Lenovo

Guida per l'utente di XClarity Controller 2

Nota: Prima di utilizzare queste informazioni, consultare le informazioni generali in Appendice B "Informazioni particolari" a pagina 233.

Prima edizione (Maggio 2021)

Contenuto

Contenuto i

Capitolo 1. Introduzione 1

Caratteristiche di XClarity Controller livelli Standard e Platinum 2

Caratteristiche di XClarity Controller livello Standard. 2

Caratteristiche di XClarity Controller livello Platinum 5

Aggiornamento di XClarity Controller. 6

Requisiti del browser Web e del sistema operativo 6

Supporto multilingua 7

Introduzione agli oggetti MIB. 8

Informazioni particolari in questo documento 8

Capitolo 2. Avvio e utilizzo dell'interfaccia Web di XClarity Controller 9

Accesso all'interfaccia Web di XClarity Controller . . 9

Configurazione della connessione di rete di XClarity Controller mediante XClarity Provisioning Manager. 10

Login a XClarity Controller 12

Descrizione delle funzioni di XClarity Controller sull'interfaccia Web 13

Capitolo 3. Configurazione di XClarity Controller 17

Configurazione dell'account utente/di LDAP . . . 17

Metodo di autenticazione utente 17

Creazione di un nuovo ruolo 18

Creazione di un nuovo account utente 19

Eliminazione di un account utente 21

Utilizzo delle password con hash per l'autenticazione 21

Configurazione delle impostazioni di login globali. 23

Configurazione di LDAP 25

Configurazione dei protocolli di rete 30

Configurazione delle impostazioni Ethernet . . 30

Configurazione di DNS 32

Configurazione di DDNS 33

Configurazione di Ethernet-over-USB 33

Configurazione di SNMP 34

Abilitazione o disabilitazione dell'accesso alla rete IPMI. 34

Configurazione delle impostazioni di rete con i comandi IPMI 35

Abilitazione del servizio e assegnazione delle porte 35

Configurazione della restrizione dell'accesso 36

Configurazione della porta USB di gestione del pannello anteriore. 37

Configurazione delle impostazioni di sicurezza. . . 38

Dashboard di sicurezza 38

Modalità di sicurezza 38

Commutazione della modalità di sicurezza . . 41

Panoramica di SSL. 42

Gestione dei certificati SSL 42

Gestione dei certificati SSL 43

Configurazione del server Secure Shell 43

Accesso IPMI-over-KCS (Keyboard Controller Style) 44

Wrapping del log SEL IPMI 44

Come impedire il downgrade del firmware di sistema -. 44

Configurazione della gestione delle chiavi di sicurezza (SKM) 44

Security Password Manager 49

Log di controllo esteso 49

Limite di login simultanei per l'account utente 49

Controllo del sistema 50

Impostazione di crittografia 50

Configurazione di Call Home. 52

Backup e ripristino della configurazione BMC . . . 54

Backup della configurazione BMC. 54

Ripristino della configurazione BMC 55

Ripristino dei valori predefiniti originali di BMC 55

Riavvio di XClarity Controller. 56

Capitolo 4. Monitoraggio dello stato del server. 57

Visualizzazione di Riepilogo integrità/Eventi di sistema attivi 57

Visualizzazione delle informazioni sul sistema . . . 58

Visualizzazione dell'utilizzo del sistema. 60

Visualizzazione dei log eventi 61

Visualizzazione dei log di controllo 62

Visualizzazione della cronologia manutenzione . . 63

Configurazione dei destinatari degli avvisi 63

Cattura dei dati della schermata dell'ultimo errore del sistema operativo 65

Capitolo 5. Configurazione del server. 67

Visualizzazione delle informazioni sull'adattatore e delle impostazioni di configurazione 67
Configurazione di modalità e ordine di avvio del sistema 67
Configurazione dell'avvio singolo 68
Gestione dell'alimentazione del server 69
- Configurazione della ridondanza dell'alimentazione 69
- Configurazione dei criteri di limite alimentazione 69
- Configurazione dei criteri di ripristino dell'alimentazione 70
- Azioni di alimentazione 70
- Gestione e monitoraggio del consumo dell'alimentazione con i comandi IPMI 71

Funzionalità di console remota 73
- Abilitazione della funzionalità di console remota 74
- Controllo di alimentazione remota 75
- Cattura della schermata nella console remota 76
- Supporto della tastiera nella console remota 76
- Supporto del mouse nella console remota. . . . 76
- Registrazione/Riproduzione video della schermata 77
- Modalità schermo della console remota . . . 77
- Metodi di montaggio dei supporti 78
- Disco remoto con client Java 82
- Errori di montaggio dei supporti 86
- Uscita dalla sessione della console remota . . 88

Download del log dei dati di servizio 88
Proprietà del server 88
- Impostazione di posizione e contatto. 88
- Impostazione dei timeout del server 89
- Messaggio di sconfinamento 90

Impostazione di data e ora di XClarity Controller . . 90

Capitolo 6. Configurazione dello storage 93

Dettaglio RAID 93
Configurazione RAID 93
- Visualizzazione e configurazione delle unità virtuali 93
- Visualizzazione e configurazione dell'inventario di storage 94

Capitolo 7. Aggiornamento del firmware del server 97

Panoramica 97
Aggiornamento firmware del sistema, dell'adattatore e dell'alimentatore 97
Aggiornamento da repository 98

Capitolo 8. Gestione licenza 103

Installazione di una chiave di attivazione 103
Rimozione di una chiave di attivazione 104
Esportazione di una chiave di attivazione 104

Capitolo 9. Gestione del gruppo adiacente. 105

Funzioni supportate 105
Rilevamento dei nodi adiacenti 106
Configurazione del gruppo adiacente 106
Provisioning del gruppo adiacente 106

Capitolo 10. API REST Redfish di Lenovo XClarity Controller. 109

Capitolo 11. Interfaccia della riga di comando 111

Accesso all'interfaccia della riga di comando . . . 111
Accesso alla sessione della riga di comando . . . 111
Configurazione del reindirizzamento da seriale a SSH 111
Sintassi dei comandi 112
Funzioni e limitazioni 112
Elenco di comandi in ordine alfabetico 113
Comandi dei programmi di utilità 115
- comando exit 115
- comando help 115
- comando history 115

Comandi di monitoraggio 116
- comando clearlog 116
- comando fans 117
- comando ffdc 117
- Comando hreport 118
- comando mhlog 119
- comando led 120
- comando readlog 121
- comando syshealth 122
- comando temps 123
- comando volts 123
- comando vpd 124

Comandi di controllo per l'accensione e il riavvio del server 125
- comando power 125
- comando reset 127
- comando fuelg 127
- comando pxeboot 128

Comando serial redirect 129
- comando console 129

Comandi di configurazione 129
comando accseccfg 129
comando alertcfg 131
comando asu 131
comando di backup 134
comando dhcpinfo 135
comando dns 136
Comando encaps 138
comando ethtousb 138
Comando firewall 139
comando gprofile 140
comando hashpw 141
comando ifconfig 142
comando keycfg 145
comando ldap 146
comando ntp 148
comando portcfg 149
comando portcontrol 150
comando ports 151
comando rdmount 152
comando restore 152
comando restoredefaults 153
comando roles 154
comando seccfg 155
comando set 155
comando smtp 155
comando snmp 156
comando snmpalerts 158
comando srcfg 160
comando sshcfg 161
comando ssl 162
comando sslcfg 163
comando storekeycfg 166
comando syncrep 168
comando thermal 169
comando timeouts 169
comando tls 170
comando trespass 171
comando uefipw 172
comando usbeth 172
comando usbfp 173
comando users 173
Comandi di controllo di IMM 177
comando alertentries 177
comando batch 180
comando clearcfg 181
comando clock 181
comando identify 182
comando info 182
comando spreset 183
Comandi Service Advisor 183
comando chconfig 183
comando chmanual 185
comando chlog 186
Comandi senza agente 186
comando storage 186
comando adapter 195
comando mvstor 197
Comandi di supporto 199
comando dbgshimm 199

Capitolo 12. Interfaccia IPMI 201
Gestione di XClarity Controller con IPMI 201
Utilizzo di IPMItool 201
Comandi IPMI con parametri OEM 202
Comando Get/Set dei parametri di configurazione LAN 202
Comandi IPMI OEM 214

Capitolo 13. Server Edge 225
Modalità di blocco del sistema 225
Gestore SED AK (Authentication Key) 226
Rete Edge 226

Appendice A. Richiesta di supporto e assistenza tecnica 229
Prima di contattare l'assistenza 229
Raccolta dei dati di servizio 230
Come contattare il supporto 231

Appendice B. Informazioni particolari 233
Marchi 234
Note importanti 234
Contaminazione da particolato 234
Dichiarazione di regolamentazione delle telecomunicazioni 235
Informazioni sulle emissioni elettromagnetiche . . . 235
Dichiarazione BSMI RoHS per Taiwan 236
Informazioni di contatto per l'importazione e l'esportazione a e da Taiwan 236

Indice 239

Capitolo 1. Introduzione

Lenovo XClarity Controller 2 (XCC2) è il controller di gestione di nuova generazione che sostituisce il controller di gestione della scheda di base per i server Lenovo ThinkSystem.

Si tratta della versione successiva del processore di servizio Integrated Management Module II (IMM2) che consolida le funzionalità di processore di servizio, Super I/O, controller video e 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 XClarity Controller CLI.
- 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 1.0.2 dell'API Redfish Scalable Platforms Management e lo schema 2016.2

Nota:

- 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.
- Per i server Flex, il CMM (Chassis Management Module) è il modulo di gestione primario per le funzioni di gestione dei sistemi. L'accesso a XClarity Controller è disponibile tramite la porta di rete sul modulo CMM.

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.

Caratteristiche di XClarity Controller livelli Standard e Platinum

XClarity Controller include funzionalità di livello Standard e Platinum. 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

Nota: Alcune funzioni potrebbero non essere disponibili per i server Flex System.

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

Caratteristiche di XClarity Controller livello Standard

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
- CLI legacy
- 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, ecc...)
- 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
- E-mail
- Eventi 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
- 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

- Rilevamento del gruppo adiacente
- 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

Caratteristiche di XClarity Controller livello Platinum

Di seguito è riportato un elenco delle caratteristiche di XClarity Controller livello Platinum:

Tutte le funzioni di XClarity Controller livello Standard più:

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 IO/IMG client locali
- Controllo di qualità/larghezza di banda
- Interazione con Virtual Console (6 utenti)
- Chat di Virtual Console
- Registrazione/Riproduzione video
- Montaggio di supporti virtuali di file http, Samba, NFS e ISO/IMG remoti
- Client Java della console remota

Reindirizzamento seriale

- Reindirizzamento seriale tramite Telnet/SSH

Protezione

- Single Sign-On
- SKLM (Security Key Lifecycle Manager)
- 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
- Contatori per lo storico dell'alimentazione
- Grafici della temperatura

Distribuzione e configurazione

- Distribuzione del sistema operativo da remoto

Aggiornamenti firmware

- Sincronizzazione con il repository
- Aggiornamento automatico
- Aggiornamento bundle firmware
- Rollback del firmware dal repository locale nella scheda MicroSD

Altre funzioni di gestione

- Gestione del gruppo adiacente

Aggiornamento di XClarity Controller

Se il server è dotato del livello Standard o Advanced 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 8 "Gestione licenza" a pagina 103.

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 48.0 o versioni successive (55.0 o versioni successive per la console remota)
- Firefox ESR 38.6.0 o versione successiva
- Microsoft Edge
- Safari 9.0.2 o versione successiva (iOS 7 o superiore 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:

- ECDHE-ECDSA-AES256-GCM-SHA384

- ECDHE-ECDSA-AES256-SHA384
- ECDHE-ECDSA-AES256-SHA
- ECDHE-ECDSA-AES128-GCM-SHA256
- ECDHE-ECDSA-AES128-SHA256
- ECDHE-ECDSA-AES128-SHA
- ECDHE-RSA-AES256-GCM-SHA384
- ECDHE-RSA-AES256-SHA384
- ECDHE-RSA-AES128-GCM-SHA256
- ECDHE-RSA-AES128-SHA256

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 in remoto utilizzando l'interfaccia Web di XClarity Controller, è necessario innanzitutto eseguire il login. 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.

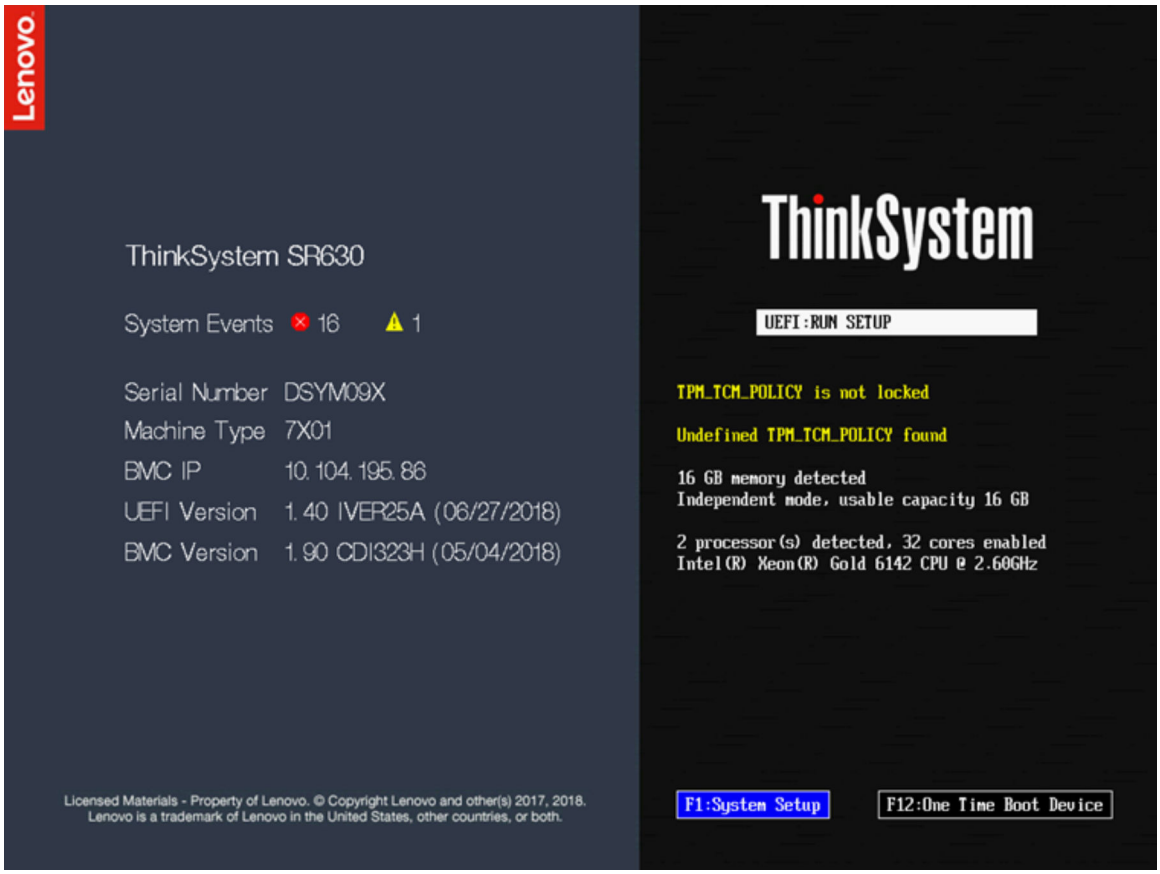
Configurazione della connessione di rete di XClarity Controller mediante XClarity Provisioning Manager

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.



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.

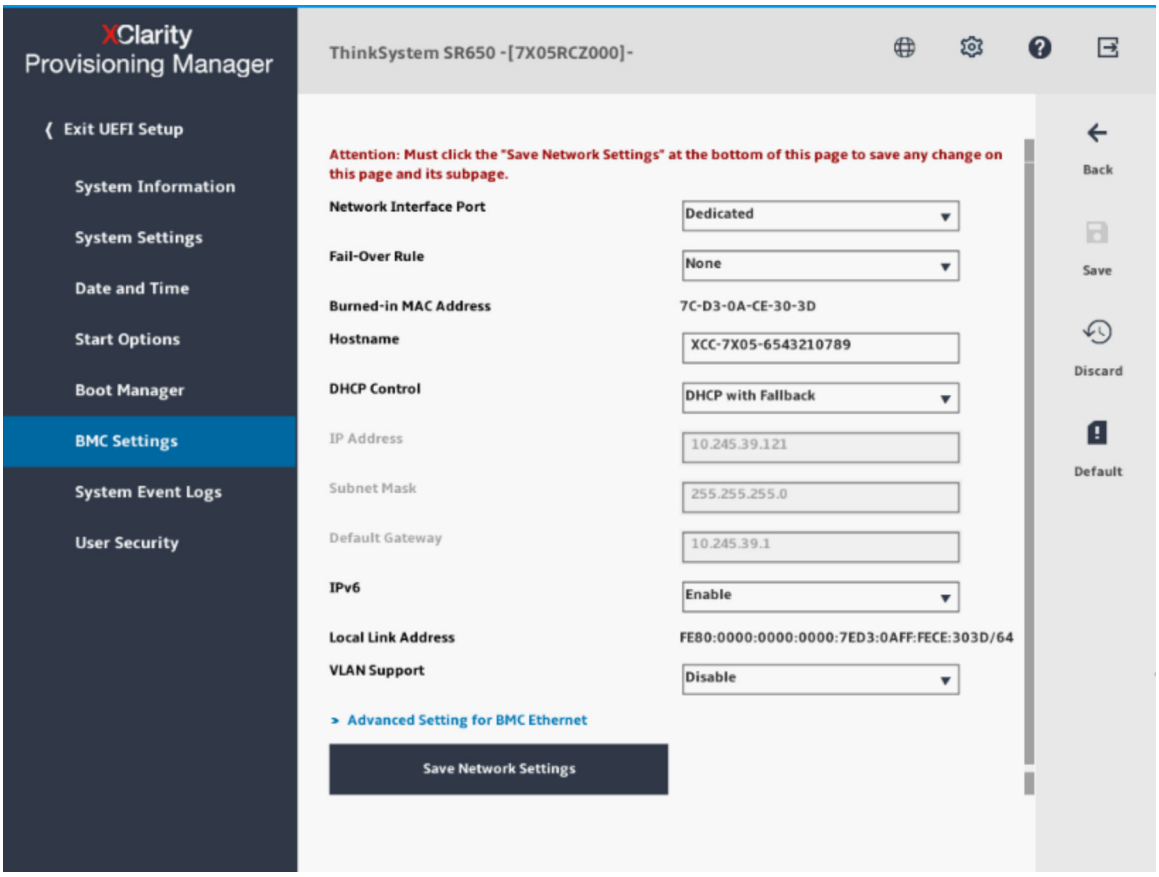
Passo 3. Dal menu principale di XClarity Provisioning Manager, selezionare **UEFI Setup**.

Passo 4. Nella schermata successiva, selezionare **BMC Settings** e fare clic su **Network Settings**.

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

- IP statico
- Abilitato per DHCP

- DHCP con fallback



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 **Network Configuration**, selezionare **Dedicated** (se disponibile) o **Shared** nel campo **Network Interface Port**.
- 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.

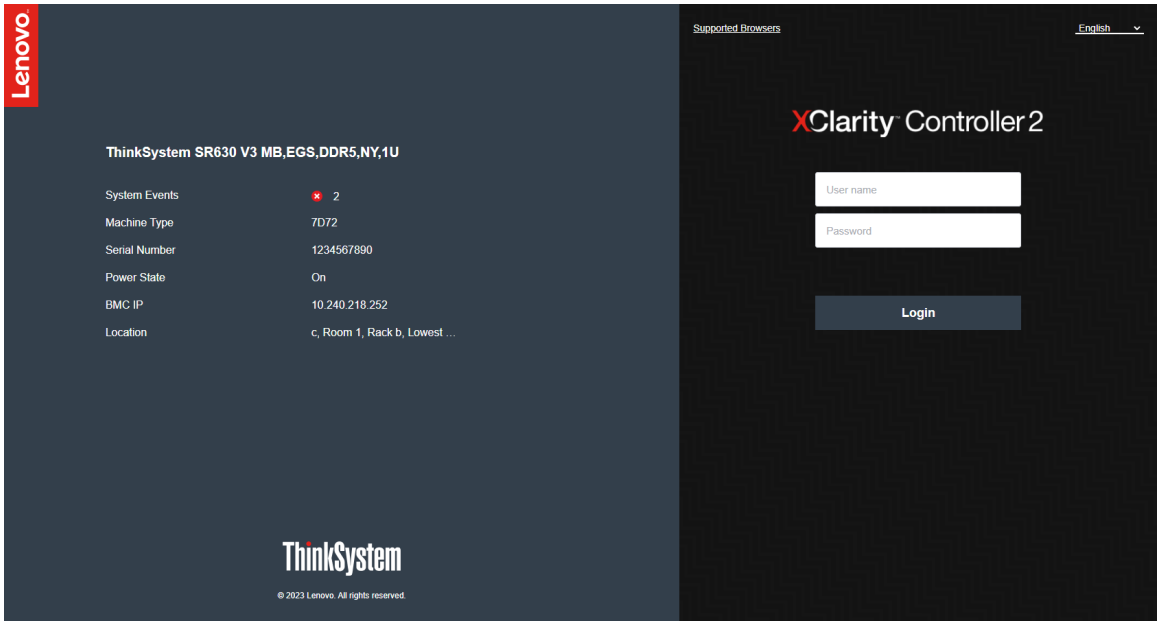
Nota: In un sistema Flex System, gli account utente di XClarity Controller possono essere gestiti tramite un modulo CMM (Chassis Management Module) Flex System e potrebbero differire dalla combinazione USERID/PASSW0RD descritta in precedenza.

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 l'indirizzo IP o il nome host di XClarity Controller a cui si desidera collegarsi.

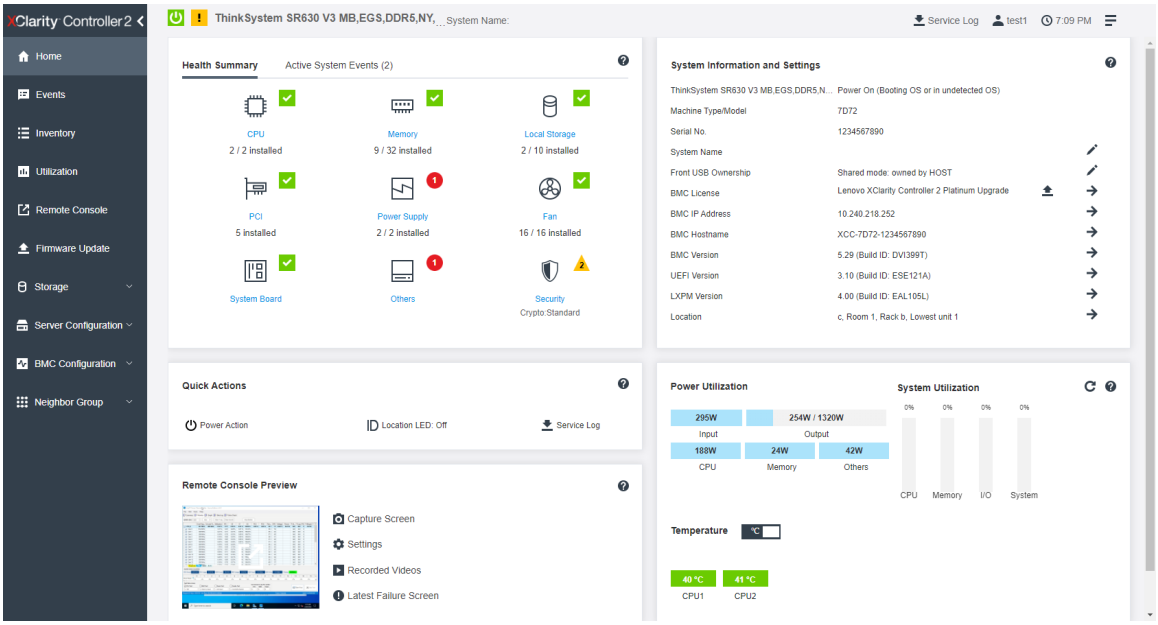
Passo 2. Selezionare la lingua desiderata dall'elenco a discesa della lingua.

Nella seguente figura viene mostrata la finestra 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 e avvertenze sono presenti attualmente nel sistema.



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

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.

Tabella 1. Funzioni di XClarity Controller

Tabella a tre colonne contenente le descrizioni delle azioni che possono essere eseguite dall'interfaccia Web di XClarity Controller.

Tab	Selezione	Descrizione
Home page	Riepilogo integrità/Eventi di sistema attivi	Mostra lo stato corrente dei componenti hardware principali nel sistema.

Tabella 1. Funzioni di XClarity Controller (continua)

Tab	Selezione	Descrizione
	Informazioni sul sistema e impostazioni	Fornisce un riepilogo delle informazioni sul 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 alimentazione/Utilizzo sistema/Temperatura	Fornisce una panoramica rapida su utilizzo alimentazione, utilizzo del sistema e temperatura globale del server correnti.
	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. La barra degli strumenti destra include le seguenti azioni rapide: • Cattura schermata • Impostazioni • Video registrati • Schermata ultimo errore
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, ad esempio il login a Lenovo 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 e i controlli nei sistemi IT.
	Cronologia manutenzione	Visualizza tutta la cronologia di aggiornamento firmware, configurazione e sostituzione hardware.
	Destinatari avvisi	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 SMM2 per ulteriori dettagli sullo stato dell'alimentazione della soluzione.
Utilizzo		Visualizza la temperatura ambiente/componente, l'utilizzo dell'alimentazione, i livelli di tensione, l'utilizzo del sottosistema e le informazioni sulla velocità della ventole del server e i relativi componenti in formato tabulare o grafico.
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.

Tabella 1. Funzioni di XClarity Controller (continua)

Tab	Selezione	Descrizione
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 è visualizzato come unità disco USB 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.
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 SMM2 per ulteriori dettagli sullo stato dell'alimentazione della soluzione.
	Proprietà del server	• Monitora varie proprietà, condizioni di stato e impostazioni del server. • Gestisce i timeout di avvio del server per rilevare un blocco e ripristinare il 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.
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.

Tabella 1. Funzioni di XClarity Controller (continua)

Tab	Selezione	Descrizione
	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.
	Call Home	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 su **Consenti accesso da** per selezionare la modalità di autenticazione dei tentativi di login. 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, 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 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, 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, selezionare la casella di controllo accanto a **Impostazioni SNMPv3**. 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.

Indirizzo per i trap

Specificare la destinazione trap per l'utente. Può essere un indirizzo IP o un nome host. Grazie ai trap, l'agent SNMP invia una notifica alla stazione di gestione relativa agli eventi (ad esempio, quando la temperatura di un processore supera il limite).

Protocollo di autenticazione
Solo **HMAC-SHA** è supportato come protocollo di autenticazione. Questo algoritmo è utilizzato dal modello di sicurezza SNMPv3 per l'autenticazione.

Protocollo privacy
Il trasferimento di dati tra il client SNMP e l'agent può essere protetto utilizzando la crittografia. I metodi supportati sono **CBC-DES** e **AES**.

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 la pagina 72 del 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, selezionare la casella di controllo accanto a **Chiave SSH**. 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 (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.

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:

- Gli utenti non potranno modificare una password, se la password è di terze parti 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.

Nota: In un sistema Flex, le impostazioni dei criteri di sicurezza dell'account sono gestite da Flex System Chassis Management Module (CMM) e non possono essere modificate mediante XCC. Quando il modulo CMM viene utilizzato per configurare i criteri di sicurezza dell'account, tenere presente che:

- A differenza di XCC, CMM non dispone dell'impostazione *Periodo di avviso scadenza password (giorni)*. Quando l'opzione *Periodo di scadenza password* viene configurata con una durata maggiore di 5 giorni nel CMM, XCC imposterà il periodo di avviso scadenza password su 5 giorni. Diversamente, se l'impostazione è inferiore a 5 giorni, il periodo di avviso scadenza password sarà identico al valore immesso nel campo *Periodo di scadenza password*.
- Per l'impostazione *Numero massimo di errori di login (volte)*, l'intervallo impostato in CMM è 0-100 volte. Tuttavia, l'intervallo definito in XCC è 0-10 volte. Pertanto, quando l'utente seleziona un valore superiore a 10 volte in CMM, in XCC il numero massimo di errori di login resterà di 10 volte.
- Per l'impostazione *Intervallo di modifica password minimo (ore)*, l'intervallo impostato in CMM è 0-1.440 ore. Tuttavia, l'intervallo definito in XCC è 0-240 ore. Pertanto, quando l'utente seleziona un valore superiore a 240 ore in CMM, in XCC l'intervallo minimo di modifica password resterà di 240 volte.

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 da 8 a 32 caratteri

Se la casella dell'opzione non è selezionata, il numero di caratteri specificato nella lunghezza minima della password può essere compreso tra 0 e 32. 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 password
Questo campo contiene la lunghezza minima della password.

Ciclo minimo di riutilizzo password
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 Server)
- Microsoft Lightweight Directory Service (Windows 2008, Windows 2012)
- Novell eDirectory Server, versione 8.7, 8.8 e 9.4
- OpenLDAP Server 2.1, 2.2, 2.3 e 2.4

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 la stringa IBMRBSPermissions. 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 privilegi possono essere configurati nella sezione Impostazioni Active Directory.

- **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.

- **Usa server preconfigurati**: è possibile configurare fino a quattro 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 42.

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

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:

- **Nessuna credenziale richiesta**

  Utilizzare questo metodo per eseguire il collegamento senza un nome distinto o una password. Questo metodo è fortemente sconsigliato perché la maggior parte dei server sono configurati per non consentire richieste di ricerca sui record di utenti specifici.

- **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 **Credenziali non richieste** o **Utilizza credenziali configurate**.

Nome 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 UID

Quando il metodo di collegamento è impostato su **Credenziali non richieste** o 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. Su server Active Directory, il nome dell'attributo è di solito **sAMAccountName**. Su server Novell eDirectory e OpenLDAP, il nome dell'attributo è **uid**. Se questo campo è lasciato vuoto, il valore predefinito sarà **uid**.

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.

L'appartenenza a gruppi nidificati è supportata solo in ambienti Active Directory. Ad esempio, se un utente è membro del Gruppo A e del Gruppo B e il Gruppo A è a sua volta membro del Gruppo C, l'utente sarà anche membro del Gruppo C. Le ricerche nidificate vengono interrotte una volta utilizzati 128 gruppi nella ricerca stessa. I gruppi in un livello saranno ricercati prima dei gruppi in un livello inferiore. I loop non vengono rilevati.

Attributo di ricerca gruppi

In un ambiente Active Directory o Novell eDirectory, il campo **Attributo di ricerca gruppi** specifica il nome dell'attributo utilizzato per identificare i gruppi ai quali appartiene un utente. In un ambiente Active Directory il nome dell'attributo è **memberOf**. In un ambiente eDirectory, il nome dell'attributo è **groupMembership**. In un ambiente server OpenLDAP, gli utenti sono di solito assegnati a gruppi

in 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 dell'attributo. Se questo campo viene lasciato vuoto, all'utente saranno assegnate le autorizzazioni di sola lettura predefinite, sempre che l'utente superi l'autenticazione utente e del gruppo.

Il valore dell'attributo restituito dal server LDAP ricercherà la stringa della parola chiave IBMRBSPermissions=. Questa stringa deve essere seguita immediatamente da una stringa di bit immessi come 12 0 (zeri) o 1 consecutivi. Ogni bit rappresenta una serie di funzioni. I bit sono numerati in base alle loro posizioni. Il bit più a sinistra è la posizione bit 0, mentre quello più a destra è la posizione bit 11. Un valore 1 in una determinata posizione abilita la funzione associata a tale posizione. Un valore 0 alla posizione di bit disabilita la funzione associata a tale posizione.

La stringa IBMRBSPermissions=010000000000 è un esempio valido. La parola chiave IBMRBSPermissions= è utilizzata per consentire il posizionamento in un punto qualsiasi nel campo. Ciò consente all'amministratore LDAP di riutilizzare un attributo esistente, impedendo in questo modo un'estensione allo schema LDAP. Ciò consente anche l'utilizzo dell'attributo per il suo scopo originale. È possibile aggiungere la stringa della parola chiave in un punto qualsiasi del 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 2. 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	Rete e sicurezza	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 2. 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 dell'adattatore di 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 avanzata dell'adattatore	Un utente non ha limitazioni per la configurazione di XClarity Controller. Inoltre, l'utente avrà accesso in gestione a XClarity Controller. L'utente potrà utilizzare le seguenti funzioni avanzate: aggiornamenti firmware, avvio di rete PXE, ripristino delle impostazioni predefinite di XClarity Controller, modifica e ripristino della configurazione dell'adattatore da un file di configurazione e riavvio/ reimpostazione di XClarity Controller.
11	Riservato	Questa posizione di bit è riservata per un uso futuro. Se nessuno dei bit è impostato, l'utente avrà autorizzazione di sola lettura. La priorità è data alle autorizzazioni di login che vengono recuperate direttamente dal record utente. Se l'attributo di autorizzazione di login non si trova nel record dell'utente, viene effettuato un tentativo di recupero delle autorizzazioni dai gruppi a cui appartiene l'utente. Ciò viene eseguito come parte della fase di autenticazione del gruppo. All'utente viene assegnato l'operatore OR inclusivo di tutti i bit per tutti i gruppi. Il bit di accesso di sola lettura (posizione 2) è impostato solo se tutti gli altri bit sono impostati su zero. Se per uno dei gruppi è impostato il bit Nega sempre (posizione 0), all'utente verrà negato l'accesso. Il bit Nega sempre (posizione 0) ha sempre la precedenza su tutti gli altri bit.

Se nessuno dei bit è impostato, l'utente avrà l'autorizzazione **Sola lettura** come impostazione predefinita.

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.

Nota: 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. Scegliere se abilitare o meno l'opzione **Abilita la sicurezza avanzata basata sui ruoli per utenti di Active Directory** in **Impostazioni Active Directory** (se si utilizza la modalità **Utilizza il server LDAP per**

autenticazione e autorizzazione) oppure configurare **Gruppi per autorizzazione locale** (se si utilizza la modalità **Utilizza il server LDAP solo per l'autenticazione** (**con autorizzazione locale**)).

- **Abilitazione della sicurezza avanzata basata sui ruoli per utenti Active Directory**

  Se viene abilitata l'impostazione di sicurezza basata sui ruoli avanzata, deve essere configurato un nome server senza formattazione che funga da nome di destinazione per questo specifico XClarity Controller. Il nome di destinazione può essere associato a uno o più ruoli sul server Active Directory mediante uno Snap-in RBS (Role-Based Security). Ciò è possibile creando destinazioni gestite e attribuendo loro nomi specifici, per poi associarle ai ruoli appropriati. Se il nome viene configurato in questo campo, offre la possibilità di definire ruoli specifici per gli utenti e XClarity Controller (destinazioni) membri dello stesso ruolo. Quando un utente esegue il login a XClarity Controller e viene autenticato tramite Active Directory, i ruoli di cui l'utente è un membro vengono recuperati dalla directory. Le autorizzazioni assegnate all'utente vengono estratte dai ruoli che hanno come membro anche una destinazione il cui nome corrisponde a quello configurato qui oppure una destinazione che corrisponde a un qualsiasi XClarity Controller. Più XClarity Controller possono condividere lo stesso nome di destinazione. Questo potrebbe essere utilizzato, per esempio, per raggruppare più XClarity Controller e assegnarli allo stesso ruolo (o agli stessi ruoli) utilizzando una singola destinazione gestita. Viceversa, a ogni XClarity Controller può essere assegnato un nome univoco.

- **Gruppi per autorizzazione locale**

  I nomi dei gruppi sono configurati per fornire specifiche di autorizzazione locali per i gruppi di utenti. A ogni nome di gruppo possono essere assegnate autorizzazioni (ruoli) corrispondenti a quanto descritto nella tabella precedente. Il server LDAP associa gli utenti a un nome del gruppo. Al momento del login, a ogni utente vengono assegnate le autorizzazioni associate al gruppo di appartenenza. I gruppi aggiuntivi possono essere configurati facendo clic sull'icona (+) o eliminati facendo clic sull'icona (x).

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 ha effetto sull'interfaccia USBLAN 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 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.

Nota: In un sistema Flex System, le impostazioni VLAN sono gestite da un CMM Flex System e non possono essere modificate da XClarity Controller.

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.

Dall'elenco **Selezione 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 `000000000000` 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 **MTU (Maximum Transmission Unit)** specificare l'unità di trasmissione massima di un pacchetto (in byte) per la propria interfaccia di rete. L'intervallo MTU è compreso tra 60 e 1500. Il valore predefinito per questo campo è 1500.

Per utilizzare una connessione Ethernet IPv6, effettuare le seguenti operazioni:

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.

Nota: In un sistema Flex System, le impostazioni DNS non possono essere modificate su XClarity Controller. Le impostazioni DNS sono gestite dal modulo CMM.

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.

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 su 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 su USB di XClarity Controller.

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

Importante: Se si disabilita Ethernet su USB, non sarà possibile eseguire un aggiornamento in banda del firmware di XClarity Controller o del server utilizzando le utility flash Linux o Windows.

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

- **Utilizza l'indirizzo locale del collegamento IPv6 per Ethernet su USB**: Questo metodo utilizza gli indirizzi IPv6 basati sull'indirizzo MAC assegnati agli endpoint dell'interfaccia Ethernet su 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 su 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 di Ethernet su USB oppure disabilitare il funzionamento predefinito di Windows utilizzando il seguente comando: *netsh interface ipv6 set global randomizeidentifiers=disabled*
- **Utilizza l'indirizzo locale del collegamento IPv4 per Ethernet su USB**: Un indirizzo IP nell'intervallo 169.254.0.0/16 viene assegnato a XClarity Controller e al lato server della rete.
- **Configura impostazione IPv4 per Ethernet su 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 su USB.

Nota:

1. Le impostazioni di configurazione IP del sistema operativo non vengono utilizzate per impostare l'indirizzo IP dell'interfaccia Ethernet-over-USB, ma per avvisare BMC che l'indirizzo IP del sistema operativo dell'interfaccia Ethernet-over-USB è stato modificato.
2. 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.

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 il **Trap SNMPv1**, **Trap SNMPv2** e/o il **Trap 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 nome 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.

Abilitazione o disabilitazione dell'accesso alla rete IPMI

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

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

Accesso IPMI-over-LAN
Fare clic sullo switch per abilitare o disabilitare l'accesso di rete IPMI a XClarity Controller.

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:

Web
Il numero di porta è 80. Questo campo non è configurabile dall'utente.

Web-over-HTTPS
In questo campo, specificare il numero di porta per Web-over-HTTPS. Il valore predefinito è 443.

REST-over-HTTPS
Il numero di porta verrà automaticamente modificato in quello specificato nel campo Web-over-HTTPS. Questo campo non è configurabile dall'utente.

Presenza remota
In questo campo, specificare il numero di porta per la presenza remota. Il valore predefinito è 3900.

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

Nota: IPMI è disabilitato per impostazione predefinita.

SFTP
Specificare in questo campo il numero di porta utilizzato per SFTP (SSH File Transfer Protocol). Il numero di porta è 115. Questo campo non è configurabile dall'utente.

Nota: IMM.SFTPPortControl=open è necessario per gli aggiornamenti in banda OneCLI.

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.

Agente 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.

Trap SNMP

In questo campo specificare il numero porta utilizzato per i trap SNMP. Il valore predefinito è 162. I numeri di porta validi sono 1-65535.

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.

Su alcuni server la porta USB del pannello anteriore può essere commutata in modo da essere collegata al server o a 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 su USB tra l'app mobile in esecuzione sul dispositivo e XClarity Controller.

Fare clic su **Rete** in **Configurazione BMC** per visualizzare o modificare le impostazioni della porta USB di gestione del pannello anteriore di XClarity Controller.

È possibile scegliere uno dei seguenti quattro tipi di impostazione:

Modalità solo host
La porta USB del pannello anteriore è sempre collegata solo al server.

Modalità solo BMC
La porta USB del pannello anteriore è sempre collegata solo a XClarity Controller.

Modalità condivisa: proprietà di BMC
La porta USB del pannello anteriore è condivisa sia dal server che da XClarity Controller, ma la porta viene commutata su XClarity Controller.

Modalità condivisa: proprietà di host
La porta USB del pannello anteriore è condivisa sia dal server che da XClarity Controller, ma la porta viene commutata sull'host.

Per ulteriori informazioni sull'app Mobile, fare riferimento al seguente sito:

http://sysmgt.lenovofiles.com/help/topic/com.lenovo.lxca.doc/lxca_usemobileapp.html

Nota:

- Se la porta USB del pannello anteriore è configurata per la modalità condivisa, la porta è collegata a XClarity Controller in assenza di alimentazione mentre è collegata al server in presenza di alimentazione. In presenza di alimentazione, il controllo della porta USB del pannello anteriore può essere commutato dal server a XClarity Controller e viceversa. In modalità condivisa, la porta può inoltre essere commutata tra l'host e XClarity Controller tenendo premuto per 3 secondi il pulsante di identificazione del pannello anteriore (per i nodi di elaborazione è possibile che sia il pulsante di gestione USB).

- Quando la porta USB è configurata in modalità condivisa ed è attualmente collegata al server, XClarity Controller è in grado di supportare un'eventuale richiesta di commutazione della porta USB del pannello anteriore su XClarity Controller. Quando questa richiesta viene eseguita, la porta USB del pannello anteriore rimarrà collegata a XClarity Controller finché non sarà cessata qualunque attività USB su XClarity Controller per il periodo specificato per il timeout di inattività.

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 170.

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 ai 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 V3.

La licenza XCC Platinum viene fornita con una terza modalità di sicurezza: modalità rigorosa aziendale. Questa modalità è più idonea per requisiti di sicurezza di alto livello.

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 alla modalità rigorosa aziendale.
- BMC opera in modalità convalidata standard.
- Richiede certificati di livello rigoroso aziendale.

- Sono consentiti solo i servizi che supportano la crittografia di livello rigoroso aziendale.
- 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 alla modalità standard.
- BMC opera in modalità convalidata standard.
- Richiede certificati di livello standard.
- I servizi che richiedono la crittografia e che non supportano la crittografia di livello standard sono disabilitati per impostazione predefinita.

Modalità di sicurezza della 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.

Matrice di servizio in tre modalità di sicurezza:

Funzione/ Servizio	**Utilizza la crittografia**	**Stato predefinito** **Predefinito**	**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	Disabilitata	No	Sì	Sì
Trap SNMPv1	No	Non configurato	No	Sì	Sì
Trap SNMPv3	Sì	Non configurato	No	Sì Se abilitato, verrà visualizzato un avviso per l'utilizzo della crittografia non FIPS	Sì
Agent SNMPv3	Sì	Non configurato	No	Sì Se abilitato, verrà visualizzato un avviso per l'utilizzo della crittografia non FIPS	Sì

Funzione/ Servizio	Utilizza la crittografia	Stato predefinito Predefinito	Supportato in Modalità rigorosa	Supportato in Modalità standard	Supportato in Modalità di compatibilità
Avvisi e-mail	Sì	Non configurato	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 configurato	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
SSDP	No	Abilitato	Sì	Sì	Sì
SSH-CLI	Sì	Abilitato	Sì	Sì	Sì
SFTP	Sì	Disabilitata	Sì	Sì	Sì
LDAP	No	Non configurato	No	Sì	Sì
LDAP sicuro	Sì	Non configurato	Sì	Sì	Sì
Gestione della chiave di sicurezza	Sì	Non configurato	Sì	Sì	Sì
Console remota	Sì	Abilitato	Sì	Sì	Sì
Supporti virtuali - CIFS	Sì	Non configurato	No	Sì	Sì
Supporti virtuali - NFS	No	Non configurato	No	Sì	Sì
Supporti virtuali - HTTPTF	Sì	Non configurato	Sì	Sì	Sì
RDOC - Locale	Sì	Non configurato	Sì	Sì	Sì

Funzione/ Servizio	Utilizza la crittografia	Stato predefinito Predefinito	Supportato in Modalità rigorosa	Supportato in Modalità standard	Supportato in Modalità di compatibilità
RDOC - CIFS	Sì	Non configurato	No	Sì	Sì
RDOC - HTTP	No	Non configurato	No	Sì	Sì
RDOC - HTTPS	Sì	Non configurato	Sì	Sì	Sì
RDOC - FTP	No	Non configurato	No	Sì	Sì
RDOC - SFTP	Sì	Non configurato	Sì	Sì	Sì
Caricamento FFDC (SFTP)	Sì	Abilitato	Sì	Sì	Sì
Caricamento FFDC (TFTP)	No	Abilitato	No	Sì	Sì
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.

È possibile utilizzare SSL con un certificato autofirmato o con un certificato che viene 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 non crea un piccolo rischio per la sicurezza. Il rischio si verifica poiché il client SSL non ha modo di convalidare l'identità del server SSL per la prima connessione che viene tentata tra il client e il server. Ad esempio, è possibile che una terza parte possa impersonare il server Web XClarity Controller e intercettare i dati che vengono trasferiti tra il server Web XClarity Controller reale e il browser Web dell'utente. 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).

Per una sicurezza più completa, è possibile utilizzare un certificato che viene firmato da una autorità di certificazione o CA (certificate authority). Per ottenere un certificato firmato, è necessario selezionare **Genera CSR (Certificate Signing Request)**. Selezionare **Scarica CSR (Certificate Signing Request)** e inviare la richiesta di firma del certificato (CSR) a una CA per ottenere un certificato firmato. Una volta ricevuto il certificato firmato, selezionare **Importa certificato firmato** per importarlo in XClarity Controller.

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

XClarity Controller richiede un certificato da utilizzare con il server HTTPS, con CIM-over-HTTPS e con il client LDAP sicuro. Inoltre, il client LDAP sicuro richiede anche l'importazione di uno o più certificati attendibili. Il certificato attendibile è utilizzato dal client LDAP sicuro per identificare correttamente il server LDAP. Tale certificato è il certificato della CA che ha firmato il certificato del server LDAP. Se il server LDAP utilizza certificati autofirmati, il certificato attendibile può essere il certificato del server LDAP stesso. Se nella propria configurazione è utilizzato più di un server LDAP, sarà necessario importare più certificati attendibili.

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 mediante uno strumento di terze parti come OpenSSL (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 **Rigenera chiave**.
- 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 l'accesso IPMI-over-KCS.

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

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.

Wrapping del log SEL IPMI

Utilizzare le informazioni in questo argomento per configurare il log SEL IPMI.

XClarity Controller fornisce un'opzione di wrapping del log SEL IPMI.

Fare clic sull'interruttore dell'angolo in alto a destra per abilitare o disabilitare il wrapping del log SEL IPMI.

Questa funzione consente la registrazione continua del log SEL IPMI. Il nuovo record SEL viene sempre aggiunto e il più vecchio viene cancellato quando il log SEL IPMI è pieno.

Nota: L'applicazione di questa impostazione richiede il riavvio del BMC.

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 impedire il downgrade del firmware di sistema

Per abilitare o disabilitare questa funzione, fare clic su **Rete** in **Configurazione BMC**. 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).

XClarity Controller utilizza la rete per recuperare le chiavi dal server di gestione delle chiavi. Il server di gestione delle chiavi deve essere accessibile a XClarity Controller. XClarity Controller fornisce il canale di comunicazione tra il server di gestione delle chiavi e il server ThinkSystem richiedente. Il firmware di XClarity Controller tenta di stabilire una connessione con ciascun server di gestione delle chiavi configurato, interrompendo l'operazione ogni volta che viene correttamente stabilita una connessione.

XClarity Controller stabilisce la comunicazione con il server di gestione delle chiavi se sono soddisfatte le condizioni elencate di seguito:

- Uno o più indirizzi IP/nomi host del server di gestione delle chiavi sono configurati in XClarity Controller.
- Due certificati (client e server) per la comunicazione con il server di gestione delle chiavi sono installati in XClarity Controller.

Nota: Configurare almeno due (primario e secondario) server di gestione delle chiavi con lo stesso protocollo per il dispositivo. Se il server di gestione delle chiavi primario non risponde al tentativo di connessione di XClarity Controller, vengono avviati tentativi di connessione con i server di gestione delle chiavi aggiuntivi fino a stabilire una connessione valida.

È necessario che sia stabilita una connessione TLS (Transport Layer Security) tra XClarity Controller e il server di gestione delle chiavi. XClarity Controller autentica il server di gestione delle chiavi confrontando il certificato del server inviato dal server di gestione delle chiavi con il certificato del server di gestione delle chiavi precedentemente importato nell'archivio attendibile di XClarity Controller. Il server di gestione delle chiavi autentica ciascun XClarity Controller con cui è in comunicazione e verifica che XClarity Controller sia autorizzato ad accedere al server di gestione delle chiavi. L'autenticazione viene effettuata confrontando il certificato del client inviato da XClarity Controller con un elenco di certificati attendibili memorizzati sul server di gestione delle chiavi.

Verrà stabilita la connessione con almeno un server di gestione delle chiavi e il gruppo di dispositivi viene considerato opzionale. Il certificato del server di gestione delle chiavi dovrà essere importato, mentre il certificato client deve essere specificato. Per impostazione predefinita, viene utilizzato il certificato HTTPS. Se si desidera sostituire il certificato, è possibile generarne uno nuovo.

Nota: Per collegare il server KMIP (KeySecure e CipherTrust), è necessario generare una richiesta di firma del certificato (CSR) e il relativo nome comune deve corrispondere al nome utente definito nel server KMIP. Quindi è necessario importare un certificato firmato dall'autorità di certificazione (CA) attendibile dal server KMIP per il CSR.

Configurazione dei server di gestione delle chiavi

Utilizzare le informazioni in questo argomento per creare il nome host o l'indirizzo IP e le informazioni sulla porta associate per il server di gestione delle chiavi.

La sezione di configurazione dei server di gestione delle chiavi è costituita dai seguenti campi:

Nome host o indirizzo IP
Digitare il nome host (se DNS è abilitato o configurato) oppure l'indirizzo IP del server di gestione delle chiavi in questo campo. È possibile aggiungere fino a quattro server.

Porta
Digitare il numero di porta del server di gestione delle chiavi in questo campo. Se il campo è vuoto, verrà utilizzato il valore predefinito 5696. I numeri di porta validi sono compresi tra 1 e 65535.

Configurazione del gruppo di dispositivi

Utilizzare le informazioni in questa sezione per configurare il gruppo di dispositivi utilizzato nel server SKLM.

Nel server SKLM, un gruppo di dispositivi consente agli utenti di gestire le chiavi SED (Self-Encrypting Drive) su più server come gruppo. Un gruppo di dispositivi con lo stesso nome deve anche essere creato sul server SKLM.

La sezione Gruppo di dispositivi contiene il campo seguente:

Gruppo di dispositivi
Un gruppo di dispositivi consente agli utenti di gestire le chiavi per i SED su più server come gruppo. Un gruppo di dispositivi con lo stesso nome deve anche essere creato sul server SKLM. Il valore predefinito per questo campo è IBM_SYSTEM_X_SED.

Definizione della gestione dei certificati

Questo argomento fornisce informazioni sulla gestione dei certificati client e server.

I certificati client e server permettono di autenticare la comunicazione tra il server SKLM e XClarity Controller che si trova nel server ThinkSystem. La gestione dei certificati client e server viene trattata in questa sezione.

Gestione dei certificati client

Questo argomento fornisce informazioni sulla gestione dei certificati client.

I certificati client sono classificati come indicato di seguito:

- Un certificato XClarity Controller assegnato automaticamente.
- Un certificato generato da una richiesta di firma del certificato (CSR) di XClarity Controller e firmata esternamente da un'autorità di certificazione (CA) di terze parti.

È richiesto un certificato client per la comunicazione con il server SKLM. Il certificato client contiene firme digitali per la CA e XClarity Controller.

Nota:

- I certificati sono mantenuti anche in seguito agli aggiornamenti firmware.
- Se non viene creato un certificato client per la comunicazione con il server SKLM, viene utilizzato il certificato del server HTTPS di XClarity Controller.
- La funzione della CA è verificare l'identità di XClarity Controller.

Per creare un certificato client, fare clic sull'icona del segno più ( ) e selezionare una delle seguenti voci:

- Genera una nuova chiave e un certificato autofirmato
- Genera una nuova chiave e una CSR (Certificate Signing Request)

L'azione **Genera una nuova chiave e un certificato autofirmato** genera una nuova chiave di crittografia e un certificato autofirmato. Nella finestra Genera una nuova chiave e un certificato autofirmato, digitare o selezionare le informazioni nei campi obbligatori e in qualsiasi campo opzionale applicabile alla configurazione (vedere la tabella di seguito). Fare clic su **OK** per generare la chiave di crittografia e il certificato. Durante la generazione del certificato autofirmato viene visualizzata una finestra di avanzamento. Una volta completata l'installazione del certificato, viene visualizzata una finestra di conferma.

Nota: La nuova chiave di crittografia e il nuovo certificato sostituiscono la chiave e il certificato esistenti.

Tabella 3. Genera una nuova chiave e un certificato autofirmato

Tabella a due colonne con intestazioni che documenta i campi obbligatori e facoltativi per l'azione Genera una nuova chiave e un certificato autofirmato. La riga inferiore copre la lunghezza di entrambe le colonne.

Tabella 3. Genera una nuova chiave e un certificato autofirmato (continua)

Campo	Descrizione
Paese[1]	Dall'elenco selezionare il paese in cui risiede fisicamente il BMC.
Stato o provincia[1]	Digitare lo stato o la provincia in cui risiede fisicamente il BMC.
Città o località[1]	Digitare la città o la località in cui risiede fisicamente il BMC.
Nome organizzazione[1]	Digitare il nome della società o dell'organizzazione che possiede il BMC.
Nome host BMC[1]	Digitare il nome host del BMC visualizzato nella barra degli indirizzi Web.
Contatto	Digitare il nome della persona di contatto responsabile del BMC.
Indirizzo e-mail	Digitare l'indirizzo e-mail della persona di contatto responsabile del BMC.
Unità organizzativa	Digitare l'unità nell'interno dell'azienda che possiede il BMC.
Cognome	Digitare il cognome della persona di contatto responsabile del BMC. Questo campo può contenere al massimo 60 caratteri.
Nome	Digitare il nome della persona di contatto responsabile del BMC. Questo campo può contenere al massimo 60 caratteri.
Iniziali	Digitare le iniziali della persona di contatto responsabile del BMC. Questo campo può contenere al massimo 20 caratteri.
Qualificatore DN	Digitare il qualificatore del nome distinto per il BMC. Questo campo può contenere al massimo 60 caratteri.

1. Questo campo è obbligatorio.

Una volta che il certificato client è stato generato, è possibile scaricarlo e archiviarlo in XClarity Controller selezionando l'azione **Scarica certificato**.

L'azione **Genera una nuova chiave e una CSR (Certificate Signing Request)** genera una nuova chiave di crittografia e una CSR. Nella finestra Genera una nuova chiave e una CSR (Certificate Signing Request), digitare o selezionare le informazioni nei campi obbligatori e in qualsiasi campo opzionale applicabile alla configurazione (vedere la tabella di seguito). Fare clic su **OK** per generare la nuova chiave di crittografia e la CSR.

Durante la generazione della CSR viene visualizzata una finestra di avanzamento, mentre al completamento dell'operazione viene visualizzata una finestra di conferma. La CSR così generata dovrà essere inviata a un'autorità di certificazione per la firma digitale. Selezionare l'azione **Scarica CSR (Certificate Signing Request)** e fare clic su **OK** per salvare la CSR sul server. È quindi possibile inviare la CSR all'autorità di certificazione per la firma.

Tabella 4. Genera una nuova chiave e una CSR (Certificate Signing Request)

Tabella a due colonne con intestazioni che documenta i campi obbligatori e facoltativi per l'azione Genera una nuova chiave e una CSR (Certificate Signing Request). La riga inferiore copre la lunghezza di entrambe le colonne.

Campo	Descrizione
Paese[1]	Dall'elenco selezionare il paese in cui risiede fisicamente il BMC.
Stato o provincia[1]	Digitare lo stato o la provincia in cui risiede fisicamente il BMC.

Tabella 4. Genera una nuova chiave e una CSR (Certificate Signing Request) (continua)

Campo	Descrizione
Città o località[1]	Digitare la città o la località in cui risiede fisicamente il BMC.
Nome organizzazione[1]	Digitare il nome della società o dell'organizzazione che possiede il BMC.
Nome host BMC[1]	Digitare il nome host del BMC visualizzato nella barra degli indirizzi Web.
Contatto	Digitare il nome della persona di contatto responsabile del BMC.
Indirizzo e-mail	Digitare l'indirizzo e-mail della persona di contatto responsabile del BMC.
Unità organizzativa	Digitare l'unità nell'interno dell'azienda che possiede il BMC.
Cognome	Digitare il cognome della persona di contatto responsabile del BMC. Questo campo può contenere al massimo 60 caratteri.
Nome	Digitare il nome della persona di contatto responsabile del BMC. Questo campo può contenere al massimo 60 caratteri.
Iniziali	Digitare le iniziali della persona di contatto responsabile del BMC. Questo campo può contenere al massimo 20 caratteri.
Qualificatore DN	Digitare il qualificatore del nome distinto per il BMC. Questo campo può contenere al massimo 60 caratteri.
Verifica password	Digitare la password per la CSR. Questo campo può contenere al massimo 30 caratteri.
Nome non strutturato	Digitare informazioni aggiuntive, quali un nome non strutturato assegnato al BMC. Questo campo può contenere al massimo 60 caratteri.
1. Questo campo è obbligatorio.	

La CSR viene firmata digitalmente dall'autorità di certificazione utilizzando lo strumento di elaborazione dei certificati dell'utente, quale *OpenSSL* o lo strumento da riga di comando *Certutil*. Tutti i certificati client firmati mediante lo strumento di elaborazione dei certificati dell'utente hanno lo stesso certificato *base*. Questo certificato *base* deve essere inoltre importato nel server SKLM, in modo che tutti i server firmati digitalmente dall'utente siano accettati dal server SKLM.

Una volta firmato dall'autorità di certificazione, il certificato deve essere importato nel BMC. Selezionare l'azione **Importa un certificato firmato**, scegliere il file da caricare come certificato client, quindi fare clic sul pulsante **OK**. Durante il caricamento del certificato firmato dall'autorità di certificazione viene visualizzata una finestra di avanzamento. Se il processo di caricamento va a buon fine, viene visualizzata una finestra Caricamento certificato. In caso contrario, viene visualizzata una finestra Errore di caricamento certificato.

Nota:

- Per una maggiore sicurezza, utilizzare un certificato firmato digitalmente da un'autorità di certificazione.
- Il certificato importato in XClarity Controller deve corrispondere alla CSR precedentemente generata.

Una volta importato un certificato firmato da un'autorità di certificazione nel BMC, selezionare l'azione **Scarica certificato**. Quando si seleziona questa azione, il certificato firmato dall'autorità di certificazione viene scaricato da XClarity Controller per essere archiviato nel sistema.

Gestione dei certificati server

Questo argomento fornisce informazioni sulla gestione dei certificati server.

Il certificato server viene generato nel server SKLM e deve essere importato in XClarity Controller prima di utilizzare la funzionalità di accesso sicuro all'unità. Per importare il certificato che autentica il server SKLM nel BMC, fare clic su **Importa un certificato** nella sezione Stato del certificato server della pagina di accesso all'unità. Mentre il file viene trasferito nello storage su XClarity Controller, viene visualizzato un indicatore di avanzamento.

Una volta completato il trasferimento del certificato server in XClarity Controller, nell'area Stato del certificato server viene visualizzato il seguente contenuto: `A server certificate is installed`.

Se si desidera rimuovere un certificato attendibile, fare clic sul pulsante **Elimina** corrispondente.

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.

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.

Impostazione di crittografia

Utilizzare le informazioni in questo argomento per comprendere le diverse impostazioni di crittografia.

Modalità di sicurezza elevata

- Sono supportate solo la crittografia moderna e quella complessa.
- Conforme a NIST.

- Conforme a PTF (Perfect Forward Secrecy).

Modalità di compatibilità

- È supportata un'ampia gamma di suite di crittografia per la massima compatibilità.
- Non conforme a PTF né a NIST.

Modalità di conformità a NIST

- È supportata un'ampia gamma di suite di crittografia per la massima compatibilità.
- Conforme a NIST.
- Conforme a PFS.

Supporto della versione TLS

- TLS 1.0 e versioni successive
- TLS 1.1 e versioni successive
- TLS 1.2 e versioni successive
- TLS 1.3

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

Fare riferimento alla seguente tabella per le differenti impostazioni che sono supportate nelle suite di crittografia TLS

Modalità di sicurezza	Versione TLS	Suite di crittografia TLS
Modalità di sicurezza elevata	TLS 1.3	• TLS_AES_256_GCM_SHA384
Modalità di sicurezza elevata	TLS 1.2	• TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 • TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 • TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
Modalità di conformità a NIST	TLS 1.3	• TLS_AES_256_GCM_SHA384 • TLS_AES_128_GCM_SHA256

Modalità di sicurezza	Versione TLS	Suite di crittografia TLS
Modalità di conformità a NIST	TLS 1.2	• TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 • TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 • TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 • TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 • TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 • 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 • TLS_RSA_WITH_AES_256_GCM_SHA384 • TLS_RSA_WITH_AES_128_GCM_SHA256 • TLS_RSA_WITH_AES_256_CBC_SHA256 • TLS_RSA_WITH_AES_128_CBC_SHA256
Modalità di compatibilità	TLS 1.3	• TLS_AES_256_GCM_SHA384 • TLS_AES_128_GCM_SHA256 • TLS_CHACHA20_POLY1305_SHA256
Modalità di compatibilità	TLS 1.2	• TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 • TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 • TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 • TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 • TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 • 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 • TLS_RSA_WITH_AES_256_GCM_SHA384 • TLS_RSA_WITH_AES_128_GCM_SHA256 • TLS_RSA_WITH_AES_256_CBC_SHA256 • TLS_RSA_WITH_AES_128_CBC_SHA256
Modalità di compatibilità	TLS 1.1 TLS 1.0	• TLS_RSA_WITH_AES_256_CBC_SHA256 • TLS_RSA_WITH_AES_128_CBC_SHA256

Configurazione di Call Home

Utilizzare le informazioni in questo argomento per configurare Call Home.

È possibile creare un server d'inoltro di servizio che invii automaticamente i dati di servizio di qualsiasi dispositivo gestito al supporto Lenovo mediante la funzione Call Home.

Lenovo si impegna a garantire la sicurezza. Se abilitata, la funzione Call Home contatta automaticamente Lenovo per aprire un ticket di assistenza e invia i dati di servizio raccolti da un dispositivo gestito ogni volta che tale dispositivo segnala un guasto hardware. I dati di servizio, che vengono in genere caricati manualmente sul supporto Lenovo, vengono inviati automaticamente al centro di supporto Lenovo su HTTPS tramite TLS 1.2 o versione successiva, i dati aziendali non vengono mai trasmessi. L'accesso ai dati di servizio nel centro di supporto Lenovo è limitato al personale di assistenza autorizzato.

Prima accesso alla pagina Call Home

Quando si accede alla pagina Call Home per la prima volta, viene visualizzata una finestra di avviso, fare clic sul collegamento per visualizzare i termini e le condizioni per continuare.

Attenzione: è necessario accettare l'**Informativa sulla privacy Lenovo** per trasferire i dati al supporto Lenovo. Questa azione deve essere eseguita solo la prima volta che si accede alla pagina.

Nota: Nella parte superiore della pagina sono disponibili il collegamento per visualizzare i termini e le condizioni, nonché l'**Informativa sulla privacy Lenovo** per poterne prendere visione in qualsiasi momento.

Configurazione di Call Home

Sono disponibili nove campi obbligatori da compilare:

- Paese
- Nome contatto
- Telefono
- E-mail
- CAP
- Nome società
- Indirizzo
- Città
- Stato

Attenzione: è necessario compilare tutti i campi richiesti oppure non sarà possibile applicare le modifiche e abilitare la **segnalazione all'assistenza Lenovo**.

Stato del ticket

Ciascun ticket può avere uno dei seguenti cinque stati:

- **In sospeso:** le informazioni sull'assistenza sono in fase di invio o in attesa di risposta.
- **Attivo:** le informazioni sull'assistenza sono state inviate correttamente e il problema è attualmente in fase di elaborazione.
- **Non riuscito:** le informazioni sull'assistenza non sono state inviate correttamente.
- **Chiuso:** il problema è stato elaborato e chiuso.
- **Annullato:** il problema è stato elaborato e annullato.

Verifica Call Home

È possibile verificare la funzione Call Home facendo clic su "Verifica Call Home", verrà visualizzato un messaggio nella parte superiore della pagina per indicare se l'operazione è stata completata correttamente. Sarà anche possibile controllare il log eventi riportato di seguito per vedere il risultato del test.

- **Azione: Annulla** Quando lo stato di un ticket è "Attivo", è possibile fare clic sull'icona "Annulla" nella colonna "Azione" per annullare il ticket.
- **Azione: Nota** Quando si fa clic sull'icona Nota nella colonna "Azione", verrà chiesto di lasciare note per l'evento corrispondente.

  Nota: Sia il titolo che il corpo del messaggio devono essere compilati perché il messaggio venga inviato correttamente. Questa funzione **invia SOLO informazioni al server**. Non serve a salvare e visualizzare le informazioni. Se si fa nuovamente clic su Nota, verrà visualizzata una nuova finestra Nota in cui lasciare un altro messaggio.

Attenzione: per eseguire correttamente la funzione Call Home, accertarsi che le impostazioni DNS siano valide e che sia disponibile una connessione all'indirizzo Internet richiesto da Call Home. Se XClarity Controller accede a Internet tramite un proxy HTTP, accertarsi che il server proxy sia configurato per l'utilizzo dell'autenticazione di base e come proxy non di terminazione.

Proxy HTTP

Il proxy HTTP viene utilizzato con due ruoli intermedi, come client HTTP e server HTTP per la sicurezza, la gestione e la funzionalità di memorizzazione nella cache. Il proxy HTTP instrada le richieste del client HTTP da un browser Web a Internet, mentre supporta la memorizzazione nella cache dei dati Internet.

- **Indirizzo server proxy:** questo campo è obbligatorio per abilitare il proxy HTTP. Può accettare solo un massimo di 63 caratteri, permettendo agli utenti di specificare l'indirizzo IP o il nome host. Il nome host contiene solo caratteri alfanumerici, di sottolineatura ("_") e trattini ("-").
- **Porta:** questo campo è obbligatorio per specificare la porta del proxy HTTP E consente solo l'immissione di numeri che vanno da 1 a 65535.
- **Verifica proxy:** per abilitare questa funzione, verificare che la funzione Proxy HTTP corrente sia disponibile inserendo la posizione e la porta proxy corrette.
- **Nome utente:** se l'opzione "**Richiede autenticazione**" è selezionata, verrà chiesto il nome utente che rappresenterà una credenziale proxy. Questo campo consente una lunghezza massima di 30 caratteri e gli spazi non sono validi.
- **Password:** questo campo è facoltativo e verrà visualizzato se l'opzione "Richiede autenticazione" è selezionata. Questo campo consente una lunghezza massima di 15 caratteri e gli spazi non sono validi.

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.
2. Verificare il file facendo clic su **Visualizza contenuto** per visualizzare i 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**. Sotto **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**
     - **Mantieni impostazioni di rete**

- 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 dei valori predefiniti originali di BMC non interessa le impostazioni UEFI.

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 70.

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.

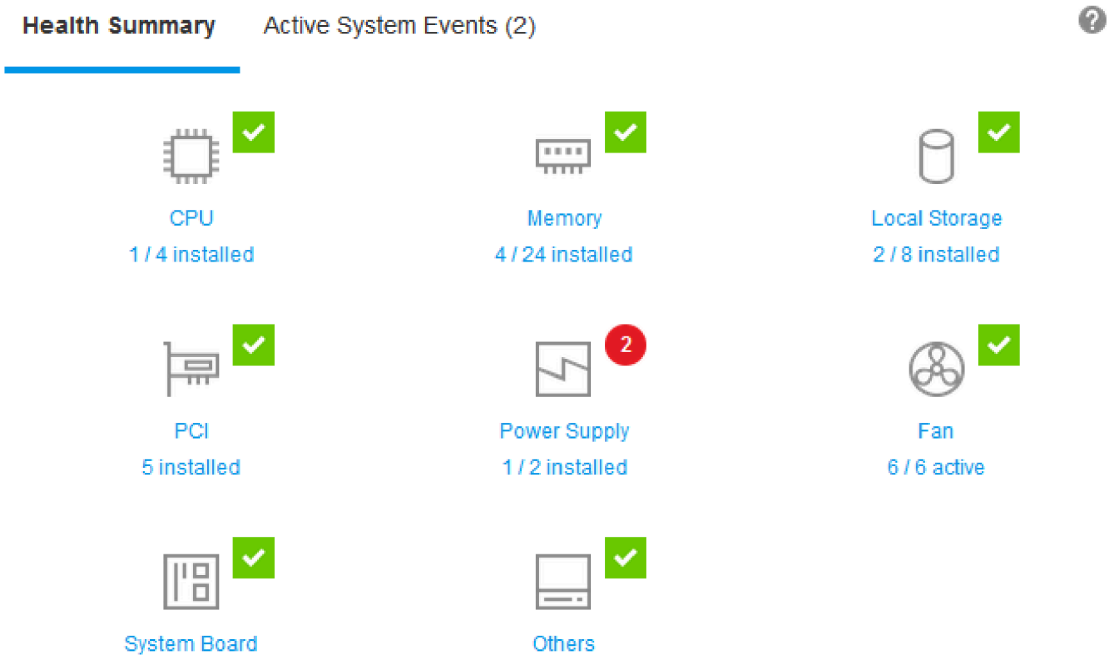
Visualizzazione di Riepilogo integrità/Eventi di sistema attivi

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:

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

Nota: Storage locale potrebbe mostrare "non disponibile" sull'icona di stato sui sistemi con una configurazione 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, si verrà indirizzato alla pagina **Inventory**.

Visualizzazione delle informazioni sul sistema

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

Il riquadro **Informazioni sul sistema e impostazioni** situato a sinistra 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
- Proprietà USB anteriore
- Licenza BMC
- Indirizzo IP BMC
- Nome host BMC
- Versione UEFI
- Versione BMC
- Versione LXPM
- Posizione

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

Tabella 5. 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 arrestato in UEFI	Il server è acceso; UEFI ha rilevato un problema ed è stato arrestato.
Avvio del sistema operativo o sistema operativo non supportato	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.
Sospendi su RAM	Il server è stato inserito nello stato di standby o di sospensione.
Sistema in esecuzione nel test di memoria	Il server è acceso e in esso sono in esecuzione gli strumenti di diagnostica della memoria.
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 si desidera modificare la proprietà dell'USB anteriore, fare clic sull'icona della matita e selezionare la modalità **Proprietà USB anteriore** desiderata dal menu a discesa. Quindi, fare clic sul segno di spunta verde.

Se il server dispone di una licenza diversa da XClarity Controller Enterprise, è possibile acquistare un upgrade della licenza per abilitare le funzioni 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 provengono tutti da ME (Node Manager) e 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.
  - Nella scheda Cronologia vengono visualizzate i grafici delle temperature cronologiche fino alle ultime 24 ore.
- **Utilizzo dell'alimentazione**
  - Visualizza il grafico a torta del consumo energetico corrente e i grafici cronologici del consumo energetico per un massimo di 24 ore.

  - 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.
  - Utilizzare la funzione di aggiornamento o ricarica del browser per aggiornare i dati sull'utilizzo correnti.
  - L'utilizzo a livello di sottosistema della CPU rappresenta la percentuale della larghezza di banda totale della CPU attualmente in uso, misurata dai contatori delle prestazioni creati nella CPU (potrebbe differire leggermente dall'utilizzo della CPU segnalato dal sistema operativo).
  - L'utilizzo del livello di sottosistema di memoria rappresenta la percentuale della larghezza di banda totale del controller del canale di memoria attualmente in uso (non riflette la quantità di memoria attualmente utilizzata).
  - L'utilizzo del livello di sottosistema I/O rappresenta la percentuale della larghezza di banda totale del traffico PCIe attualmente in uso.
  - Larghezza di banda calcolata come percentuale della larghezza di banda della memoria utilizzata e massima disponibile (al secondo).
- **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 vi saranno modifiche se la ventola funziona 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 avvertenza 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 blu attorno all'icona indica che il tipo di evento verrà visualizzato.
- **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 61.

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

Per aggiungere e modificare le notifiche e-mail e syslog o i destinatari di trap SNMP, utilizzare le informazioni in questo argomento.

Di seguito è riportata una descrizione delle azioni che possono essere eseguite nella scheda **Destinatari degli avvisi**.

Le seguenti azioni possono essere eseguite nella sezione dei destinatari **E-mail/Syslog**.

- **Crea**: selezionare questa azione per creare nuovi destinatari e-mail e syslog aggiuntivi. È possibile configurare fino a 12 destinatari e-mail e syslog.
  - **Crea destinatario e-mail**: selezionare questa azione per creare un destinatario e-mail.
    - Immettere il nome e l'indirizzo e-mail del destinatario.
    - Scegliere se abilitare o disabilitare la notifica degli eventi. Se disabilitata, l'account resterà configurato, ma non verrà inviata alcuna e-mail.
    - Selezionare i tipi di eventi che verranno notificati al destinatario. Se si fa clic sull'elenco a discesa accanto alle etichette di categoria Critico, Attenzione o Sistema, è possibile selezionare o deselezionare le notifiche per componenti specifici nella categoria.
    - È possibile scegliere se includere i contenuti del log di eventi nell'avviso e-mail.
    - L'indice specifica quale dei 12 slot destinatari è stato assegnato.
    - In questa sezione è possibile configurare il server e-mail a cui verranno inviati gli eventi. In alternativa, fare clic sull'azione Server SMTP nella parte superiore della sezione. Per i dettagli di configurazione, consultare l'azione Server SMTP riportata di seguito.
  - **Crea destinatario syslog**: selezionare questa azione per creare i destinatari syslog.
    - Immettere il nome e l'indirizzo IP o il nome host del server Syslog.
    - Scegliere se abilitare o disabilitare la notifica degli eventi. Se disabilitata, l'account resterà configurato, ma non verrà inviata alcuna e-mail.
    - L'indice specifica quale dei 12 slot destinatari è stato assegnato.
    - Selezionare i tipi di eventi che verranno inviati al server syslog. Se si fa clic sul menu a discesa accanto alle etichette di categoria Critico, Attenzione o Sistema, è possibile selezionare o deselezionare le notifiche per componenti specifici nella categoria.
- **Server SMTP**: selezionare questa azione per configurare le relative impostazioni per il server e-mail SMTP. È possibile configurare solo un server e-mail. La stessa configurazione e-mail viene utilizzata quando si inviano gli avvisi a tutti i destinatari e-mail configurati. BMC passa automaticamente da una connessione sicura a una connessione crittografata per il trasferimento della posta mediante il comando STARTTLS in modo uniforme tramite la porta 587, se il server di posta di destinazione lo supporta.
  - Immettere il nome host o l'indirizzo IP e il numero della porta di rete del server e-mail.

  - Se il server e-mail richiede l'autenticazione, selezionare la casella di controllo **Richiedi autenticazione** e immettere il nome utente e la password. Selezionare il tipo di autenticazione richiesta dal server e-mail, un metodo challenge-response (**CRAM-MD5**) o credenziali semplici (**LOGIN**).
  - Alcune reti possono bloccare le e-mail in uscita se il valore reverse-path è errato. Per impostazione predefinita, XClarity Controller utilizzerà il formato alertmgr@domain, dove il dominio è il nome di dominio specificato nella sezione DDNS della pagina Web della rete di XClarity Controller. È possibile specificare le proprie informazioni sul mittente al posto di quelle predefinite.
  - È possibile verificare la connessione al server e-mail per accertarsi che le impostazioni e-mail siano state configurate correttamente. XClarity Controller visualizzerà un messaggio che indica se la connessione è riuscita.
- **Nuovo tentativo e ritardo**: selezionare questa azione per configurare le relative impostazioni per le opzioni di nuovo tentativo e ritardo.
  - L'impostazione Limite tentativo specifica il numero di volte che XClarity Controller proverà a inviare un avviso se il tentativo iniziale non è riuscito.
  - Il ritardo tra le voci specifica il periodo di tempo che XClarity Controller attenderà dopo l'invio di un avviso a un destinatario, prima di inviare un avviso al destinatario successivo.
  - Il ritardo tra i tentativi specifica il periodo di tempo che XClarity Controller attenderà dopo un tentativo non riuscito, prima di provare nuovamente a inviare l'avviso.
- **Protocollo**: selezionare questa azione per configurare le impostazioni specifiche per il protocollo di connessione.
  - È possibile scegliere tra **Protocollo TCP** o **Protocollo UDP**, questa impostazione verrà applicata a tutti i destinatari syslog.
- Se creati in precedenza, i destinatari e-mail o syslog verranno elencati in questa sezione.
  - Per modificare le impostazioni relative ai destinatari e-mail o syslog, fare clic sull'icona della matita sotto l'intestazione dell'azione, sulla riga accanto al destinatario che si desidera configurare.
  - Per eliminare un destinatario e-mail o syslog, fare clic sull'icona del cestino.
  - Per inviare un avviso di prova a un destinatario e-mail o Syslog, fare clic sull'icona dell'aeroplano di carta.

Le seguenti azioni possono essere eseguite nel segmento utente **SNMPv3**.

- **Crea**: selezionare questa azione per creare i destinatari del trap SNMPv3.
  - Selezionare l'account utente da associare ai trap SNMPv3. L'account utente deve essere uno dei dodici account utente locali.
  - Specificare il nome host o l'indirizzo IP del gestore SNMPv3 che riceverà i trap SNMPv3.
  - XClarity Controller utilizza l'algoritmo hash HMAC-SHA per eseguire l'autenticazione con il gestore SNMPv3. Questo è l'unico algoritmo supportato.
  - La password della privacy viene utilizzata con il protocollo di privacy per crittografare i dati SNMP.
  - L'**impostazione globale SNMPv3** si applica a tutti i destinatari del trap SNMPv3. Queste impostazioni possono essere configurate creando un destinatario del trap SNMPv3 oppure facendo clic sull'azione Impostazioni SNMPv3, nella parte superiore del segmento utente **SNMPv3**.
    - Scegliere se abilitare o disabilitare i trap SNMPv3. Se disabilitati, le impostazioni resteranno configurate, ma non verrà inviato alcun trap SNMPv3.
    - Le informazioni relative al contatto e alla posizione del BMC sono obbligatorie e possono essere configurate sulla pagina Web "Proprietà del server". Consultare la sezione "Impostazione di posizione e contatto" a pagina 88 per maggiori informazioni.

  - Selezionare i tipi di eventi che causeranno l'invio dei trap al gestore SNMPv3. Se si fa clic sul menu a discesa accanto alle etichette di categoria Critico, Attenzione o Sistema, è possibile selezionare o deselezionare le notifiche per componenti specifici nella categoria.

  Nota: Il trasferimento di dati tra il client SNMP e l'agente può essere protetto utilizzando la crittografia. I metodi supportati per il **protocollo di privacy** sono CBC-DES e AES.

- Se creati in precedenza, i destinatari dei trap SNMPv3 verranno elencati in questa sezione.
  - Per modificare le impostazioni di un destinatario SNMPv3, fare clic sull'icona della matita sotto l'intestazione dell'azione, sulla riga accanto al destinatario che si desidera configurare.
  - Per eliminare un destinatario SNMPv3, fare clic sull'icona del cestino.

Cattura dei dati della schermata dell'ultimo errore del sistema operativo

Utilizzare le informazioni in questo argomento per acquisire e visualizzare una schermata di errore del sistema operativo.

La schermata del sistema operativo viene automaticamente acquisita quando si verifica il timeout del Watchdog del sistema operativo. Se si verifica un evento che causa l'arresto del sistema operativo, la funzione Watchdog sistema operativo viene attivata e il contenuto dello schermo viene acquisito. XClarity Controller è in grado di memorizzare una sola cattura della schermata. Quando si verifica il timeout del Watchdog del sistema operativo, una nuova cattura della schermata sovrascrive la cattura precedente. La funzione Watchdog sistema operativo deve essere abilitata per catturare la schermata di errore del sistema operativo. Per impostare il Watchdog Timer del sistema operativo, vedere "Impostazione dei timeout del server" a pagina 89 per maggiori informazioni. La funzionalità di cattura della schermata di errore del sistema operativo è disponibile soltanto con i livelli di funzionalità Advanced o Enterprise di XClarity Controller. Consultare la documentazione relativa al proprio server per informazioni relative al livello di funzionalità di XClarity Controller installato sul proprio server.

Selezionare l'azione **Schermata ultimo errore** nella sezione **Console remota** della home page di XClarity Controller per visualizzare un'immagine della schermata del sistema operativo catturata quando si è verificato il timeout del Watchdog del sistema operativo. La cattura può inoltre essere visualizzata facendo clic su **Servizio**, quindi su **Schermata ultimo errore** nella sezione **Azione rapida** della home page. Se non si è verificato alcun timeout del Watchdog del sistema operativo né è stata acquisita una schermata del sistema operativo, viene visualizzato un messaggio indicante che la schermata di errore non è stata creata.

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

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 la modalità e 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 la modalità di avvio del sistema, sono disponibili le seguenti due opzioni:

Avvio UEFI
Selezionare questa opzione per configurare un server che supporta Unified Extensible Firmware Interface (UEFI). Se si stanno avviando sistemi operativi abilitati per UEFI, questa opzione potrebbe ridurre i tempi di avvio disabilitando le ROM di opzione legacy.

Avvio legacy
Selezionare questa opzione se si configura un server per avviare un sistema operativo che richiede il firmware legacy (BIOS). Selezionare questa opzione solo se si avviano sistemi operativi non abilitati per UEFI.

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.

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

Quando si modifica il tipo di avvio da eseguire con il dispositivo di avvio singolo, è anche possibile specificare di utilizzare un avvio legacy o UEFI. Fare clic sulla casella di controllo **Preferisci avvio legacy** per impostare un avvio da BIOS legacy. Deselezionare la casella se si preferisce un avvio UEFI. 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 uno chassis con nodi server ad alta densità o blade, il raffreddamento e l'alimentazione dello chassis sono controllati dal controller di gestione dello chassis anziché da XClarity Controller.

Configurazione della ridondanza dell'alimentazione

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

Nota: Attualmente l'utente non può modificare i criteri per il risparmio di energia dei sistemi AMD.

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.
- **Ridondante (N+1)**: è disponibile una fonte di alimentazione primaria in grado di fornire alimentazione al sistema. Inoltre è disponibile almeno una fonte di alimentazione di backup da utilizzare, in caso di errore della fonte primaria. La fonte di backup è progettata per fornire energia sufficiente per mantenere il sistema in esecuzione, finché la fonte primaria non viene riparata o sostituita. La ridondanza N+1 fornisce un livello inferiore di tolleranza di errore rispetto alla ridondanza N+N.
- **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 con processori AMD non supportano gli utenti nella configurazione della funzione dei criteri di limite alimentazione.

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**.

È possibile abilitare il limite alimentazione tramite le misure del consumo di alimentazione CA o del consumo di alimentazione CC Nel menu a discesa selezionare il tipo di misurazioni che saranno utilizzate per determinare il limite alimentazione. Quando si passa tra CA e CC, il numero sul dispositivo di scorrimento 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.

Nota: L'opzione **Criteri alimentazione** non è disponibile se XClarity Controller si trova in uno chassis con nodi server ad alta densità o blade. I criteri di alimentazione vengono controllati tramite il controller di gestione dello chassis anziché XClarity Controller.

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.

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

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

Nota: L'opzione **Criteri di ripristino alimentazione** non è disponibile in uno chassis con nodi server ad alta densità o blade. I criteri di ripristino dell'alimentazione vengono controllati tramite il controller di gestione dello chassis anziché XClarity Controller.

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 6. 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 server	Selezionare questa azione per accendere il server e avviare il sistema operativo.
Spegni server normalmente	Selezionare questa azione per arrestare il sistema operativo e spegnere il server.
Spegni 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 server e visualizza configurazione 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.	

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.

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 XClarity Controller livello Advanced e di XClarity Controller livello Enterprise 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 da XClarity Controller livello Standard a XClarity Controller livello Advanced o XClarity Controller livello Enterprise, vedere "Aggiornamento di XClarity Controller" a pagina 6.

Utilizzare le funzioni di console remota per:

- Visualizzare video in remoto con una risoluzione grafica massima di 1280 x 1024 a 72 Hz o 75 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 50 MB.

Nota:

- Quando la funzione di console remota viene avviata in modalità multiutente (XClarity Controller con il set di funzioni di XClarity Controller livello Enterprise 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.

Come citato in precedenza, la funzionalità di console remota di XClarity Controller è disponibile solo con le funzioni di XClarity Controller livello Advanced e di XClarity Controller livello Enterprise. 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 a XClarity Controller livello Advanced, installarla in base alle istruzioni in "Installazione di una chiave di attivazione" a pagina 103.

Per utilizzare la funzionalità di console remota, effettuare le seguenti operazioni:

1. Fare clic sull'immagine con una freccia bianca in posizione diagonale nella sezione della console remota della home page di XClarity Controller o nella pagina Web della console remota.
2. Selezionare una delle seguenti modalità:

- Avvia console remota in modalità utente singolo
- Avvia console remota in modalità multiutente

Nota: XClarity Controller con la funzione di XClarity Controller livello Enterprise impostata supporta fino a sei sessioni video simultanee in modalità multiutente.

3. Selezionare se consentire o meno ad altri di richiedere l'invio di una richiesta di disconnessione a un utente della console remota qualora un altro utente desideri utilizzare la funzione di console remota, ma tale funzione è già in uso in Modalità utente singolo, o quando la funzione di console remota è utilizzata dal numero massimo di utenti consentito in Modalità multiutente. **Nessun intervallo del tempo di risposta** specifica il tempo di attesa di XClarity Controller prima della disconnessione automatica dell'utente, qualora non venga ricevuta alcuna risposta alla richiesta di disconnessione.
4. Selezionare se si desidera o meno consentire la registrazione degli ultimi tre video di avvio del server.
5. Selezionare se si desidera o meno consentire la registrazione degli ultimi tre video di arresto anomalo del server.
6. Selezionare se consentire o meno la cattura della schermata di errore del sistema operativo con un errore HW.
7. Fare clic su **Avvia console remota** per aprire la pagina della console remota in un'altra scheda. Quando tutte le sessioni possibili della console remota sono in uso, verrà visualizzata una finestra di dialogo, Che potrà essere utilizzata dall'utente per inviare una richiesta di disconnessione a un utente della console remota che ha abilitato l'impostazione **Consenti ad altri utenti di richiedere la disconnessione della mia sessione remota**. L'utente potrà accettare o rifiutare la richiesta di disconnessione. Se l'utente non risponde entro l'intervallo specificato nell'impostazione **Nessun intervallo del tempo di risposta**, la sessione utente verrà terminata automaticamente da XClarity Controller.

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 PNG.

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. Altre macro del server possono essere definite utilizzando Lenovo XClarity Essentials e scaricate da XClarity Controller. Queste macro sono definite per tutti gli utenti della funzione di console remota.
- Fare clic su **Configura** per aggiungere o rimuovere le macro definite dall'utente. Le macro definite dall'utente sono definite solo per l'utente della console remota corrente. Gli utenti della console remota non saranno in grado di visualizzare le macro definite da altri utenti.
  - Fare clic sull'icona Aggiungi macro e premere le sequenze di tasti desiderate, quindi fare clic su **Aggiungi** per aggiungere una nuova macro.
  - Per rimuovere una macro definita dall'utente, selezionarla dall'elenco e fare clic sull'icona del cestino.
  - Per inviare una macro definita dall'utente al server, selezionare l'opzione **Macro definite dall'utente** e fare clic sulla macro che si desidera inviare.

Supporto del mouse nella console remota

Utilizzare queste informazioni per comprendere le opzioni per il controllo remoto del mouse.

La finestra della console remota offre diverse opzioni per il controllo del mouse, tra cui controllo del mouse assoluto, controllo del mouse relativo (nessuna accelerazione) e controllo del mouse (RHEL, versioni meno recenti di Linux).

Controllo del mouse assoluto e relativo

Utilizzare queste informazioni per accedere alle opzioni assolute o relative per il controllo del mouse.

Per accedere alle opzioni assolute o relative per il controllo del mouse, effettuare le seguenti operazioni:

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

Passo 2. Fare clic su **Impostazioni mouse** dal menu a discesa.

Passo 3. Selezionare una delle modalità **Accelerazione mouse** seguenti:

Posizionamento assoluto (Windows, versione più recente di Linux e Mac OS X)
Il client invia i messaggi delle posizioni del mouse al server che sono relativi all'origine dell'area di visualizzazione (in alto a sinistra).

Posizionamento relativo, nessuna accelerazione
Il client invia la posizione del mouse come offset dalla posizione del mouse precedente.

Posizionamento relativo (distribuzione Linux precedente)
Questa modalità applica un fattore di accelerazione per allineare meglio il mouse su alcune destinazioni Linux. Le impostazioni di accelerazione sono state selezionate per aumentare al massimo la compatibilità con le distribuzioni Linux precedenti.

Registrazione/Riproduzione video della schermata

Utilizzare le informazioni riportate in questa sezione per registrare o riprodurre i video della schermata di presenza remota.

L'interfaccia Web di XClarity Controller fornisce una funzione di tipo DVR per supportare la registrazione e la riproduzione di video della schermata di presenza remota. Questa funzione supporta solo la registrazione di video in una cartella di rete. Attualmente, sono supportati i protocolli NFS e CIFS. Di seguito sono riportati i passaggi per utilizzare la funzione di riproduzione e registrazione.

1. Nella pagina Web della console remota, fare clic su **Registrazione schermata** per aprire la finestra delle impostazioni.
2. Nella finestra delle impostazioni, potrebbe essere necessario specificare le seguenti informazioni.
   - Se è selezionato il tipo di montaggio "CIFS", specificare i parametri **Cartella remota**, **Nome utente** e **Password**. Il formato per la cartella remota CIFS è "**//<indirizzo IP remoto>/<nome cartella>**". Ad esempio: //xxx.xxx.xxx.xxx/cartella.
   - Se è selezionato il tipo di montaggio "NFS", specificare il parametro **Cartella remota**. Il formato per la cartella remota NFS è "**<indirizzo IP remoto>:/<nome cartella>**". Ad esempio: xxx.xxx.xxx.xxx:/cartella.
   - Specificare il nome del file del video, se necessario. Se il nome del file è già stato fornito, verrà visualizzata una finestra con un messaggio di errore. Per sovrascrivere il nome del file esistente, scegliere "Sovrascrivi nome file". Se la casella "Auto" è selezionata, il nome del file del video verrà generato automaticamente.
   - "Dimensione massima file" indica la dimensione massima del file video prima che la registrazione video venga interrotta automaticamente.
   - "Durata massima registrazione" indica la durata massima del video prima che la registrazione venga interrotta automaticamente.
3. Fare clic su **Avvia registrazione** per avviare la registrazione del video.
4. Fare clic su **Interrompi registrazione** per interrompere la registrazione del video. Verrà visualizzata una finestra popup con il messaggio "Registrazione video completata", che contiene le informazioni principali sulla registrazione del video.
5. Scaricare i video registrati da NFS o CIFS nella cartella locale. Nella sezione "Anteprima console remota" della home page di XClarity Controller, fare clic su **Video registrati** e selezionare il file video da riprodurre.

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.

Ridimensionamento schermo
Se è abilitata la scala, l'immagine video viene ridimensionata affinché l'immagine completa rientri nella finestra della console.

Schermo di origine
L'immagine video ha le stesse dimensioni del server. Le barre di scorrimento vengono visualizzate se è necessario per consentire la visualizzazione delle aree dell'immagine video che non rientrano nella finestra.

Modalità colore
Regola l'intensità colore della finestra della console remota. Esistono due opzioni di modalità colore:

- Colore: 7, 9, 12, 15 e 23 bit
- Scala di grigi: 16, 32, 64 e 128 sfumature

Nota: Le modifiche della modalità colore vengono in genere apportate se si dispone di una connessione al server remoto con una larghezza di banda limitata e si desidera ridurre la richiesta di larghezza di banda.

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 XClarity Controller livello Enterprise.

Per montare i supporti locali, fare clic su **Attiva** nella sezione **Monta supporti locali**. È possibile montare simultaneamente fino a quattro file sul server.

Nota:

- Quando si utilizza il browser Google Chrome, è disponibile un'opzione di montaggio aggiuntiva denominata **Monta file/cartelle** per trascinare e rilasciare i file e le cartelle.
- Se sono in corso più sessioni della console remota simultanee con XClarity Controller, questa funzione può essere attivata solo da una delle sessioni.

- 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 supporti virtuali di sola lettura, selezionare la casella di controllo.
    - Immettere le credenziali necessarie per l'accesso di XClarity Controller al file sul sistema remoto.

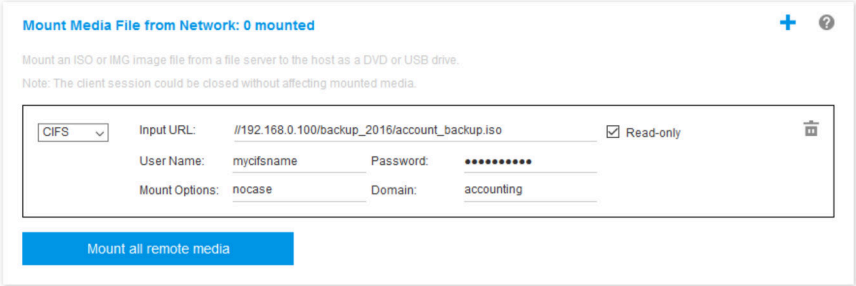
      Nota: XClarity Controller non supporta spazi nel nome utente, nella password o nell'URL. Assicurarsi che le credenziali di login del server CIFS non siano configurate con uno spazio nel nome utente o nella password e che l'URL non contenga uno spazio.
    - Le opzioni di montaggio sono facoltative e 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 supporti virtuali 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 supporti virtuali 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 86.

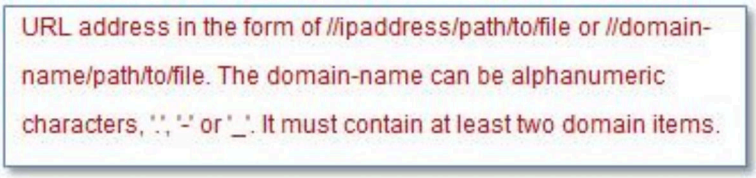
  Fare clic su **Monta tutti i supporti remoti** per montare il file come supporti virtuali. Per rimuovere i supporti virtuali, fare clic sull'icona del cestino a destra dei supporti montati.
- Nella memoria di XClarity Controller è possibile caricare fino a due file, i quali possono essere montati come supporti virtuali utilizzando la funzione RDOC di XClarity Controller. La dimensione totale di entrambi i file non deve superare 50 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.



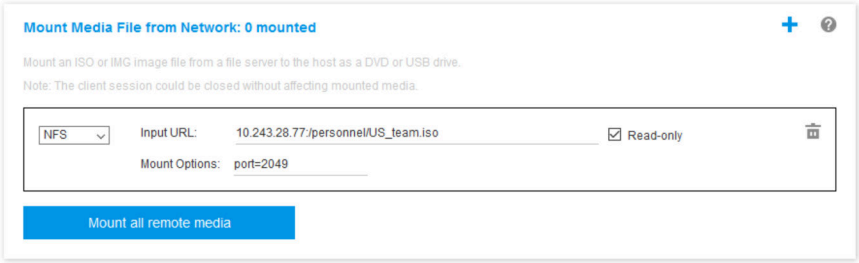
Il BMC fornisce linee guida quando si specifica l'URL. Se l'URL immesso non è valido, il pulsante di montaggio verrà disattivato e sotto il campo dell'URL verrà visualizzato del testo di colore rosso che mostra il formato previsto per l'URL.



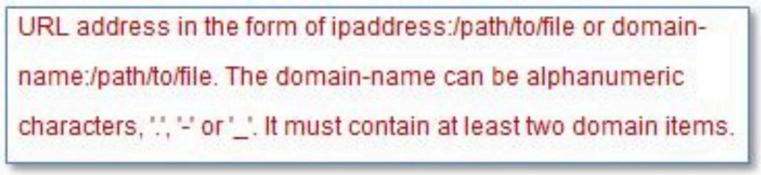
– **NFS - Network File System**: vedere la descrizione precedente per dettagli.

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.

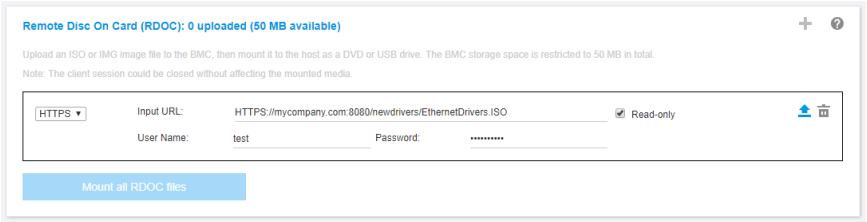


- **HTTPS (Hypertext Transfer Protocol Secure)**:
  - Immettere l'URL che individua il file sul sistema remoto.
  - Se si desidera che il file venga presentato sul server come supporti virtuali di sola lettura, selezionare la casella di controllo.
  - Immettere le credenziali necessarie per l'accesso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

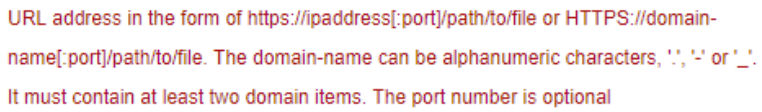
  Nota:

  - 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 86.
  - 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.



- **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 supporti virtuali 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 supporti virtuali di sola lettura, selezionare la casella di controllo.

Fare clic su **Monta tutti i file RDOC** per montare il file sotto come supporti virtuali. 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
```

Disco remoto con client Java

In questa sezione viene descritto come montare i supporti locali mediante il client Java.

È possibile utilizzare il client Java per assegnare al server un'unità CD o DVD, un'unità minidisco, un'unità flash USB presente sul computer oppure è possibile specificare un'immagine del disco sul computer che sia utilizzata dal server. È possibile utilizzare l'unità per funzioni quali il riavvio (avvio) del server, l'aggiornamento del codice, l'installazione del nuovo software sul server e l'installazione o l'aggiornamento del sistema operativo sul server. È possibile accedere al disco remoto. Le unità e le immagini del disco sono visualizzate come unità USB sul server.

Nota: Java della console remota supporta uno dei seguenti ambienti Java e può essere aperto solo se il client HTML5 non è in esecuzione.

1. Oracle Java Runtime Environment 1.8/Java SE 8 o versione più recente
2. OpenJDK 8. La distribuzione di AdoptOpenJDK con HotSpot JVM è supportata.

Se si utilizza AdoptOpenJDK, è necessario utilizzare https://openwebstart.com/ in OSX, Windows e Linux.

Creazione di un file di immagine

Per creare un nuovo file di immagine da una cartella di origine specificata, completare le seguenti operazioni:

1. Fare clic sull'opzione **Crea immagine** nella scheda **Supporti virtuali** della finestra Virtual Media Java Client. Viene visualizzata la finestra "Crea immagine dalla cartella".
2. Fare clic sul pulsante **Sfoglia** associato al campo **Cartella di origine** per selezionare la cartella di origine specifica.

3. Fare clic sul pulsante **Sfoglia** associato al campo **Nuovo file di immagine** per selezionare il file di immagine da utilizzare.
4. Fare clic sul pulsante **Crea immagine**.

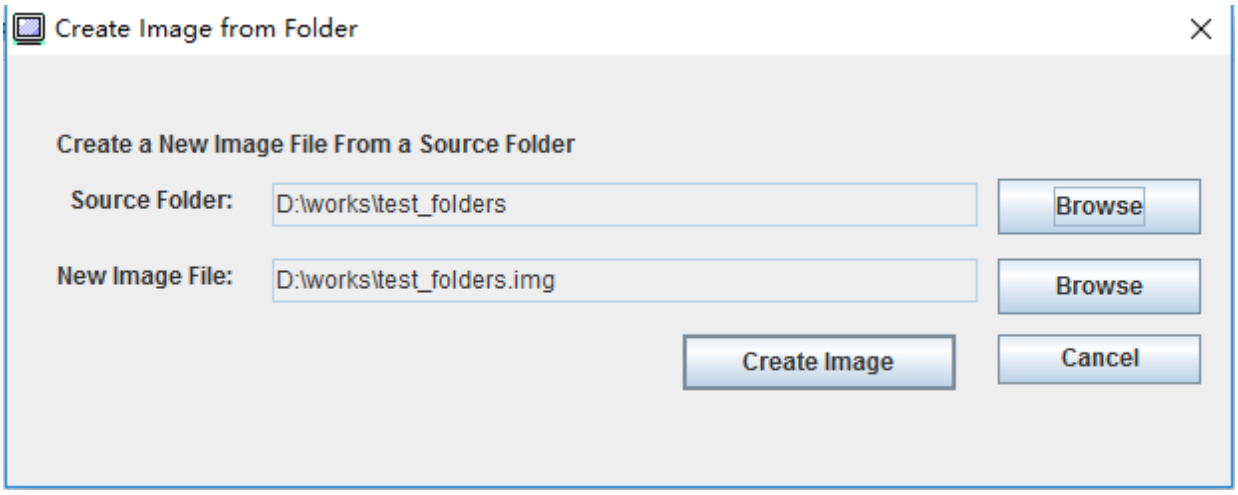


Figura 1. Creazione di un file di immagine

Selezione dei dispositivi da montare

Per montare l'immagine locale, la cartella e l'unità CD/DVD/USB, completare le seguenti operazioni:

Fare clic sull'opzione **Seleziona dispositivi da montare** nella scheda **Supporti virtuali** della finestra Virtual Media Java Client. Viene visualizzata la finestra "Seleziona dispositivi da montare".

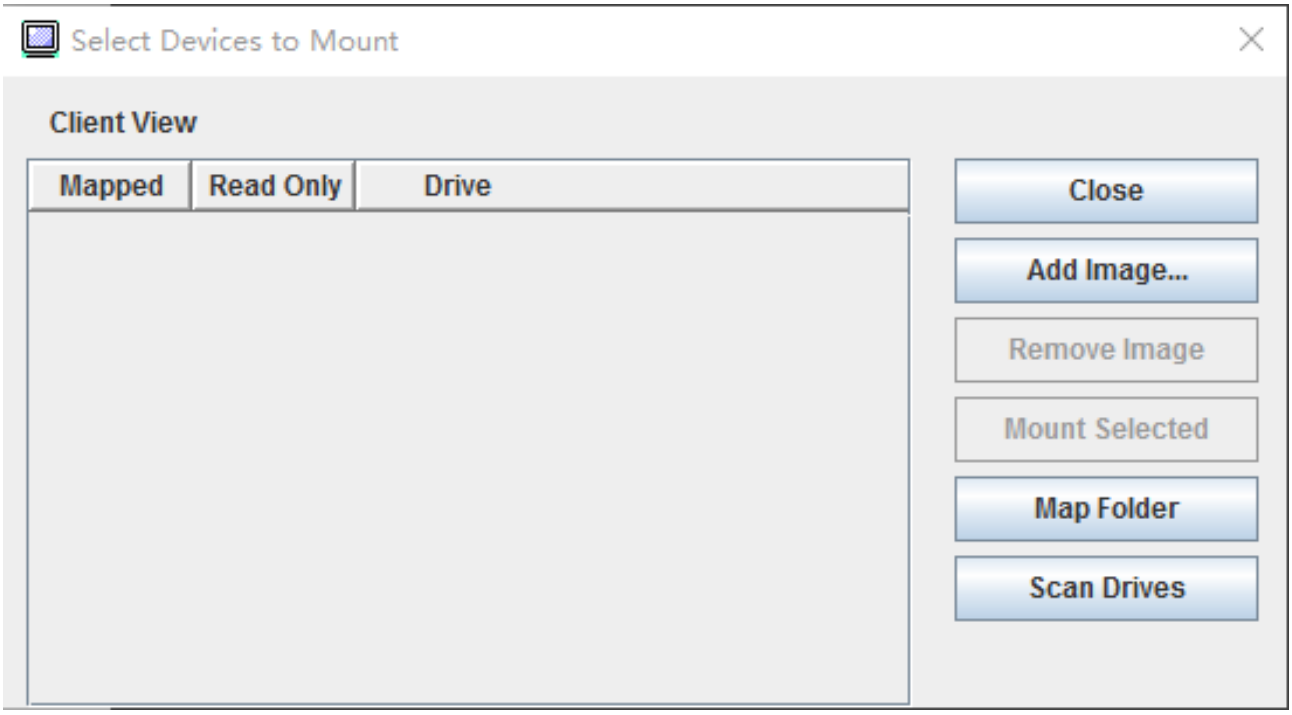


Figura 2. Finestra "Seleziona dispositivi da montare"

È possibile montare l'immagine locale, la cartella e l'unità CD/DVD/USB, completando le seguenti operazioni:

- **Montaggio immagine locale**:
  1. Fare clic sul pulsante **Aggiungi immagine** per selezionare l'immagine che si desidera montare.
  2. Controllare l'opzione **Elemento associato**.
  3. Selezionare l'opzione **Sola lettura** per abilitare la funzione, se necessario.
  4. Fare clic sul pulsante **Monta elemento selezionato** per montare correttamente l'immagine locale.

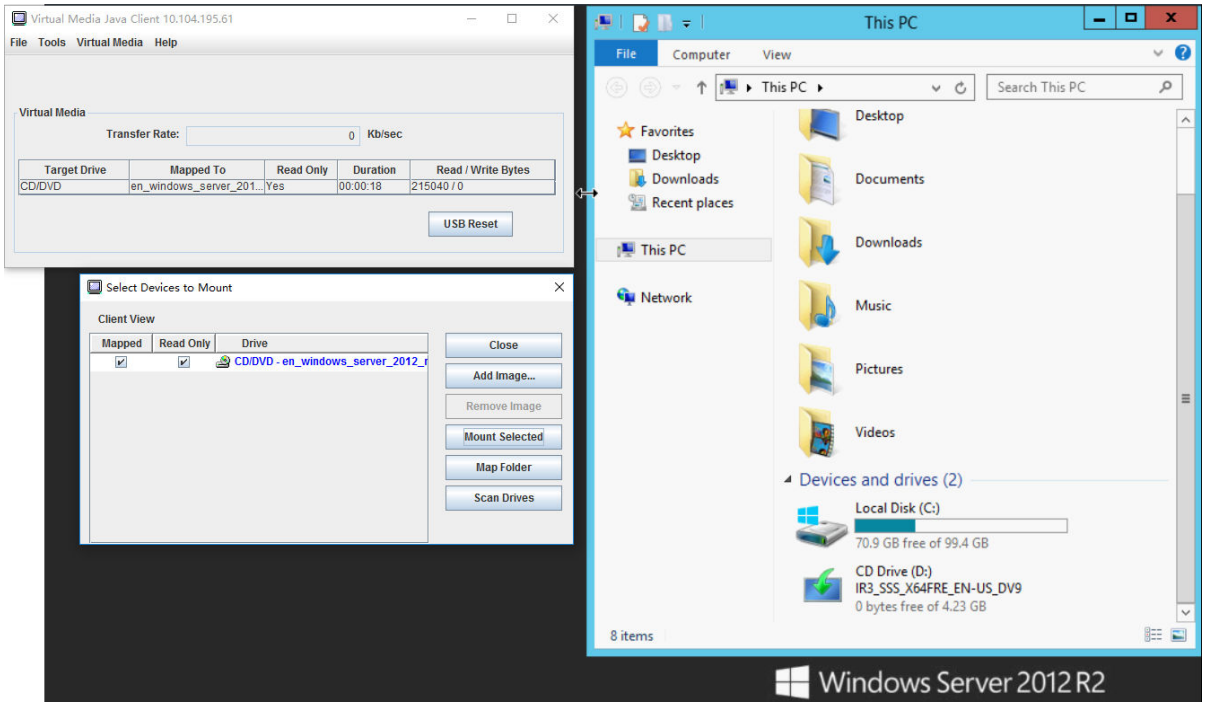


Figura 3. Montaggio immagine locale

- **Montaggio cartella locale**:
  1. Fare clic sul pulsante **Associa cartella** per selezionare la cartella locale che si desidera montare.
  2. Fare clic sul pulsante **Monta elemento selezionato** per montare correttamente la cartella locale.

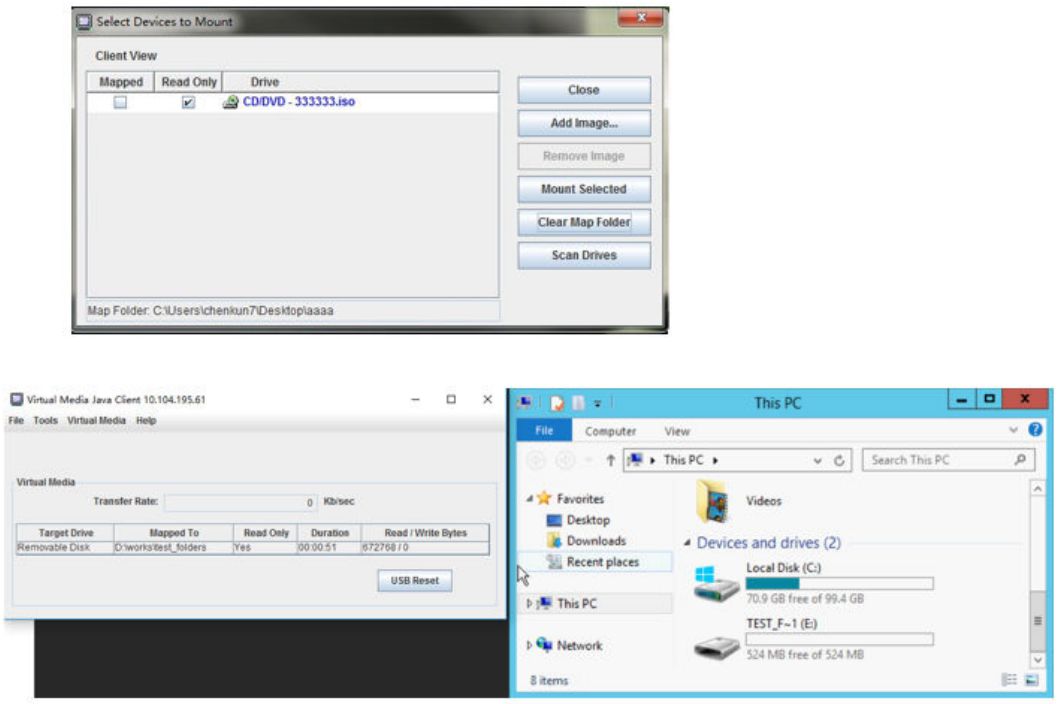


Figura 4. Montaggio cartella locale

- **Montaggio unità CD/DVD o USB**:
  1. Fare clic sul pulsante **Esegui scansione unità** per rilevare le unità CD/DVD o USB collegate.
  2. Controllare l'opzione **Elemento associato**.
  3. Selezionare l'opzione **Sola lettura** per abilitare la funzione, se necessario.
  4. Fare clic sul pulsante **Monta elemento selezionato** per montare correttamente l'immagine locale.

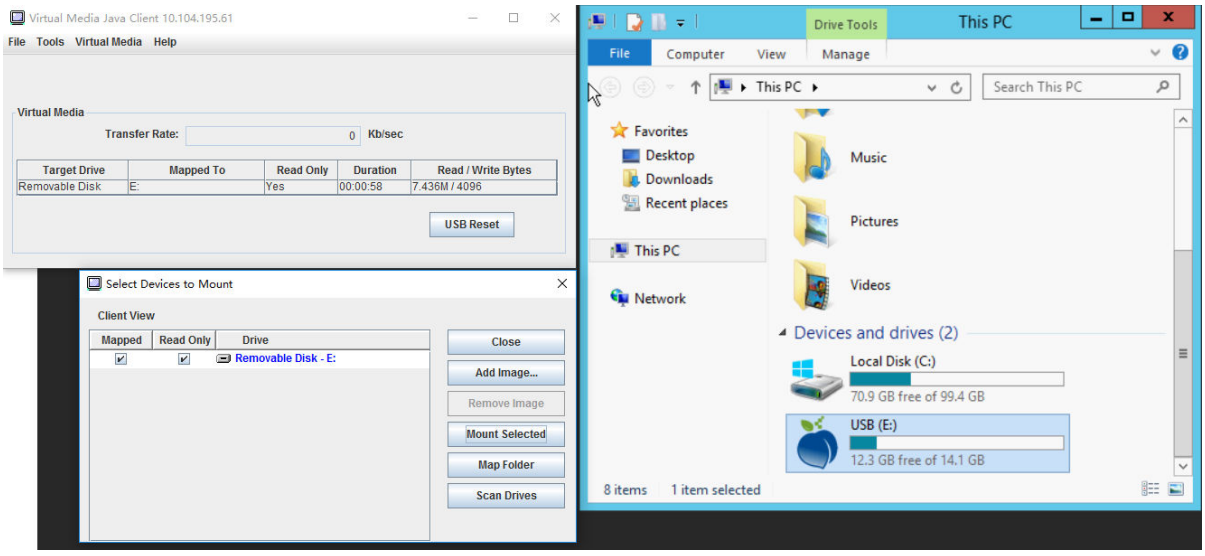


Figura 5. Montaggio unità CD/DVD o USB

La finestra "Seleziona dispositivi da montare" contiene un elenco dei dispositivi locali correnti disponibili per il montaggio. Questa finestra contiene i seguenti campi e pulsanti:

- Il campo **Elemento associato** contiene la casella di controllo che consente di selezionare i dispositivi da montare o associare.
- Il campo **Sola lettura** contiene la casella di controllo che consente di selezionare i dispositivi associati o montati di *sola lettura* sul server host.
- Il campo **Unità** contiene il percorso del dispositivo sul computer locale.
- Fare clic sul pulsante **Chiudi** per chiudere la finestra "Seleziona dispositivi da montare".
- Fare clic sul pulsante **Aggiungi immagine** per selezionare l'immagine del dischetto e il file di immagine ISO nel file system locale che si desidera aggiungere all'elenco dei dispositivi.
- Fare clic sul pulsante **Rimuovi immagine** per rimuovere un'immagine aggiunta all'elenco dei dispositivi.
- Fare clic sul pulsante **Monta elemento selezionato** per montare o associare tutti i dispositivi controllati per il montaggio o l'associazione nel campo **Elemento associato**.

  Nota: La cartella verrà montata in modalità di sola lettura.
- Fare clic sul pulsante **Esegui scansione unità** per aggiornare l'elenco dei dispositivi locali.

Selezione dei dispositivi da smontare

Per smontare i dispositivi del server host, completare le seguenti operazioni:

1. Fare clic sull'opzione **Smonta tutto** nella scheda **Supporti virtuali** della finestra Virtual Media Java Client.
2. Dopo aver selezionato l'opzione **Smonta tutto** viene visualizzata una finestra di conferma "Smonta tutto". Se si accetta, *tutti* i dispositivi del server host sul server verranno smontati.

   Nota: Non è possibile smontare le singole unità.

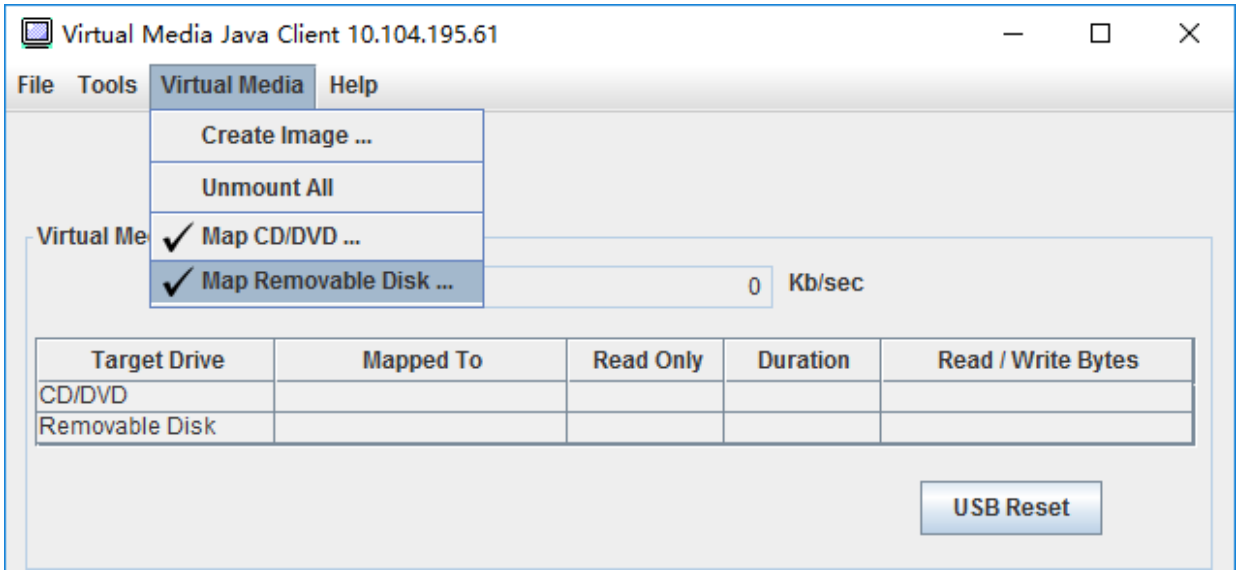


Figura 6. Smontaggio di tutti gli elementi

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.

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 conterà i seguenti dati: informazioni sul sistema, inventario del sistema, utilizzo del sistema, tabella SMBIOS, lettura dei sensori, log eventi, chiave FOD, chiave SLP, configurazione UEFI e configurazione XClarity Controller 2.

L'utente può posizionare il mouse sull'opzione Informazioni di base e fare clic sulla finestra mobile per visualizzare alcuni dati effettivi da esportare.

Anche se le informazioni di base sono obbligatorie, l'utente ha la possibilità di esportare 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>_xcc_mini-log_<date>-<time>.zip`

Ad esempio: 7X2106Z01A_2345678_xcc_mini-log_170511-175656.zip.

Oltre al formato zip, i dati di servizio possono essere scaricati anche utilizzando il formato tzz. tramite **Sfoglia cronologia...**. Il completamento del formato tzz richiede del tempo, pertanto non verrà visualizzato immediatamente dopo l'esportazione dei file zip. Tzz utilizza un algoritmo di compressione differente e può essere estratto con un programma di utilità come "lzop".

Sfoglia cronologia... conserverà inoltre i log di servizio esportati di recente.

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.

Nota: Il campo è facoltativo e non è configurabile in un nodo Flex.

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.

Nota: Il campo è facoltativo e non è configurabile in un nodo Flex.

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:

Watchdog sistema operativo
Questa opzione consente di monitorare il sistema operativo per garantire che non sia bloccato. Per questa funzione, è necessario che sia abilitata l'interfaccia Ethernet-over-USB. Consultare "Configurazione di Ethernet-over-USB" a pagina 33 per ulteriori informazioni. XClarity Controller contatta il sistema operativo in base a un intervallo configurato in **Ora watchdog sistema operativo**. Se non risponde prima dell'ora prevista per il controllo successivo, il sistema operativo viene considerato come bloccato in XClarity Controller. XClarity Controller acquisirà il contenuto dello schermo del server ed eseguirà un riavvio del server per tentare di ripristinare l'operazione. XClarity Controller riavvierà il server una sola volta. Se il sistema operativo continua a bloccarsi dopo il riavvio, il server non verrà riavviato continuamente, ma verrà lasciato nello stato di blocco, affinché il problema possa essere esaminato e risolto. Per riattivare la funzione Watchdog sistema operativo, spegnere e riaccendere il server. Per abilitare la funzione Watchdog sistema operativo, selezionare un intervallo nel menu a discesa Ora watchdog sistema operativo e fare clic su **Applica**. Per disabilitare la funzione Watchdog sistema operativo, selezionare **Nessuno** nel menu a discesa Ora watchdog sistema operativo.

Watchdog del programma di caricamento

La funzione Watchdog del programma di caricamento monitora l'intervallo tra il completamento di POST e l'inizio dell'esecuzione del sistema operativo. Per questa funzione, è necessario che sia abilitata l'interfaccia Ethernet-over-USB. Consultare "Configurazione di Ethernet-over-USB" a pagina 33 per ulteriori informazioni. Al termine di POST, XClarity Controller avvia un timer e inizia a contattare il sistema operativo. Se il sistema operativo non risponde in base al tempo configurato in Watchdog del programma di caricamento, l'avvio del sistema operativo viene considerato come bloccato in XClarity Controller. XClarity Controller eseguirà pertanto un riavvio del server per tentare di ripristinare l'operazione. XClarity Controller riavvierà il server una sola volta. Se l'avvio del sistema operativo continua a bloccarsi dopo il riavvio, il server non verrà riavviato continuamente, ma verrà lasciato nello stato di blocco, affinché il problema possa essere esaminato e risolto. La funzione Watchdog del programma di caricamento viene riattivata quando il server viene spento e riacceso o quando il server viene correttamente avviato nel sistema operativo. Per abilitare la funzione Watchdog del programma di caricamento, selezionare un intervallo nel menu a discesa Watchdog del programma di caricamento e fare clic su **Applica**. Per disabilitare la funzione Watchdog del programma di caricamento, selezionare **Nessuno** nel menu a discesa Watchdog del programma di caricamento.

Abilita ritardo spegnimento

Utilizzare il campo Ritardo spegnimento per specificare il numero di minuti che il sottosistema XClarity Controller dovrà attendere per l'arresto del sistema operativo prima di forzarne lo spegnimento. 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.

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.
- 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.
- Non è possibile modificare le impostazioni di data e ora di XClarity Controller in un sistema Flex System.

Capitolo 6. 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:

- Dettaglio
- Configurazione RAID

Dettaglio RAID

Utilizzare le informazioni in questo argomento per eseguire la funzione Dettaglio RAID.

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.

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.

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 sotto forma di "schede dei dischi 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 "la scheda del disco virtuale".

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.

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. 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.

      Per alcuni livelli RAID, è richiesto un intervallo. È inoltre necessario che nell'intervallo sia presente una quantità minima di unità.

      1) Per tali tipi di situazioni, nell'interfaccia Web viene visualizzato **Intervallo 1** per impostazione predefinita.
      2) Selezionare le unità e fare clic su **Aggiungi membro** per aggiungere unità a **Intervallo 1**. Quando in **Intervallo 1** non è presente un numero sufficiente di unità, disabilitare il collegamento **Aggiungi intervallo**.
      3) Fare clic su **Aggiungi intervallo** per aggiungere **Intervallo 2**. Selezionare le unità e fare clic su **Aggiungi membro** per l'aggiunta a **Intervallo 2**.
      4) Fare clic su **Aggiungi membro** per aggiungere unità all'ultimo intervallo. Se si desidera aggiungere di nuovo le unità a **Intervallo 1**, è necessario fare clic su Intervallo 1 e selezionare le unità da aggiungere a **Intervallo 1**.
      5) Se viene raggiunto il numero di intervalli massimo, disabilitare **Aggiungi intervallo**.

   b. 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, creare un disco virtuale che utilizza 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. Se sono presenti più dischi virtuali, verrà abilitata l'icona **Rimuovi**. 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 disco virtuale** 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, ovvero nome unità, stato RAID, tipo, numero di serie, numero parte, numero FRU 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.
  - **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 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 7. Aggiornamento del firmware del server

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

Panoramica

Informazioni generali sull'aggiornamento del firmware del server.

L'opzione **Aggiornamento firmware** sul riquadro di navigazione ha 4 funzioni:

- **Firmware di sistema:** panoramica dello stato e della versione del firmware di sistema. E per eseguire l'aggiornamento firmware del sistema.
- **Firmware dell'adattatore:** panoramica del firmware dell'adattatore installato, del relativo stato e della relativa versione. E per eseguire l'aggiornamento firmware dell'adattatore.
- **Firmware dell'alimentatore:** panoramica della versione del firmware dell'unità di alimentazione. E per eseguire l'aggiornamento firmware dell'alimentatore.
- **Aggiornamento da repository:** sincronizzazione del firmware del server con repository remoto CIFS/NFS per l'aggiornamento in blocco.

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

- **Attivo:** il firmware è attivo.
- **Inattivo:** il firmware non è attivo.
- **In sospeso:** il firmware è in attesa di diventare attivo.
- **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 o inatteso.
- 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 70.

Aggiornamento da repository

Aggiornamento del firmware del server da un repository remoto

Nota: *La funzionalità CITF/NFS/HTTPS/Cronologia firmware integrato richiede la licenza XCC Platinum.*

Panoramica

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.

Se si utilizza il montaggio CIFS o NFS, i file di metadati devono essere posizionati nella directory radice del file system condiviso di rete, con i payload 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 di firmware e XCC (un dispositivo elettronico) 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 l'**aggiornamento dal repository** l'utente può configurare XCC per sincronizzare il firmware del server con un repository del firmware CIFS/NFS remoto. 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.

Sono disponibili cinque stati di 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.

Quando l'utente fa clic su **Interrompi aggiornamento**, annullerà gli aggiornamenti in coda dopo il completamento dell'aggiornamento del pacchetto di installazione corrente.

Per aggiornare da repository, effettuare le seguenti operazioni:

1. Fare clic su **Connetti** al repository remoto dopo aver immesso le informazioni del repository remoto.
2. Fare clic su **Aggiorna** per iniziare l'aggiornamento batch.
3. Fare clic su **Visualizza dettagli** per visualizzare lo stato di aggiornamento, sono disponibili 5 categorie di stato come indicato in precedenza.
4. Fare clic su **Interrompi aggiornamento** annullerà gli aggiornamenti in coda dopo il completamento dell'aggiornamento del pacchetto di installazione corrente.
5. Fare clic su **Disconnetti** per scollegarlo dal repository remoto.
6. 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 70.

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.

Aggiornamento con Redfish

L'interfaccia Redfish utilizza il payload in formato JSON per semplificare la lettura e la scrittura da parte dell'utente. XCC Redfish offre un'API standard (SimpleUpdate) per recuperare il file del bundle di aggiornamento da un URI tramite HTTP/HTTPS/SFTP/TFTP, nonché un aggiornamento push HTTP multiparte per eseguire il push del file del bundle di aggiornamento UpdateService. È possibile utilizzare un comando o un singolo strumento client Redfish per eseguire aggiornamenti firmware e query dello stato dell'aggiornamento.

Comando di esempio per eseguire il push del file del bundle a XCC e generare l'attività di trasferimento e verifica dei file:

curl -s -k -u USERID:PASSW0RD-F 'UpdateParameters={"Targets":[]};type=application/json' -F 'UpdateFile=@./NY7D72-IB-320.zip;type=application/octet-stream' https://10.240.218.157:443/mfwupdate

```
{
  "ld": "f2fd6e9d-cOa6-4b11-b9f6-69a17a1 ,
  "Name": "Task f2fd6e9d-cOa6-4b11-b9f6-69a17a1 e579c",
  "@odata.type": "#Task.v1_5_1. Task",
  "@odata.id': "[redfish/v 1 fTaskServicefTasks/f2fd6e9d-cOa6-4b11-b9f6-69a 17a1 e579c",
  "Messages": [l
  "Description": "This resource represents a task for a Redfish implementation."
  "StartTime": "2022-03-21 TOT 16:41 +00:00",
  "TaskMonitor": "/redfish/v1fTaskSen.'ice/cO69ed4a-e754-497O-ab9a-922e8a3eO76b",
  "@odata.context": "'redfish/v1/$metadata#Task.Task",
  "@odata.etag":
  "PercentCompIete": O,
  "HidePayload": true,
  "TaskState": "New"
}
```

Comando di esempio per richiedere all'API di rispondere con l'ID processo per l'aggiornamento firmware, una volta completati il trasferimento e la convalida dell'immagine:

https://10.240.218.157/ redfish/v1/TaskService/Tasks/f2fd6e9d c0a6 4b11 b9f6 69a17a1e579c

```
{
  "@odata.etag": ,
  "Name-: "Task f2fd6e9d-cOa6-4b11-b9f6-69a17a1e579c",
  Task",
  "IredfishNI/TaskSemcenasksff2fd6e9d-cOa6-4bI I-b9f6-69aI 7a1e579c",
  "Messages": [
    {
      "Resolution": "Follow the referenced job and monitor the job for further updates.",
    "@odata.type":
    'MessageSeverity": "OK",
    "MessageArgs": [
    "IredfishtvI/JobService/JObs/JObROOOOOI-lJPdate"
  ],
  "Messageld": "Update. 1 .O.OperationTransitionedToJob",
  "Message": "The update operation has transitioned to the job at URI 'Iredfsh/vl
 IJobService/Jobs/JobROOOOO1-Update'."
  }
  ],
  "Description": "This resource represents a task for a Redfish implementation.",
```

```
  "HidePayIoad": true,
  "StartTime":
  "TaskMonitor: "'redfish1v1/TaskseNice/c069ed4a-e754-4970-ab9a-922e8a3e076b",
  "TaskStatus": "OK",
  "@odata.context-: "'redfish/v1/$metadata#Task.Task",
  "ld": "f2fd6e9d-c0a6-4b11-b9f6-6ga17a 1 e579c",
  "Percentcomplete": 100,
  "EndTime": 2022-03-21
  "TaskState": "Completed"
}
```


Eseguendo una query per l'ID processo, XCC restituisce i passaggi del processo per tutti i pacchetti firmware nel bundle di aggiornamento, come mostrato di seguito:

https://10.240.218.157/redfish/v1/JobService/Jobs/JobR000001-Update


```
{
"@odata.etag": "\"1647847200776\"", "PercentComplete": 100, "@odata.type": "#Job.v1_0_7.Job",
"@odata.id": "/redfish/v1/JobService/Jobs/JobR000001-Update", "Messages": [
{
"Resolution": "None.",
"@odata.type": "#Message.v1_1_2.Message", "MessageSeverity": "OK",
"MessageArgs": [ "NY7D72-IB-320.zip",
"HardDiskDrive"
],
"MessageId": "Update.1.0.UpdateSuccessful ",
"Message": " Device 'HardDiskDrive' successfully updated with image 'NY7D72-IB-320.zip'."
},
{
"Resolution": "None.",
"@odata.type": "#Message.v1_1_2.Message", "MessageSeverity": "OK",
"MessageArgs": [ "NY7D72-IB-320.zip",
"/redfish/v1/UpdateService/FirmwareInventory/UEFI"
],
"MessageId": "Update.1.0.UpdateSuccessful",
"Message": "Device '/redfish/v1/UpdateService/FirmwareInventory/UEFI' successfully
 updated with image 'NY7D72-IB-320.zip'. "
},
{
"Resolution": "None.",
"@odata.type": "#Message.v1_1_2.Message", "MessageSeverity": "Critical",
"MessageArgs": [ "NY7D72-IB-320.zip",
"/redfish/v1/UpdateService/FirmwareInventory/BMC-Primary"
],
"MessageId": "Update.1.0.ApplyFailed",
"Message": "Installation of image 'NY7D72-IB-320.zip' to '/redfish/v1/UpdateService/FirmwareInventory/BMC-Primary' failed."
}
],
"Description": "This resource is used to represent a job for a Redfish implementation.",
"StartTime": "2022-03-21T07:16:58+00:00",
"Id": "JobR000001-Update",
"EndTime": "2022-03-21T07:20:00+00:00",
"@odata.context": "/redfish/v1/$metadata#Job.Job", "Steps": {
"@odata.id": "/redfish/v1/JobService/Jobs/JobR000001-Update/Steps"
},
"Name": "JobR000001-Update", "StepOrder": [
"lnvgy_fw_drives_all.samsung.pm1735.cq-cq37_anyos_comp.lvt", "lnvgy_fw_uefi_ese103a-1.00_anyos_comp.uxz",
 "lnvgy_fw_xcc_esx301p-0.01_anyos_comp.uxz"
],
"JobState": "Completed"
```


Quando il passaggio del processo viene sottoposto a query, XCC restituisce informazioni aggiuntive ai singoli aggiornamenti firmware:

https://10.240.218.157/redfish/v1/JobService/Jobs/JobR000001-

Update/Steps/lnvgy_fw_drives_all.samsung.pm1735.cq-cq37_anyos_comp.lvt


```
{
"@odata.etag": "\"1647847202778\"", "PercentComplete": 1, "@odata.type": "#Job.v1_0_7.Job",
"@odata.id": "/redfish/v1/JobService/Jobs/JobR000001-Update/Steps/lnvgy_fw_drives_all.samsung.pm1735.cq-
 cq37_anyos_comp.lvt",
"Messages": [],
"Description": "This resource is used to represent a job for a Redfish implementation.", "StartTime":
 "2022-03-21T07:16:58+00:00",
"@odata.context": "/redfish/v1/$metadata#Job.Job",
"Id": "lnvgy_fw_drives_all.samsung.pm1735.cq-cq37_anyos_comp.lvt", "Name":
 "lnvgy_fw_drives_all.samsung.pm1735.cq-cq37_anyos_comp.lvt", "EndTime": "2022-03-21T07:20:02+00:00",

"JobState": "Completed"
```


Eseguire un download dal repository remoto e aggiornare come mostrato di seguito:

```
system> syncrep
syncrep [options] Launch firmware sync from remote repository options:
-t protocol to connect repository. The local type will reboot host immediately.
 (eg: syncrep -t samba -l url -u user -p password; syncrep -t local -l /bulk/bundle.tgz;
syncrep -t http -l http://IP/bundle.tgz)
-l location of remote repository (URL format)
-u User
-p Password
-o option (extra option string for samba and nfs mounts)
-d domain (domain for samba mount)
-q query current update status
-c cancel the sync process
-r <> firmware rollback
-gl get repository list
```

Capitolo 8. 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 103, "Rimozione di una chiave di attivazione" a pagina 104 o "Esportazione di una chiave di attivazione" a pagina 104. Per informazioni sulla gestione di una chiave di attivazione mediante la CLI di XClarity Controller, vedere "comando keycfg" a pagina 145.

Per registrare un ID per l'amministrazione della licenza di XClarity Controller, fare clic sul collegamento seguente: http://thinksystem.lenovofiles.com/help/index.jsp

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

Attenzione: Non è possibile eseguire direttamente l'aggiornamento da XClarity Controller livello Standard alla funzionalità di livello Enterprise. Per poter attivare la funzionalità di livello Enterprise, sarà in primo luogo necessario eseguire l'aggiornamento al livello Advanced.

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 o su **Annulla** per interrompere l'installazione. Per completare l'operazione, fare clic su **OK** nella finestra Aggiungi chiave di attivazione o su **Annulla** per terminare l'installazione.

La finestra Operazione riuscita indica che la chiave di attivazione è stata installata.

Nota:

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

Passo 4. Fare clic su **OK** per chiudere la finestra Operazione riuscita.

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'operazione di eliminazione oppure su **Annulla** per conservare il file della chiave.
La chiave di attivazione selezionata verrà rimossa dal server e non sarà più visualizzata nella pagina Gestione licenze.

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 l'esportazione della chiave di attivazione oppure su **Annulla** per annullare la richiesta di esportazione della chiave.

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

Capitolo 9. Gestione del gruppo adiacente

La gestione dal gruppo adiacente di Lenovo XClarity Controller è un gruppo di gestione virtuale tra i server Lenovo ThinkSystem che gestiscono più server su un singolo XCC.

Lenovo XClarity Controller (XCC) è un processore di servizio integrato che sostituisce il noto controller di gestione della scheda di base (Baseboard Management Controller, BMC) per i server Lenovo ThinkSystem che forniscono funzioni di configurazione, gestione e monitoraggio del server.

Di solito, XCC può gestire solo un singolo server. Tuttavia il software di gestione centralizzato, Lenovo XClarity Administrator (LXCA), facilita la gestione della scalabilità su più server. Se LXCA non è distribuito sul campo, in particolare per gli utenti PMI, ogni nodo deve essere configurato singolarmente, generando un processo inefficace. Per evitare questo scenario, la funzione del gruppo adiacente XCC è progettata per creare un gruppo di gestione virtuale tra i server Lenovo ThinkSystem che gestiscono più server su un singolo XCC. Questa funzione fornisce un metodo flessibile di avvio di una distribuzione rapida per più server in un segmento di rete locale.

Funzioni supportate

Informazioni generali sulle funzioni supportate dal gruppo adiacente.

Il **gruppo adiacente XCC** fornisce le seguenti funzioni:

- Rilevamento dei nodi adiacenti situati nello stesso segmento di rete locale.
- Monitoraggio dell'integrità del sistema e dello stato di alimentazione dei nodi adiacenti.
- Configurazione del gruppo adiacente nel nodo principale.
- Clonazione della configurazione di sistema su più membri del gruppo adiacente.
- Avvio di aggiornamenti firmware simultanei su più membri del gruppo adiacente.
- Il nodo XCC principale supporta un massimo di 200 nodi.

Server ThinkSystem che supportano le funzioni del gruppo adiacente XCC

Server	Tipi di macchina
ThinkSystem SR630 V3	7D72, 7D73
ThinkSystem SR650 V3	7D75, 7D76
Lenovo ThinkSystem ST650 V3	7D7A, 7D7B, 7D7C
Lenovo ThinkSystem SD650 V3	7D7M
Lenovo ThinkSystem SD650-I V3	7D7L
Lenovo ThinkSystem SR635 V3	7D9G, 7D9H
Lenovo ThinkSystem SR645 V3	7D9C, 7D9D
Lenovo ThinkSystem SR655 V3	7D9E, 7D9F
Lenovo ThinkSystem SR665 V3	7D9A, 7D9B
ThinkSystem SD665 V3	7D9P
ThinkSystem SR675 V3	7D9Q, 7D9R

Nota: La funzione di gruppo adiacente XCC verrà inclusa nelle versioni successive dei server Lenovo ThinkSystem.

Rilevamento dei nodi adiacenti

Utilizzare le informazioni in questo argomento per rilevare i nodi adiacenti.

Ogni istanza XCC rileva i server adiacenti nello stesso segmento di rete locale utilizzando il messaggio multicast SSDP (Simple Service Discovery Protocol).

Di seguito sono elencati i prerequisiti di un server per essere rilevato da un'istanza XCC:

1. La porta SSDP (Simple Service Discovery Protocol) 1900 è abilitata in XCC (**Configurazione BMC -> Rete -> SSDP**).
2. La gestione del gruppo adiacente è configurata per essere abilitata (disabilitata per impostazione predefinita).

La pagina Rilevamento consente di monitorare le informazioni sul sistema, l'alimentazione in tempo reale e lo stato di integrità di tutti i nodi rilevati. La colonna **Ultimo rilevamento** indica il timestamp di ricezione dell'ultimo messaggio SSDP dai nodi adiacenti. Questa colonna viene aggiornata regolarmente, tranne se il nodo adiacente non è in linea o l'impostazione SSDP/Gestione gruppo adiacente è disabilitata.

Configurazione del gruppo adiacente

Utilizzare le informazioni in questo argomento per eseguire la configurazione del gruppo adiacente.

Un gruppo adiacente viene visualizzato sulla pagina Web di XCC specificando il nome del gruppo.

Verificare che il nome del nuovo gruppo sia univoco e non esista nel segmento di rete locale.

Una volta creato un nuovo gruppo:

- L'istanza XCC corrente viene aggiunta automaticamente.
- L'istanza XCC corrente diventa il nodo principale del nuovo gruppo adiacente XCC.
- A tutte le altre istanze XCC nello stesso segmento di rete locale viene inviata immediatamente una notifica e la pagina Web di rilevamento adiacente XCC di ciascun server viene aggiornata.
- Il nodo principale di un gruppo può selezionare uno o più server adiacenti da unire al gruppo, specificando le credenziali di amministratore XCC del server adiacente.
- Una volta che i nodi adiacenti verificano correttamente le credenziali dell'utente, accettano la richiesta dal nodo principale e quindi si uniscono a questo gruppo come nuovi membri.

Provisioning del gruppo adiacente

Utilizzare le informazioni in questo argomento per eseguire il provisioning del gruppo adiacente.

Il provisioning del gruppo adiacente è una funzione che distribuisce la configurazione a più membri del gruppo. È costituito da **Configurazione clone** e **Aggiornamento firmware dal repository.**

Configurazione clone viene utilizzato per propagare la configurazione del sistema XCC corrente ai membri selezionati dello stesso tipo di macchina. La configurazione clonata include:

1. Configurazione server: opzioni di avvio, criteri per il risparmio di energia, proprietà del server.

2. Configurazione BMC: rete (ad eccezione dell'indirizzo IP e delle relative impostazioni), sicurezza, utente/LDAP (inclusi account utente e password), Call Home.

Aggiornamento firmware dal repository avvia l'aggiornamento firmware contemporaneamente per i membri selezionati, specificando un repository del firmware condiviso sul protocollo Common Internet File System (CIFS) o Network File System (NFS). L'aggiornamento firmware può essere applicato a più tipi di macchina contemporaneamente, purché nel repository condiviso siano disponibili le immagini firmware applicabili.

Quando l'aggiornamento firmware del gruppo adiacente è in corso, è possibile monitorarne l'avanzamento nella colonna Stato e dettagli.

Capitolo 10. API REST Redfish di Lenovo XClarity Controller

Lenovo XClarity Controller fornisce una serie di API REST, con conformità Redfish, facili da utilizzare per accedere ai dati e ai servizi di Lenovo XClarity Controller dalle applicazioni in esecuzione all'esterno del framework Lenovo XClarity Controller.

Ciò consente di semplificare l'integrazione delle funzionalità di Lenovo XClarity Controller in altri software, in esecuzione sullo stesso sistema come server Lenovo XClarity Controller o su un sistema remoto all'interno della stessa rete. Queste API sono basate sull'API REST standard del settore e accessibili tramite il protocollo HTTPS.

La guida per l'utente dell'API REST Redfish di XClarity Controller è disponibile qui: https://sysmgt.lenovofiles.com/help/topic/com.lenovo.systems.management.xcc.restapi.doc/xcc_restapi_book.pdf.

Lenovo fornisce script Redfish open source di esempio che possono essere utilizzate come riferimento per lo sviluppo di software che comunicano con l'API REST Lenovo Redfish. Questi script di esempio sono disponibili qui:

- Python: https://github.com/lenovo/python-redfish-lenovo
- PowerShell: https://github.com/lenovo/powershell-redfish-lenovo

Le specifiche DMTF relative all'API Redfish sono disponibili all'indirizzo: https://redfish.dmtf.org/. Questo sito Web fornisce le specifiche generali e altri materiali di riferimento sull'API REST Redfish.

Capitolo 11. 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 111).

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.

L'utente sarà collegato alla riga di comando. 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 di 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> ?
```
- In un sistema Flex System, alcune impostazioni sono gestite dal CMM e non possono essere modificate con XClarity Controller.

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 accseccfg" a pagina 129
- "comando adapter" a pagina 195
- "comando alertcfg" a pagina 131
- "comando alertentries" a pagina 177
- "comando asu" a pagina 131
- "comando di backup" a pagina 134
- "comando batch" a pagina 180
- "comando chconfig" a pagina 183
- "comando chlog" a pagina 186
- "comando chmanual" a pagina 185

- "comando clearcfg" a pagina 181
- "comando clearlog" a pagina 116
- "comando clock" a pagina 181
- "comando console" a pagina 129
- "comando dbgshimm" a pagina 199
- "comando dhcpinfo" a pagina 135
- "comando dns" a pagina 136
- "Comando encaps" a pagina 138
- "comando ethtousb" a pagina 138
- "comando exit" a pagina 115
- "comando fans" a pagina 117
- "comando ffdc" a pagina 117
- "Comando firewall" a pagina 139
- "comando fuelg" a pagina 127
- "comando gprofile" a pagina 140
- "comando hashpw" a pagina 141
- "comando help" a pagina 115
- "comando history" a pagina 115
- "Comando hreport" a pagina 118
- "comando identify" a pagina 182
- "comando ifconfig" a pagina 142
- "comando info" a pagina 182
- "comando keycfg" a pagina 145
- "comando ldap" a pagina 146
- "comando led" a pagina 120
- "comando mhlog" a pagina 119
- "comando mvstor" a pagina 197
- "comando ntp" a pagina 148
- "comando portcfg" a pagina 149
- "comando portcontrol" a pagina 150
- "comando ports" a pagina 151
- "comando power" a pagina 125
- "comando pxeboot" a pagina 128
- "comando rdmount" a pagina 152
- "comando readlog" a pagina 121
- "comando reset" a pagina 127
- "comando restore" a pagina 152
- "comando restoredefaults" a pagina 153
- "comando roles" a pagina 154
- "comando seccfg" a pagina 155
- "comando set" a pagina 155

- "comando smtp" a pagina 155
- "comando snmp" a pagina 156
- "comando snmpalerts" a pagina 158
- "comando spreset" a pagina 183
- "comando srcfg" a pagina 160
- "comando sshcfg" a pagina 161
- "comando ssl" a pagina 162
- "comando sslcfg" a pagina 163
- "comando storage" a pagina 186
- "comando storekeycfg" a pagina 166
- "comando syncrep" a pagina 168
- "comando syshealth" a pagina 122
- "comando temps" a pagina 123
- "comando thermal" a pagina 169
- "comando timeouts" a pagina 169
- "comando tls" a pagina 170
- "comando trespass" a pagina 171
- "comando uefipw" a pagina 172
- "comando usbeth" a pagina 172
- "comando usbfp" a pagina 173
- "comando users" a pagina 173
- "comando volts" a pagina 123
- "comando vpd" a pagina 124

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 di IMM.

Utilizzare il comando **clearlog** per cancellare il log eventi di 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.

La seguente tabella mostra gli argomenti per le opzioni.

Tabella 7. comando clearlog

La seguente tabella a una riga e due colonne contiene l'opzione e la relativa descrizione.

Opzione	Descrizione
-t <all | platform | audit>	Tipo di evento, scegliere il tipo di evento da cancellare. Se non specificato, verranno selezionati tutti i tipi di eventi.

Descrizioni del tipo di evento

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

comando fans

Questo comando viene utilizzato per visualizzare la velocità della 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 ffdc

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

Utilizzare il comando **ffdc** (first failure data capture) per generare e trasferire i dati di servizio all'assistenza.

Il seguente elenco riporta i comandi da utilizzare con il comando **ffdc**:

- **generate**, crea un nuovo file di dati di servizio
- **status**, controlla lo stato di un file di dati di servizio
- **copy**, copia i dati di servizio esistenti
- **delete**, elimina i dati di servizio esistenti

La seguente tabella mostra gli argomenti per le opzioni.

Tabella 8. comando ffdc

La seguente tabella multiriga a tre colonne contiene le opzioni, le descrizioni delle opzioni e i valori associati per le opzioni.

Opzione	Descrizione	Valori
-t	Numero tipo	1 (dump del processore) e 4 (dati di servizio). Il dump del processore contiene tutti i log e i file disponibili. I dati di servizio contengono solo un subset di log e file. Il valore predefinito è 1.
-f [1]	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 [1]	L'indirizzo del server tftp/ sftp	
-pn [1]	Il numero di porta del server tftp/sftp	Il valore predefinito è 69/22.

Tabella 8. comando ffdc (continua)

Opzione	Descrizione	Valori
-u [1]	Il nome utente per il server sftp	
-pw [1]	La password per il server sftp	

1. Argomento aggiuntivo per i comandi **generate** e **copy**

Sintassi:
```
ffdc [options]
option:
  -t 1 or 4
  -f
  -ip ip_address
  -pn port_number
  -u username
  -pw password
```

Esempio:
```
system> ffdc generate
Generating ffdc...
system> ffdc status
Type 1 ffdc: in progress
system> ffdc copy -t 1 -ip 192.168.70.230 -u User2 -pw Passw0rd -f /tmp/
Waiting for ffdc.....
Copying ffdc...
ok
system> ffdc status
Type 1 ffdc: completed
8737AC1_DSY0123_xcc_120317-153327.tgz


system> ffdc generate
Generating ffdc...
system> ffdc status
Type 1 ffdc: in progress
system> ffdc status
Type 1 ffdc: in progress
system> ffdc copy -ip 192.168.70.230
Copying ffdc...
ok
system> ffdc status
Type 1 ffdc: completed
8737AC1_DSY0123_xcc_120926-105320.tgz
system>
```

Comando hreport

Utilizzare questo comando visualizzare il report di integrità incorporato.

La seguente tabella mostra i comandi hreport.

Tabella 9. Comandi hreport

La seguente tabella multiriga a due colonne contiene le descrizioni dei vari comandi hreport.

Tabella 9. Comandi hreport (continua)

Opzione	Descrizione
generazione	Crea un nuovo report di integrità
stato	Controlla lo stato
copy	Copia il report di integrità esistente
delete	Elimina il report di integrità esistente

La seguente tabella riporta gli argomenti per le opzioni generate e copy.

Tabella 10. Opzioni generate e copy

La seguente tabella multiriga a due colonne contiene le opzioni e le descrizioni associate alle opzioni generate e copy del comando.

Opzione	Descrizione
-f	Nome file remoto o directory di destinazione sftp. Il valore predefinito è il nome generato dal sistema. Per sftp, utilizzare il percorso completo o una/davanti al nome della directory (~/ o /tmp/)
-ip	Indirizzo del server tftp/sftp
-pn	Numero di porta del server tftp/sftp (valore predefinito 69/22)
-u	Nome utente per il server sftp
-pw	Password per il server sftp

comando mhlog

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

La seguente tabella mostra gli argomenti per le opzioni.

Tabella 11. comando mhlog

La seguente tabella multiriga a due colonne contiene le opzioni e le relative descrizioni.

Opzione	Descrizione
-c <count>	Visualizza le voci relative al numero ("count") (1-250)
-i <index>	Visualizza le voci a partire dall'indice (1-250)
-f	Nome file remoto del file di log
-ip	Indirizzo del server tftp/sftp
-pn	Numero di porta del server tftp/sftp (valore predefinito 69/22)
-u	Nome utente per il server sftp
-pw	Password per il server sftp

Esempio

L'aspetto dello schermo sarà simile al seguente:

```
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
```

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.

Tabella 12. comando led

La seguente tabella multiriga a tre colonne contiene le opzioni, le descrizioni delle opzioni e i valori associati per le opzioni.

Opzione	Descrizione	Valori
-l	Ottiene lo stato di tutti i LED del sistema e dei relativi componenti secondari	
-chklog	Spegne il LED del log di controllo	off
-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)

Sintassi:

```
led [options]
option:
  -l
  -chklog off
  -identify state
  -d time
```

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 di IMM. Vengono visualizzati cinque log di eventi alla volta. Le voci sono visualizzate dalle più recenti alle più vecchie.

readlog visualizza le prime cinque voci nel log di eventi, a partire dalla più recente, alla sua prima esecuzione. Quindi vengono visualizzate le successive cinque per ogni altra chiamata.

readlog -a visualizza tutte le voci nel log di eventi, a partire dalla più recente.

readlog -f reimposta il contatore e visualizza le prime 5 voci nel log di eventi, a partire dalla più recente.

readlog -date *data* visualizza le voci del log di eventi per la data specificata, in formato mm/gg/aa. È possibile avere un elenco di date separate da una barra verticale (|).

readlog -sev *severity* visualizza le voci del log di eventi per il livello di gravità specificato (E, W, I). È possibile avere un elenco di livelli di gravità separati da una barra verticale (|).

readlog -i *ip_address* imposta l'indirizzo IPv4 o IPv6 del server TFTP o SFTP su cui è salvato il log di eventi. Le opzioni del comando **-i** e **-l** sono utilizzate insieme per specificare il percorso.

readlog -l *filename* imposta il nome del file del log di eventi. Le opzioni del comando **-i** e **-l** sono utilizzate insieme per specificare il percorso.

readlog -pn *port_number* visualizza o imposta il numero di porta del server TFTP o SFTP (valore predefinito 69/22).

readlog -u *username* specifica il nome utente per il server SFTP.

readlog -pw *password* specifica la password per il server SFTP.

Sintassi:
```
readlog [options]
option:
  -a
  -f
  -date date
  -sev severity
  -i ip_address
  -l filename
  -pn port_number
  -u username
  -pw password
```

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 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 [argument]
argument:
  summary      -display the system health summary
  activeevents -display active events
  cooling - display cooling devices health status
  power - display power modules health status
  storage - display local storage health status
  processors - display processors health status
  memory - display memory health status
```

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.

```
Example
system> temps
Temperatures are displayed in degrees Fahrenheit/Celsius

         WR       W       T      SS      HS
-------------------------------------------
CPU1     N/A     N/A    80/27   N/A     N/A
CPU2     N/A     N/A    80/27   N/A     N/A
DASD1  66/19   73/23   82/28  88/31   92/33
Amb    59/15   70/21   83/28  90/32   95/35
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.

```
Example:
system> volts

      i HSL    SSL    WL     WRL    V      WRH    WH    SSH    HSH
-------------------------------------------------------------------
5v     5.02  4.00  4.15  4.50  4.60  5.25  5.50  5.75   6.00
3.3v   3.35  2.80  2.95  3.05  3.10  3.50  3.65  3.70   3.85
12v    12.25 11.10 11.30 11.50 11.85 12.15 12.25 12.40  12.65
-5v    -5.10 -5.85 -5.65 -5.40 -5.20 -4.85 -4.65 -4.40  -4.20
-3.3v -3.35 -4.10 -3.95 -3.65 -3.50 -3.10 -2.95 -2.80  -2.70
VRM1                          3.45
VRM2                          5.45
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 sys  - displays Vital Product Data for the system
vpd bmc  - displays Vital Product Data for the management controller
vpd uefi - displays Vital Product Data for system BIOS
vpd lxpm  - displays Vital Product Data for system LXPM
vpd fw   - displays Vital Product Data for the system firmware
vpd comp - displays Vital Product Data for the system components
vpd pmem - displays Vital Product Data for Intel Optane PMem
vpd pcie - displays Vital Product Data for PCIe devices
```

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.

La seguente tabella riporta una serie di comandi che possono essere utilizzati con il comando **power**.

Tabella 13. comando power

La seguente tabella multiriga a tre colonne contiene i comandi di alimentazione, le descrizioni dei comandi e i valori associati ai comandi.

Comando	Descrizione	Valore
accensione	Utilizzare questo comando per accendere il server.	on, off
power off	Utilizzare questo comando per spegnere il server. **Nota:** L'opzione **-s** arresta il sistema operativo prima che il server venga spento.	on, off
power cycle	Utilizzare questo comando per spegnere e riaccendere il server. **Nota:** L'opzione **-s** arresta il sistema operativo prima che il server venga spento.	
power enterS3	Utilizzare questo comando per attivare la modalità S3 (sospensione) del sistema operativo. **Nota:** Questo comando viene utilizzato solo quando il sistema operativo è acceso. La modalità S3 non è supportata su tutti i server.	
power rp	Utilizzare questa opzione per specificare i criteri di ripristino dell'alimentazione.	alwayson|alwaysoff|restore
power S3resume	Utilizzare questo comando per riattivare il sistema operativo dalla modalità S3 (sospensione). **Nota:** Questo comando viene utilizzato solo quando il sistema operativo è acceso. La modalità S3 non è supportata su tutti i server.	
power state	Utilizzare questo comando per visualizzare lo stato di alimentazione e lo stato corrente del server.	on, off

La seguente tabella contiene le opzioni per i comandi **power on**, **power off** e **power cycle**.

Tabella 14. comando power

La seguente tabella multiriga a tre colonne contiene le opzioni, le descrizioni delle opzioni e i valori associati per le opzioni.

Tabella 14. comando power (continua)

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.	**Nota:** I valori di questa opzione sono riportati su linee separate a causa delle limitazioni di spazio. Sun|Mon|Tue|Wed|Thu| Fri|Sat|Day|clear
-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**.	

Sintassi:
```
power on
power off [-s]
power state
power cycle [-s]
```

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 13:00
```

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.

La seguente tabella mostra gli argomenti per le opzioni.

Tabella 15. comando reset

La seguente tabella multiriga a tre colonne contiene le opzioni, le descrizioni delle opzioni e i valori associati per le opzioni.

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.	

Sintassi:

```
reset [option]
option:
-s
-d
-nmi
```

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. La seguente tabella mostra gli argomenti per le opzioni.

Tabella 16. comando fuelg

La seguente tabella multiriga a tre colonne contiene le opzioni, le descrizioni delle opzioni e i valori associati per le opzioni.

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.	input, output
-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

Tabella 16. comando fuelg (continua)

Opzione	Descrizione	Valori
-period	Un valore numerico per visualizzare la cronologia (1, 6, 12, 24 ore)	valore numerico in ore
-pm	Impostare la modalità dei criteri per la perdita di alimentazione ridondante.	• **bt** - base con limitazione • **rt** - ridondante con limitazione (predefinita) • **ort** - ridondante N_1 con limitazione
-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
-perf	Visualizza l'utilizzo corrente dell'elaborazione, inclusi sistema, microprocessore e I/O.	percentuale
-pc	Visualizza il consumo di energia corrente	• **output** - visualizza il consumo corrente di energia CC. Per i server rack e tower includerà il consumo energetico del sistema, della CPU, della memoria e di altri componenti. Per i server blade ITE includerà solo il consumo energetico del sistema. • **input** - visualizza il consumo corrente di energia in ingresso, incluso il consumo energetico del sistema.

Sintassi:
```
fuelg [options]
option:
  -pme on|off
  -pcapmode input|output
  -pcap
  -history
  -period
  -pm bt|r|rt
  -zm on|off
  -perf
  -pc input|output
```

Esempio:
```
system> fuelg
-pme: on
system>
```

comando pxeboot

Questo comando visualizza e imposta la condizione di Preboot eXecution Environment.

L'esecuzione di **pxeboot** senza opzioni restituisce l'impostazione di Preboot eXecution Environment corrente. La seguente tabella mostra gli argomenti per le opzioni.

Tabella 17. comando pxeboot

La seguente tabella a riga singola con tre colonne contiene l'opzione, la descrizione dell'opzione e i valori associati per l'opzione.

Tabella 17. comando pxeboot (continua)

Opzione	Descrizione	Valori
-en	Imposta la condizione di Preboot eXecution Environment per il successivo riavvio del sistema.	abilitato, disabilitato

Sintassi:
```
pxeboot [options]
option:
  -en state
```

Esempio:
```
system> pxeboot
-en disabled
system>
```

Comando serial redirect

Questo argomento contiene il comando serial redirect.

Esiste solo un comando di reindirizzamento seriale: "comando console" a pagina 129.

comando console

Questo comando viene utilizzato per avviare una sessione della console per il reindirizzamento seriale.

Utilizzare il comando **console** per avviare una sessione della console per il reindirizzamento seriale sulla porta seriale designata di IMM.

Sintassi:
```
console 1
```

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.

Se il comando **accseccfg** viene eseguito senza opzioni, saranno visualizzate le informazioni sulla sicurezza di tutti gli account. La seguente tabella mostra gli argomenti per le opzioni.

Tabella 18. comando accseccfg

La seguente tabella multiriga a tre colonne contiene le opzioni, le descrizioni delle opzioni e i valori associati per le opzioni.

Tabella 18. comando accseccfg (continua)

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
-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

Syntax:

```
accseccfg [options]
option:
   -legacy
   -high
   -custom
   -am authentication methoc
   -lp lockout_period
   -pe time_period
   -pr state
   -pc state
   -pd number_characters
   -pl number_characters
   -ci minimum_interval
   -lf number_failures
   -chgnew state
   -rc reuse_cycle
   -wt timeout
```

Esempio:

```
system> accseccfg
-legacy
```

```
-am local
-lp 2
-pe 0
-pr off
-pd 1
-pl 4
-ci 0
-lf 0
-chgnew off
-rc 0
-wt user
system>
```

comando alertcfg

Utilizzare questo comando per visualizzare e configurare i parametri globali di avviso remoto di IMM.

Se il comando **alertcfg** viene eseguito senza opzioni, saranno visualizzati tutti i parametri globali di avviso remoto. La seguente tabella mostra gli argomenti per le opzioni.

Tabella 19. comando alertcfg

La seguente tabella multiriga a tre colonne contiene le opzioni, le descrizioni delle opzioni e i valori associati per le opzioni.

Opzione	Descrizione	Valori
-dr	Imposta il tempo di attesa tra nuovi tentativi prima che IMM invii di nuovo un avviso.	Da 0 a 4 minuti, in incrementi da 0,5 minuti
-da	Imposta il tempo di attesa prima che IMM invii un avviso al destinatario successivo nell'elenco.	Da 0 a 4 minuti, in incrementi da 0,5 minuti
-rl	Imposta il numero di tentativi aggiuntivi di invio di un avviso da parte di IMM, se i tentativi precedenti non sono riusciti.	Da 0 a 8

Sintassi:

```
alertcfg [options]
  options:
   -rl retry_limit
   -dr retry_delay
   -da agent_delay
```

Esempio:

```
system>alertcfg
-dr 1.0
-da 2.5
-rl 5
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 abbiano effetto, il sistema host dovrà essere riavviato.

La seguente tabella riporta un sottoinsieme di comandi che possono essere utilizzati con il comando **asu**.

Tabella 20. comando asu

La seguente tabella multiriga a tre colonne contiene un sottoinsieme di comandi che possono essere utilizzati in combinazione con il comando **asu**. Sono forniti i dati descrittivi e i valori associati per i comandi.

Comando	Descrizione	Valore
delete	Utilizzare questo comando per eliminare un'istanza o un record di un'impostazione. L'impostazione deve essere un'istanza che consenta l'eliminazione, ad esempio iSCSI. AttemptName.1.	*setting_instance*
informazioni utili	Utilizzare questo comando per visualizzare le informazioni sulla guida per una o più impostazioni.	*impostazione*
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 value*
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.	*impostazione*
show	Utilizzare questo comando per visualizzare il valore corrente di una o più impostazioni.	*impostazione*
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.	*impostazione*
Nota: • Nella sintassi del comando, *setting* è il nome di un'impostazione che si desidera visualizzare o modificare e *value* è il valore di tale impostazione. • *Setting* può essere più di un nome, tranne nel caso in cui si utilizzi il comando **set**. • *Setting* può contenere caratteri jolly, ad esempio un asterisco (*) o un punto interrogativo (?). • *Setting* può essere un gruppo, il nome di un'impostazione o **all**.		

Nel seguente elenco sono riportati alcuni esempi di sintassi per il comando **asu**:

- Per visualizzare tutte le opzioni del comando asu, immettere `asu --help`.
- Per visualizzare la guida dettagliata di tutti i comandi, immettere `asu -v --help`.
- Per visualizzare la guida dettagliata di un comando, immettere `asu -v set --help`.
- Per modificare un valore, immettere `asu set` *setting value*.
- Per visualizzare il valore corrente, immettere `asu show` *setting*.
- Per visualizzare le impostazioni in formato batch lungo, immettere `asu show -l -b all`
- Per visualizzare tutti i valori possibili per un'impostazione, immettere `asu showvalues` *setting*. 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>
```

La seguente tabella mostra gli argomenti per le opzioni.

Tabella 21. 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**.	
--help[1]	Visualizza la guida per il comando. L'opzione --help viene inserita dopo il comando, ad esempio **asu show --help**.	
-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 22. 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 di backup

Utilizzare questo comando di backup per creare un file di backup contenente le impostazioni di sicurezza del sistema corrente.

La seguente tabella mostra gli argomenti per le opzioni.

Tabella 23. comando di backup

La seguente tabella multiriga a tre colonne contiene le opzioni, le descrizioni delle opzioni e i valori associati per le opzioni.

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
-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
-fd	Nome file per la descrizione XML dei comandi CLI di backup	Nome file valido

Sintassi:

```
backup [options]
  option:
   -f    filename
   -pp   password
   -ip   ip address
   -pn   port number
   -u    username
   -pw   password
   -fd   filename
```

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 eth0
```

Example:

```
system> dhcpinfo eth0
   -server :  10.240.0.10
   -n      :  XCC-7X19-123456789A
   -i      :  10.243.4.66
   -i6     :  ::
   -g      :  10.243.0.1
   -s      :  255.255.240.0
   -d      :  labs.lenovo.com
   -d6     :
   -dns1   :  10.240.0.10
   -dns2   :  10.240.0.11
   -dns3   :  0.0.0.0
   -dns61  :  ::
   -dns62  :  ::
   -dns63  :  ::
```

La seguente tabella descrive l'output dall'esempio.

Tabella 24. comando dhcpinfo

La seguente tabella multiriga a due colonne descrive le opzioni utilizzate nell'esempio precedente.

Opzione	Descrizione
-server	Il server DHCP che ha assegnato la configurazione
-n	Nome host assegnato
-i	Indirizzo IPv4 assegnato
-g	Indirizzo gateway assegnato
-s	Maschera di sottorete assegnata
-d	Nome di dominio 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
-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.

Nota: In un sistema Flex System le impostazioni DNS non possono essere modificate in IMM. Le impostazioni DNS sono gestite dal modulo CMM.

Se si esegue il comando **dns** senza opzioni, saranno visualizzate tutte le informazioni sulla configurazione DNS. La seguente tabella mostra gli argomenti per le opzioni.

Tabella 25. comando dns

La seguente tabella multiriga a tre colonne contiene le opzioni, le descrizioni delle opzioni e i valori associati per le opzioni.

Opzione	Descrizione	Valori
-state	Stato DNS	on, off
-ddns	Stato DDNS	abilitato, disabilitato
-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.
-p	Priorità IPv4/IPv6	ipv4, ipv6

Sintassi:
```
dns [options]
option:
  -state state
  -ddns state
  -i1 first_ipv4_ip_address
  -i2 second_ipv4_ip_address
  -i3 third_ipv4_ip_address
  -i61 first_ipv6_ip_address
  -i62 second_ipv6_ip_address
  -i63 third_ipv6_ip_address
  -p priority
```

Nota: Il seguente esempio mostra una configurazione di IMM su cui è disabilitato DNS.

Esempio:
```
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>
```
La seguente tabella descrive le opzioni utilizzate nell'esempio precedente.

Tabella 26. emissione del comando dns

La seguente tabella multiriga a due colonne descrive le opzioni utilizzate nell'esempio precedente.

Tabella 26. emissione del comando dns (continua)

Opzione	Descrizione
-state	Stato del DNS (`on` o `off`)
-i1	Indirizzo IP del server DNS IPv4 primario
-i2	Indirizzo IP del server DNS IPv4 secondario
-i3	Indirizzo IP del server DNS IPv4 terziario
-i61	Indirizzo IP del server DNS IPv6 primario
-i62	Indirizzo IP DNS IPv6 secondario
-i63	Indirizzo IP del server DNS IPv6 terziario
-ddns	Stato del DDNS (`enabled` o `disabled`)
-dnsrc	Nome di dominio DDNS preferito (`dhcp` o `manual`)
-ddn	DDN specificato manualmente
-ddncur	DDN corrente (sola lettura)
-p	Server DNS preferiti (`ipv4` o `ipv6`)

Comando encaps

Utilizzare questo comando per consentire a BMC di uscire dalla modalità di incapsulamento.

La seguente tabella mostra gli argomenti per le opzioni.

Tabella 27. Comando encaps

La seguente tabella a una riga e due colonne contiene le opzioni e le relative descrizioni.

Opzione	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 su USB.

Il comando consente di associare un numero di porta Ethernet esterna a un numero di porta differente per Ethernet su USB.

L'esecuzione del comando **ethtousb** senza opzioni visualizza le informazioni su Ethernet su USB. La seguente tabella mostra gli argomenti per le opzioni.

Tabella 28. comando ethtousb

La seguente tabella multiriga a tre colonne contiene le opzioni, le descrizioni delle opzioni e i valori associati per le opzioni.

Tabella 28. comando ethtousb (continua)

Opzione	Descrizione	Valori
-en	Stato Ethernet su USB	abilitato, disabilitato
-m*x*	Configura l'associazione delle porte per l'indice *x*	Coppia di porte, separate da due punti (:), in formato *porta1:porta2* 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 su USB.
-rm	Rimuove l'associazione della porta per l'indice specificato	Da 1 a 10 Gli indici di associazione della porta vengono visualizzati utilizzando il comando **ethtousb** senza opzioni.

Sintassi:
```
ethtousb [options]
option:
  -en state
  -mxport_pair
  -rm map_index
```

Esempio:
```
system> ethtousb  -en enabled -m1 100:200 -m2 101:201
system> ethtousb
 -en enabled
 -m1 100:200
 -m2 101:201
system> ethtousb -rm 1
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.

La seguente tabella mostra gli argomenti per le opzioni.

Tabella 29. Comando firewall

La seguente tabella multiriga a tre colonne contiene le opzioni e le relative descrizioni.

Opzione	Descrizione	Valori
-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.
-bbd	Blocca la data di inizio	Data con formato <AAAA-MM-GG>
-bed	Blocca la data di fine	Data con formato <AAAA-MM-GG>

Tabella 29. Comando firewall (continua)

Opzione	Descrizione	Valori
-bbt	Blocca l'ora di inizio	Ora con formato <HH:MM>
-bet	Blocca l'ora data di fine	Ora con formato <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
-iplf	Numero massimo di errori di login prima che l'indirizzo IP sia bloccato. **Nota:** Se questo valore non è 0, deve essere maggiore di o uguale a <Numero massimo di errori di login> impostato da <*accseccfg -lf*>	Valore numerico compreso tra 0 e 32, 0 = nessun blocco
-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

Esempio:

```
· “firewall”: Show all options’ value and IP addresses blocking list.
· “firewall -bips  192.168.1.1,192.168.1.0/24,192.168.1.1-192.168.1.5”: Block the access from multi IPs
· “firewall -bti 01:00-02:00,05:05-10:30,14:15-20:00”: Block all access during 01:00-02:00,05:05-10:30,14:15-20:00 every day.
· “firewall –clr all”: Clear all rules of “Block List and Time Restriction”.
· “firewall -iplp 60”:Set IP address lockout period to 60 minutes.
· “firewall -iplf 5”:Set maximum number of login failures to 5 timesi.
· “firewall -ipbl -del 192.168.100.1”:Delete 192.168.100.1 from IP address blocking list.
· “firewall –ipbl -del 3fcc:1234::2”:Delete 3fcc:1234::2 from IP address blocking list.
· “firewall –ipbl –clrall”:  Delete all blocking IP addresses.
· “firewall –ipbl –show”:    Show all blocking IP addresses.
```

comando gprofile

Utilizzare questo comando per visualizzare e configurare i profili di gruppo per IMM.

La seguente tabella mostra gli argomenti per le opzioni.

Tabella 30. comando gprofile

La seguente tabella multiriga a tre colonne contiene le opzioni, le descrizioni delle opzioni e i valori associati per le opzioni.

Tabella 30. comando gprofile (continua)

Opzione	Descrizione	Valori
-clear	Elimina un gruppo	abilitato, disabilitato
-n	Il nome del gruppo	Una stringa contenente fino a 63 caratteri per *group_name*. Il valore *group_name* deve essere univoco.
-a	Livello di autorizzazione basata su ruoli	supervisore, operatore, rbs <elenco ruoli>: nsc|am|rca|rcvma|pr|bc|cel|ac I valori dell'elenco di ruoli sono specificati utilizzando un elenco di valori separati da una barra verticale.
-h	Visualizza le opzioni e l'uso del comando	

Sintassi:
```
gprofile [1 - 16 group_profile_slot_number] [options]
options:
-clear state
-n  group_name
-a  authority level:
    -nsc network and security
    -am user account management
    -rca remote console access
    -rcvma remote console and remote disk access
    -pr remote server power/restart access
    -bc basic adapter configuration
    -cel ability to clear event logs
    -ac advanced adapter configuration
-h help
```

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.

La seguente tabella mostra gli argomenti per le opzioni.

Tabella 31. comando hashpw

La seguente tabella multiriga a tre colonne contiene le opzioni, le descrizioni delle opzioni e i valori associati per le opzioni.

Opzione	Descrizione	Valori
-sw	Stato dello switch della password di terze parti	abilitato, disabilitato
-re	Stato di lettura della password di terze parti **Nota:** La lettura può essere impostata se lo switch è abilitato.	abilitato, disabilitato

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.

Digitare `ifconfig eth0` per visualizzare la configurazione dell'interfaccia Ethernet corrente. 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.

Nota: In un sistema Flex System le impostazioni VLAN sono gestite da un CMM Flex System e non possono essere modificate da IMM.

La seguente tabella mostra gli argomenti per le opzioni.

Tabella 32. comando ifconfig

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	Indirizzo MAC integrato (di sola lettura e non configurabile)	
-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)
-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.
-r	Velocità di trasferimento dati	10, 100, auto
-d	Modalità duplex	full, half, auto
-m	MTU	Valore numerico compreso tra 60 e 1.500.
-l	LAA	Formato dell'indirizzo MAC. Gli indirizzi multicast non sono consentiti (il primo byte deve essere pari).
-dn	Nome di dominio	Il nome di dominio in formato valido.
-auto	L'impostazione di autonegoziazione, che determina se le impostazioni della velocità di trasferimento dati e della rete duplex possono essere configurate	true, false
-ghn	Consente di ottenere il nome host da DHCP	disabled, enabled

Tabella 32. comando ifconfig (continua)

Opzione	Descrizione	Valori
-nic	Modalità NIC dello switch[1]	shared, dedicated, shared:nixX[2]
-failover[2]	Modalità failover	none, shared, shared:nicX
-nssync[3]	Sincronizzazione delle impostazioni di rete	abilitato, disabilitato
-address_table	Tabella di indirizzi IPv6 generati automaticamente e delle lunghezze dei relativi prefissi **Nota:** L'opzione è visibile solo se sono abilitati IPv6 e la configurazione automatica senza stato.	Questo valore è di sola lettura e non è configurabile.
-ipv6	Stato IPv6	disabled, enabled
-lla	Indirizzo locale del collegamento **Nota:** L'indirizzo locale del collegamento viene visualizzato solo se è abilitato IPv6.	Questo indirizzo locale del collegamento è determinato da IMM. Questo valore è di sola lettura e non è configurabile.
-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	Stato DHCPv6	abilitato, disabilitato
-sa6	Stato di configurazione automatica senza stato IPv6	abilitato, disabilitato
-vlan	Abilita o disabilita l'etichettatura VLAN	abilitato, disabilitato
-vlanid	Etichetta di identificazione del pacchetto di rete per IMM	Valore numerico compreso tra 1 e 4.094.

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:nicX 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 di failover indicherà a IMM di passare alla porta di rete condivisa, se la porta dedicata 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.

Sintassi:
```
ifconfig eth0 [options]
```

options:

-state *interface_state*
-c *config_method*
-i *static_ipv4_ip_address*
-g *ipv4_gateway_address*
-s *subnet_mask*
-n *hostname*
-r *data_rate*
-d *duplex_mode*
-m *max_transmission_unit*
-l *locally_administered_MAC*
-b *burned_in_MAC_address*
-dn *domain_name*
-auto *state*
-nic *state*
-failover mode
-nssync *state*
-address_table
-lla ipv6_link_local_addr
-dhcp6 *state*
-ipv6 *state*
-ipv6static *state*
-sa6 *state*
-i6 *static_ipv6_ip_address*
-g6 *ipv6_gateway_address*
-p6 *length*
-vlan *state*
-vlanid *VLAN ID*

Esempio:

```
system> ifconfig eth0
-state    :   enabled
-c        :   dthens
-ghn      :   disabled
-i        :   192.168.70.125
-g        :   0.0.0.0
-s        :   255.255.255.0
-n        :   IMM00096B9E003A
-auto     :   true
-r        :   auto
-d        :   auto
-vlan     :   disabled
-vlanid   :   1
-m        :   1500
-b        :   00:09:6B:9E:00:3A
-l        :   00:00:00:00:00:00
-dn       :
-ipv6     :   enabled
-ipv6static :   disabled
-i6       :   ::
-p6       :   64
-g6       :   ::
-dhcp6    :   enabled
-sa6      :   enabled
-lla      :   fe80::6eae:8bff:fe23:91ae
-nic :   shared:nic3
      nic1: dedicate
      nic2: ext card slot #3
      nic3: ext card slot #5  [active]
-address_table    :
```

```
system> ifconfig eth0 -c static -i 192.168.70.133
These configuration changes will become active after the next reset of the IMM.
```

comando keycfg

Utilizzare questo comando per visualizzare, aggiungere o eliminare le chiavi di attivazione.

Le chiavi di attivazione controllano l'accesso alle funzioni IMM facoltative.

Nota:

- 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.
- 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.

La seguente tabella mostra gli argomenti per le opzioni.

Tabella 33. comando keycfg

La seguente tabella multiriga a tre colonne contiene le opzioni, le descrizioni delle opzioni e i valori associati per le opzioni.

Opzione	Descrizione	Valori
-add	Aggiunge la chiave di attivazione	Valori per le opzioni dei comandi -ip, -pn, -u, -pw e -f
-ip	Indirizzo IP del server TFTP con la chiave di attivazione da aggiungere	Indirizzo IP valido per il server TFTP
-pn	Numero di porta per il server TFTP/SFTP con la chiave di attivazione da aggiungere	Numero di porta valido per il server TFTP/SFTP (valore predefinito 69/22)
-u	Nome utente per il server SFTP con la chiave di attivazione da aggiungere	Nome utente valido per il server SFTP
-pw	Password per il server SFTP con la chiave di attivazione da aggiungere	Password valida per il server SFTP
-f	Nome file per la chiave di attivazione da aggiungere	Nome file valido per il file della chiave di attivazione
-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

Sintassi:

```
keycfg [options]
option:
```

```
-add
   -ip tftp/sftp server ip address
   -pn pn port number of tftp/sftp server (default 69/22)
   -u  username for sftp server
   -pw password for sftp server
   -f  filename
   -del   n ( where n is a valid ID number from listing)
   -deltype x ( where x is a Type value)
```

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.

La seguente tabella mostra gli argomenti per le opzioni.

Tabella 34. comando ldap

La seguente tabella multiriga a tre colonne contiene le opzioni, le descrizioni delle opzioni e i valori associati per le opzioni.

Opzione	Descrizione	Valori
-a	Metodo di autenticazione utente	Solo locale, solo LDAP, prima locale quindi LDAP, prima LDAP quindi locale
-aom	Modalità sola autenticazione	abilitato, disabilitato
-b	Metodo di collegamento	anonimo, collegamento con DN e password del client, collegamento con 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*
-f	Filtro di gruppi	Stringa contenente un massimo di 127 caratteri per *group_filter*
-fn	Nome forest	Per ambienti di Active Directory. Stringa contenente un massimo di 127 caratteri.
-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.

Tabella 34. comando ldap (continua)

Opzione	Descrizione	Valori
-ep	Password crittografata	Password di ripristino/backup (solo per uso interno)
-r	Nome distinto voce radice	Stringa contenente un massimo di 127 caratteri per *root_dn*
-rbs	Sicurezza avanzata basata sui ruoli per gli utenti di Active Directory	abilitato, disabilitato
-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*
-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*
-t	Nome destinazione server	Se è abilitata l'opzione rbs, questo campo specifica il nome di una destinazione che può essere associata a uno o più ruoli sul server Active Directory mediante lo strumento Snap-in RBS (Role-Based Security).
-u	Attributo di ricerca UID	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	

Sintassi:

```
ldap [options]
options:
   -a loc|ldap|locld|ldloc
   -aom enable/disabled
   -b anon|client|login
   -c client_dn
   -d search_domain
   -f group_filter
   -fn forest_name
   -g group_search_attr
   -l string
   -p client_pw
   -pc confirm_pw
   -ep encrypted_pw
   -r root_dn
   -rbs enable|disabled
```

-s1ip *host name/ip_addr*
-s2ip *host name/ip_addr*
-s3ip *host name/ip_addr*
-s4ip *host name/ip_addr*
-s1pn *port_number*
-s2pn *port_number*
-s3pn *port_number*
-s4pn *port_number*
-t *name*
-u *search_attrib*
-v *off|on*
-h

comando ntp

Utilizzare questo comando per visualizzare e configurare il protocollo NTP (Network Time Protocol).

La seguente tabella mostra gli argomenti per le opzioni.

Tabella 35. comando ntp

La seguente tabella multiriga a tre colonne contiene le opzioni, le descrizioni delle opzioni e i valori associati per le opzioni.

Opzione	Descrizione	Valori
-en	Abilita o disabilita il protocollo NTP (Network Time Protocol).	abilitato, disabilitato
-i[1]	Nome o indirizzo IP del server NTP (Network Time Protocol). Questo è il numero di indice del server NTP (Network Time Protocol).	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.
-f	La frequenza (in minuti) con cui l'orologio di 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.

1. -i è uguale a i1.

Sintassi:
```
ntp [options]
options:
-en state
-i  hostname/ip_addr
-f  frequency
-synch
```

Esempio:
```
system> ntp
-en: disabled
-f: 3 minutes
-i: not set
```

comando portcfg

Utilizzare questo comando per configurare IMM per la funzione di reindirizzamento seriale.

IMM deve essere configurato in modo che corrisponda alle impostazioni della porta seriale interna del server. Per modificare la configurazione della porta seriale, immettere le opzioni seguite dai valori. Per modificare questa configurazione, è necessario disporre almeno dell'autorizzazione Configurazione sicurezza e networking adattatore.

Nota: La porta seriale esterna del server può essere utilizzata da IMM solo per la funzionalità IPMI. La CLI non è supportata attraverso la porta seriale. Le opzioni **serred** e **cliauth** che erano presenti nella CLI di Remote Supervisor Adapter II non sono supportate.

L'esecuzione del comando **portcfg** senza opzioni visualizza la configurazione della porta seriale. La seguente tabella mostra gli argomenti per le opzioni.

Nota: Il numero di bit di dati (8) è impostato nell'hardware e non può essere modificato.

Tabella 36. comando portcfg

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	Velocità in baud	9600, 19200, 38400, 57600, 115200
-p	Parità	none, odd, even
-s	Bit di arresto	1, 2
-climode	Modalità CLI	0, 1, 2 Dove: • 0 = none: la CLI è disabilitata • 1 = cliems: la CLI è abilitata con sequenze di tasti compatibili con EMS • 2 = cliuser: la CLI è abilitata con sequenze di tasti definite dall'utente

Sintassi:

```
portcfg [options]
 options:
   -b baud_rate
   -p parity
   -s stopbits
   -climode mode
```

Esempio:

```
system> portcfg
-b: 57600
-climode: 2 (CLI with user defined keystroke sequence)
-p: even
-s: 1
system> portcfg -b 38400
ok
system>
```

comando portcontrol

Utilizzare questo comando per attivare o disattivare una porta di servizio di rete.

Attualmente questo comando supporta solo il controllo della porta per il protocollo IPMI. Digitare **portcontrol** per visualizzare lo stato della porta IPMI. Per abilitare o disabilitare la porta di rete IPMI, digitare l'opzione **-ipmi** seguita dai valori **on** o **off** .

Tabella 37. comando portcontrol

La seguente tabella multiriga a tre colonne contiene le opzioni, le descrizioni delle opzioni e i valori associati per le opzioni.

Opzione	Descrizione	Valori
-all	Abilita o disabilita tutte le interfacce e i protocolli di rilevamento	on, off
-cim	Abilita o disabilita il rilevamento CIM	on, off
-ipmi	Abilita o disabilita l'accesso ipmi tramite LAN	on, off
-ipmi-kcs	Abilita o disabilita l'accesso ipmi dal server	on, off
-rest	Abilita o disabilita il rilevamento REST	on, off
-slp	Abilita o disabilita il rilevamento SLP	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

Sintassi:

```
portcontrol [options]
 options:
   -ipmi on/off
```

Esempio:

```
system> portcontrol
cim : on
ipmi : on
ipmi-kcs : on
rest : on
slp : on
snmp : off
ssdp : on
cli : on
web : on
```

comando ports

Utilizzare questo comando per visualizzare e configurare le porte di IMM.

L'esecuzione del comando **ports** senza opzioni visualizza le informazioni per tutte le porte di IMM. La seguente tabella mostra gli argomenti per le opzioni.

Tabella 38. comando ports

La seguente tabella multiriga a tre colonne contiene le opzioni, le descrizioni delle opzioni e i valori associati per le opzioni.

Opzione	Descrizione	Valori
-open	Visualizza le porte aperte	
-reset	Reimposta le porte sulle impostazioni predefinite	
-httpp	Numero di porta HTTP	Numero di porta predefinito: 80
-httpsp	Numero di porta HTTPS	Numero di porta predefinito: 443
-sshp	Numero di porta della CLI legacy SSH	Numero di porta predefinito: 22
-snmpap	Numero di porta agent SNMP	Numero di porta predefinito: 161
-snmptp	Numero di porta trap SNMP	Numero di porta predefinito: 162
-rpp	Numero di porta presenza remota	Numero di porta predefinito: 3900
-cimhp	Numero di porta CIM su HTTP	Numero di porta predefinito: 5988
-cimhsp	Numero di porta CIM su HTTPS	Numero di porta predefinito: 5989

Sintassi:

```
ports [options]
option:
  -open
  -reset
  -httpp port_number
  -httpsp port_number
  -sshp port_number
  -snmpap port_number
  -snmptp port_number
  -rpp port_number
  -cimhp port_number
  -cimhsp port_number
```

Esempio:

```
system> ports
-httpp 80
-httpsp 443
-rpp 3900
-snmpap 161
-snmptp 162
-sshp 22
-cimhp 5988
-cimhsp 5989
system>
```

comando rdmount

Utilizzare questo comando per montare immagini del disco remoto o condivisioni di rete

La seguente tabella mostra gli argomenti per le opzioni.

Tabella 39. Comando rdmount

La seguente tabella multiriga a due colonne contiene le opzioni e le relative descrizioni.

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.

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.

La seguente tabella mostra gli argomenti per le opzioni.

Tabella 40. comando restore

La seguente tabella multiriga a tre colonne contiene le opzioni, le descrizioni delle opzioni e i valori associati per le opzioni.

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
-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

Sintassi:
```
restore [options]
option:
  -f filename
  -pp password
  -ip ip_address
  -pn port_number
username
  -pw password
```

Esempio:
```
system> restore f xcc-back.cli pp xxxxxx ip 192.168.70.200
ok
system>
```

comando restoredefaults

Utilizzare questo comando per ripristinare tutti i valori predefiniti originali di IMM.

- Non esiste alcuna opzione per il comando **restoredefaults**.
- Verrà richiesto di confermare il comando prima che questo venga elaborato.

Sintassi:
```
restoredefaults
```

Esempio:
```
system> restoredefaults

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 roles

Utilizzare questo comando per visualizzare o configurare i ruoli.

La seguente tabella mostra gli argomenti per le opzioni.

Tabella 41. comando roles

La seguente tabella multiriga a tre colonne contiene le opzioni, le descrizioni delle opzioni e i valori associati per le opzioni.

Opzione	Descrizione	Valori
-n	Ruolo da configurare	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 (supporti virtuali) • **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	

Sintassi

```
   roles [-options] - display/configure roles
   - role_account -role number[3-31]
options:
   -n        - role name (limited to 32 characters)
   -p        - privilege (custom:am|rca|rcvma|pr|cel|bc|nsc|ac|us)
      am     - User account management access
      rca    - Remote console access
      rcvma  - Remote console and remote disk (virtual media) access
      pr     - Remote server power/restart access
      cel    - Ability to clear event logs
      bc     - Adapter Configuration (basic)
      nsc    - Adapter Configuration (network and security)
      ac     - Adapter Configuration (advanced)
      us     - UEFI Security
      Note: the above custom permission flags can be used in any combination
   -d        - delete a row
```

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 seccfg

Utilizzare questo comando eseguire il rollback del firmware.

La seguente tabella mostra gli argomenti per le opzioni.

Tabella 42. Comando seccfg

La seguente tabella multiriga a due colonne contiene le opzioni e le relative descrizioni.

Opzione	Descrizione	Valore
-fwrb	Consente di eseguire il rollback del firmware alle versioni precedenti	yes, no
-aubp	Abilita o disabilita la funzione di backup automatico per la promozione primaria	abilitato, disabilitato

comando set

Utilizzare questo comando per modificare alcune impostazioni di IMM.

- Alcune impostazioni di 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 43. comando set

La seguente tabella a riga singola con tre colonne contiene la descrizione dei comandi e le informazioni associate.

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 smtp

Utilizzare questo comando per visualizzare e configurare le impostazioni per l'interfaccia SMTP.

L'esecuzione del comando **SMTP** senza opzioni visualizza tutte le informazioni sull'interfaccia SMTP. La seguente tabella mostra gli argomenti per le opzioni.

Tabella 44. comando smtp

La seguente tabella multiriga a tre colonne contiene le opzioni, le descrizioni delle opzioni e i valori associati per le opzioni.

Opzione	Descrizione	Valori
-auth	Supporto di autenticazione SMTP	abilitato, disabilitato
-authepw	Password crittografata per l'autenticazione SMTP	Stringa password valida
-authmd	Metodo di autenticazione SMTP	CRAM-MD5, LOGIN
-authn	Nome utente di autenticazione SMTP	Stringa (massimo 256 caratteri)
-authpw	Password di autenticazione SMTP	Stringa (massimo 256 caratteri)
-pn	Numero di porta SMTP	Numero di porta valido
-s	Nome host o indirizzo IP del server SMTP	Nome host o indirizzo IP valido (massimo 63 caratteri)

Sintassi:
```
smtp [options]
option:
  -auth enabled|disabled
  -authepw password
  -authmd CRAM-MD5|LOGIN
  -authn username
  -authpw password
  -s ip_address_or_hostname
  -pn port_number
```

Esempio:
```
system> smtp
-s test.com
-pn 25
system>
```

comando snmp

Utilizzare questo comando per visualizzare e configurare le informazioni sull'interfaccia SNMP.

L'esecuzione del comando **snmp** senza opzioni visualizza tutte le informazioni sull'interfaccia SNMP. La seguente tabella mostra gli argomenti per le opzioni.

Tabella 45. comando snmp

La seguente tabella multiriga a tre colonne contiene le opzioni, le descrizioni delle opzioni e i valori associati per le opzioni.

Tabella 45. comando snmp (continua)

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.
-t1	Trap SNMPv1	on, off
-t2	Trap SNMPv2	on, off
-t	Trap SNMPv3	on, off
-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 "".
-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 "".
-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 "".
-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 "".
-ci	Nome host/indirizzo IP della comunità SNMP	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 45. comando snmp (continua)

Opzione	Descrizione	Valori
-cti	Indirizzo IP/nome host della comunità del trap SNMPv2	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.
-eid	ID motore SNMP	Stringa (massimo 1-27 caratteri)

Sintassi:
```
snmp [options]
option:
 -a3 state
  -t state
  -l location
  -cn contact_name
  -t1 state
  -c community name
  -ci community IP address/hostname
  -t2 state
  -ct community name
  -cti community IP address/hostname
  -eid engine id
```

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.

L'esecuzione di **snmpalerts** senza opzioni visualizza tutte le impostazioni degli avvisi SNMP. La seguente tabella mostra gli argomenti per le opzioni.

Tabella 46. comando snmpalerts

La seguente tabella multiriga a tre colonne contiene le opzioni, le descrizioni delle opzioni e i valori associati per le opzioni.

Tabella 46. comando snmpalerts (continua)

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 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
-crten	Invia avvisi di eventi critici	abilitato, disabilitato
-wrn	Imposta gli eventi di avvertenza che inviano gli avvisi	all, none, custom:rp|te|vo|po|fa|cp|me|ot 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
-wrnen	Invia avvisi di eventi di avvertenza	abilitato, disabilitato

Tabella 46. comando snmpalerts (continua)

Opzione	Descrizione	Valori
-sys	Imposta gli eventi di routine che inviano gli avvisi	all, none, custom:lo|tio|ot|po|bf|til|pf|el|ne 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
-sysen	Invia avvisi di eventi di routine	abilitato, disabilitato

Sintassi:
```
snmpalerts [options]
   options:
     -status status
     -crt event_type
     -crten state
     -wrn event_type
     -wrnen state
     -sys event_type
     -sysen state
```

comando srcfg

Utilizzare questo comando al fine di indicare la sequenza di tasti per accedere alla CLI dalla modalità di reindirizzamento seriale.

Per modificare la configurazione di reindirizzamento seriale, immettere le opzioni seguite dai valori. Per modificare questa configurazione, è necessario disporre almeno dell'autorizzazione Configurazione sicurezza e networking adattatore.

Nota: L'hardware di IMM non fornisce una funzione pass-through da porta seriale a porta seriale. Pertanto le opzioni `-passthru` e `entercliseq` presenti nella CLI di Remote Supervisor Adapter II non sono supportate.

L'esecuzione del comando **srcfg** senza opzioni visualizza la sequenza di tasti di reindirizzamento seriale corrente. La seguente tabella riporta gli argomenti per l'opzione del comando `srcfg -entercliseq`.

Tabella 47. comando srcfg

La seguente tabella a riga singola con tre colonne contiene l'opzione, la descrizione dell'opzione e le informazioni sul valore per l'opzione.

Tabella 47. comando srcfg (continua)

Opzione	Descrizione	Valori
-entercliseq	Immettere una sequenza di tasti per la CLI	La sequenza di tasti definita dall'utente per accedere alla CLI. **Nota:** Questa sequenza deve essere formata da 1 a 15 caratteri. Il simbolo di accento circonflesso (^) ha un significato speciale in questa sequenza. Esso indica il tasto Ctrl per i tasti associati alle sequenze Ctrl (ad esempio, ^[per il tasto escape e ^M per il ritorno a capo). Tutte le occorrenze di ^ sono interpretate come parte di una sequenza Ctrl. Fare riferimento a una tabella di conversione da ASCII a tasti per un elenco completo delle sequenze Ctrl. Il valore predefinito per questo campo è ^[(che è Esc seguito da (.

Sintassi:
```
srcfg [options]
options:
-entercliseq entercli_keyseq
```

Esempio:
```
system> srcfg
-entercliseq ^[Q
system>
```

comando sshcfg

Utilizzare questo comando per visualizzare e configurare i parametri SSH.

L'esecuzione del comando **sshcfg** senza opzioni visualizza tutti i parametri SSH. La seguente tabella mostra gli argomenti per le opzioni.

Tabella 48. comando sshcfg

La seguente tabella multiriga a tre colonne contiene le opzioni, le descrizioni delle opzioni e i valori associati per le opzioni.

Opzione	Descrizione	Valori
-cstatus	Lo stato della CLI di SSH	abilitato, disabilitato
-hk gen	Genera la chiave privata del server SSH	
-hk rsa	Visualizza la chiave pubblica RSA del server	

Sintassi:
```
sshcfg [options]
option:
  -cstatus state
  -hk gen
  -hk rsa
```

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 ssl

Utilizzare questo comando per visualizzare e configurare i parametri SSL.

Per abilitare un client SSL, è necessario che sia installato un certificato client. L'esecuzione del comando **ssl** senza opzioni visualizza i parametri SSL. La seguente tabella mostra gli argomenti per le opzioni.

Tabella 49. comando ssl

La seguente tabella multiriga a tre colonne contiene le opzioni, le descrizioni delle opzioni e i valori associati per le opzioni.

Opzione	Descrizione	Valori
-ce	Abilita o disabilita un client SSL	on, off
-se	Abilita o disabilita un server SSL	on, off
-cime	Abilita o disabilita CIM su HTTPS sul server SSL	on, off

Sintassi:

```
portcfg [options]
 options:
  -ce state
  -se state
  -cime state
```

Parametri: i seguenti parametri sono presentati nella visualizzazione dello stato delle opzioni per il comando **ssl** e sono emessi solo dalla CLI:

Abilitazione trasporto sicuro server
Questa visualizzazione di stato è di sola lettura e non può essere impostata direttamente.

Stato chiave Web/CMD server
Questa visualizzazione di stato è di sola lettura e non può essere impostata direttamente. I valori di output possibili della riga comandi sono:

Chiave privata e cert/CSR non disponibili

Chiave privata e cert firmato dalla CA installati

Chiave privata e certificato autofirmato generato automaticamente installati

Chiave privata e certificato autofirmato installato

Chiave privata memorizzata, CSR disponibile per il download

Stato chiave CSR server SSL
Questa visualizzazione di stato è di sola lettura e non può essere impostata direttamente. I valori di output possibili della riga comandi sono:

Chiave privata e cert/CSR non disponibili

Chiave privata e cert firmato dalla CA installati

Chiave privata e certificato autofirmato generato automaticamente installati

Chiave privata e certificato autofirmato installato

Chiave privata memorizzata, CSR disponibile per il download

Stato chiave LDAP client SSL
Questa visualizzazione di stato è di sola lettura e non può essere impostata direttamente. I valori di output possibili della riga comandi sono:

Chiave privata e cert/CSR non disponibili

Chiave privata e cert firmato dalla CA installati

Chiave privata e certificato autofirmato generato automaticamente installati

Chiave privata e certificato autofirmato installato

Chiave privata memorizzata, CSR disponibile per il download

Stato chiave CSR client SSL

Questa visualizzazione di stato è di sola lettura e non può essere impostata direttamente. I valori di output possibili della riga comandi sono:

Chiave privata e cert/CSR non disponibili

Chiave privata e cert firmato dalla CA installati

Chiave privata e certificato autofirmato generato automaticamente installati

Chiave privata e certificato autofirmato installato

Chiave privata memorizzata, CSR disponibile per il download

comando sslcfg

Utilizzare questo comando per visualizzare e configurare SSL per IMM e gestire i certificati.

L'esecuzione del comando **sslcfg** senza opzioni visualizza tutte le informazioni di configurazione SSL. Il comando **sslcfg** viene utilizzato per generare una nuova chiave di crittografia e un certificato autofirmato o una richiesta di firma del certificato (CSR). La seguente tabella mostra gli argomenti per le opzioni.

Tabella 50. comando sslcfg

La seguente tabella multiriga a tre colonne contiene le opzioni, le descrizioni delle opzioni e i valori associati per le opzioni.

Opzione	Descrizione	Valori
-server	Stato server SSL	abilitato, disabilitato **Nota:** Il server SSL può essere abilitato solo se è presente un certificato valido.
-client	Stato client SSL	abilitato, disabilitato **Nota:** Il client SSL può essere abilitato solo se è presente un certificato client o server valido.
-cim	Stato CIM su HTTPS	abilitato, disabilitato **Nota:** CIM su HTTPS può essere abilitato solo se è presente un certificato server o client 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 50. comando sslcfg (continua)

Opzione	Descrizione	Valori
-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	Scarica file certificato	Questa opzione non utilizza alcun argomento ma è necessario specificare anche i valori per l'opzione dei comandi **-cert** o **-csr** (a seconda del tipo di certificato scaricato). Questa opzione non utilizza argomenti ma è necessario specificare anche i valori per l'opzione dei comandi **-i** e **-l** (facoltativa).
-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 3 nell'opzione del comando.
-c	Paese	Il codice paese (2 lettere) **Nota:** Obbligatorio quando si genera un certificato autofirmato o una CSR.
-sp	Stato o provincia	Stringa racchiusa tra virgolette (massimo 60 caratteri) **Nota:** Obbligatorio quando si genera un certificato autofirmato o una CSR.
-cl	Città o località	Stringa racchiusa tra virgolette (massimo 50 caratteri) **Nota:** Obbligatorio quando si genera un certificato autofirmato o una CSR.
-on	Nome organizzazione	Stringa racchiusa tra virgolette (massimo 60 caratteri) **Nota:** Obbligatorio quando si genera un certificato autofirmato o una CSR.
-hn	Nome host IMM	Stringa (massimo 60 caratteri) **Nota:** Obbligatorio quando si genera un certificato autofirmato o una CSR.
-cp	Contatto	Stringa racchiusa tra virgolette (massimo 60 caratteri) **Nota:** Facoltativo quando si genera un certificato autofirmato o una CSR.
-ea	Indirizzo e-mail della persona di contatto	Indirizzo e-mail valido (massimo 60 caratteri) **Nota:** Facoltativo quando si genera un certificato autofirmato o una CSR.
-ou	Unità organizzativa	Stringa racchiusa tra virgolette (massimo 60 caratteri) **Nota:** Facoltativo quando si genera un certificato autofirmato o una CSR.

Tabella 50. comando sslcfg (continua)

Opzione	Descrizione	Valori
-s	Cognome	Stringa racchiusa tra virgolette (massimo 60 caratteri) **Nota:** Facoltativo quando si genera un certificato autofirmato o una CSR.
-gn	Nome	Stringa racchiusa tra virgolette (massimo 60 caratteri) **Nota:** Facoltativo quando si genera un certificato autofirmato o una CSR.
-in	Iniziali	Stringa racchiusa tra virgolette (massimo 20 caratteri) **Nota:** Facoltativo quando si genera un certificato autofirmato o una CSR.
-dq	Qualificatore nome di dominio	Stringa racchiusa tra virgolette (massimo 60 caratteri) **Nota:** Facoltativo quando si genera un certificato autofirmato o una CSR.
-cpwd	Invalida password	Stringa (minimo 6 caratteri, massimo 30 caratteri) **Nota:** Facoltativo quando si genera una CSR.
-un	Nome non strutturato	Stringa racchiusa tra virgolette (massimo 60 caratteri) **Nota:** Facoltativo quando si genera una CSR.

Sintassi:

```
sslcfg [options]
option:
  -server state
  -client state
  -cim state
  -cert certificate_type
  -csr certificate_type
  -i ip_address
port number
user name
  -pw password
  -l filename
  -dnld
  -upld
  -tc xaction
  -c country_code
  -sp state_or_province
  -cl city_or_locality
  -on organization_name
  -hn bmc_hostname
  -cp contact_person
  -ea email_address
  -ou organizational_unit
  -s surname
  -gn given_name
  -in initials
  -dq dn_qualifier
  -cpwd challenge_password
  -un unstructured_name
```

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 CIM 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 Lenovo -hn XCC-5cf3fc6e0c9d
  -cp Contact -ea "" -ou""
  ok
  ```

L'esempio precedente viene visualizzato su più righe per limitazioni di spazio.

- 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 Lenovo -hn XCC-5cf3fc6e0c9d
  -cp Contact -ea "" -ou "
  ok
  ```

  L'esempio precedente viene visualizzato su più righe per limitazioni di spazio.

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 storekeycfg

Utilizzare questo comando per configurare il nome host o l'indirizzo IP e la porta di rete per un server SKLM.

È possibile configurare fino a quattro destinazioni server SKLM. Il comando **storekeycfg** può inoltre essere utilizzato per installare e rimuovere i certificati utilizzati da IMM per l'autenticazione al server SKLM.

La seguente tabella mostra gli argomenti per le opzioni.

Tabella 51. comando storekeycfg

La seguente tabella multiriga a tre colonne contiene le opzioni, le descrizioni delle opzioni e i valori associati per le opzioni.

Tabella 51. comando storekeycfg (continua)

Opzione	Descrizione	Valori
-add	Aggiunge la chiave di attivazione	I valori per le opzioni del comando sono -ip, -pn, -u, -pw e -f
-ip	Nome host o indirizzo IP del server TFTP/SFTP	Nome host o indirizzo IP valido del server TFTP/SFTP
-pn	Numero di porta del server TFTP o 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
-f	Nome file per la chiave di attivazione	Nome file valido per il nome file della chiave di attivazione
-del	Utilizzare questo comando per eliminare la chiave di attivazione in base al numero di indice	Numero di indice della chiave di attivazione valido dall'elenco keycfg
-dgrp	Aggiunge il gruppo di dispositivi	Nome del gruppo di dispositivi
-sxip	Aggiunge il nome host o l'indirizzo IP del server SKLM	Nome host o indirizzo IP valido del server SKLM; Valore numerico di 1, 2, 3 o 4
-sxpn	Aggiunge il numero di porta del server SKLM	Numero di porta valido per il server SKLM; Valore numerico di 1, 2, 3 o 4
-testx	Verifica la configurazione e la connessione al server SKLM	Valore numerico di 1, 2, 3 o 4
-h	Visualizza le opzioni e l'uso del comando	

Sintassi:

```
storekeycfg [options]
 options:
  -add state
  -ip ip_address
  -pn port_number
  -u username
  -pw password
  -f filename
  -del key_index
  -dgrp device_group_name
  -sxip ip_address
  -sxpn port_number
  -testx numeric value of SKLM server
  -h
```

Esempi:

Per importare il certificato server SKLM, immettere il seguente comando:

```
system> storekeycfg
add -ip 192.168.70.200 -f tklm-server.der
system> ok
```

Per configurare il numero di porta e l'indirizzo del server SKLM, digitare il seguente comando:

```
system> storekeycfg
-s1ip 192.168.70.249
system> ok
```

Per impostare il nome del gruppo di dispositivi, digitare il seguente comando:

```
system> storekeycfg
-dgrp IBM_SYSTEM_X_SED
system> ok
```

comando syncrep

Utilizzare questo comando per avviare la sincronizzazione del firmware dal repository remoto.

La seguente tabella mostra gli argomenti per le opzioni.

Tabella 52. comando syncrep

La seguente tabella multiriga a tre colonne contiene le opzioni, le descrizioni delle opzioni e i valori associati per le opzioni.

Opzione	Descrizione	Valori
-t	Protocollo di connessione del repository	samba, nfs
-l	Posizione del repository remoto	In formato URL
-u	Utente	
-p	Password	
-o	Opzione	Stringa di opzione extra per montaggi samba e nfs
-d	Dominio	Dominio per montaggio samba
-q	Stato dell'aggiornamento corrente della query	
-c	Annullamento del processo di sincronizzazione	

Sintassi

```
syncrep [options]  Launch firmware sync from remote repository
options:
     -t <samba|nfs> protocol to connect repository
     -l location of remote repository (URL format)
     -u User
     -p Password
     -o option (extra option string for samba and nfs mounts)
     -d domain (domain for samba mount)
     -q query current update status
     -c cancel the sync process
```

Esempio

```
(1) start sync with repository
system> syncrep -t samba -l url -u user -p password
(2) query current update status
system> syncrep -q
(3)cancel the sync process
system> syncrep -c
```

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.

Tabella 53. comando thermal

La seguente tabella multiriga a tre colonne contiene le opzioni, le descrizioni delle opzioni e i valori associati per le opzioni.

Opzione	Descrizione	Valori
-mode	Visualizza i criteri della modalità termica e configura la tabella termica dei sistemi host (sola lettura)	normale, prestazioni, minima, efficienza, personalizzato
-table <vendorID_deviceID><table_number>	<vendorID_deviceID> specificare il fornitore e l'ID dispositivo del componente che richiede un raffreddamento alternativo.	8 caratteri esadecimali
	<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

Sintassi:

```
thermal [options]
option:
  -mode thermal_mode
  -table vendorID_devicetable_number
```

Esempio:

```
system> thermal
-mode normal
-table 80860126 1 10DE0DFA 3
system>
```

comando timeouts

Utilizzare questo comando per visualizzare o modificare i valori di timeout.

- Per visualizzare i valori di timeout, immettere `timeouts`.
- Per modificare i valori di timeout, immettere le opzioni seguite dai valori.
- Per modificare i valori di timeout, è necessario avere almeno l'autorizzazione di configurazione dell'adattatore.

La seguente tabella mostra gli argomenti per i valori di timeout. Questi valori corrispondono alle opzioni a discesa della scala graduata per i timeout del server sull'interfaccia Web.

Tabella 54. comando timeouts

La seguente tabella multiriga a quattro colonne contiene le opzioni, le descrizioni delle opzioni e i valori associati per le opzioni.

Opzione	Timeout	Unità	Valori
-f	Ritardo spegnimento	minuti	disabled, 0.5, 1, 2, 3, 4, 5, 7.5, 10, 15, 20, 30, 60, 120
-l	Timeout programma di caricamento	minuti	disabled, 0.5, 1, 1.5, 2, 2.5, 3, 3.5, 4, 4.5, 5, 7.5, 10, 15, 20, 30, 60, 120
-o	Timeout del sistema operativo	minuti	disabled, 2.5, 3, 3.5, 4
-s	Cattura della schermata di errore del sistema operativo con errore HW	/	disabled, enabled

Sintassi:
```
timeouts [options]
options:
-f power_off_delay_watchdog_option
-o OS_watchdog_option
-l loader_watchdog_option
-s OS failure screen capture with HW error
```

Esempio:
```
system> timeouts
-o disabled
-l 3.5
-f disabled
-s disabled
system> timeouts -o 2.5
ok
system> timeouts
-o 2.5
-l 3.5
-f disabled
-s disabled
```

comando tls

Utilizzare questo comando per impostare il livello minimo di TLS.

La seguente tabella mostra gli argomenti per le opzioni.

Tabella 55. comando tls

La seguente tabella multiriga a tre colonne contiene le opzioni, le descrizioni delle opzioni e i valori associati per le opzioni.

Tabella 55. comando tls (continua)

Opzione	Descrizione	Valori
-min	Seleziona il livello minimo di TLS	1.1, 1.2[1], 1.3
-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.

Utilizzo:

```
tls [-options] - configures the minimum TLS level
   -min <1.1 | 1.2 | 1.3> - Selects the minimum TLS level
   -h - Lists usage and options
```

Esempi:

Per indicazioni sull'utilizzo di questo comando, eseguire il comando seguente:

```
system> tls
-h
system>
```

Per ottenere la versione corrente di TLS, eseguire il comando seguente:

```
system> tls
-min 1.2
system>
```

Per modificare la versione corrente di TLS in 1.2, eseguire il comando seguente:

```
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.

La seguente tabella mostra gli argomenti per le opzioni.

Tabella 56. comando uefipw

La seguente tabella multiriga a due colonne contiene le opzioni e le relative descrizioni.

Opzione	Descrizione
-s	Consente di configurare i messaggi di sconfinamento
-h	Elenca l'uso e le opzioni

Sintassi:

```
usage:
   trespass display the trespass message
```

```
   -s <trespass message> configure trespass message
   -h - Lists usage and options
```

Esempio:

Nota: Il messaggio di sconfinamento non contiene spazi.

```
system> trespass -s testingmessage
ok
system> trespass
testingmessage

The trespass message contains spaces:
system> trespass -s "testing message"
ok
system> trespass
testing message
```

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.

La seguente tabella mostra gli argomenti per le opzioni.

Tabella 57. comando uefipw

La seguente tabella multiriga a due colonne contiene le opzioni e le relative descrizioni.

Opzione	Descrizione
-cp	Password corrente (limite di 20 caratteri)
-p	Password nuova (limite di 20 caratteri)
-cep	Password corrente crittografata
-ep	Nuova password crittografata

Sintassi:

```
usage:
   uefipw [-options] - Configure the UEFI admin password
options:
   -cp      - current password (limited to 20 characters)
   -p       - new password (limited to 20 characters)
   -cep     - current password encrypted
   -ep      - new password encrypted
```

comando usbeth

Utilizzare questo comando per abilitare o disabilitare l'interfaccia LAN su USB in banda.

Sintassi:

```
usbeth [options]
options:
-en <enabled|disabled>
```

Esempio:

```
system>usbeth
-en : disabled
system>usbeth -en enabled
ok
system>usbeth
-en : disabled
```

comando usbfp

Utilizzare questo comando per controllare l'utilizzo della porta USB del pannello anteriore in BMC

La seguente tabella mostra gli argomenti per le opzioni.

Tabella 58. Comando usbfp

La seguente tabella multiriga a due colonne contiene le opzioni e le relative descrizioni.

Opzione	Descrizione
-mode <bmc | server | shared>	Imposta la modalità di utilizzo su BMC, server o shared (condiviso)
-it <minutes>	Timeout di inattività in minuti (modalità condivisa)
-btn <on | off>	Abilita l'uso del pulsante ID per attivare/disattivare il proprietario (modalità condivisa)
-own <bmc | server >	Imposta il proprietario su bmc o server (modalità condivisa)

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. La seguente tabella mostra gli argomenti per le opzioni.

Tabella 59. comando users

La seguente tabella multiriga a tre colonne contiene le opzioni, le descrizioni delle opzioni e i valori associati per le opzioni.

Opzione	Descrizione	Valori
-user_index	Numero di indice account utente	Da 1 a 12, inclusi, oppure `all` per tutti gli utenti.
-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 caratteri e massimo 20. Un valore null crea un account senza una password che l'utente deve impostare durante il primo login.
-r	Nome del ruolo	Come elencato nel comando "comando roles" a pagina 154
-ep	Password di crittografia (per backup/ripristino)	Password valida

Tabella 59. comando users (continua)

Opzione	Descrizione	Valori
-clear	Cancella l'account utente specificato 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.	Il numero di indice dell'account utente da cancellare deve essere specificato nel formato: `users -clear -`*user_index*
-curr	Visualizza gli utenti correntemente collegati	
-sauth	Protocollo di autenticazione SNMPv3	HMAC-SHA, nessuno
-spriv	Protocollo privacy SNMPv3	CBC-DES, AES, none
-spw	Password della privacy SNMPv3	Password valida
-sepw	Password della privacy SNMPv3 (crittografata)	Password valida
-sacc	Tipo di accesso SNMPv3	get, set
-strap	Nome host trap SNMPv3	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. • Per i nodi Flex, i comandi utente sono limitati solo agli account IPMI e SNMP locali. L'opzione `-pk` non è supportata per Flex Systems.
-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`.

Tabella 59. comando users (continua)

Opzione	Descrizione	Valori
-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`. • Per i nodi Flex, i comandi utente sono limitati solo agli account IPMI e SNMP locali. L'opzione `-remove` non è supportata per Flex Systems.
-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=="` • Per i nodi Flex, i comandi utente sono limitati solo agli account IPMI e SNMP locali. L'opzione `-add` non è supportata per Flex Systems.
-upld	Carica una chiave pubblica SSH *(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 chiave, 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`. • Per i nodi Flex, i comandi utente sono limitati solo agli account IPMI e SNMP locali. L'opzione `-upld` non è supportata per Flex Systems.
-dnld	Scarica la chiave pubblica SSH specificata *(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`.

Tabella 59. comando users (continua)

Opzione	Descrizione	Valori
-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."`.

Sintassi:

```
users [-options] - display/configure user accounts
options:
   -[1-12]  - user account number
   -l       - display password expiration days
   -n       - username (limited to 16 characters)
   -p       - password (limited to 32 characters)
   -shp     - set hashpassword (total 64 characters)
   -ssalt   - set salt (limited to 64 characters)
   -ghp     - get hashpassword
   -gsalt   - get salt
   -ep      - encrypted password (used with backup/restore )
   -r       - role name as listed in roles command
   -clear   - clear user account
   -curr    - display current users
   -sauth   (none|HMAC-SHA)           - snmpv3 authentication protocol
   -spriv   (none|CBC-DES|AES)        - snmpv3 privacy protocol
   -spw     password                    - snmpv3 privacy password
   -sepw    encryptedpassword          - snmpv3 privacy password (encrypted)
   -sacc    (Get)                  - snmpv3 Access type
   -strap   hostname                    - snmpv3 trap hostname
```

```
   -pk      - SSH public keys options:
       -e       - Displays the entire key in OpenSSH format
       -remove  - Removes the specified key for the specified user
       -add     - Adds a public key for the specified user
       -upld    - Used to upload a public key in OpenSSH/RFC4716 format
       -dnld    - Used to download the specified public key to a TFTP/SFTP server
       -i       - IP address of the TFTP/SFTP
       -pn      - port number of tftp/sftp server (default 69/22)
       -u       - username for sftp server
       -pw      - password for sftp server
       -l       - Filename of the key file when uploading or downloading via TFTP/SFTP
       -af      - accept connections from host, in the format: from="<list>", where
                  <list> is a comma-separated list of hostnames and IP addresses
                  (limited to 511 characters)
       -cm      - comment (limited to 255 characters, must be quote-delimited)
```

Esempio:

```
system> users
 Account      Login ID      Advanced Attribute              Role             Password Expires
 -------      --------      ------------------              ------             ----------------
    1           USERID                  Native                 Administrator                    89 day(s)
system> users -2 -n sptest -p Passw0rd12 -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
 Account      Login ID      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  Admini
system> users -5 ghp
292bcbc41bb078cf5bd258db60b63a4b337c8c954409442cfad7148bc6428fee
system> users -5 gsalt
abc
```

Comandi di controllo di IMM

Questo argomento fornisce un elenco alfabetico dei comandi CLI di controllo di IMM.

Attualmente esistono 7 comandi di controllo di IMM:

comando alertentries

Utilizzare questo comando per gestire i destinatari degli avvisi.

- **alertentries** senza opzioni visualizza tutte le opzioni di immissione degli avvisi.
- **alertentries -number -test** genera un avviso di prova sul numero di indice del destinatario specificato.
- **alertentries -number** (dove numero è un valore compreso tra 0 e 12) visualizza le impostazioni di immissione degli avvisi per il numero indice del destinatario specificato o consente di modificare le impostazioni di avviso per tale destinatario.

La seguente tabella mostra gli argomenti per le opzioni.

Tabella 60. comando alertentries

La seguente tabella multiriga a tre colonne contiene le opzioni, le descrizioni delle opzioni e i valori associati per le opzioni.

Tabella 60. comando alertentries (continua)

Opzione	Descrizione	Valori
-number	Il numero di indice del destinatario dell'avviso da visualizzare, aggiungere, modificare o eliminare	Da 1 a 12
-status	Lo stato del destinatario dell'avviso	on, off
-type	Tipo di avviso	email, syslog
-log	Include il log di eventi nell'e-mail dell'avviso	on, off
-n	Il nome del destinatario dell'avviso	String
-e	L'indirizzo e-mail del destinatario dell'avviso	Indirizzo e-mail valido
-ip	Nome host o indirizzo IP Syslog	Nome host o indirizzo IP valido
-pn	Numero di porta syslog	Numero di porta valido
-del	Elimina il numero di indice del destinatario specificato	
-test	Genera un avviso di prova al numero di indice del destinatario specificato	
-crt	Imposta gli eventi critici che inviano gli avvisi	all, none, custom:te|vo|po|di|fa|cp|me|in|re|ot Le impostazioni personalizzate degli avvisi critici sono specificate mediante un elenco di valori separati da barre verticali nel formato **alertentries -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
-crten	Invia avvisi di eventi critici	abilitato, disabilitato

Tabella 60. comando alertentries (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 Le impostazioni personalizzate degli avvisi di avvertenza sono specificate mediante un elenco di valori separati da barre verticali nel formato **alertentries -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
-wrnen	Invia avvisi di eventi di avvertenza	abilitato, disabilitato
-sys	Imposta gli eventi di routine che inviano gli avvisi	all, none, custom:lo|tio|ot|po|bf|til|pf|el|ne Le impostazioni personalizzate degli avvisi di routine sono specificate mediante un elenco di valori separati da barre verticali nel formato **alertentries -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
-sysen	Invia avvisi di eventi di routine	abilitato, disabilitato

Sintassi:

```
alertentries [options]
   options:
   -number recipient_number
      -status status
      -type alert_type
      -log include_log_state
      -n recipient_name
      -e email_address
      -ip ip_addr_or_hostname
      -pn port_number
      -del
      -test
      -crt event_type
      -crten state
      -wrn event_type
```

```
-wrnen state
-sys event_type
-sysen state
```

Esempio:

```
system> alertentries
1. test
2. <not used>
3. <not used>
4. <not used>
5. <not used>
6. <not used>
7. <not used>
8. <not used>
9. <not used>
10. <not used>
11. <not used>
12. <not used>

system> alertentries -1
-status off
-log off
-n test
-e test@mytest.com
-crt all
-wrn all
-sys none
system>
```

comando batch

Utilizzare questo comando per eseguire uno o più comandi CLI contenuti in un file.

- 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.

La seguente tabella mostra gli argomenti per le opzioni.

Tabella 61. comando batch

La seguente tabella multiriga a tre colonne contiene le opzioni, le descrizioni delle opzioni e i valori associati per le opzioni.

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

Sintassi:

```
batch [options]
option:
  -f filename
  -ip ip_address
  -pn port_number
 user name
  -pw password
```

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 clearcfg

Utilizzare questo comando per ripristinare i valori predefiniti originali della configurazione di IMM.

Per emettere questo comando è necessario disporre almeno dell'autorizzazione per la configurazione avanzata dell'adattatore. Una volta cancellata la configurazione di IMM, IMM verrà riavviato.

comando clock

Utilizzare questo comando per visualizzare la data e l'ora correnti. È possibile configurare le impostazioni di offset UTC e ora legale.

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.

Per un offset UTC di +2, -7, -6, -5, -4 e -3 sono necessarie 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).

Sintassi:

```
clock [options]
options:
-u UTC offset
-dst on/off/special case
-host - local | utc , format of time obtained from host (default: utc)
Windows systems use local, Linux uses utc
```

Esempio:

```
system> clock
12/12/2011 13:15:23 GMT-5:00 dst on
```

comando identify

Utilizzare questo comando per accendere o spegnere il LED di identificazione chassis o per farlo lampeggiare.

L'opzione **-d** può essere utilizzata con l'opzione **-s on** per accendere il LED solo per il numero di secondi specificato con l'opzione **-d**. Il LED si spegne dopo il numero di secondi specificato.

Sintassi:
```
identify [options]
options:
-s on/off/blink
-d seconds
```

Esempio:
```
system> identify
-s off
system> identify -s on -d 30
ok
system>
```

comando info

Utilizzare questo comando per visualizzare e configurare le informazioni su IMM.

L'esecuzione del comando **info** senza opzioni visualizza tutte le informazioni di contatto e relative alla posizione di IMM. La seguente tabella mostra gli argomenti per le opzioni.

Tabella 62. comando info

La seguente tabella multiriga a tre colonne contiene le opzioni, le descrizioni delle opzioni e i valori associati per le opzioni.

Opzione	Descrizione	Valori
-name	Nome di IMM	String
-contact	Nome della persona di contatto di IMM	String
-location	Posizione di IMM	String
-room[1]	ID spazio IMM	String
-rack[1]	ID rack IMM	String
-rup[1]	Posizione di IMM nel rack	String
-ruh	Altezza dell'unità rack	Sola lettura
-bbay	Posizione vano blade	Sola lettura

1. Il valore è di sola lettura e non può essere reimpostato se IMM si trova in un sistema Flex System.

Sintassi:
```
info [options]
option:
  -name xcc_name
  -contact contact_name
  -location xcc_location
  -room room_id
  -rack rack_id
```

-rup *rack_unit_position*
-ruh *rack_unit_height*
-bbay *blade_bay*

comando spreset

Utilizzare questo comando per riavviare IMM.

Per emettere questo comando è necessario disporre almeno dell'autorizzazione per la configurazione avanzata dell'adattatore.

Comandi Service Advisor

Questo argomento fornisce un elenco alfabetico dei comandi CLI di Service Advisor.

Attualmente sono disponibili 3 comandi di Service Advisor:

comando chconfig

Utilizzare questo comando per visualizzare e configurare le impostazioni di Service Advisor.

- Prima di configurare qualsiasi altro parametro è necessario accettare i termini e le condizioni di Service Advisor, utilizzando l'opzione del comando **chconfig - Li**.
- Per abilitare il supporto di Service Advisor, sono obbligatori tutti i campi relativi alle informazioni di contatto e il campo **Centro di assistenza** (mediante l'opzione del comando chconfig -sc).
- Se è richiesto un proxy HTTP è necessario configurare tutti i campi del proxy HTTP.

La seguente tabella mostra gli argomenti per le opzioni.

Tabella 63. comando chconfig

La seguente tabella multiriga a tre colonne contiene le opzioni, le descrizioni delle opzioni e i valori associati per le opzioni.

Opzione	Descrizione	Valori
-li	Visualizza o accetta i termini e le condizioni di Service Advisor **Nota:** I termini e le condizioni devono essere accettati prima di configurare eventuali altri parametri.	view, accept
-sa	Lo stato del supporto di Service Advisor **Nota:** Per abilitare Service Advisor, devono essere soddisfatti i seguenti criteri: • Il codice del paese è obbligatorio. • Tutte le opzioni nelle informazioni di contatto di Service Advisor sono obbligatorie.	abilitato, disabilitato
-sc	Il codice del paese per il centro di assistenza	Il codice del paese ISO di due caratteri
Opzioni per le informazioni di contatto di Service Advisor:		
-cn	Nome della persona di contatto primaria	Stringa racchiusa tra virgolette (massimo 30 caratteri)

Tabella 63. comando chconfig (continua)

Opzione	Descrizione	Valori
-cph	Numero di telefono della persona di contatto primaria	Stringa racchiusa tra virgolette (5-30 caratteri)
-ce	Indirizzo e-mail della persona di contatto primaria **Nota:** I caratteri alfanumerici ".", "-" o "_" sono accettabili come ID utente o nome host. L'indirizzo e-mail deve contenere almeno due voci di dominio e l'ultimo elemento di dominio deve essere di 2 - 4 caratteri alfabetici.	Indirizzo e-mail valido in formato `userid@hostname` (massimo 30 caratteri)
-co	Nome dell'organizzazione o dell'azienda della persona di contatto primaria	Stringa racchiusa tra virgolette (massimo 30 caratteri)
-ca	Indirizzo della posizione della macchina	Stringa racchiusa tra virgolette (massimo 30 caratteri)
-cci	Città della posizione della macchina	Stringa racchiusa tra virgolette (massimo 30 caratteri)
-cs	Stato della posizione della macchina	Stringa racchiusa tra virgolette (massimo 30 caratteri)
-cz	Codice postale della posizione della macchina	Stringa racchiusa tra virgolette (massimo 9 caratteri)
Opzioni alternative per le informazioni di contatto di Service Advisor:		
-an	Nome della persona di contatto alternativa	Stringa racchiusa tra virgolette (massimo 30 caratteri)
-aph	Numero di telefono della persona di contatto alternativa	Stringa racchiusa tra virgolette (5-30 caratteri)
-ae	Indirizzo e-mail della persona di contatto alternativa **Nota:** I caratteri alfanumerici ".", "-" o "_" sono accettabili come ID utente o nome host. L'indirizzo e-mail deve contenere almeno due voci di dominio e l'ultimo elemento di dominio deve essere di 2 - 4 caratteri alfabetici.	Indirizzo e-mail valido in formato `userid@hostname` (massimo 30 caratteri)
-ao	Nome dell'organizzazione o dell'azienda della persona di contatto alternativa	Stringa racchiusa tra virgolette (massimo 30 caratteri)
-aa	Indirizzo della posizione alternativa della macchina	Stringa racchiusa tra virgolette (massimo 30 caratteri)
-aci	Città della posizione alternativa della macchina	Stringa racchiusa tra virgolette (massimo 30 caratteri)
-as	Stato della posizione alternativa della macchina	Stringa racchiusa tra virgolette (massimo 30 caratteri)
-az	Codice postale della posizione alternativa della macchina	Stringa racchiusa tra virgolette (massimo 9 caratteri)
Opzioni impostazioni del proxy HTTP:		
-loc	Posizione del proxy HTTP	Nome host completo o indirizzo IP del proxy HTTP (massimo 63 caratteri)
-po	Porta del proxy HTTP	Numero di porta valido (1-65535)

Tabella 63. comando chconfig (continua)

Opzione	Descrizione	Valori
-ps	Stato del proxy HTTP	abilitato, disabilitato
-pw	Password del proxy HTTP	Password valida, racchiusa tra virgolette (massimo 15 caratteri)
-epw	Password crittografata del proxy HTTP	Password valida, racchiusa tra virgolette (massimo 15 caratteri)
-u	Nome utente del proxy HTTP	Nome utente valido, racchiuso tra virgolette (massimo 30 caratteri)
-test	Verifica il proxy HTTP	

Sintassi:

```
chconfig [options]
option:
  -li view|accept
  -sa enable|disable
  -sc service_country_code
  -ce contact_email
  -cn contact_name
  -co company_name
  -cph contact_phone
  -cpx contact_extension_phone
  -an alternate_contact_name
  -ae alternate_contact_email
  -aph alternate_contact_phone
  -apx alternate_contact_extension_phone
  -mp machine_phone_number
  -loc hostname/ip_address
  -po proxy_port
  -ps proxy_status
  -pw proxy_pw
  -ccl machine_country_code
  -u proxy_user_name
```

comando chmanual

Utilizzare questo comando per generare una richiesta di call home manuale.

Nota: I destinatari del messaggio call home vengono configurati mediante il comando **chconfig**.

- Il comando **chmanual -test** genera un messaggio Test Call Home.

La seguente tabella mostra gli argomenti per le opzioni.

Tabella 64. comando chmanual

La seguente tabella multiriga a tre colonne contiene le opzioni, le descrizioni delle opzioni e i valori associati per le opzioni.

Opzione	Descrizione	Valori
-test	Genera un messaggio di prova per i destinatari call home	

Sintassi:

```
chmanual [options]
Generates a manual Call Home or a Test Call Home
  -test: Generate a test Call Home.
```

comando chlog

Utilizzare questo comando per visualizzare gli ultimi cinque eventi Call Home e annullare il caso associato all'evento in base al numero del caso.

Il comando **chlog** visualizza le ultime cinque voci del log delle attività call home generate dal server o dall'utente. La voce call home più recente viene mostrata per prima. Il server non invierà gli eventi duplicati se non riconosciuti come corretti nel log delle attività.

La seguente tabella mostra gli argomenti per le opzioni.

Tabella 65. comando chconfig

La seguente tabella multiriga a tre colonne contiene le opzioni, le descrizioni delle opzioni e i valori associati per le opzioni.

Opzione	Descrizione	Valori
-c	Annulla il caso associato all'evento in base al numero del caso	

Sintassi:

```
chlog[-options]
       Displays the last five call home events that were generated either by
       the system or the user (most recent call home entry first.)

       -c: cancel the case associated with the event by caseNumber
```

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.

La seguente tabella mostra gli argomenti per le opzioni.

Tabella 66. comando storage

La seguente tabella multiriga a tre colonne contiene le opzioni, le descrizioni delle opzioni e i valori associati per le opzioni.

Tabella 66. comando storage (continua)

Opzione	Descrizione	Valori
-list	Visualizza l'elenco delle destinazioni di storage gestite da IMM.	*controllers*|*pools*|*volumes*|*drives* Dove *target* è: • *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 associate al controller RAID[1]
-list -target *target_id*	Visualizza l'elenco delle *destinazioni* di storage gestite da IMM in base a *target_id*.	*pools*|*volumes*|*drives ctrl[x]*|*pool[x]* Dove *target* e *target_id* sono: • *pools ctrl[x]*: visualizza l'elenco dei pool di storage associati al controller RAID, in base a target_id[1] • *volumes ctrl[x]*|*pool[x]*: visualizza l'elenco dei volumi di storage associati al controller RAID, in base a target_id[1] • *drives ctrl[x]*|*pool[x]*: visualizza l'elenco delle unità di storage associate al controller RAID, in base a target_id[1]
-list flashdimms	Visualizza l'elenco dei DIMM flash gestiti da IMM.	
-list devices	Visualizza lo stato di tutti i dischi e dei DIMM flash 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]* |*flashdimm[x]* [3]
-show *target_id* info	Visualizza informazioni dettagliate per la destinazione selezionata gestita da IMM.	Dove *target_id* è: *ctrl[x]*|*vol[x]*|*disk[x]*|*pool[x]* |*flashdimm[x]* [3]
-show *target_id firmware*[3]	Visualizza informazioni sul firmware per la destinazione selezionata gestita da IMM.	Dove *target_id* è: *ctrl[x]*|*disk[x]*|*flashdimm[x]*[2]
-showlog *target_id<m:n*|*all>*[3]	Visualizza i log eventi della destinazione selezionata gestita da IMM.	Dove *target_id* è: *ctrl[x]*[4] *m:n*|*all* Dove *m:n* è il numero massimo di log di eventi Dove *all* indica tutti i log di eventi
-config ctrl -scanforgn -target *target_id*[3]	Rileva la configurazione RAID esterna.	Dove *target_id* è: *ctrl[x]*[5]

Tabella 66. comando storage (continua)

Opzione	Descrizione	Valori
-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]
-config ctrl -clrcfg -target *target_id*[3]	Cancella la configurazione RAID.	Dove *target_id* è: *ctrl[x]*[5]
-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 -addhsp *-[dedicated pools]* -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 -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]

Tabella 66. comando storage (continua)

Opzione	Descrizione	Valori
-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*>] sono i criteri di scrittura su cache: – Digitare *0* per i criteri Write Through – Digitare *1* per i criteri Write Back – Digitare *2* per i criteri Write With Battery Backup Unit (BBU) • [-r <*0*|*1*|*2*>] sono i criteri di lettura della cache: – Digitare *0* per i criteri No Read Ahead – Digitare *1* per i criteri Read Ahead – Digitare *2* per i criteri Adaptive 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]
-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*|*1ERLQ0*|*1E0RLQ0*>] 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*>] sono i criteri di scrittura su cache: – Digitare *0* per i criteri Write Through – Digitare *1* per i criteri Write Back

Tabella 66. comando storage (continua)

Opzione	Descrizione	Valori
		– Digitare *2* per i criteri Write With Battery Backup Unit (BBU) • [-r <*0*|*1*|*2*>] sono i criteri di lettura della cache: – Digitare *0* per i criteri No Read Ahead – Digitare *1* per i criteri Read Ahead – Digitare *2* per i criteri Adaptive 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 128 K o 1 M • -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*|*1ERLQ0*|*1E0RLQ0*>] 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]

Tabella 66. comando storage (continua)

Opzione	Descrizione	Valori
-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.

Sintassi:
```
storage [options]
option:
  -config ctrl|drv|vol -option [-options] -target target_id
  -list controllers|pools|volumes|drives
  -list pools -target ctrl[x]
  -list volumes -target ctrl[x]|pool[x]
  -list drives -target ctrl[x]|pool[x]
  -list devices
  -list flashdimms
  -show target_id
  -show {ctrl[x]|pool[x]|disk[x]|vol[x]|flashdimm[x]} info
  -show {ctrl[x]|disk[x]|flashdimm[x]}firmware
  -showlog ctrl[x]m:n|all
  -h help
```

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 flashdimms
flashdimm[1]    Flash DIMM 1
flashdimm[4]    Flash DIMM 4
flashdimm[9]    Flash DIMM 9
system>
system> storage
-list pools
pool[0-0]    Storage Pool 0
pool[0-1]    Storage Pool 1
system>
system> storage
-list volumes
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.: 12345678901
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
Storage Pool 0
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 flashdimm[15]
Name: CPU1 DIMM 15
Health Status: Normal
Operational Status: Online
Capacity(GB): 400GB
Model Type: DDR3
```

```
Part Number: 93E4040OGGM101PAT
FRU S/N: 44000000
Manuf ID: Diablo Technologies
Temperature: OC
Warranty Writes: 100%
Write Endurance: 100%
F/W Level: A201.0.0.49152
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.

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.`
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.

La seguente tabella mostra gli argomenti per le opzioni.

Tabella 67. comando adapter

La seguente tabella multiriga a tre colonne contiene le opzioni, le descrizioni delle opzioni e i valori associati per le opzioni.

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|chips]* 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 • *chips*: visualizza tutte le informazioni sul chip GPU per l'adattatore
-h	Visualizza le opzioni e l'uso del comando	

Sintassi:
```
adapter [options]
option:
  -list
  -show target_id [info|firmware|ports|chips]
  -h help
```

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> 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
```

comando mvstor

Utilizzare questo comando per ottenere le informazioni sull'inventario correlate a M.2 e gestire i volumi virtuali.

La seguente tabella mostra gli argomenti per le opzioni.

Tabella 68. comando mvstor

La seguente tabella multiriga a due colonne contiene le opzioni e le relative descrizioni.

Tabella 68. comando mvstor (continua)

Opzione	Descrizione
-h/?	Consente di stampare le informazioni della guida per questo comando
-version	Consente di visualizzare le informazioni sul firmware del controller
-disks	Consente di visualizzare le informazioni sui dischi multimediali
-volumes	Consente di visualizzare le informazioni sui volumi virtuali
-create	Consente di creare un volume virtuale e di specificare VD_Name, RaidLevel e StripeSize
-delete	Consente di eliminare un volume virtuale
-import	Consente di importare un volume virtuale esterno. Dopo l'importazione un riavvio del sistema ricostruirà automaticamente il volume virtuale.

Utilizzo

```
   mvstor [-options] - raid configuration for SATA/NVMe RAID boot solution.
options:
   -version                    - displays controller firmware version.
   -disks                      - displays information of media disks.
   -volumes                    - displays information of virtual disks
   -create -slot <slot_no> -name <vd name> -level <0|1> -stripe <32|64|128|256|512> - create virtual volume.
       Marvell SATA RAID: stripe size can only be 32k or 64k
       Marvell NVMe RAID: vd name is unapplicable. The name will always be VD_0.
   -delete -slot <slot_no> -id <0|1>          - delete the virtual volume
   -import -slot <slot_no> -id <0|1>          - import a foreign virtual volume
```

Esempio

```
system> mvstor -version
    Controller Slot      Device Name                                                Version
1                ThinkSystem M.2 SATA 2-Bay RAID Enablement Kit        2.3.20.1203


system> mvstor -disks
  Controller Slot 1    M.2 Bay0         128GB M.2 SATA SSD     LEN
  Controller Slot 1    M.2 Bay1         128GB M.2 SATA SSD     LEN

system> mvstor -volumes
Controller Slot 1:
    VD_ID:         0
    VD_Name:       VD_Test
    PD_Member:     0,1
    RaidLevel:     1
    StripSize:     64k
    VD_Capacity:   117 GB
    VD_Status:     Optimal
       1              64k           29 GB            Optimal

system> mvstor -delete –slot 1 -id 0
VD_ID 0 is deleted

system> mvstor -create –slot 1 -name M2RAID -level 1 -strip 64
New volume is created

system> mvstor -import –slot 1 -id 0
VD_ID 0 is imported
```

Comandi di supporto

Questo argomento fornisce un elenco alfabetico di comandi di supporto.

Esiste solo un comando di supporto: "comando dbgshimm" a pagina 199.

comando dbgshimm

Utilizzare questo comando sbloccare l'accesso alla rete per la shell di debug sicura.

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

La seguente tabella mostra gli argomenti per le opzioni.

Tabella 69. Comando dbgshimm

La seguente tabella multiriga a due colonne contiene le opzioni e le relative descrizioni.

Opzione	Descrizione
stato	Visualizza lo stato
abilita	Abilita l'accesso del debug (predefinita se non è specificata alcuna opzione)
disabilita	Disabilita l'accesso del debug

Capitolo 12. 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 201.

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 201.

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 Flex e Stark, l'impostazione di negoziazione automatica non è modificabile, poiché potrebbe interrompere il percorso di comunicazione della rete mediante 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>

Capitolo 13. Server Edge

In questo argomento vengono descritte le funzioni specifiche per i server Edge.

Nota:

1. Al primo accesso, il sistema richiede di modificare la password XCC.
2. L'opzione IPMI-over-LAN è disabilitata per impostazione predefinita.
3. L'opzione IPMI-over-KCS è disabilitata per impostazione predefinita.

Modalità di blocco del sistema

Quando lo stato dell'opzione **Modalità di blocco del sistema** è attivo, significa che il sistema è in modalità di blocco. È possibile attivare il sistema e sbloccarlo. In caso contrario, l'avvio del sistema host non sarà autorizzato.

Fare clic su **Sicurezza** in **Configurazione BMC** e scorrere fino alla sezione **Modalità di blocco del sistema**.

Modalità di blocco del sistema

Per attivare il sistema e uscire dalla **Modalità di blocco del sistema**, completare le seguenti operazioni.

1. Fare clic sul pulsante **Disattiva** per visualizzare la finestra **Attivazione Key Vault** che contiene il **Testo di verifica**.
2. Contattare l'amministratore IT e fornire il **Testo di verifica**.
3. Ottenere la **Risposta alla richiesta di verifica** dall'amministratore IT e immetterla nella finestra **Attivazione Key Vault**..
4. Fare clic sul pulsante **OK** e quindi su **Applica**.
5. Se tutte le impostazioni funzionano correttamente, l'opzione **Modalità di blocco del sistema** verrà modificata in **Disattiva**.

Nota: Quando lo stato della modalità di blocco del sistema è attivo, qualsiasi accesso ai segreti di sistema, come le chiavi SED AK (Authentication Key), viene **negato**.

Per forzare il sistema ad attivare la modalità di blocco del sistema, completare le seguenti operazioni.

1. Fare clic sul pulsante **Attiva**.
2. Fare clic sul pulsante **OK** e quindi su **Applica**.

Rilevamento del movimento

È possibile abilitare questa funzione per proteggere il server rilevando qualsiasi movimento fisico del server.
Se il rilevamento del movimento è abilitato, è possibile configurare i seguenti elementi, a seconda delle preferenze e della configurazione.

- **Livello di sensibilità**: selezionare il livello di sensibilità tra **Basso**, **Medio** e **Alto**, in base alle preferenze.
- **Orientamento**: selezionare la configurazione tra **Desktop verticale**, **Montaggio a parete (orizzontale)**, **Montaggio a parete (verticale)**, **Su ripiano** e **Montaggio a soffitto**.

Nota: Il rilevamento del movimento verrà disabilitato automaticamente quando viene attivata la modalità di blocco del sistema.

Rilevamento intrusione chassis

È possibile abilitare questa funzione per proteggere il server rilevando qualsiasi movimento fisico del coperchio superiore.

Configurazioni aggiuntive

Se è installato il pacchetto LOM con supporto wireless, sono disponibili tre impostazioni in caso venga rilevato un evento di manomissione.

In alcuni rari casi, ThinkShield Key Vault Portal potrebbe non essere in grado di verificare il **Testo di verifica**. In questo caso, potrebbe essere necessario reimpostare il contatore interno del dispositivo, prima di attivare il dispositivo secondo la richiesta dell'amministratore IT.

Gestore SED AK (Authentication Key)

Per i sistemi dotati di unità SED (Self-Encrypting Drive), questa funzione controlla la distribuzione della chiave SED AK (Authentication Key) del BMC. È possibile utilizzare la chiave SED AK (Authentication Key) per codificare le unità di avvio e dati e avviare il sistema senza intervento manuale.

Nota: Questa operazione non è consentita quando il sistema non è attivato (asserzione della modalità di blocco del sistema) o l'utente corrente non è autorizzato a gestire la chiave SED AK (Authentication Key).

Fare clic su **Sicurezza** in **Configurazione BMC** e scorrere fino alla sezione **Gestore SED AK (Authentication Key)**.

Modifica della chiave SED AK

Genera SED AK da passphrase: impostare la password e reinserirla per la conferma. Fare clic su **Rigenera** per ottenere la nuova chiave SED AK.

Genera SED AK casuale: fare clic su **Rigenera** per ottenere una chiave SED AK casuale.

Backup della chiave SED AK: impostare la password e reinserirla per la conferma. Fare clic su **Avvia backup** per eseguire il backup della chiave SED AK; scaricare quindi il file SED AK e archiviarlo in tutta sicurezza per un uso futuro.

Nota: Se si utilizza il file SED AK di backup per ripristinare una configurazione, il sistema richiederà la password impostata in questo passaggio.

Ripristino della chiave SED AK: è possibile eseguire questa attività solo quando l'unità SED non funziona correttamente. Sono disponibili due metodi di ripristino della chiave SED AK:

- **Ripristina SED AK utilizzando la passphrase**: utilizzare la password impostata nella modalità **Genera SED AK dalla passphrase** per ripristinare la chiave SED AK.
- **Recupera SED AK dal file di backup**: caricare il file di backup generato nella modalità **Backup della chiave SED AK** e immettere la password del file di backup corrispondente per ripristinare la chiave SED AK.

Rete Edge

La pagina di questa funzione è supportata solo quando è installato il pacchetto LOM con supporto wireless.

Per ulteriori informazioni sulle tabelle preimpostate della topologia di rete, visitare il sito https://thinksystem.lenovofiles.com/help/topic/SE350/pdf_files.html.

Connettività Wi-Fi

Fare clic su **Abilitata** per configurare le impostazioni in base alla configurazione Wi-Fi.

Connettività LTE

Questa voce consente di controllare la connettività LTE per la scheda di rete Edge.

Indirizzo della scheda di rete Edge

Stato **IPv4 o IPv6**	Stato **server DHCP**	**Metodo**
Disabilitata	**Disabilitata**	**Ottenimento IP da DHCP**
Abilitato	**Abilitato**	**Utilizzo indirizzo IP statico**
Abilitato	**Disabilitata**	**Ottenimento IP da DHCP** o **Utilizzo indirizzo IP statico**, a seconda dell'utilizzo.

Bridge di rete BMC

È possibile accedere al BMC mediante le seguenti opzioni: **Porte downlink**, **Porte Wi-Fi**, **Porte uplink** o **Nessuno**.

Nota: Selezionare **Nessuno** per disabilitare questa funzione.

Risoluzione dei problemi della scheda di rete Edge

Riavvia immediatamente: con questo pulsante è possibile riavviare la scheda di rete.

Reimposta i valori predefiniti: con questo pulsante è possibile reimpostare le impostazioni predefinite della scheda di rete.

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 sistema operativo.

La documentazione relativa ai prodotti ThinkSystem è disponibili nella posizione seguente:

http://thinksystem.lenovofiles.com/help/index.jsp

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, consultare 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 http://sysmgt.lenovofiles.com/help/topic/com.lenovo.systems.management.xcc2.doc/NN1ia_c_servicesandsupport.html.
  - Per ulteriori informazioni sull'utilizzo dell'interfaccia CLI per la raccolta dei dati di servizio, vedere http://sysmgt.lenovofiles.com/help/topic/com.lenovo.systems.management.xcc2.doc/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 http://sysmgt.lenovofiles.com/help/topic/com.lenovo.lxca.doc/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 http://sysmgt.lenovofiles.com/help/topic/toolsctr_cli_lenovo/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 la Lenovo intenda renderli disponibili in tutti i paesi in cui opera. 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. Qualsiasi prodotto, programma o servizio funzionalmente equivalente che non violi alcun diritto di proprietà intellettuale Lenovo può essere utilizzato. 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 SIA IMPLICITA, INCLUSE, MA NON LIMITATE, 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. Nessuno 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 varii.

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 varii significativamente. Alcune misurazioni possono essere state effettuate sul 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 70. 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:

http://thinksystem.lenovofiles.com/help/index.jsp

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

accensione e riavvio del server
  comandi 125
Accesso all'unità
  gestione certificati 166
  sicurezza 166
Accesso IPMI-over-KCS
  configurazione 44
accesso remoto 2
account utente
  creazione 173
  eliminazione 21
Account utente SNMPv3
  configurazione 173
adiacente, gruppo
  funzione 105
  installazione 106
  provisioning 106
adiacente, nodo
  rilevamento 106
alimentazione
  gestione mediante i comandi IPMI 71
  monitoraggio mediante i comandi IPMI 71
assegnazione automatica
  certificato 46
assegnazioni delle porte
  configurazione 35
  impostazioni 35
assistenza e supporto
  hardware 231
  prima di contattare l'assistenza 229
  software 231
attributo di autorizzazione di login
  LDAP 146
attributo di ricerca gruppi
  LDAP 146
Attributo di ricerca UID
  Server LDAP 146
autenticazione tentativi di login 17
autonegoziazione
  impostazione 142
avvisi importanti 234

B

BIOS (Basic Input/Output System) 1
BMC
  certificate signing request 46
bridging ipmi
  gestione dell'alimentazione 72
  tramite XClarity Controller 72

C

call home
  Configurazione 52
cattura della schermata blu 76
cattura della schermata del sistema operativo 76
certificate signing request
  BMC 46
certificato server
  gestione 49
Certificato SKLM
  gestione 46
chiave di attivazione
  esportazione 104
  gestione 145
  installazione 103, 145
  rimuovi 104, 145
chiavi di crittografia
  gestione centralizzata 44
Chiavi SSH
  utente 173
CIM-over-HTTPS
  gestione certificati 162–163
  sicurezza 162–163
classificazioni dei certificati
  assegnazione automatica 46
  Con firma CA 46
client
  gestione certificati 46
comandi
  accseccfg 129
  adattatore 195
  alertcfg 131
  alertentries 177
  alimentazione 125
  asu 131
  backup 134
  batch 180
  chconfig 183
  chlog 186
  chmanual 185
  clearcfg 181
  clearlog 116
  clock 181
  console 129
  dbgshimm 199
  dhcpinfo 135
  dns 136
  encaps 138
  ethtousb 138
  ffdc 117
  firewall 139
  fuelg 127
  gprofile 140
  hashpw 141
  history 115
  hreport 118
  identificazione 182
  ifconfig 142
  imposta 155
  info 182
  informazioni utili 115
  keycfg 145
  ldap 146
  led 120
  mhlog 119
  mvstor 197
  ntp 148
  portcfg 149
  portcontrol 150
  porte 151
  pxeboot 128
  rdmount 152
  readlog 121
  reset 127
  restore 152
  restoredefaults 153
  roles 154
  seccfg 155
  smtp 155
  snmp 156
  snmpalerts 158

spreset 183
srcfg 160
sshcfg 161
ssl 162
sslcfg 163
storage 186
storekeycfg 166
syncrep 168
syshealth 122
temps 123
thermal 169
timeouts 169
TLS 170
trespass 171
uefipw 172
usbeth 172
usbfp 173
uscita 115
utenti 173
ventole 117
volts 123
vpd 124
comandi dei programmi di utilità 115
comandi di configurazione 129
Comandi di controllo di IMM 177
comandi di monitoraggio 116
Comandi di supporto 199
comandi ipmi
consumo energetico 71
Comandi IPMI OEM 214
Comandi senza agente 186
comandi Service Advisor 183
comandi, elenco in ordine alfabetico 113
comandi, tipi
accensione e riavvio del server 125
configurazione 129
controllo di IMM 177
monitor 116
programmi di utilità 115
Senza agente 186
serial redirect 129
Service Advisor 183
Supporto 199
comando accseccfg 129
comando adapter 195
comando alertcfg 131
comando alertentries 177
comando asu 131
comando batch 180
comando chconfig 183
comando chlog 186
comando chmanual 185
comando clearcfg 181
comando clearlog 116
comando clock 181
comando console 129
comando dbgshimm 199
comando dhcpinfo 135
comando di backup 134
comando dns 136
Comando encaps 138
comando ethtousb 138
comando exit 115
comando fans 117
comando ffdc 117
Comando firewall 139
comando fuelg 127
comando gprofile 140
comando hashpw 141
comando help 115
comando history 115
Comando hreport 118
comando identify 182
comando ifconfig 142
comando info 182
comando keycfg 145
comando ldap 146
comando led 120
comando mhlog 119
comando mvstor 197
comando ntp 148
comando portcfg 149
comando portcontrol 150
comando ports 151
comando power 125
comando pxeboot 128
comando rdmount 152
comando readlog 121
comando reset 127
comando restore 152
comando restoredefaults 153
comando roles 154
comando seccfg 155
comando serial redirect 129
comando set 155
comando smtp 155
comando snmp 156
comando snmpalerts 158
comando spreset 183
comando srcfg 160
comando sshcfg 161
comando ssl 162
comando sslcfg 163
comando storage 186
dispositivi di storage 186
comando storekeycfg 166
comando syncrep 168
comando syshealth 122
comando temps 123
comando thermal 169
comando timeouts 169
Comando TLS 170
comando trespass 171
comando uefipw 172
comando usbeth 172
Comando usbfp 173
comando users 173
comando volts 123
comando vpd 124
come impedire il downgrade del firmware di sistema
configurazione 44
command-line interface (CLI)
accesso 111
descrizione 111
funzioni e limitazioni 112
sintassi dei comandi 112
Comunità SNMPv1
gestione 156
Con firma CA
certificato 46
configurazione
Accesso IPMI-over-KCS 44
Account utente SNMPv3 173
assegnazioni delle porte 35
come impedire il downgrade del firmware di sistema 44
Controllo del sistema 50
DDNS 136
DNS 136
elementi bloccati e restrizione di orario 36
Ethernet 142
Ethernet-over-USB 138
Gruppo di dispositivi SKLM 45
Impostazioni DDNS 33
Impostazioni degli avvisi SNMPv3 34
impostazioni di sicurezza 38
Impostazioni DNS 32
Impostazioni Ethernet 30, 202
Impostazioni Ethernet su USB 33
Impostazioni LDAP 25
IPMI 34

IPv4 142
IPv6 142
LDAP 146
limite di login simultanei per l'account utente 49
livelli di sicurezza account utente 129
porta di servizio di rete 150
porta seriale 149
porte 151
protocolli di rete 30
security password manager 49
Server di repository delle chiavi SKLM 45
Server LDAP 146
Server SSH 43
SMTP 155
SNMPv1 156
Trap SNMPv1 156
USB 138
Wrapping del log SEL IPMI 44
Configurazione
impostazioni di login globali 23
porta USB di gestione del pannello anteriore 37
reindirizzamento da seriale a SSH 111
configurazione del gruppo adiacente
gruppo adiacente 106
configurazione del server
opzioni per configurare
il server 67
Configurazione del server
Configurazione RAID 93
Dettaglio RAID 93
informazioni sugli adattatori 67
configurazione dello storage
opzioni per configurare
lo storage 93
configurazione di XClarity Controller
opzioni per configurare
XClarity Controller 17
Configurazione di XClarity Controller
configurazione di call home 52
configurazione predefinita
IMM 153
Configurazione RAID
Configurazione del server 93
configurazione server
proprietà del server 88
connessione di rete 10
indirizzo IP statico predefinito 10
indirizzo IP statico, predefinito 10
Indirizzo IP, statico predefinito 10
console remota
cattura della schermata 76
comandi di alimentazione e riavvio 75
controllo del mouse assoluto 76
controllo del mouse relativo 76
controllo del mouse relativo per Linux (accelerazione Linux predefinita) 76
sessione supporti virtuali 73
supporto del mouse 76
supporto tastiera 76
visualizzatore video 73
console remota e supporto del mouse 76
consumo energetico
comandi ipmi 71
contaminazione da particolato 234
contaminazione gassosa 234
contaminazione, particolato e gassosa 234
Contatto SNMPv1
impostazione 156
Contatto SNMPv3
impostazione 156
controller di gestione della scheda di base (BMC) 1
controllo del mouse
assoluto 76
relativo 76
relativo con accelerazione Linux predefinita 76
controllo del mouse assoluto 76
controllo del mouse relativo 76
controllo del mouse relativo per Linux (accelerazione Linux predefinita) 76
controllo del sistema
Controllo del sistema 50
Controllo del sistema
impostazioni 50
controllo di alimentazione remota 75
creazione
account utente 173
creazione di una pagina Web di supporto personalizzata 229
cronologia manutenzione 63

D

data
imposta 181
data e ora, XClarity Controller
impostazione 90
Dati della schermata di errore del SO
cattura 65
dati di servizio 230
dcmi
funzioni e comandi 73
gestione dell'alimentazione 73
DDNS
configurazione 136
gestione 136
nome di dominio personalizzato 136
Nome di dominio specificato dal server DHCP 136
origine nome di dominio 136
delete
utente 173
Destinatari trap SNMP 63
Dettaglio RAID
Configurazione del server 93
Dichiarazione BSMI RoHS per Taiwan 236
dichiarazione di regolamentazione delle telecomunicazioni 235
dispositivi di storage
comando storage 186
DNS
configurazione 136
Indirizzamento IPv4 136
Indirizzamento IPv6 136
indirizzamento server 136
Server LDAP 146
dominio di ricerca
Server LDAP 146

E

elementi bloccati e restrizione di orario
impostazioni 36
elenco di comandi in ordine alfabetico 113
elimina gruppo
abilita, disabilita 140
errori di montaggio dei supporti 86
esportazione
chiave di attivazione 104
Ethernet
configurazione 142
Ethernet avanzate
impostazioni 30, 202
Ethernet-over-USB
configurazione 138
inoltro porta 138
eventi di sistema attivi
panoramica 57

F

Features on Demand
  funzione di installazione 145
  funzione di rimozione 145
  gestione 145
filtro di gruppi
  LDAP 146
finestra eventi
  log 61–62
firmware
  visualizzazione del server 124
firmware del server
  aggiornamento 97–98
Firmware del server ThinkSystem
  descrizione 1
firmware, server
  aggiornamento 97–98
Flex System 1
FoD
  funzione di installazione 145
  funzione di rimozione 145
  gestione 145
Funzionalità di console remota 73
  abilitazione 74
funzione di console remota 73
funzione di installazione
  Features on Demand 145
  FoD 145
funzione di rimozione
  Features on Demand 145
  FoD 145
funzioni di livello Standard 2
funzioni di XClarity Controller 2
Funzioni di XClarity Controller
  livello Standard 2
  sull'interfaccia Web 13
Funzioni di XClarity Controller caratteristiche del livello platinum
  livello platinum 5
funzioni e comandi
  dcmi 73
  gestore nodi 72

G

gestione
  certificato server 49
  Certificato SKLM 46
  chiave di attivazione 145
  Comunità SNMPv1 156
  DDNS 136
  Features on Demand 145
  FoD 145
  Indirizzo MAC 142
  utente 173
gestione centralizzata
  chiavi di crittografia 44
gestione certificati
  Accesso all'unità 166
  CIM-over-HTTPS 162–163
  client 46
  LDAP 162–163
  Server 49
  Server HTTPS 162–163
  Server SSH 161
gestione dei certificati client
  assegnazione automatica 46
  Con firma CA 46
Gestione dei certificati SKLM
  pagina di accesso all'unità 46
Gestione del gruppo adiacente 105
gestione dell'alimentazione
  bridging ipmi 72
  dcmi 73
  utilizzo dei comandi IPMI 71
gestione di
  eventi nel log di controllo 62
  eventi nel log di eventi 61
Gestione di BMC
  Configurazione BMC
    backup e ripristino della configurazione BMC 54
    configurazione BMC di backup 54
    ripristino della configurazione BMC 55
    ripristino delle impostazioni predefinite 55
Gestione di XClarity Controller
  configurazione di account utente 17
  configurazione di LDAP 17
  creazione di un nuovo ruolo 18
  creazione di un nuovo utente locale 19
  eliminazione di un account utente 21
  impostazioni di sicurezza 38
  Proprietà di XClarity Controller
    data e ora 90
Gestione licenza 103
gestione server
  Dati della schermata di errore del SO 65
  firmware del server 97–98
  modalità di avvio del sistema 67
  ordine di avvio del sistema 67
  registrazione/riproduzione video della schermata 77
  singola occorrenza 68
  timeout del server, impostazione 89
gestore nodi
  funzioni e comandi 72
gruppo adiacente
  funzione 105
  gruppo adiacente 105
  installazione 106
  provisioning 106
gruppo di dispositivi
  pagina di accesso all'unità 45
Gruppo di dispositivi SKLM
  configurazione 45

I

IMM
  configurazione predefinita 153
  reimpostazione della configurazione 153
  reset 183
  ripristino della configurazione 152
  spreset 183
imposta
  data 181
  ora 181
  Porta agent SNMP 151
  Porta CIM su HTTPS 151
  Porta CLI SSH 151
  porta console remota 151
  Porta HTTP 151
  Porta HTTPS 151
  Porta trap SNMP 151
  Sequenza chiavi CLI 149
impostazione
  autonegoziazione 142
  Contatto SNMPv1 156
  Contatto SNMPv3 156
  data e ora di XClarity Controller 90
  Metodo di autenticazione utente 129
  MTU 142
  nome host 142
  Porta CIM su HTTP 151
  Porta del server LDAP 146
  timeout di inattività Web 129
  unità di trasmissione massima 142
impostazione dei numeri di porta 151
impostazione dei timeout del server 89

Impostazione di crittografia
  Impostazione di crittografia 50
impostazione posizione e contatto 88
impostazioni
  assegnazioni delle porte 35
  avanzate 30, 50, 202
  Avviso SNMP 34
  Controllo del sistema 50
  DDNS 33
  DNS 32
  elementi bloccati e restrizione di orario 36
  Ethernet 30, 202
  Ethernet-over-USB 33
  LDAP 25
  login 23
    impostazioni dei criteri di sicurezza dell'account 23
  Server SSH 43
  sicurezza 38
impostazioni di login globali
  impostazioni dei criteri di sicurezza dell'account 23
impostazioni di rete
  Comandi IPMI 35
Impostazioni SNMPv3
  utente 173
Indirizzamento IPv4
  DNS 136
Indirizzamento IPv6
  DNS 136
indirizzamento server
  DNS 136
Indirizzo IP
  Configurazione 9
  IPv4 9
  IPv6 9
  Server LDAP 146
  Server SMTP 155
indirizzo IP statico predefinito 10
indirizzo IP statico, predefinito 10
Indirizzo IP, statico predefinito 10
Indirizzo MAC
  gestione 142
Informazioni di contatto per l'importazione e l'esportazione a e da Taiwan 236
informazioni particolari 233
informazioni particolari e dichiarazioni 8
informazioni sugli adattatori
  Configurazione del server 67
informazioni sul sistema 58
  visualizzazione 58
informazioni utili 229
inoltro porta
  Ethernet-over-USB 138
installazione
  chiave di attivazione 103, 145
Interfaccia IPMI
  descrizione 201
interfaccia Web
  login all'interfaccia Web 12
interfaccia Web, avvio e utilizzo 9
Introduzione agli oggetti MIB 8
inventario di storage 94
IPMI
  configurazione 34
  gestione del server remoto 201
IPMItool 201
IPv4
  configurazione 142
IPv6 9
  configurazione 142

L

LDAP
  attributo di autorizzazione di login 146
  attributo di ricerca gruppi 146
  configurazione 146
  Configurazione 17
  filtro di gruppi 146
  gestione certificati 162–163
  nome destinazione server 146
  sicurezza 162–163
  sicurezza avanzata basata sui ruoli 173
  sicurezza basata sui ruoli, avanzata 173
  Utenti di Active Directory 173
l'utilizzo del sistema
  visualizzazione 60
limite di login simultanei per l'account utente
  configurazione 49
  limite di login simultanei per l'account utente 49
livelli basati su ruoli
  operatore 140
  rbs 140
  supervisore 140
livelli di sicurezza account utente
  configurazione 129
log dei dati di servizio
  download 88
  raccolta 88
log di controllo 62
Log di controllo esteso
  log di controllo esteso 49
Log eventi di 61
login
  impostazioni 23
login a XClarity Controller 12

M

marchi 234
metodi di montaggio dei supporti 78
Metodo di autenticazione utente 17
  impostazione 129
metodo di collegamento
  Server LDAP 146
minimi, livelli
  TLS 170
modalità schermo della console remota 77
modulo di gestione avanzata 1
monitoraggio alimentazione
  utilizzo dei comandi IPMI 71
monitoraggio dello stato del server 57
MTU
  impostazione 142

N

nodo adiacente
  rilevamento 106
nome destinazione server
  LDAP 146
nome destinazione, server
  LDAP 146
nome di dominio, personalizzato
  DDNS 136
nome di dominio, specificato dal server DHCP
  DDNS 136
nome distinto client
  Server LDAP 146
nome distinto radice
  Server LDAP 146
nome distinto, client
  Server LDAP 146
nome distinto, radice
  Server LDAP 146
nome host

impostazione 142
Server LDAP 146
Server SMTP 155
note, importanti 234
notifiche e-mail e syslog 63
numeri di porta
impostazione 151
numeri di telefono 231
numeri di telefono per assistenza e supporto hardware 231
numeri di telefono per l'assistenza e il supporto software 231
numero di porta
Server LDAP 146
Server SMTP 155
nuovo account locale
creazione 19
nuovo ruolo
creazione 18

O

OneCLI 1
opzione
SKM 44
opzione del messaggio di sconfinamento 90
opzione di gestione dell'alimentazione
azioni di alimentazione 70
criteri di limite alimentazione 69
criteri di ripristino dell'alimentazione 70
ridondanza alimentazione 69
Scheda Gestione server 69
opzione di sicurezza
Scheda Accesso all'unità 44–45
Opzione di sicurezza
Scheda Accesso all'unità 45–46
ora
imposta 181
origine nome di dominio
DDNS 136

P

pagina di accesso all'unità
configurazione 45
Gestione dei certificati SKLM 46
gruppo di dispositivi 45
server di gestione delle chiavi 45
pagina Web di supporto personalizzata 229
pagina Web di supporto, personalizzata 229
panoramica 57
controllo del sistema 50
dashboard di sicurezza 38
modalità di sicurezza 38
SSL 42
password
Server LDAP 146
utente 173
password con hash 21
Porta agent SNMP
imposta 151
Porta CIM su HTTP
impostazione 151
Porta CIM su HTTPS
imposta 151
Porta CLI SSH
imposta 151
porta console remota
imposta 151
Porta del server LDAP
impostazione 146
porta di servizio di rete
configurazione 150
Porta HTTP
imposta 151
Porta HTTPS
imposta 151
porta seriale
configurazione 149
Porta trap SNMP
imposta 151
porte
configurazione 151
impostazione dei numeri 151
visualizzazione aperte 151
pre-configurato
Server LDAP 146
proprietà del protocollo di rete
Accesso IPMI-over-KCS 44
assegnazioni delle porte 35
come impedire il downgrade del firmware di sistema 44
DDNS 33
DNS 32
elementi bloccati e restrizione di orario 36
Ethernet-over-USB 33
Impostazioni di avviso SNMP 34
Impostazioni Ethernet 30, 202
IPMI 34
proprietà del server
configurazione server 88
impostazione posizione e contatto 88
provisioning del gruppo adiacente
gruppo adiacente 106
Pubblicazioni online
informazioni sugli aggiornamenti della documentazione 1
informazioni sugli aggiornamenti firmware 1
informazioni sul codice di errore 1

R

raccolta dei dati di servizio 230
raccolta del log dei dati di servizio 88
registrazione/riproduzione video della schermata
gestione server 77
reimpostazione della configurazione
IMM 153
reindirizzamento da seriale a SSH 111
requisiti
browser Web 6
sistema operativo 6
requisiti del browser 6
Requisiti del browser Web 6
requisiti del sistema operativo 6
reset
IMM 183
riavvio di XClarity Controller 56
Richiesta di supporto 229
rilevamento dei nodi adiacenti
nodo adiacente 106
rimuovi
chiave di attivazione 104, 145
ripristino della configurazione
IMM 152

S

Scheda Accesso all'unità
opzione di sicurezza 44–46
Scheda Gestione server
opzione di gestione dell'alimentazione 69
security password manager
configurazione 49
security password manager 49
Sequenza chiavi CLI
imposta 149
Server

gestione certificati 49
opzioni di configurazione 67
server di gestione delle chiavi
configurazione 45
pagina di accesso all'unità 45
Server Flex 1
Server HTTPS
gestione certificati 162–163
sicurezza 162–163
Server LDAP
Attributo di ricerca UID 146
configurazione 146
DNS 146
dominio di ricerca 146
Indirizzo IP 146
metodo di collegamento 146
nome distinto client 146
nome distinto radice 146
nome host 146
numero di porta 146
password 146
pre-configurato 146
Server SSH
gestione certificati 161
sicurezza 161
sicurezza
Accesso all'unità 166
CIM-over-HTTPS 162–163
commutare la modalità di sicurezza 41
gestione dei certificati SSL 42
Gestione dei certificati SSL 43
LDAP 162–163
panoramica del dashboard di sicurezza 38
panoramica della modalità di sicurezza 38
Panoramica di Controllo del sistema 50
panoramica di SSL 42
Server HTTPS 162–163
Server SSH 43, 161
sicurezza avanzata basata sui ruoli
LDAP 173
sicurezza basata sui ruoli, avanzata
LDAP 173
singola occorrenza
impostazione 68
SKLM
server di gestione delle chiavi 45
SKM
opzione 44
SMTP
configurazione 155
indirizzo IP del server 155
nome host del server 155
numero di porta del server 155
SNMPv1
configurazione 156
SOL (Serial over LAN) 201
SSL
gestione certificati 43
gestione dei certificati 42
stato del server
monitoraggio 57
stato hardware 57
storage
opzioni di configurazione 93
strumenti
IPMItool 201
supporto del mouse nella console remota 76
supporto multilingua 7
supporto per più lingue 7
supporto tastiera nella console remota 76
switch
modalità di sicurezza 41

T

timeout del server
selezioni 89
timeout di inattività Web
impostazione 129
timeout sessione di inattività Web 23
TLS
livello minimo 170
Trap SNMPv1
configurazione 156

U

unità di trasmissione massima
impostazione 142
USB
configurazione 138
uscita dalla sessione della console remota 88
utente
Chiavi SSH 173
delete 173
gestione 173
Impostazioni SNMPv3 173
password 173
utenti
visualizzazione corrente 173
Utenti di Active Directory
LDAP 173
utilizzo
funzione di console remota 73
utilizzo del sistema 60

V

Visualizzatore video
cattura della schermata 76
comandi di alimentazione e riavvio 75
controllo del mouse assoluto 76
controllo del mouse relativo 76
controllo del mouse relativo per Linux (accelerazione Linux predefinita) 76
modalità colore video 76
supporto del mouse 76
visualizzazione corrente
utenti 173
visualizzazione delle informazioni sul firmware
Server 124
visualizzazione e configurazione delle unità virtuali 93
visualizzazione porte aperte 151

W

Wrapping del log SEL IPMI
configurazione 44
Wrapping del log SEL IPMI 44

X

XClarity Controller
bridging ipmi 72
configurazione del protocollo di rete 30
connessione di rete 10
descrizione 1
funzioni 2
interfaccia Web 9
nuove funzioni 1
opzioni di configurazione 17
reindirizzamento seriale 111

XClarity Controller livello Platinum 2
XClarity Controller livello Standard 2
XClarity Provisioning Manager
Setup Utility 10

Lenovo

Numero di parte: SP47A30085

Printed in China

(1P) P/N: SP47A30085