedure per la risoluzione dei problemi e informazioni relative ai messaggi e ai codici di errore. Se si ritiene che si stia verificando un problema di software, consultare la documentazione relativa al programma o al sistema operativo.

La documentazione relativa ai prodotti ThinkSystem è disponibili nella posizione seguente:

https://pubs.lenovo.com/

È possibile effettuare i seguenti passaggi per provare a risolvere il problema autonomamente:

- Verificare che tutti i cavi siano connessi.
- Controllare gli interruttori di alimentazione per accertarsi che il sistema e i dispositivi opzionali siano accesi.
- Controllare il software, il firmware e i driver di dispositivo del sistema operativo aggiornati per il proprio prodotto Lenovo. I termini e le condizioni della garanzia Lenovo specificano che l'utente, proprietario del prodotto Lenovo, è responsabile della manutenzione e dell'aggiornamento di tutto il software e il firmware per il prodotto stesso (a meno che non sia coperto da un contratto di manutenzione aggiuntivo). Il tecnico dell'assistenza richiederà l'aggiornamento di software e firmware, se l'aggiornamento del software contiene una soluzione documentata per il problema.
- Se è stato installato nuovo hardware o software nel proprio ambiente, fare riferimento a http://www.lenovo.com/serverproven/ per verificare che l'hardware e il software siano supportati dal prodotto.
- Accedere all'indirizzo http://datacentersupport.lenovo.com e individuare le informazioni utili alla risoluzione del problema.
  - Controllare i forum Lenovo all'indirizzo https://forums.lenovo.com/t5/Datacenter-Systems/ct-p/sv_eg per verificare se altri utenti hanno riscontrato un problema simile.

È possibile risolvere molti problemi senza assistenza esterna seguendo le procedure di risoluzione dei problemi fornite da Lenovo nella guida online o nella documentazione del prodotto Lenovo. La documentazione del prodotto Lenovo descrive inoltre i test di diagnostica che è possibile effettuare. La documentazione della maggior parte dei sistemi, dei sistemi operativi e dei programmi contiene procedure per la risoluzione dei problemi e informazioni relative ai messaggi e ai codici di errore. Se si ritiene che si stia verificando un problema di software, vedere la documentazione relativa al programma o sistema operativo.

Raccolta delle informazioni necessarie per contattare il sevizio di supporto

Se si ritiene di necessitare di un intervento di assistenza contemplato nella garanzia per il proprio prodotto Lenovo, i tecnici dell'assistenza saranno in grado di offrire un servizio più efficiente se ci si prepara prima di mettersi in contatto. È possibile, inoltre, consultare la sezione http://datacentersupport.lenovo.com/warrantylookup per ulteriori informazioni sulla garanzia del prodotto.

Raccogliere le informazioni seguenti da fornire al tecnico dell'assistenza. Questi dati consentiranno al tecnico dell'assistenza di fornire rapidamente una soluzione al problema e di verificare di ricevere il livello di assistenza definito nel contratto di acquisto.

- I numeri di contratto dell'accordo di manutenzione hardware e software, se disponibili
- Numero del tipo di macchina (identificativo macchina a 4 cifre Lenovo)
- Numero modello
- Numero di serie
- Livelli del firmware e UEFI di sistema correnti
- Altre informazioni pertinenti quali messaggi di errore e log

In alternativa, anziché contattare il supporto Lenovo, è possibile andare all'indirizzo https://www-947.ibm.com/support/servicerequest/Home.action per inviare una ESR (Electronic Service Request). L'inoltro di una tale richiesta avvierà il processo di determinazione di una soluzione al problema rendendo le informazioni disponibili ai tecnici dell'assistenza. I tecnici dell'assistenza Lenovo potranno iniziare a lavorare sulla soluzione non appena completata e inoltrata una ESR (Electronic Service Request).

Raccolta dei dati di servizio

Al fine di identificare chiaramente la causa principale di un problema del server o su richiesta del supporto Lenovo, potrebbe essere necessario raccogliere i dati di servizio che potranno essere utilizzati per ulteriori analisi. I dati di servizio includono informazioni quali i log eventi e l'inventario hardware.

I dati di servizio possono essere raccolti mediante i seguenti strumenti:

- **Lenovo XClarity Controller**

  È possibile utilizzare l'interfaccia CLI o Web di Lenovo XClarity Controller per raccogliere i dati di servizio per il server. Il file può essere salvato e inviato al supporto Lenovo.

  - Per ulteriori informazioni sull'utilizzo dell'interfaccia Web per la raccolta dei dati di servizio, vedere https://pubs.lenovo.com/xcc3/nn1ia_c_servicesandsupport.html.
  - Per ulteriori informazioni sull'utilizzo dell'interfaccia CLI per la raccolta dei dati di servizio, vedere https://pubs.lenovo.com/xcc3/nn1ia_r_ffdccommand.html.

- **Lenovo XClarity Administrator**

  Lenovo XClarity Administrator può essere configurato in modo da raccogliere e inviare file di diagnostica automaticamente al supporto Lenovo quando si verificano determinati eventi che richiedono assistenza in Lenovo XClarity Administrator e negli endpoint gestiti. È possibile scegliere di inviare i file di diagnostica al Supporto Lenovo mediante Call Home oppure a un altro fornitore di servizi tramite SFTP. 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.

Ulteriori informazioni sulla configurazione della notifica automatica dei problemi sono disponibili all'interno di Lenovo XClarity Administrator all'indirizzo https://pubs.lenovo.com/lxca/admin_setupcallhome.html.

- **Lenovo XClarity Provisioning Manager**

  Utilizzare la funzione Raccogli dati di servizio di Lenovo XClarity Provisioning Manager per raccogliere i dati di servizio del sistema. È possibile raccogliere i dati del log di sistema esistenti oppure eseguire una nuova diagnosi per raccogliere dati aggiornati.

- **Lenovo XClarity Essentials**

  Lenovo XClarity Essentials può essere eseguito in banda dal sistema operativo. Oltre ai dati di servizio dell'hardware, Lenovo XClarity Essentials è in grado di raccogliere informazioni sul sistema operativo, quali il log eventi del sistema operativo.

  Per ottenere i dati di servizio, è possibile eseguire il comando `getinfor`. Per ulteriori informazioni sull'esecuzione di `getinfor`, vedere https://pubs.lenovo.com/lxce-onecli/onecli_r_getinfor_command.html.

Come contattare il supporto

È possibile contattare il supporto per ottenere aiuto in caso di problemi.

È possibile ricevere assistenza hardware attraverso un fornitore di servizi Lenovo autorizzato. Per individuare un fornitore di servizi autorizzato da Lenovo a fornire un servizio di garanzia, accedere all'indirizzo https://datacentersupport.lenovo.com/us/en/serviceprovider e utilizzare il filtro di ricerca per i vari paesi. Per i numeri di telefono del supporto Lenovo, vedere https://datacentersupport.lenovo.com/us/en/supportphonelist per i dettagli sul supporto per la propria area geografica.

Appendice B. Informazioni particolari

I riferimenti contenuti in questa pubblicazione relativi a prodotti, servizi o funzioni Lenovo non implicano che Lenovo intenda renderli disponibili in tutti i paesi. Consultare il proprio rappresentante Lenovo locale per in formazioni sui prodotti e servizi disponibili nel proprio paese.

Qualsiasi riferimento a un prodotto, programma o servizio Lenovo non implica che debba essere utilizzato esclusivamente quel prodotto, programma o servizio Lenovo. È possibile utilizzare qualsiasi prodotto, programma o servizio con funzionalità equivalenti che non violi alcun diritto di proprietà intellettuale Lenovo. È comunque responsabilità dell'utente valutare e verificare la possibilità di utilizzare altri prodotti, programmi o servizi.

Lenovo può avere applicazioni di brevetti o brevetti in corso relativi all'argomento descritto in questo documento. La distribuzione del presente documento non concede né conferisce alcuna licenza in virtù di alcun brevetto o domanda di brevetto. Per ricevere informazioni, è possibile inviare una richiesta scritta a:

Lenovo (United States), Inc.
1009 Think Place
Morrisville, NC 27560
U.S.A.
Attention: Lenovo VP of Intellectual Property

LENOVO FORNISCE QUESTA PUBBLICAZIONE "COSÌ COM'È" SENZA ALCUN TIPO DI GARANZIA, SIA ESPRESSA CHE IMPLICITA, INCLUSE, A TITOLO ESEMPLIFICATIVO, LE GARANZIE IMPLICITE DI NON VIOLAZIONE, COMMERCIABILITÀ O IDONEITÀ PER UNO SCOPO PARTICOLARE. Alcune giurisdizioni non consentono la rinuncia a garanzie esplicite o implicite in determinate transazioni, quindi la presente dichiarazione potrebbe non essere applicabile all'utente.

Questa pubblicazione potrebbe contenere imprecisioni tecniche o errori tipografici. Le modifiche alle presenti informazioni vengono effettuate periodicamente; tali modifiche saranno incorporate nelle nuove pubblicazioni della pubblicazione. Lenovo si riserva il diritto di apportare miglioramenti e modifiche al prodotto o al programma descritto nel manuale in qualsiasi momento e senza preavviso.

I prodotti descritti in questa documentazione non sono destinati all'utilizzo di applicazioni che potrebbero causare danni a persone. Le informazioni contenute in questa documentazione non influiscono o modificano le specifiche o le garanzie dei prodotti Lenovo. Nessuna parte di questa documentazione rappresenta l'espressione o una licenza implicita fornita nel rispetto dei diritti di proprietà intellettuale di Lenovo o di terze parti. Tutte le informazioni in essa contenute sono state ottenute in ambienti specifici e vengono presentate come illustrazioni. Quindi, è possibile che il risultato ottenuto in altri ambienti operativi vari.

Lenovo può utilizzare o distribuire le informazioni fornite dagli utenti secondo le modalità ritenute appropriate, senza incorrere in alcuna obbligazione nei loro confronti.

Tutti i riferimenti ai siti Web non Lenovo contenuti in questa pubblicazione sono forniti per consultazione; per essi Lenovo non fornisce alcuna approvazione. I materiali reperibili presso questi siti non fanno parte del materiale relativo al prodotto Lenovo. L'utilizzo di questi siti Web è a discrezione dell'utente.

Qualsiasi dato sulle prestazioni qui contenuto è stato determinato in un ambiente controllato. Quindi, è possibile che il risultato ottenuto in altri ambienti operativi vari significativamente. Alcune misurazioni possono essere state effettuate sui sistemi a livello di sviluppo e non vi è alcuna garanzia che tali misurazioni resteranno invariate sui sistemi generalmente disponibili. Inoltre, alcune misurazioni possono essere state stimate mediante estrapolazione. I risultati reali possono variare. Gli utenti di questo documento dovrebbero verificare i dati applicabili per il proprio ambiente specifico.

Marchi

Lenovo, il logo Lenovo, ThinkSystem, Flex System, System x, NeXtScale System e x Architecture sono marchi di Lenovo negli Stati Uniti e/o in altri paesi.

Intel e Intel Xeon sono marchi di Intel Corporation negli Stati Uniti e in altri paesi.

Internet Explorer, Microsoft e Windows sono marchi del gruppo di società Microsoft.

Linux è un marchio registrato di Linus Torvalds.

Nomi di altre società, prodotti o servizi possono essere marchi di altre società.

Note importanti

La velocità del processore indica la velocità del clock interno del microprocessore; anche altri fattori influenzano le prestazioni dell'applicazione.

La velocità dell'unità CD o DVD corrisponde alla velocità di lettura variabile. Le velocità effettive variano e, spesso, sono inferiori al valore massimo possibile.

Quando si fa riferimento alla memoria del processore, alla memoria reale e virtuale o al volume dei canali, KB indica 1.024 byte, MB indica 1.048.576 byte e GB indica 1.073.741.824 byte.

Quando si fa riferimento alla capacità dell'unità disco fisso o ai volumi di comunicazioni, MB indica 1.000.000 byte e GB indica 1.000.000.000 byte. La capacità totale accessibile all'utente potrebbe variare a seconda degli ambienti operativi.

Per calcolare la capacità massima dell'unità disco fisso interna, si deve ipotizzare la sostituzione delle unità disco fisso standard e l'inserimento delle unità di dimensioni massime attualmente supportate (e disponibili presso Lenovo) in tutti i vani dell'unità disco fisso.

La memoria massima potrebbe richiedere la sostituzione della memoria standard con un modulo di memoria opzionale.

Ogni cella di memoria in stato solido dispone di un numero finito e intrinseco di cicli di scrittura a cui la cella può essere sottoposta. Pertanto, un dispositivo in stato solido può essere soggetto a un numero massimo di cicli di scrittura, espresso come `total bytes written` (TBW). Un dispositivo che ha superato questo limite potrebbe non riuscire a rispondere a comandi generati dal sistema o potrebbe non consentire la scrittura. Lenovo non deve essere considerata responsabile della sostituzione di un dispositivo che abbia superato il proprio numero massimo garantito di cicli di programmazione/cancellazione, come documentato nelle OPS (Official Published Specifications) per il dispositivo.

Lenovo non fornisce garanzie sui prodotti non Lenovo. Il supporto, se presente, per i prodotti non Lenovo viene fornito dalla terza parte e non da Lenovo.

Qualche software potrebbe risultare differente dalla corrispondente versione in commercio (se disponibile) e potrebbe non includere guide per l'utente o la funzionalità completa del programma.

Contaminazione da particolato

Attenzione: I particolati atmosferici (incluse lamelle o particelle metalliche) e i gas reattivi da soli o in combinazione con altri fattori ambientali, quali ad esempio umidità o temperatura, potrebbero rappresentare un rischio per il dispositivo, come descritto in questo documento.

I rischi rappresentati dalla presenza di livelli eccessivi di particolato o concentrazioni eccessive di gas nocivi includono un danno che potrebbe portare al malfunzionamento del dispositivo o alla totale interruzione del suo funzionamento. Tale specifica sottolinea dei limiti per i particolati e i gas con l'obiettivo di evitare tale danno. I limiti non devono essere considerati o utilizzati come limiti definitivi, in quanto diversi altri fattori, come temperatura o umidità dell'aria, possono influenzare l'impatto derivante dal trasferimento di contaminanti gassosi e corrosivi ambientali o di particolati. In assenza dei limiti specifici che vengono sottolineati in questo documento, è necessario attuare delle pratiche in grado di mantenere livelli di gas e di particolato coerenti con il principio di tutela della sicurezza e della salute umana. Se Lenovo stabilisce che i livelli di particolati o gas presenti nell'ambiente del cliente hanno causato danni al dispositivo, può porre come condizione per la riparazione o la sostituzione di dispositivi o di parti di essi, l'attuazione di appropriate misure correttive al fine di attenuare tale contaminazione ambientale. L'attuazione di tali misure correttive è responsabilità del cliente.

Tabella 59. Limiti per i particolati e i gas

Agente contaminante	**Limiti**
Particolato	• L'aria del locale deve essere continuamente filtrata con un'efficienza di rimozione della polvere atmosferica del 40% (MERV 9) in conformità allo standard ASHRAE 52.2[1]. • L'aria che penetra in un centro dati deve essere filtrata a un'efficienza del 99,97% o superiore, utilizzando filtri HEPA (high-efficiency particulate air) conformi a MIL-STD-282. • L'umidità relativa deliquescente della contaminazione particellare deve essere superiore al 60%[2]. • Il locale deve essere privo di contaminazioni conduttive, ad esempio whisker di zinco.
Gassoso	• Rame: Classe G1 come per ANSI/ISA 71.04-1985[3] • Argento: tasso di corrosione inferiore a 300 Å in 30 giorni

[1] ASHRAE 52.2-2008 - **Method of Testing General Ventilation Air-Cleaning Devices for Removal Efficiency by Particle Size**. Atlanta: American Society of Heating, Refrigerating and Air-Conditioning Engineers, Inc.

[2] Per umidità relativa deliquescente della contaminazione da particolato si intende l'umidità relativa in base alla quale la polvere assorbe abbastanza acqua da diventare umida e favorire la conduzione ionica.

[3] ANSI/ISA-71.04-1985. **Condizioni ambientali per la misurazione dei processi e i sistemi di controllo: inquinanti atmosferici**. Instrument Society of America, Research Triangle Park, North Carolina, U.S.A.

Dichiarazione di regolamentazione delle telecomunicazioni

Questo prodotto potrebbe non essere certificato nel proprio paese per qualsiasi tipo di connessione a interfacce di reti di telecomunicazioni pubbliche. Potrebbero essere necessarie ulteriori certificazioni previste dalle legislazioni nazionali prima di effettuare una qualsiasi connessione di questo tipo. Rivolgersi a un rappresentante o rivenditore Lenovo per informazioni.

Informazioni sulle emissioni elettromagnetiche

Quando si collega un monitor all'apparecchiatura, è necessario utilizzare il cavo del monitor indicato ed eventuali dispositivi di eliminazione dell'interferenza forniti con il monitor.

Ulteriori avvisi sulle emissioni elettromagnetiche sono disponibili all'indirizzo:

https://pubs.lenovo.com/

Dichiarazione BSMI RoHS per Taiwan

單元 Unit	限用物質及其化學符號 Restricted substances and its chemical symbols					
	鉛Lead (Pb)	汞Mercury (Hg)	鎘Cadmium (Cd)	六價鉻 Hexavalent chromium (Cr^{+6})	多溴聯苯 Polybrominated biphenyls (PBB)	多溴二苯醚 Polybrominated diphenyl ethers (PBDE)
機架	○	○	○	○	○	○
外部蓋板	○	○	○	○	○	○
機械組合件	–	○	○	○	○	○
空氣傳動設備	–	○	○	○	○	○
冷卻組合件	–	○	○	○	○	○
內存模塊	–	○	○	○	○	○
處理器模塊	–	○	○	○	○	○
鍵盤	–	○	○	○	○	○
調製解調器	–	○	○	○	○	○
監視器	–	○	○	○	○	○
滑鼠	–	○	○	○	○	○
電纜組合件	–	○	○	○	○	○
電源	–	○	○	○	○	○
儲備設備	–	○	○	○	○	○
電池匣組合件	–	○	○	○	○	○
有mech的電路卡	–	○	○	○	○	○
無mech的電路卡	–	○	○	○	○	○
雷射器	–	○	○	○	○	○

備考1. 〝超出0.1 wt %〞及〝超出0.01 wt %〞係指限用物質之百分比含量超出百分比含量基準值。

Note1 : “exceeding 0.1wt%” and “exceeding 0.01 wt%” indicate that the percentage content of the restricted substance exceeds the reference percentage value of presence condition.

備考2. 〝○〞係指該項限用物質之百分比含量未超出百分比含量基準值。

Note2 : “○”indicates that the percentage content of the restricted substance does not exceed the percentage of reference value of presence.

備考3. 〝-〞係指該項限用物質為排除項目。

Note3 : The “-“ indicates that the restricted substance corresponds to the exemption.

Informazioni di contatto per l'importazione e l'esportazione a e da Taiwan

Sono disponibili alcuni contatti per informazioni sull'importazione e l'esportazione a e da Taiwan.

委製商/進口商名稱: 台灣聯想環球科技股份有限公司
進口商地址: 台北市南港區三重路 66 號 8 樓
進口商電話: 0800-000-702

Indice

A

B

C

D

E

F

G

I

L

M

N

O

P

R

S

T

U

V

X