



# Guia do Usuário do XClarity Controller 3



**Nota:** Antes de usar estas informações, leia as informações gerais em [Apêndice B "Avisos" na página 183](#).

Primeira edição (outubro de 2024)

© Copyright Lenovo 2024.

**AVISO DE DIREITOS LIMITADOS E RESTRITOS:** se dados ou software forem fornecidos de acordo com um contrato de GSA (Administração de Serviços Geral), o uso, a reprodução ou a divulgação estarão sujeitos às restrições definidas no Contrato N° GS-35F-05925.

---

# Conteúdo

## Conteúdo . . . . . i

### Capítulo 1. Introdução. . . . . 1

Recursos de nível padrão e Premier do XClarity Controller . . . . .	2
Recursos de nível padrão do XClarity Controller . . . . .	2
Recursos de nível Premier do XClarity Controller . . . . .	5
Atualizando o XClarity Controller . . . . .	6
Requisitos de navegador da Web e sistema operacional . . . . .	6
Suporte a vários idiomas . . . . .	7
Introdução a MIBs . . . . .	7
Avisos usados neste documento . . . . .	8

### Capítulo 2. Abrindo e usando a interface da Web do XClarity Controller . . . . . 9

Acessando a interface da Web do XClarity Controller . . . . .	9
Configurando a conexão de rede do XClarity Controller por meio do XClarity Provisioning Manager . . . . .	10
Efetuando login no XClarity Controller . . . . .	12
Descrição das funções do XClarity Controller na interface da Web . . . . .	13

### Capítulo 3. Configurando o XClarity Controller . . . . . 17

Configurando contas de usuário/LDAP . . . . .	17
Método de autenticação do usuário . . . . .	17
Criando uma função . . . . .	18
Criando uma nova conta do usuário . . . . .	19
Exclusão de uma conta do usuário . . . . .	21
Usando as senhas com hash para autenticação . . . . .	21
Configurando as definições de login global . . . . .	23
Configurando LDAP . . . . .	25
Configurando protocolos de rede . . . . .	30
Configurando as definições de Ethernet . . . . .	30
Configurando o DNS . . . . .	32
Configurando o DDNS . . . . .	32
Configurando Ethernet sobre USB . . . . .	32
Configurando o SNMP . . . . .	33
Ativando o acesso à rede IPMI . . . . .	34
Configurando definições de rede com comandos do IPMI . . . . .	35
Ativação de serviço e atribuição de porta . . . . .	35

Configurando a restrição de acesso . . . . .	35
Configurando a porta USB do painel frontal para gerenciamento . . . . .	37
Configurando as definições de segurança . . . . .	37
Painel de segurança . . . . .	37
Modo de segurança . . . . .	37
Alternância do modo de segurança . . . . .	42
Visão geral do SSL . . . . .	42
Manipulação de certificado SSL . . . . .	42
Gerenciamento de certificado SSL . . . . .	43
Configurando o servidor Shell Seguro . . . . .	44
Acesso da IPMI sobre Keyboard Controller Style (KCS) . . . . .	44
Evitar o rebaixamento do firmware do sistema . . . . .	45
Configurando o Gerenciamento de Chaves de Segurança (SKM) . . . . .	45
Security password manager . . . . .	45
Log de auditoria estendida . . . . .	45
Limitar o login simultâneo por conta do usuário . . . . .	46
Protetor do sistema . . . . .	46
Suporte da versão do TLS . . . . .	47
Backup e restauração da configuração do BMC . . . . .	47
Backup da configuração do BMC . . . . .	47
Restaurando a configuração do BMC . . . . .	48
Redefinindo o BMC para o padrão de fábrica . . . . .	48
Reiniciando o XClarity Controller . . . . .	49

### Capítulo 4. Monitorando o status de servidor . . . . . 51

Exibindo o resumo de funcionamento/eventos ativos de sistema . . . . .	51
Exibindo as informações do sistema . . . . .	53
Exibindo a utilização do sistema . . . . .	54
Exibindo logs de eventos . . . . .	55
Exibindo logs de auditoria . . . . .	56
Exibindo o histórico de manutenção . . . . .	56
Configurando destinatários de alertas . . . . .	57

### Capítulo 5. Configurando o servidor . . . . . 59

Exibindo as informações e as definições de configuração do adaptador . . . . .	59
Configurando o modo e a sequência de inicialização do sistema . . . . .	59
Configurando inicialização única . . . . .	60

Gerenciando a energia do servidor . . . . .	60	Acessando a interface da linha de comandos . . . . .	89
Configurando a redundância de energia . . . . .	61	Fazendo login na sessão de linha de comandos . . . . .	89
Configurando a política de limitação de energia . . . . .	61	Configurando o redirecionamento serial para SSH . . . . .	89
Configurando a política de restauração de energia . . . . .	62	Sintaxe do comando . . . . .	90
Ações de energia . . . . .	62	Recursos e limitações . . . . .	90
Gerenciando e monitorando o consumo de energia com os comandos da IPMI . . . . .	63	Listagem alfabética de comandos . . . . .	91
Baixando log de dados de serviço . . . . .	65	Comandos de utilitário . . . . .	93
Propriedades do servidor . . . . .	66	Comando exit. . . . .	93
Definindo o local e o contato . . . . .	66	Comando help . . . . .	93
Configurando tempos limites do servidor . . . . .	67	Comando history . . . . .	93
Mensagem de infração . . . . .	67	Comandos do monitor . . . . .	93
Serviço de soluções . . . . .	68	Comando clearlog . . . . .	94
Definindo a data e a hora do XClarity Controller . . . . .	68	Comando fans . . . . .	94
Configurando o chassi D3 V2 . . . . .	69	Comando mhlog. . . . .	94
		Comando led . . . . .	95
		Comando readlog . . . . .	97
		Comando servicelog . . . . .	98
		Comando syshealth . . . . .	99
		Comando temps. . . . .	100
		Comando volts . . . . .	101
		Comando vpd. . . . .	101
<b>Capítulo 6. Recurso de Console Remoto. . . . .</b>	<b>71</b>	Comandos de controle de energia e reinicialização do servidor. . . . .	102
Habilitando o recurso de console remoto . . . . .	72	Comando power. . . . .	102
Controle remoto de energia . . . . .	72	Comando reset . . . . .	103
Tela de captura do console remoto . . . . .	72	Comando fuelg . . . . .	104
Suporte a teclado de console remoto . . . . .	73	Comando pxeboot. . . . .	105
Modos de tela de console remoto. . . . .	73	Comandos de configuração . . . . .	105
Métodos de montagem de mídia . . . . .	73	Comando accseccfg . . . . .	105
Problemas de erro de montagem de mídia . . . . .	77	Comando asu. . . . .	106
Saindo da sessão de console remoto . . . . .	78	Comando backup . . . . .	109
		Comando dhcpinfo . . . . .	110
		Comando dns. . . . .	110
		Comando encaps . . . . .	111
		Comando ethtousb . . . . .	112
		Comando firewall . . . . .	112
		Comando hashpw . . . . .	114
		Comando ifconfig . . . . .	115
		Comando keycfg . . . . .	117
		Comando ldap . . . . .	117
		Comando ntp . . . . .	119
		Comando portcontrol. . . . .	120
		Comando ports . . . . .	121
		Comando rdmount. . . . .	121
		Comando restore . . . . .	122
		Comando roles . . . . .	123
		Comando rtd . . . . .	123
		Comando seccfg . . . . .	124
		Comando securityinfo . . . . .	124
<b>Capítulo 7. Configurando o armazenamento . . . . .</b>	<b>79</b>		
Detalhe do armazenamento . . . . .	79		
Configuração de RAID . . . . .	79		
Exibindo e configurando unidades virtuais . . . . .	79		
Exibindo e configurando o inventário de armazenamento . . . . .	81		
<b>Capítulo 8. Atualizando o firmware de servidor . . . . .</b>	<b>83</b>		
Visão geral da atualização de firmware . . . . .	83		
Atualização de firmware do sistema, adaptador e PSU . . . . .	84		
Atualização do repositório. . . . .	84		
<b>Capítulo 9. Gerenciamento de licenças . . . . .</b>	<b>87</b>		
Instalando uma chave de ativação . . . . .	87		
Removendo uma chave de ativação . . . . .	87		
Exportando uma chave de ativação . . . . .	88		
<b>Capítulo 10. Interface da linha de comandos . . . . .</b>	<b>89</b>		

Comando securitymode. . . . .	125
Comando set . . . . .	125
Comando snmp . . . . .	126
Comando snmpalerts. . . . .	128
Comando sshcfg . . . . .	129
Comando sslcfg . . . . .	130
Comando syslock . . . . .	132
Comando thermal . . . . .	133
Comando tls . . . . .	134
Comando trespass. . . . .	135
Comando uefipw . . . . .	135
Comando usbeth . . . . .	136
Comando users . . . . .	136
Comandos de controle do IMM. . . . .	140
Comando batch . . . . .	140
Comando clock . . . . .	141
Comando info. . . . .	142
Comando spreset . . . . .	142
Comandos sem agente . . . . .	142
Comando storage . . . . .	143
Comando adapter . . . . .	151
Comandos de suporte . . . . .	152
Comando dbgshbmc . . . . .	152

**Capítulo 11. Interface IPMI . . . . .155**

Gerenciando o XClarity Controller com a IPMI . . . . .	155
Usando o IPMItool. . . . .	155
Comandos IPMI com parâmetros OEM . . . . .	156
Obter/definir parâmetros de configuração	
LAN . . . . .	156
Comandos OEM IPMI . . . . .	168

**Apêndice A. Obtendo ajuda e assistência técnica . . . . .179**

Antes de Ligar . . . . .	179
Coletando dados de serviço . . . . .	180
Entrando em contato com o Suporte . . . . .	181

**Apêndice B. Avisos . . . . .183**

Marcas Registradas . . . . .	184
Notas Importantes. . . . .	184
Contaminação por partículas . . . . .	185
Declaração regulamentar de telecomunicação. . . . .	185
Avisos de Emissão Eletrônica . . . . .	185
Declaração RoHS BSMI de Taiwan . . . . .	186
Informações de contato de Taiwan para importação e exportação . . . . .	186

**Índice. . . . .189**



---

# Capítulo 1. Introdução

O Lenovo XClarity Controller 3 (XCC3) é o controlador de gerenciamento de última geração para servidores Lenovo ThinkSystem.

O controlador consolida a funcionalidade do processador de serviço, Super E/S, controlador de vídeo e recursos de presença remota em um único chip na placa-mãe do servidor. Ele fornece os recursos a seguir:

- Opção de uma conexão Ethernet dedicada ou compartilhada para gerenciamento de sistemas
- Suporte para HTML5
- Suporte para acesso via XClarity Mobile
- XClarity Provisioning Manager
- Configuração remota usando o XClarity Essentials ou a CLI do XClarity Controller.
- Capacidade de aplicativos e ferramentas acessarem o XClarity Controller, local ou remotamente
- Recursos aprimorados de presença remota.
- Suporte de API REST (esquema Redfish) para os aplicativos de software e serviços adicionais relacionados à Web.

## Notas:

- O XClarity Controller oferece suporte à API do Redfish Scalable Platforms Management, especificação 1.16.0, e ao esquema 2022.2
- Na interface da Web do XClarity Controller, o BMC é usado ao fazer referência ao XCC.
- Uma porta de rede de gerenciamento de sistemas dedicada pode não estar disponível em alguns servidores ThinkSystem; para esses servidores o acesso ao XClarity Controller está disponível apenas por meio de uma porta de rede compartilhada com o sistema operacional do servidor.

Este documento explica como usar as funções do XClarity Controller em um servidor ThinkSystem. O XClarity Controller funciona com o XClarity Provisioning Manager e UEFI para fornecer a capacidade de gerenciamento de sistemas para servidores ThinkSystem.

Para verificar se há atualizações de firmware, conclua as etapas a seguir.

**Nota:** Na primeira vez que você acessa o Support Portal, deve escolher a categoria do produto, a família de produtos e os números do modelo para seu servidor. A próxima vez que acessar o Support Portal, os produtos selecionados inicialmente serão pré-carregados pelo website e apenas os links para seus produtos serão exibidos. Para alterar ou incluir em sua lista de produtos, clique no link **Gerenciar minhas listas de produtos**. São feitas periodicamente mudanças no website. Os procedimentos para localizar firmware e documentação podem variar ligeiramente do que está descrito nesse documento.

1. Acesse <http://datacentersupport.lenovo.com>.
2. Em **Support (Suporte)**, selecione **Data Center**.
3. Enquanto o conteúdo é carregado, selecione **Servers (Servidores)**.
4. Em **Select Series (Selecionar série)**, primeiro selecione a série do hardware específico do servidor e, em **Select SubSeries (Selecionar sub-série)**, selecione a sub-série específica do servidor e, por fim, em **Select Machine Type (Selecionar tipo de máquina)**, selecione o tipo de máquina específico.

---

## Recursos de nível padrão e Premier do XClarity Controller

Com o XClarity Controller, são oferecidos os níveis de funcionalidade padrão e Premier do XClarity Controller. Consulte a documentação de seu servidor para obter informações adicionais sobre o nível do XClarity Controller instalado em seu servidor. Todos os níveis fornecem o seguinte:

- Acesso remoto e gerenciamento ininterruptos do servidor
- Gerenciamento remoto independente do status do servidor gerenciado
- Controle remoto de hardware e sistemas operacionais

## Recursos de nível padrão do XClarity Controller

Veja a seguir uma lista dos recursos de nível padrão do XClarity Controller:

### Interfaces de gerenciamento padrão de mercado

- Interface IPMI 2.0
- Redfish
- DCMI 1.5
- SNMPv3

### Outras interfaces de gerenciamento

- Web
- SSH CLI
- Painel frontal USB - painel do operador virtual por dispositivo móvel

### Controle de Energia/Redefinição

- Ligar
- Encerramento temporário/permanente
- Controle de ativação planejada
- Redefinição de Sistema
- Controle ordem de inicialização

### Logs de eventos

- IPMI SEL
- Log legível para o usuário
- Log de auditoria
- Mini-log

### Monitoramento de ambiente

- Monitoramento livre de agente
- Monitoramento de Sensor
- Controle de Ventilador
- Controle de LED
- Erros de chipset (Caterr, IERR etc.)
- Indicação de Funcionamento do Sistema

- Monitoramento de desempenho OOB para adaptadores de E/S
- Exibição e exportação de inventário

## **RAS**

- NMI virtual
- Recuperação automática de firmware
- Promoção automatizada de firmware de backup
- Watchdog de POST
- Watchdog do carregador de SO
- Watchdog de SO
- Captura de tela azul (falha do SO, no FFDC)
- Ferramentas de diagnóstico integradas
- Call Home

## **Configuração de rede**

- IPv4
- IPv6
- Endereço IP, máscara de sub-rede, gateway
- Modos de atribuição de endereços IP
- Nome do host
- Endereço MAC programável
- Seleção dual de MAC (se suportado pelo hardware do servidor)
- Reatribuições de porta de rede
- Marcação de VLAN

## **Protocolos de rede**

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

## **Alertas**

- Traps PET
- TRAPs SNMP v1, v2c e v3

- E-mail
- Assinaturas de notificação do Redfish

### **Presença Remota**

- Disco Remoto na Placa (RDOC)

### **Redirecionamento serial**

- IPMI SOL
- Configuração de porta serial, incluindo autoridade e velocidade
- Buffer do console serial (120s)

### **Segurança**

- CRTM do processador não host
- Atualizações de firmware assinado digitalmente
- Role Based Access Control (RBAC)
- Contas de usuários locais
- Contas do usuário LDAP/AD
- Retrocesso seguro do firmware
- NIST SP 800-131a
- Detecção de intrusão no chassi (se suportado pelo hardware do servidor)
- Somente protocolos seguros e criptografados ativados
- Criação de logs de auditoria das alterações de configuração e ações do servidor
- Autenticação de chave pública (PK)
- Desativação/realocação do sistema (RTD/ERTD)
- Suporte para PFR
- FIPS 140-3
- Modos de segurança e painel de segurança
- Armazenamento de senha segura

### **Gerenciamento de Energia**

- Medidor de energia em tempo real

### **Features on Demand**

- Repositório da chave de ativação

### **Implantação e configuração**

- Configuração remota
- Passagem do SO
- Pacotes de drivers e ferramentas de implantação e configuração incorporadas
- Backup e restauração da configuração
- Tamanho RDOC estendido (com cartão MicroSD)
- Perfis térmicos configuráveis

### **Atualizações de firmware**

- Atualização livre de agente
- Atualização remota

## **Recursos de nível Premier do XClarity Controller**

Veja a seguir uma lista dos recursos de nível Premier do XClarity Controller:

**Todos os ["Recursos de nível padrão do XClarity Controller" na página 2.](#)**

### **Logs de eventos**

- Log de substituição do componente

### **RAS**

- Captura de inicialização
- Captura de vídeo de falha

### **Alertas**

- Syslog

### **Presença Remota**

- KVM remoto
- Montagem de arquivos ISO/IMG de clientes locais
- Controle de qualidade/largura da banda
- Montagem de mídia virtual de http, Samba e NFS de arquivos ISO/IMG remotos

### **Redirecionamento serial**

- Redirecionamento serial via SSH-CLI

### **Segurança**

- Logon único
- Security Key Lifecycle Manager (SKLM/KMIP)
- Bloqueio de endereços IP
- Modo de segurança estrito corporativo (compatível com CNSA)
- Protetor do sistema

### **Gerenciamento de Energia**

- Limitação de energia
- Monitoramento de desempenho OOB - medidas de desempenho do sistema
- Gráficos de energia em tempo real
- Gráficos de temperatura

### **Implantação e configuração**

- Implementação remota de sistema operacional

### **Atualizações de firmware**

- Sincronizar com repositório

- Atualização do pacote de firmware do System Pack
- Reversão de firmware do repositório local no cartão MicroSD

## Atualizando o XClarity Controller

Se o servidor veio com o nível padrão da funcionalidade de firmware do XClarity Controller, talvez seja possível atualizar a funcionalidade do XClarity Controller no servidor. Para obter informações adicionais, sobre níveis de upgrade disponíveis e como pedi-los, consulte [Capítulo 9 "Gerenciamento de licenças" na página 87](#).

---

## Requisitos de navegador da Web e sistema operacional

Use as informações neste tópico para exibir a lista de navegadores suportados, de conjuntos de criptografia e sistemas operacionais para o servidor.

A interface da Web do XClarity Controller requer um dos seguintes navegadores da Web:

- Chrome 64.0 ou superior (64.0 ou superior para o console remoto)
- Firefox ESR 78.0 ou superior
- Microsoft Edge 79.0 ou superior
- Safari 12.0 ou superior (iOS 7 ou posterior e OS X)

**Nota:** O suporte para o recurso de console remoto não está disponível por meio do navegador em sistemas operacionais de dispositivo móvel.

Os navegadores listados acima correspondem àqueles suportados atualmente pelo firmware do XClarity Controller. O firmware do XClarity Controller pode ser aprimorado periodicamente para incluir suporte para outros navegadores.

Dependendo da versão do firmware no XClarity Controller, o suporte ao navegador da Web pode variar dos navegadores listados nesta seção. Para ver a lista de navegadores suportados para o firmware atualmente no XClarity Controller, clique na lista de menu **Navegadores Suportados** da página de login do XClarity Controller.

Para aumentar a segurança, apenas cifras extremamente fortes são suportadas ao usar HTTPS. Ao usar HTTPS, a combinação de sistema operacional cliente e navegador deve suportar um dos seguintes conjuntos de cifras:

- TLS\_AES\_256\_GCM\_SHA384
- TLS\_CHACHA20\_POLY1305\_SHA256
- TLS\_AES\_128\_GCM\_SHA256
- TLS\_AES\_128\_CCM\_8\_SHA256
- TLS\_AES\_128\_CCM\_SHA256
- TLS\_ECDHE\_RSA\_WITH\_AES\_256\_GCM\_SHA384
- TLS\_DHE\_RSA\_WITH\_AES\_256\_GCM\_SHA384
- TLS\_ECDHE\_ECDSA\_WITH\_AES\_256\_GCM\_SHA384
- TLS\_ECDHE\_RSA\_WITH\_AES\_128\_GCM\_SHA256
- TLS\_ECDHE\_RSA\_WITH\_CHACHA20\_POLY1305
- TLS\_DHE\_RSA\_WITH\_AES\_128\_GCM\_SHA256
- TLS\_ECDHE\_ECDSA\_WITH\_AES\_128\_GCM\_SHA256

- TLS\_ECDHE\_ECDSA\_WITH\_CHACHA20\_POLY1305
- TLS\_ECDHE\_RSA\_WITH\_AES\_256\_CBC\_SHA384
- TLS\_ECDHE\_RSA\_WITH\_AES\_128\_CBC\_SHA256
- TLS\_DHE\_RSA\_WITH\_AES\_256\_CBC\_SHA256
- TLS\_DHE\_RSA\_WITH\_AES\_128\_CBC\_SHA256
- TLS\_ECDHE\_ECDSA\_WITH\_AES\_256\_CBC\_SHA384
- TLS\_ECDHE\_ECDSA\_WITH\_AES\_128\_CBC\_SHA256

**Nota:** O cache de seu navegador da Internet armazena informações sobre páginas da Web que você visita para que elas sejam carregadas mais rapidamente no futuro. Após uma atualização flash do firmware do XClarity Controller, seu navegador pode continuar a usar as informações de seu cache em vez de recuperá-las do XClarity Controller. Depois de atualizar o firmware do XClarity Controller, é recomendável limpar o cache do navegador para assegurar que as páginas da Web servidas pelo XClarity Controller sejam exibidas corretamente.

---

## Suporte a vários idiomas

Use as informações neste tópico para visualizar a lista de idiomas suportados pelo XClarity Controller.

Por padrão, o idioma escolhido para a interface da Web do XClarity Controller é o inglês. A interface é capaz de exibir diversos idiomas. Eles incluem os seguintes:

- Francês
- Alemão
- Italiano
- Japonês
- Coreano
- Português (Brasil)
- Russo
- Chinês simplificado
- Espanhol (internacional)
- Chinês tradicional

Para escolher o idioma de sua preferência, clique na seta ao lado do idioma atualmente selecionado. Um menu suspenso será exibido para escolha do idioma preferencial.

As strings de texto que são geradas pelo firmware do XClarity Controller são exibidas no idioma ditado pelo navegador. Se o navegador especificar um idioma diferente de um de idiomas traduzidos listados acima, o texto será exibido em inglês. Além disso, qualquer string de texto que é exibida pelo firmware do XClarity Controller, mas não é gerada pelo controlador do XClarity Controller (por exemplo, mensagens geradas por UEFI, por adaptadores PCIe etc.) é exibida em inglês.

A entrada de texto específico de idioma diferente do inglês, como **Mensagem de Infração**, não é suportada atualmente. Apenas texto digitado em inglês é suportado.

---

## Introdução a MIBs

Use as informações neste tópico para acessar a Base de Informações de Gerenciamento.

As MIBs SNMP podem ser baixadas do <https://support.lenovo.com/> (Pesquisar por tipo de máquina no portal). Inclui as quatro MIBs a seguir.

- A **MIB do SMI** descreve a estrutura de informações de gerenciamento para o Lenovo Data Center Group.
- A **MIB do produto** descreve o identificador de objeto para os produtos Lenovo.
- A **MIB do XCC** fornece informações de inventário e monitoramento do Lenovo XClarity Controller.
- A **MIB do XCC Alert** define traps para condições de alerta detectadas pelo Lenovo XClarity Controller.

**Nota:** A ordem de importação para as quatro MIBs é **MIB do SMI** → **MIB do produto** → **MIB do XCC** → **MIB do XCC Alert**.

---

## Avisos usados neste documento

Use estas informações para compreender os avisos que são utilizados neste documento.

Os seguintes avisos são utilizados na documentação:

- **Nota:** estes avisos fornecem dicas, diretrizes ou recomendações importantes.
- **Importante:** estes avisos fornecem informações ou avisos que podem ajudar a evitar situações inconvenientes ou problemáticas.
- **Atenção:** estes avisos indicam danos potenciais aos programas, dispositivos ou dados. Um aviso de atenção é colocado antes da instrução ou situação em que o dano poderá ocorrer.

---

## Capítulo 2. Abrindo e usando a interface da Web do XClarity Controller

Este tópico descreve os procedimentos de login e as ações que podem ser executadas a partir da interface da Web do XClarity Controller.

O XClarity Controller combina as funções do processador de serviço, um controlador de vídeo e a função de presença remota em um único chip. Primeiro faça login usando a interface da Web do XClarity Controller para acessar o XClarity Controller remotamente. Este capítulo descreve os procedimentos de login e as ações que podem ser executadas a partir da interface da Web do XClarity Controller.

---

### Acessando a interface da Web do XClarity Controller

As informações neste tópico explicam como acessar a interface da Web do XClarity Controller.

O XClarity Controller oferece suporte ao endereçamento IPv4 estático e Protocolo de Configuração de Host Dinâmico (DHCP). O endereço IPv4 estático padrão designado ao XClarity Controller é 192.168.70.125. O XClarity Controller é configurado inicialmente para tentar obter um endereço de um servidor DHCP e, se não conseguir, ele usará o endereço IPv4 estático.

O XClarity Controller também oferece suporte ao IPv6, mas não tem um endereço IP IPv6 estático fixo por padrão. Para o acesso inicial ao XClarity Controller em um ambiente IPv6, é possível usar o endereço IP IPv4 ou o endereço local do link IPv6. O XClarity Controller gera um endereço IPv6 local de link exclusivo, usando o endereço MAC IEEE 802 inserindo dois octetos com dois valores hexadecimais de 0xFF e 0xFE no meio do MAC de 48 bits conforme descrito em RFC4291 e invertendo o 2º bit da direita no primeiro octeto do endereço MAC. Por exemplo, se o endereço MAC for 08-94-ef-2f-28-af, o endereço local do link será o seguinte:

```
fe80::0a94:eff:fe2f:28af
```

Ao acessar o XClarity Controller, as condições de IPv6 a seguir estarão definidas como padrão:

- A configuração de endereço IPv6 automática é habilitada.
- A configuração de endereço IP estático IPv6 é desabilitada.
- O DHCPv6 é habilitado.
- A configuração automática stateless é habilitada.

O XClarity Controller fornece a opção de usar uma conexão de rede de gerenciamento de sistemas **dedicada** (se aplicável) ou uma que seja **compartilhada** com o servidor. A conexão padrão para servidores montados em rack e torre é utilizar o conector de rede de gerenciamento de sistemas **dedicada**.

A conexão de rede de gerenciamento de sistemas dedicada na maioria dos servidores é fornecida usando um controlador de interface de rede 1Gbit. Entretanto, em alguns sistemas, a conexão de rede de gerenciamento de sistemas dedicada pode ser fornecida utilizando-se a interface Network Controller Sideband Interface (NCSI) com uma das portas de rede de um controlador de interface de rede de várias portas. Nesse caso, a conexão de rede de gerenciamento de sistemas dedicada é limitada à velocidade de 10/100 da interface lateral. Para obter informações e todas as limitações da implementação da porta de gerenciamento no sistema, consulte a documentação do sistema.

**Nota:** Uma porta de rede de gerenciamento de sistemas **dedicada** pode não estar disponível em seu servidor. Se o hardware não tiver uma porta de rede **dedicada**, a configuração **compartilhada** será a única configuração do XClarity Controller disponível.

## Configurando a conexão de rede do XClarity Controller por meio do XClarity Provisioning Manager

Use as informações neste tópico para configurar uma conexão de rede do XClarity Controller por meio do XClarity Provisioning Manager.

Depois de iniciar o servidor, é possível usar o XClarity Provisioning Manager para configurar a conexão de rede do XClarity Controller. O servidor com o XClarity Controller deve estar conectado a um servidor DHCP, ou a rede do servidor deve estar configurada para usar o endereço IP estático do XClarity Controller. Para configurar a conexão de rede do XClarity Controller por meio do Setup Utility, conclua as etapas a seguir:

Etapa 1. Ligar o servidor. A tela de boas-vindas do ThinkSystem é exibida.

**Nota:** Pode levar até 40 segundos após a conexão do servidor à energia CA para que o botão de controle de energia se torne ativo.

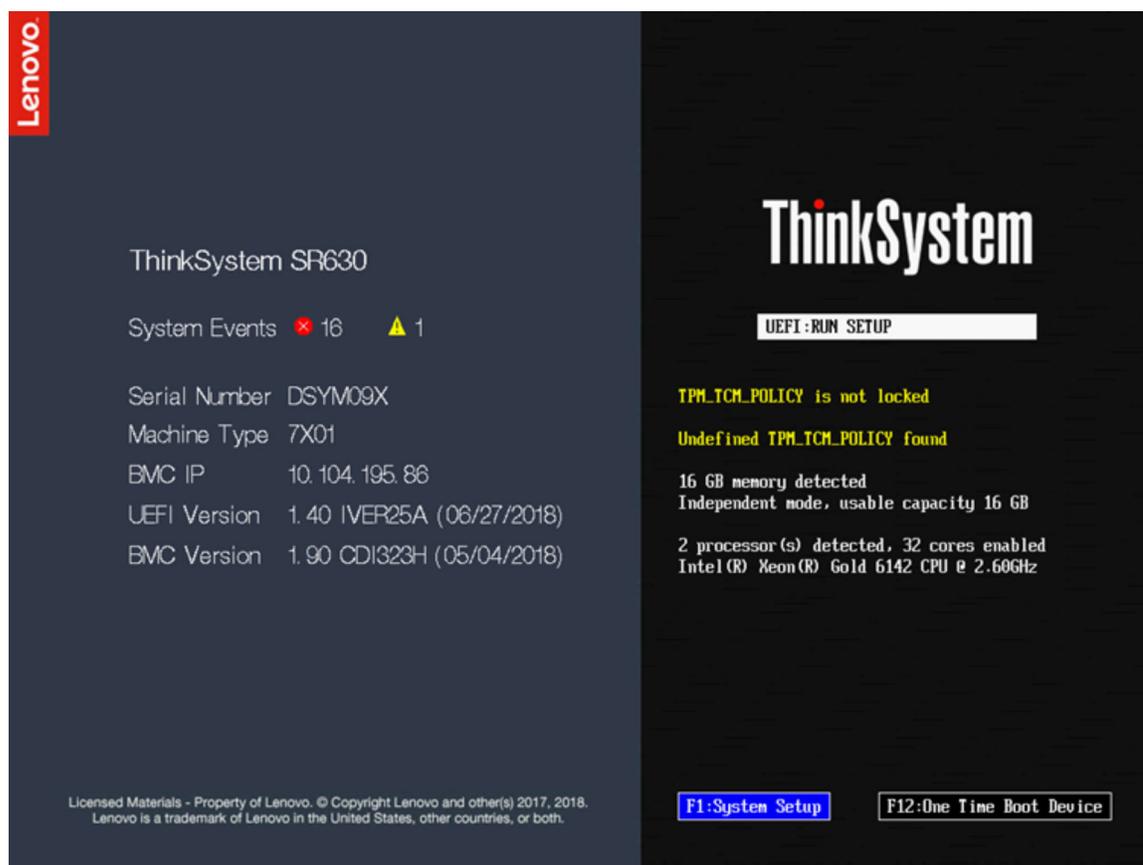


Figura 1. Tela de boas-vindas do ThinkSystem

Etapa 2. Quando o prompt <F1> System Setup for exibido, pressione F1. Se tiver configurado uma senha de inicialização e uma senha de administrador, será necessário digitar a senha de administrador para acessar o XClarity Provisioning Manager.

Etapa 3. No menu principal do XClarity Provisioning Manager, selecione **UEFI Setup**.

Etapa 4. Na próxima tela, selecione **BMC Settings**; em seguida, clique em **Network Settings**.

Etapa 5. Há três opções de conexão de rede do XClarity Controller no campo **DHCP Control**:

- IP estático

- DHCP ativado
- DHCP com fallback

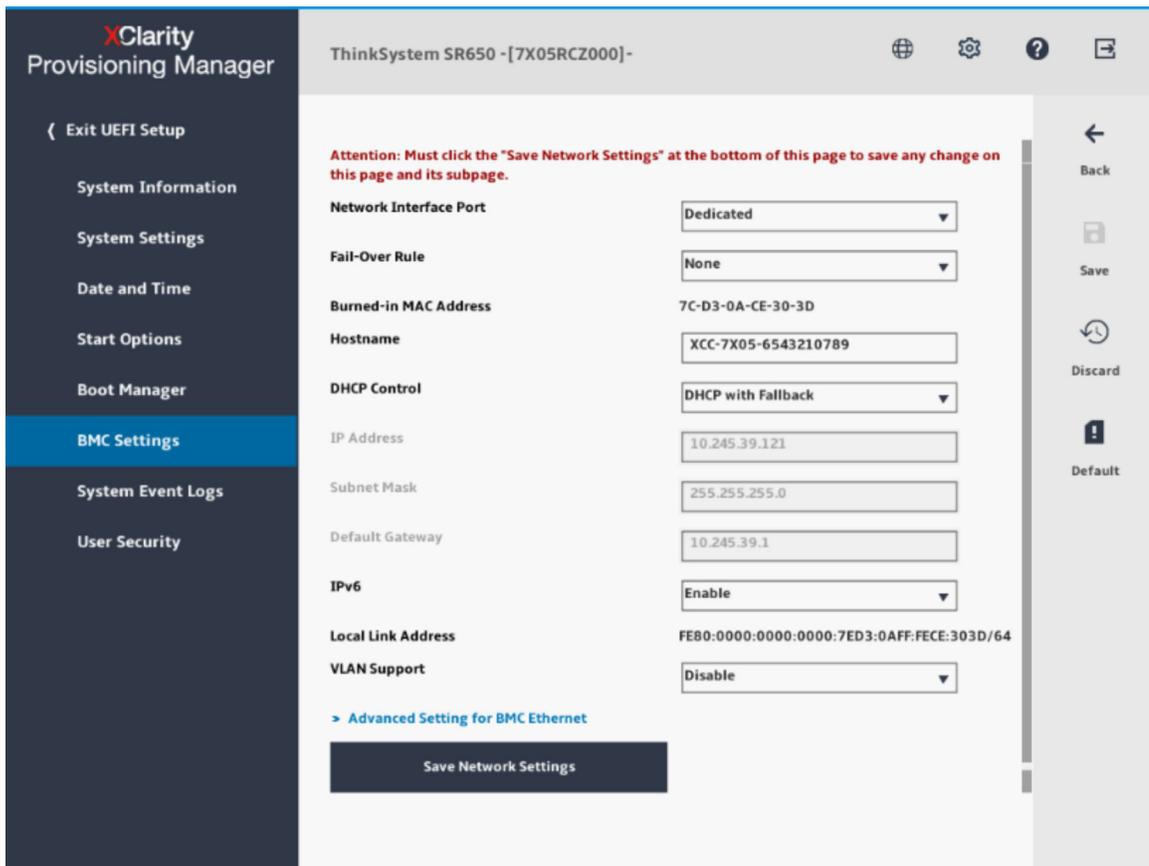


Figura 2. Configurações de conexão de rede

- Etapa 6. Selecione uma das opções de conexão de rede.
- Etapa 7. Se você optar por usar um endereço IP estático, especifique o endereço IP, a máscara de sub-rede e o gateway padrão.
- Etapa 8. É possível também usar o Lenovo XClarity Controller Manager para selecionar uma conexão de rede dedicada (se o seu servidor tiver uma porta de rede dedicada) ou uma conexão de rede do XClarity Controller compartilhada.

**Notas:**

- Uma porta de rede de gerenciamento de sistemas dedicada pode não estar disponível em seu servidor. Se o hardware não tiver uma porta de rede dedicada, a configuração **compartilhada** será a única configuração do XClarity Controller disponível. Na tela **Network Configuration**, selecione **Dedicated** (se aplicável) ou **Shared** no campo **Network Interface Port**.
- Para localizar os locais dos conectores Ethernet em seu servidor que são usados pelo XClarity Controller, consulte a documentação fornecida com seu servidor.

Etapa 9. Clique em **Salvar**.

Etapa 10. Saia do XClarity Provisioning Manager.

**Notas:**

- É preciso aguardar aproximadamente 1 minuto para que as mudanças entrem em vigor antes que o firmware do servidor esteja funcional novamente.
- Também é possível configurar a conexão de rede do XClarity Controller por meio da interface da Web do XClarity Controller ou da interface da linha de comandos (CLI). Na interface da Web do XClarity Controller, as conexões de rede podem ser configuradas clicando em **Configuração do BMC** no painel esquerdo de navegação, e selecionando **Rede**. Na CLI do XClarity Controller, as conexões de rede são configuradas usando vários comandos que dependem da configuração de sua instalação.

## Efetuando login no XClarity Controller

Use as informações neste tópico para acessar o XClarity Controller por meio da interface da Web do XClarity Controller.

**Importante:** O XClarity Controller é definido inicialmente com um nome de usuário de USERID e senha de PASSWORD (com um zero, não a letra O). Essa configuração de usuário padrão tem acesso de Supervisor. Altere esse nome de usuário e senha durante a configuração inicial para segurança aprimorada. Depois de fazer a alteração, você não poderá definir PASSWORD como a senha de login novamente.

Para acessar o XClarity Controller por meio da interface da Web do XClarity Controller, execute as seguintes etapas:

- Etapa 1. Abra um navegador da Web. No campo Endereço ou URL, digite `https://` seguido pelo endereço IP ou o nome do host do XClarity Controller ao qual você deseja se conectar.
- Etapa 2. Selecione o idioma desejado na lista suspensa de idiomas.

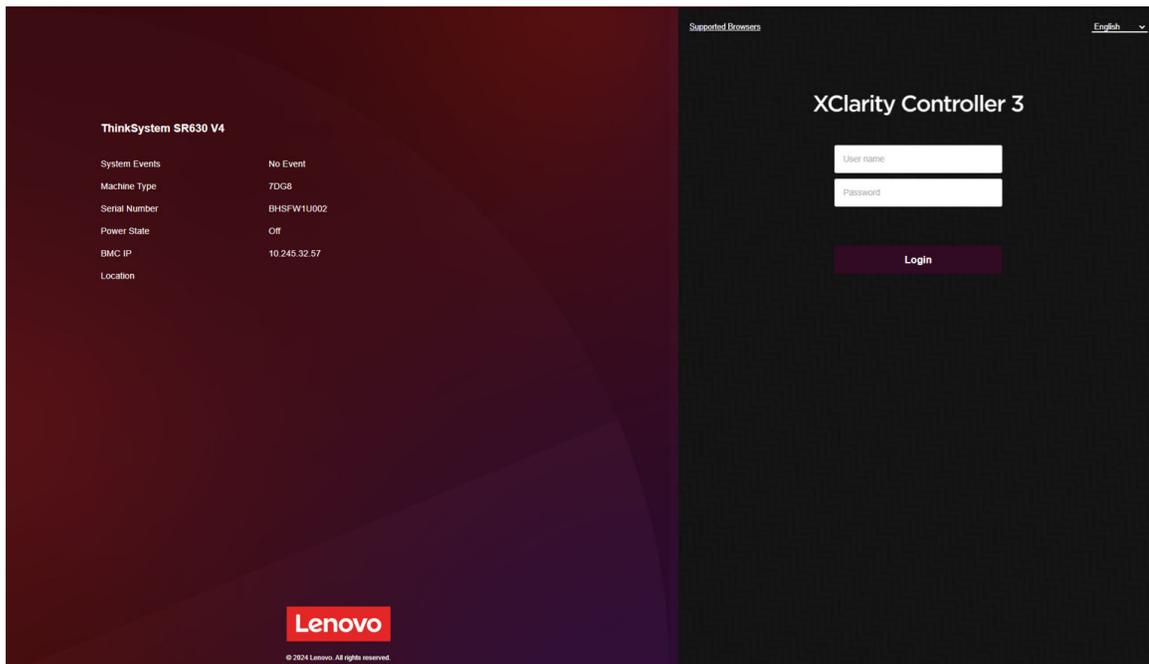


Figura 3. Página de login

- Etapa 3. Digite seu nome de usuário e senha na janela Login do XClarity Controller. Se estiver usando o XClarity Controller pela primeira vez, será possível obter seu nome de usuário e a senha a partir de seu administrador do sistema. Todas as tentativas de login são documentadas no log de eventos. Dependendo de como o seu administrador do sistema configurou o ID do usuário, talvez seja necessário inserir uma nova senha depois de fazer login.

Etapa 4. Clique em **Login** para iniciar a sessão. O navegador abre a página inicial do XClarity Controller , conforme mostrado na ilustração a seguir. A página inicial exibe informações sobre o sistema que o XClarity Controller além de ícones indicando quantos erros críticos **1** e quantos avisos **1** estão presentes atualmente no sistema.

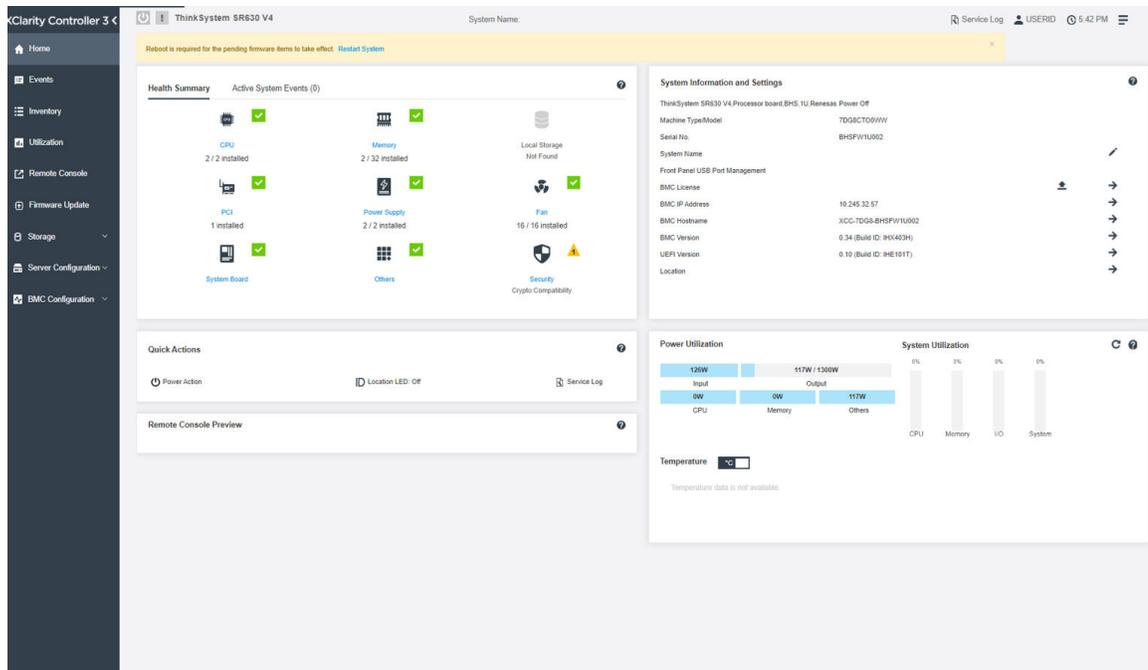


Figura 4. Página Inicial

A página inicial é dividida essencialmente em duas seções. A primeira seção é o painel de navegação esquerdo, que é um conjunto de tópicos que permitem executar as seguintes ações:

- Monitorar o status do servidor
- Configurar o servidor
- Configurar o XClarity Controller ou o BMC
- Atualizar o firmware

A segunda seção corresponde às informações gráficas fornecidas à direita do painel de navegação. O formato modular fornece uma visualização rápida do status do servidor e algumas ações rápidas que podem ser executadas.

## Descrição das funções do XClarity Controller na interface da Web

As informações neste tópico explicam as funções do XClarity Controller na interface da Web.

Veja a seguir uma tabela que descreve as funções do XClarity Controller no painel de navegação esquerdo.

**Nota:** Ao navegar pela interface da Web, também é possível clicar no ícone de ponto de interrogação para obter ajuda online.

Tab	Seleção	Descrição
Início	Resumo do funcionamento/ Eventos de sistema ativos	Mostra o status atual dos principais componentes de hardware no sistema.

Tab	Seleção	Descrição
	Informações e configurações do sistema	Fornece um resumo de informações comuns do sistema.
	Ações rápidas	Fornece um link rápido para controlar o LED de energia e de local do servidor, e um botão para baixar os dados de serviço.
	Utilização de energia	Fornece uma visão geral rápida da utilização de energia atual.
	Visualização do console remoto	Controla o servidor no nível do sistema operacional. É possível visualizar e operar o console do servidor do computador. A seção de console remoto na página inicial do XClarity Controller exibe uma imagem de tela com o botão Iniciar.
Eventos	Log de Eventos	Fornece uma lista histórica de todos eventos de gerenciamento e de hardware.
	Log de auditoria	Fornece um registro histórico das ações do usuário.
	Histórico de manutenção	Exibe todo o histórico de atualização de firmware, configuração e substituição de hardware.
	Destinatários de alertas <b>Nota:</b> Esse recurso será suportado em uma atualização futura.	Gerencia quem será notificado sobre eventos do sistema. Ela permite configurar cada destinatário e gerenciar as configurações que se aplicam a todos os destinatários de eventos. Também é possível gerar um evento de teste para verificar as configurações de notificação.
Inventário		Exibe todos os componentes no sistema, juntamente com seus status e principais informações. É possível clicar em um dispositivo para visualizar informações adicionais.  <b>Nota:</b> Consulte a interface da Web do SMM3 para obter mais detalhes do status de energia da solução.
Utilização		Exibe informações de temperatura ambiente/componente, utilização de energia, níveis de tensão e velocidade do ventilador do servidor e seus componentes em formatos gráficos ou tabulares.
Console Remoto		Fornece acesso à funcionalidade do console remoto. É possível usar o recurso de mídia virtual para montar arquivos ISO ou IMG que estão localizados no sistema ou em um local de rede que possa ser acessado pelo BMC usando CIFS, NFS, HTTPS ou SFTP. O disco montado aparece como uma unidade de disco USB ou DVD ROM conectada ao servidor.
Atualização de firmware		<ul style="list-style-type: none"> <li>• Exibe níveis de firmware.</li> <li>• Atualiza o firmware do XClarity Controller e o firmware do servidor.</li> <li>• Atualize o firmware do XClarity Controller do repositório.</li> </ul>
Armazenamento	Detalhe	Exibe a estrutura física dos dispositivos de armazenamento e a configuração de armazenamento.
	Configuração de RAID	Visualize ou modifique a configuração atual do RAID, incluindo as informações de discos virtuais e dispositivos de armazenamento físico.
Configuração do Servidor	Adaptadores	Exibe informações dos adaptadores de rede instalados e as configurações que podem ser definidas por meio do XClarity Controller.

Tab	Seleção	Descrição
	Opções de inicialização	<ul style="list-style-type: none"> <li>• Selecione o dispositivo de inicialização para inicialização única durante a próxima reinicialização do servidor.</li> <li>• Altere o modo de inicialização e as configurações de ordem de inicialização.</li> </ul>
	Política de energia	<ul style="list-style-type: none"> <li>• Configura a redundância de energia durante o evento de uma falha de fonte de alimentação.</li> <li>• Configura a política do limitação de energia.</li> <li>• Configure a política de restauração de energia.</li> </ul> <p><b>Nota:</b> Consulte a interface da Web do SMM3 para obter mais detalhes do status de energia da solução.</p>
	Propriedades do servidor	<ul style="list-style-type: none"> <li>• Monitora várias propriedades, condições de status e configurações de seu servidor.</li> <li>• Gerencie os atrasos de desligamento do servidor.</li> <li>• Crie a Mensagem de Infração. Uma Mensagem de Infração é uma mensagem que você pode criar para os usuários verem quando fazem login no XClarity Controller.</li> </ul>
	Chassi <b>Nota:</b> Este item está disponível apenas em nós compatíveis com o chassi D3 V2.	<ul style="list-style-type: none"> <li>• Exibe as informações do chassi.</li> <li>• Reinicie o nó ou simule um reposicionamento físico do nó.</li> <li>• Exibe a preferência de seleção do chassi provisório.</li> <li>• Exibe o histórico de manutenção do chassi.</li> </ul>
Configuração do BMC	Backup e restauração	Redefine os padrões de fábrica do XClarity Controller, a configuração de backup atual ou restaura a configuração a partir de um arquivo.
	Licença	Gerencia chaves de ativação para recursos opcionais do XClarity Controller.
	Rede	Configura propriedades, status e configurações de rede do XClarity Controller.
	Segurança	Configura propriedades, status e configurações de segurança do XClarity Controller.
	Usuário/LDAP	<ul style="list-style-type: none"> <li>• Configura os perfis de login do XClarity Controller e as definições globais de login.</li> <li>• Exibe as contas do usuário que estão atualmente conectadas ao XClarity Controller.</li> <li>• A guia LDAP configura a autenticação do usuário para uso com um ou mais servidores LDAP. Isso também permite que você habilite ou desabilite a segurança LDAP e gerencie seus certificados.</li> </ul>
Call Home <b>Nota:</b> Esse recurso será suportado em uma atualização futura.	Configure a opção Call Home para coletar informações sobre o sistema e enviá-las à Lenovo para serviços.	



---

## Capítulo 3. Configurando o XClarity Controller

Use as informações neste capítulo para entender as opções disponíveis para as configurações do XClarity Controller.

Ao configurar o XClarity Controller, as seguintes opções de chave estão disponíveis:

- Backup e restauração
- Licença
- Rede
- Segurança
- Usuário/LDAP

---

### Configurando contas de usuário/LDAP

Use as informações neste tópico para entender como as contas de usuário são gerenciadas.

Clique em **Usuário/LDAP** em **Configuração do BMC** para criar, modificar e visualizar contas de usuário e definir configurações de LDAP.

A guia **Usuário Local** mostra as contas de usuário definidas no XClarity Controller e quais estão conectadas atualmente no XClarity Controller.

A guia **LDAP** mostra a configuração de LDAP para acessar as contas de usuário que são mantidas em um servidor LDAP.

### Método de autenticação do usuário

Use as informações neste tópico para entender os modos que o XClarity Controller usa para autenticar tentativas de login.

Clique no menu suspenso ao lado da opção **Permitir logins de** para selecionar como as tentativas de login do usuário são autenticadas. É possível selecionar um dos métodos de autenticação a seguir:

- **Somente local:** os usuários são autenticados por uma pesquisa da conta de usuário local configurada no XClarity Controller. Se não houver correspondência do ID do usuário e senha, o acesso será negado.
- **Somente LDAP:** o XClarity Controller tenta autenticar o usuário com as credenciais mantidas em um servidor LDAP. As contas de usuário locais no XClarity Controller **não são** pesquisadas com esse método de autenticação.
- **Local primeiro, depois LDAP:** A autenticação local é tentada primeiro. Se a autenticação local falhar, então, será tentada a autenticação LDAP.
- **LDAP primeiro, depois usuário local:** a autenticação LDAP é tentada primeiro. Se a autenticação LDAP falhar, então, será tentada a autenticação local.

#### Notas:

- Somente as contas localmente administradas são compartilhadas com as interfaces IPMI e SNMP. Essas interfaces não suportam autenticação LDAP.
- Os usuários da IPMI e do SNMP podem fazer login usando as contas localmente administradas quando o campo **Permitir logins de** é configurado como **Somente LDAP**.

## Criando uma função

Use as informações neste tópico para criar uma função.

### Criar função

Clique na guia **Funções** e clique em **Criar** para criar uma função personalizada.

Preencha os seguintes campos: **Nome de função** e **Nível de autoridade**. Para obter mais detalhes sobre o nível de autoridade, consulte esta seção.

A função criada é fornecida ao usuário no menu suspenso de função na seção do usuário.

**Nota:** A função usada no Usuário e LDAP não tem permissão para editar e excluir o nome da função, mas tem acesso para modificar a permissão personalizada correspondente.

### Nível de autoridade

Uma função personalizada tem permissão para ativar quaisquer combinações dos seguintes privilégios:

#### Configuração – Rede e Segurança do BMC

Um usuário pode modificar parâmetros de configuração nas páginas Segurança do BMC e Rede.

#### Gerenciamento de Contas do Usuário

Um usuário pode incluir, modificar ou excluir usuários, e alterar as configurações de login global.

#### Acesso ao Console Remoto

Um usuário pode acessar o console remoto.

#### Acesso ao Console Remoto e ao Disco Remoto

Um usuário pode acessar o console remoto e o recurso de mídia virtual.

#### Ligar/Reiniciar Servidor Remoto

Um usuário pode executar funções de ligar e reiniciar o servidor.

#### Configuração – Básica

Um usuário pode modificar parâmetros de configuração nas páginas Propriedades e Eventos do Servidor.

#### Capacidade de Limpar Logs de Eventos

Um usuário pode limpar os logs de eventos. Qualquer um pode examinar os logs de eventos; mas é obrigatório ter este nível de autoridade para limpar os logs.

#### Configuração – Avançada (Atualização de firmware, Reiniciar BMC, Restaurar configuração)

Um usuário não tem restrições ao configurar o XClarity Controller. Além disso, considera-se que o usuário tem acesso administrativo ao XClarity Controller. O acesso administrativo inclui as seguintes funções avançadas: atualizações de firmware, inicialização de rede PXE, restauração dos padrões de fábrica do XClarity Controller, modificação e restauração das configurações do XClarity Controller de um arquivo de configuração e reinicialização e reconfiguração do XClarity Controller.

#### Configuração – Segurança do UEFI

Um usuário pode modificar as configurações de Segurança do UEFI.

### Funções predefinidas

As funções a seguir são predefinidas e não podem ser editadas nem excluídas:

#### Administrador

A função Administrador não tem restrições e pode executar todas as operações.

#### Somente Leitura

A função Somente leitura pode exibir informações do servidor, mas não pode executar uma operação que afeta o estado do sistema, como salvar, modificar, limpar, reinicializar e atualizar o firmware.

### Operador

O usuário com a função Operador tem os seguintes privilégios:

- Configuração – Rede e Segurança do BMC
- Ligar/Reiniciar Servidor Remoto
- Configuração – Básica
- Capacidade de Limpar Logs de Eventos
- Configuração – Avançada (Atualização de firmware, Reiniciar BMC, Restaurar configuração)

## Criando uma nova conta do usuário

Use as informações neste tópico para criar um novo usuário local.

### Criar Usuário

Clique na guia **usuários locais** e clique em **Criar** para Criar uma nova conta de usuário.

Preencha os seguintes campos: **Nome do usuário**, **Senha**, **Confirmar senha** e selecione uma **Função** no menu suspenso. Para obter mais detalhes sobre a **Função**, consulte a seção a seguir.

### Função

As funções a seguir são predefinidas enquanto uma nova função personalizada pode ser criada de acordo com as necessidades do usuário:

### Administrador

A função Administrador não tem restrições e pode executar todas as operações.

### Somente Leitura

A função Somente leitura pode exibir informações do servidor, mas não pode executar uma operação que afeta o estado do sistema, como salvar, modificar, limpar, reinicializar e atualizar o firmware.

### Operador

O usuário com a função Operador tem os seguintes privilégios:

- Configuração – Rede e Segurança do BMC
- Ligar/Reiniciar Servidor Remoto
- Configuração – Básica
- Capacidade de Limpar Logs de Eventos
- Configuração – Avançada (Atualização de firmware, Reiniciar BMC, Restaurar configuração)

## Configurações de SNMPv3

Para ativar o acesso SNMPv3 para um usuário, clique no botão **Editar** ao lado do usuário correspondente e, em seguida, marque **SNMP** na lista suspensa da **Interface Acessível ao Usuário**. As opções de acesso de usuário a seguir são explicadas:

### Tipo de acesso

Apenas as operações **GET** são suportadas. O XClarity Controller não oferece suporte a operações SNMPv3 **SET**. O SNMP3 só pode executar operações de consulta.

### Protocolo de autenticação

Esse algoritmo é usado pelo modelo de segurança SNMPv3 para autenticação. Os seguintes protocolos são suportados:

- Nenhum(a)
- HMAC-SHA (padrão)
- HMAC-SHA224
- HMAC-SHA256
- HMAC-SHA384
- HMAC-SHA512

### Protocolo de privacidade

A transferência de dados entre o cliente SNMP e o agente pode ser protegida usando criptografia. Os seguintes métodos são suportados:

- Nenhum(a)
- CBC-DES
- AES (padrão)
- AES192
- AES256
- AES192C
- AES256C

**Notas:** Mesmo se strings repetitivas de uma senha forem usadas por um usuário de SNMPv3, o acesso ainda será permitido para o XClarity Controller. Dois exemplos são mostrados para referência.

- Se a senha for definida como "11111111" (número de oito dígitos contendo oito vezes o número 1), o usuário ainda poderá acessar o XClarity Controller se a senha for inserida acidentalmente com mais de oito dígitos 1. Por exemplo, se a senha for inserida como "1111111111" (número de 10 dígitos contendo dez vezes o número 1), o acesso ainda será concedido. A string repetitiva será considerada tendo a mesma chave.
- Se a senha for definida como "bertbert", o usuário ainda poderá acessar o XClarity Controller se a senha for inserida acidentalmente como "bertbertbert". Ambas as senhas podem ter a mesma chave.

Para obter mais detalhes, consulte **Considerações de segurança** no documento Padrão de Internet Standard RFC 3414 (<https://tools.ietf.org/html/rfc3414>).

### Chave SSH

O XClarity Controller oferece suporte à autenticação de chave pública SSH (tipo de chave RSA). Para adicionar uma chave SSH à conta do usuário local, clique no botão **Editar** ao lado do usuário correspondente e marque **Chave SSH** na lista suspensa da **Interface Acessível ao Usuário**. As duas opções a seguir são fornecidas:

#### Selecionar arquivo de chave

Selecione o arquivo de chave SSH a ser importado para o XClarity Controller de seu servidor.

#### Inserir a chave em um campo de texto

Cole ou digite os dados da chave SSH no campo de texto.

### Notas:

- Algumas ferramentas da Lenovo podem criar uma conta do usuário temporária para acesso ao XClarity Controller quando as ferramentas são executadas no sistema operacional do servidor. Essa conta temporária não é visualizada e não usa nenhuma das 12 posições de conta de usuário local. A conta é

criada com um nome de usuário aleatório (por exemplo, "20luN4SB") e senha. A conta pode ser usada apenas para acessar o XClarity Controller na interface interna de Ethernet sobre USB, e apenas para as interfaces Redfish e SFTP. A criação e a remoção dessa conta temporária são gravadas no log de auditoria, bem como as ações realizadas pela ferramenta com essas credenciais.

- Para o ID do mecanismo de SNMPv3, o XClarity Controller usa uma string hexadecimal para indicar o ID. Essa string hexadecimal é convertida do nome do host do XClarity Controller padrão. Consulte o exemplo a seguir:

O nome do host "XCC-7x06-S4AHJ300" primeiro é convertido no formato ASCII: 88 67 67 45 55 88 48 54 45 83 52 65 72 74 51 48 48

A string hexadecimal é criada usando o formato ASCII (ignore os espaços intermediários): 58 43 43 2d 37 58 30 36 2d 53 34 41 48 4a 33 30 30

## Exclusão de uma conta do usuário

Use as informações neste tópico para remover uma conta de usuário local.

Para excluir uma conta de usuário local, clique no ícone de lixeira na linha da conta que deseja remover. Se você tiver autorização, poderá remover sua própria conta ou a conta de outros usuários, a menos que seja a única conta remanescente com privilégios de **gerenciamento de contas de usuário**.

## Usando as senhas com hash para autenticação

Use as informações neste tópico para entender como usar as senhas com hash para autenticação.

Além do uso de senhas e contas de usuário LDAP/AD, o XClarity Controller também oferece suporte a senhas com hash de terceiros para autenticação. A senha especial usa um formato de hash unidirecional (SHA256) e é compatível com as interfaces da web do XClarity Controller, do OneCLI e da CLI. No entanto, observe que a autenticação de XCC SNMP, interfaces de IPMI e CIM não oferecem suporte a senhas com hash de terceiros. Apenas a ferramenta OneCLI e a interface CLI de XCC CLI podem criar uma nova conta com uma senha com hash ou executar uma atualização de senha com hash. O XClarity Controller também permite que a ferramenta OneCLI e a interface CLI do XClarity Controller recuperem a senha com hash se a capacidade de leitura de senha com hash estiver habilitada.

### Configuração da senha com hash por meio da Web do XClarity Controller

Clique em **Segurança** em **Configuração do BMC** e role até a sessão **Gerenciador de senhas de segurança** para ativar ou desativar a função de **Senha de terceiros**. Se ativada, uma senha com hash de terceiros será usada para autenticação de login. A recuperação da senha com hash terceiros do XClarity Controller também pode ser ativada ou desativada.

**Nota:** Por padrão, as funções **Senha de terceiros** e **Permitir a recuperação de senha de terceiros** estão desativadas.

Para verificar se a senha do usuário é **Nativa** ou **Senha de terceiros**, clique em **Usuário/LDAP** em **Configuração do BMC** para obter detalhes. As informações estarão na coluna **Atributo avançado**.

#### Notas:

- Os usuários não poderão alterar uma senha se ela for uma senha de terceiros e os campos **Senha** e **Confirmar senha** estiverem desativados.
- Se a senha de terceiros tiver expirado, uma mensagem de aviso será exibida durante o processo de login de usuário.

### Configuração de senha com hash por meio da função OneCLI

- Ativando o recurso  
\$ sudo OneCli config set IMM.ThirdPartyPassword Enabled
- Criando senha com hash (sem Salt). Veja a seguir um log de exemplo para o XClarity Controller usando a senha **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 ""
```

- Criando usuário com senha com hash (com Salt). Veja a seguir um log de exemplo para o XClarity Controller usando a senha **password123**. Salt=abc.

```
$ pwhash = `echo -n password123abc | openssl dgst -sha256 | awk '{print $NF}``
$ echo $pwhash 292bc41bb078cf5bd258db60b63a4b337c8c954409442cfad7148bc6428fee
$ sudo OneCli config set IMM.Loginid.3 Admin
$ sudo OneCli config set IMM.SHA256Password.3 $pwhash
$ sudo OneCli config set IMM.SHA256PasswordSalt.3 'abc'
```

- Recuperando a senha com hash e salt.

```
$ sudo OneCli config set IMM.ThirdPartyPasswordReadable Enabled
$ sudo OneCli config show IMM.SHA256Password.3
$ sudo OneCli config show IMM.SHA256PasswordSalt.3
```

- Excluindo a senha com hash e salt.

```
$ sudo OneCli config set IMM.SHA256Password.3 ""
$ sudo OneCli config set IMM.SHA256PasswordSalt.3 ""
```

- Configurando a senha com hash para uma conta existente.

```
$ 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:** Enquanto a senha com hash estiver sendo definida, essa senha entrará em vigor imediatamente. A senha padrão original não estará mais em vigor. Neste exemplo, a senha padrão original **Passw0rd123abc** não pode ser mais usada até que a senha com hash seja excluída.

### Configuração de senha com hash por meio da função CLI

- Ativando o recurso  
> hashpw -sw enabled
- Criando senha com hash (sem Salt). Veja a seguir um log de exemplo para o XClarity Controller usando a senha **password123**.

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

```
5e884898da28047151d0e56f8dc6292773603d0d6aabbdd62a11ef721d1542d8
```

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

- Criando usuário com senha com hash (com Salt). Veja a seguir um log de exemplo para o XClarity Controller usando a senha **password123**. Salt=abc.

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

```
$ echo $pwhash 292bcbcb41bb078cf5bd258db60b63a4b337c8c954409442cfad7148bc6428fee
```

```
> users -3 -n Admin -shp 292bcbcb41bb078cf5bd258db60b63a4b337c8c954409442cfad7148bc6428fee -ssalt 'abc' -a super
```

- Recuperando a senha com hash e salt.

```
> hashpw -re enabled
```

```
> users -3 -ghp -gsalt
```

- Excluindo a senha com hash e salt.

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

- Configurando a senha com hash para uma conta existente.

```
> users -2 -n admin -p Passw0rd123abc -shp
```

```
5e884898da28047151d0e56f8dc6292773603d0d6aabbdd62a11ef721d1542d8 -a super
```

**Nota:** Enquanto a senha com hash estiver sendo definida, essa senha entrará em vigor imediatamente. A senha padrão original não estará mais em vigor. Neste exemplo, a senha padrão original **Passw0rd123abc** não pode ser mais usada até que a senha com hash seja excluída.

Depois que a senha com hash for configurada, não será possível usá-la para fazer login no XClarity Controller. Ao fazer login, será necessário usar a senha de texto simples. No exemplo a seguir, a senha de texto simples é "password123".

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

```
5e884898da28047151d0e56f8dc6292773603d0d6aabbdd62a11ef721d1542d8
```

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

## Configurando as definições de login global

Use as informações neste tópico para definir as configurações de login e da política de senha que se aplicam a todos os usuários.

### Tempo limite da sessão de inatividade da Web

Use as informações neste tópico para definir o tempo limite da sessão de inatividade da Web.

No campo **Tempo Limite da Sessão de Inatividade da Web**, é possível especificar por quanto tempo, em minutos, o XClarity Controller aguarda antes de desconectar uma sessão da Web inativa. O tempo de espera máximo é 1.440 minutos. Se configurado como 0, a sessão da Web nunca expirará.

O firmware do XClarity Controller oferece suporte a até seis sessões da Web simultâneas. Para liberar sessões para serem usadas por outras pessoas, é recomendável que você efetue logout da sessão da Web quando tiver concluído, em vez de contar com o tempo-limite de inatividade para fechar automaticamente sua sessão.

**Nota:** Se você deixar o navegador aberto em uma página da Web do XClarity Controller que é atualizada automaticamente, sua sessão da Web não fechará automaticamente devido à inatividade.

## Configurações de Política de Segurança de Conta

Use estas informações para entender e definir a política de segurança da conta para o servidor.

As informações a seguir são uma descrição dos campos para as configurações de segurança.

### Forçar a alterar senha no primeiro acesso

Depois de configurar um novo usuário com uma senha padrão, a seleção dessa caixa forçará esse usuário a alterar sua senha na primeira vez que fizer login. O valor padrão para esse campo é ter a caixa de seleção habilitada.

### Senha complexa necessária

A caixa de opção está marcada como padrão e a senha complexa deve seguir as seguintes regras:

- Conter apenas os seguintes caracteres (sem caracteres de espaço em branco permitidos): A-Z, a-z, 0-9, ~!@#\$%^&\*()-+={}|;:'"<>?/\_
- Deve conter pelo menos uma letra
- Deve conter pelo menos um número
- Deve conter pelo menos duas das seguintes combinações:
  - Pelo menos uma letra maiúscula.
  - Pelo menos uma letra minúscula.
  - Pelo menos um caractere especial.
- Nenhum outro caractere (em particular, espaços ou caracteres de espaço em branco) é permitido
- As senhas não podem ter mais do que duas instâncias consecutivas do mesmo caractere (isto é, "aaa").
- A senha não pode ser literalmente a mesma que o nome do usuário, simplesmente repetindo o nome do usuário uma ou mais vezes ou uma ordem de caracteres inversa do nome do usuário.
- As senhas devem ter no mínimo 8 e no máximo 255 caracteres.

Se a caixa de opção não estiver marcada, o número especificado no comprimento mínimo da senha poderá ser configurado como 0 – 255 caracteres. A senha da conta pode ficar em branco se o comprimento mínimo da senha for definido como 0.

### Período de Expiração da Senha (dias)

Esse campo contém a idade máxima da senha que é permitida antes que a senha precise ser alterada.

### Período de aviso de expiração da senha (dias)

Esse campo contém o número de dias em que um usuário é advertido antes que a senha expire.

### Comprimento mínimo de senha (caracteres)

Esse campo contém o comprimento mínimo da senha.

### Ciclo mínimo de reutilização de senha (vezes)

Esse campo contém o número de senhas anteriores que não podem ser reutilizadas.

### Intervalo Mínimo de Mudança de Senha (Horas)

Esse campo contém quanto tempo um usuário deve aguardar entre as mudanças de senha.

### Número Máximo de Falhas de Login (Vezes)

Esse campo contém o número de tentativas de login com falha que é permitido antes que o usuário seja bloqueado por um período de tempo.

### **Período de Bloqueio Após Máximo de Falhas de Login (Minutos)**

Esse campo especifica quanto tempo (em minutos) o subsistema do XClarity Controller desativará as tentativas de login remoto depois que o número máximo de falhas de login foi atingido.

## **Configurando LDAP**

Use as informações neste tópico para visualizar ou alterar as configurações de LDAP do XClarity Controller.

O suporte de LDAP inclui:

- Suporte para protocolo LDAP versão 3 (RFC-2251)
- Suporte para APIs de cliente LDAP padrão (RFC-1823)
- Suporte para a sintaxe padrão de filtro de pesquisa do LDAP (RFC-2254)
- Suporte para extensão Lightweight Directory Access Protocol (v3) para Transport Layer Security (RFC-2830)

A implementação de LDAP oferece suporte aos seguintes servidores LDAP:

- Microsoft Active Directory (Windows 2003, Windows 2008, Windows 2012, Windows 2016, Windows 2019)
- Modo de aplicativo do Microsoft Active Directory (Windows 2003, Windows 2008)
- Serviço de diretório Microsoft Lightweight (Windows 2008, Windows 2012, Windows 2016, Windows 2019)
- Novell eDirectory Server, versão 8.7 e 8.8
- Servidor OpenLDAP 2.1, 2.2, 2.3, 2.4, 2.5 e 2.6

Clique na guia **LDAP** para visualizar ou modificar as de LDAP do XClarity Controller.

O XClarity Controller pode autenticar remotamente o acesso de um usuário por um servidor LDAP central em vez das contas de usuário locais que estão armazenadas no próprio XClarity Controller ou além delas. Os privilégios podem ser designados para cada conta de usuário usando o valor do "atributo de Permissão de Login". Também é possível usar o servidor LDAP para designar usuários a grupos e executar a autenticação de grupos, além da autenticação normal do usuário (verificação de senha). Por exemplo, um XClarity Controller pode ser associado a um ou mais grupos; o usuário só aprovará a autenticação do grupo se o usuário pertencer a pelo menos um grupo que está associado ao XClarity Controller.

Para configurar um servidor LDAP, conclua as seguintes etapas:

1. Em **Informações do servidor LDAP**, as opções a seguir estão disponíveis na lista de itens:

- **Usar o servidor LDAP apenas para autenticação (com autorização local)**: essa seleção direcionará o XClarity Controller para usar as credenciais apenas para fazer a autenticação no servidor LDAP e para recuperar informações de associação ao grupo. Os nomes e as funções do grupo podem ser configurados na seção **Grupos para Autorização Local**.
- **Usar o servidor LDAP para autenticação e autorização**: essa seleção direcionará o XClarity Controller para usar as credenciais para fazer a autenticação no servidor LDAP e para identificar a permissão de um usuário.

**Nota:** Os servidores LDAP a serem usados para autenticação podem ser configurados manualmente ou descobertos dinamicamente por meio de registros DNS SRV.

- **Usar servidores pré-configurados**: você pode configurar até três servidores LDAP digitando o endereço IP ou o nome do host de cada servidor se o DNS estiver habilitado. O número da porta para

cada servidor é opcional. Se esse campo for deixado em branco, o valor padrão de 389 será usado para conexões LDAP não asseguradas. Para conexões seguras, o padrão da porta padrão é 636. Pelo menos um servidor LDAP deve ser configurado.

- **Usar DNS para localizar servidores:** é possível optar por descobrir dinamicamente os servidores LDAP. Os mecanismos descritos em RFC2782 (um DNS RR para especificar o local de serviços) são utilizados para localizar o servidor LDAP. Isso é conhecido como DNS SRV. É necessário especificar um nome de domínio totalmente qualificado (FQDN) para ser usado como o nome do domínio na solicitação DNS SRV.
  - **Floresta AD:** em um ambiente com grupos universais em domínios cruzados, o nome de floresta (conjunto de domínios) deve ser configurado para descobrir os catálogos globais necessários (GC). Em um ambiente no qual a associação ao grupo de domínio cruzado não é aplicável, esse campo pode ser deixado em branco.
  - **Domínio AD:** será necessário especificar um nome de domínio totalmente qualificado (FQDN) para ser usado como o nome do domínio na solicitação DNS SRV.

Se desejar habilitar o LDAP seguro, clique na caixa de seleção **Habilitar LDAP seguro**. Para oferecer suporte ao LDAP seguro, um certificado SSL válido deve ser instalado e pelo menos um certificado confiável de cliente SSL deve ser importado para o XClarity Controller. Seu servidor LDAP deve oferecer suporte ao TLS versão 1.2 para ser compatível com o cliente LDAP seguro XClarity Controller. Para obter informações adicionais sobre manipulação de certificado, consulte "[Manipulação de certificado SSL](#)" na página 42.

2. Preencha as informações em **Parâmetros adicionais**. Veja a seguir as explicações dos parâmetros.

#### Tipo de LDAP

Selecione o tipo de servidor LDAP para autenticação baseada em LDAP. Os seguintes tipos de servidor estão disponíveis:

- **OpenLDAP**  
OpenLDAP
- **Active Directory**  
Diretório: Windows Active Directory
- **Outro**  
Diretório: Apache Directory, eDirectory etc.

#### Método de ligação

Para poder procurar ou consultar o servidor LDAP, você deve enviar uma solicitação de ligação. Esse campo controla como essa ligação inicial para o servidor LDAP é executada. Os métodos de ligação a seguir estão disponíveis:

- **Usar credenciais configuradas**  
Use esse método para ligação com o DN e senha do cliente configurados.
- **Usar credenciais de login**  
Use esse método para ligação com as credenciais que são fornecidas durante o processo de login. O ID do usuário pode ser fornecido utilizando um DN, um DN parcial, um nome de domínio totalmente qualificado ou por meio de um ID do usuário que corresponda ao campo Atributo de Pesquisa de UID configurado no XClarity Controller. Se as credenciais apresentadas forem semelhantes a um DN parcial (por exemplo, cn=joe), esse DN parcial será adicionado ao DN Raiz configurado, em uma tentativa de criar um DN que corresponda ao registro do usuário. Se a tentativa de ligação falhar, será feita uma tentativa final de ligar adicionando cn = à credencial de login e adicionando a cadeia de caracteres resultante ao DN raiz configurado.

Se a ligação inicial for bem-sucedida, será realizada uma pesquisa para localizar no servidor LDAP uma entrada que pertença ao usuário que está efetuando login. Se necessário, será feita uma segunda tentativa de ligação, desta vez, com o DN recuperado do registro LDAP do usuário e a senha inserida durante o processo de login. Se a segunda tentativa de ligação falhar, o usuário terá o acesso negado. A segunda associação é executada somente quando os métodos de associação **Usar Credenciais Configuradas** são usados.

#### **Nome distinto do cliente**

O DN (Nome Distinto do Cliente) a ser usado para a associação inicial. E é limitado a um máximo de 300 caracteres.

#### **Senha do cliente**

A senha para este cliente distinto.

#### **DN raiz**

Esse é o nome distinto (DN) da entrada raiz da árvore de diretórios no servidor LDAP (por exemplo, dn=mycompany,dc=com). Esse DN é usado como o objeto base para todas as solicitações de pesquisa.

#### **Atributo de pesquisa do nome de login do usuário**

Quando o método de associação é definido como **Usar Credenciais Configuradas**, a associação inicial ao servidor LDAP é seguida por uma solicitação de pesquisa que recupera informações específicas sobre o usuário, incluindo o DN do usuário, permissões de login e associação de grupo. Essa solicitação de pesquisa deve especificar o nome do atributo que representa os IDs de usuário nesse servidor. Esse nome de atributo é configurado nesse campo. Em servidores Active Directory, o nome do atributo é geralmente **CN** ou **sAMAccountName**. Em servidores Novell eDirectory e OpenLDAP, o nome do atributo é uid. Se esse campo for deixado em branco, o padrão será **sAMAccountName**.

#### **Filtro de Grupo**

O campo **Filtro de Grupo** é usado para autenticação de grupo. A autenticação de grupo será tentada após as credenciais do usuário serem verificadas com êxito. Se a autenticação de grupo falhar, a tentativa do usuário de efetuar login será negada. Quando configurado, o filtro de grupo é usado para especificar a quais grupos o XClarity Controller pertence. Isso significa que, para ter êxito, o usuário deve pertencer a pelo menos um dos grupos configurados para a autenticação de grupo. Se o campo **Filtro de Grupo** for deixado em branco, a autenticação de grupo automaticamente será bem-sucedida. Se o filtro de grupo for configurado, será feita uma tentativa de corresponder pelo menos um grupo na lista a um grupo ao qual o usuário pertence. Se não houver nenhuma correspondência, o usuário falhará na autenticação e terá o acesso negado. Se houver pelo menos uma correspondência, a autenticação de grupo será bem-sucedida. As comparações fazem distinção entre maiúsculas e minúsculas. O filtro é limitado a 511 caracteres e pode consistir em um ou mais nomes de grupos. O caractere de dois-pontos (:) deve ser usado para delimitar diversos nomes de grupos. Os espaços à esquerda e à direita são ignorados, mas qualquer outro espaço é tratado como parte do nome do grupo.

**Nota:** O caractere curinga (\*) não é mais tratado como um curinga. O conceito de curinga foi descontinuado para evitar exposições de segurança. Um nome de grupo pode ser especificado como um DN completo ou usando apenas a parte de **cn**. Por exemplo, um grupo com um DN cn=adminGroup, dc=mycompany, dc=com pode ser especificado usando o DN real ou com adminGroup.

#### **Atributo de Pesquisa de Associação de Grupo**

O campo **Atributo de Pesquisa de Grupo** especifica o nome do atributo usado para identificar os grupos aos quais um usuário pertence. Em servidores Active Directory, o nome do atributo é geralmente **memberOf**. Nos servidores Novell eDirectory, o nome do atributo é

**groupMembership.** Em servidores OpenLDAP, os usuários geralmente são atribuídos a grupos cujo objectClass é igual a PosixGroup. Neste contexto, esse campo especifica o nome do atributo que é usado para identificar os membros de um PosixGroup específico. O nome do atributo é **memberUid**. Se esse campo ficar em branco, o nome do atributo no filtro assumirá por padrão **memberOf**.

### Atributo de Permissão de Login

Quando um usuário é autenticado por meio de um servidor LDAP com sucesso, as permissões de login para o usuário devem ser recuperadas. Para recuperar as permissões de login, o filtro de procura que é enviado ao servidor deve especificar o nome do atributo que está associado às permissões de login. O campo **Atributo de Permissão de Login** especifica o nome do atributo. Se estiver usando o servidor LDAP para autenticação e autorização, mas esse campo ficar em branco, o usuário recusará o acesso.

O valor do atributo retornado pelas pesquisas do servidor LDAP deve ser uma cadeia de caracteres de bits inserida como 13 0s ou 1s consecutivos ou uma cadeia de caracteres de bits como 13 0s ou 1s consecutivos no total. Cada bit representa um conjunto de funções. Os bits são numerados de acordo com suas posições. O bit mais à esquerda é a posição de bit 0 e o bit mais à direita é a posição de bit 12. Um valor de 1 em uma posição de bit habilita a função associada a essa posição de bits. Um valor de 0 em uma posição de bit desativa a função que está associada a essa posição de bit.

A cadeia de caracteres 010000000000 é um exemplo válido, que é usado para permitir que ele seja colocado em qualquer campo. O atributo que você usar pode permitir uma sequência de formatação livre. Quando o atributo é recuperado com êxito, o valor retornado pelo servidor LDAP é interpretado de acordo com as informações na tabela a seguir.

Tabela 1. Bits de permissão

Tabela de três colunas que contém explicações de posição de bit.

Posição do Bit	Função	Explicação
0	Negar Sempre	A autenticação de um usuário sempre falhará. Essa função pode ser usada para bloquear um determinado usuário ou usuários associados a um determinado grupo.
1	Acesso de Supervisor	Privilégios de administrador são concedidos a um usuário. O usuário tem acesso de leitura/gravação a cada função. Se você configurar esse bit, não terá de configurar individualmente os outros bits.
2	Acesso Somente Leitura	Um usuário possui acesso somente leitura e não pode executar nenhum procedimento de manutenção (por exemplo, reinicialização, ações remotas ou atualizações de firmware) nem fazer modificações (por exemplo, as funções salvar, limpar ou restaurar). A posição de bit 2 e todos os demais bits são mutuamente exclusivos, com a posição de bit 2 tendo a precedência mais baixa. Quando qualquer outro bit for configurado, esse bit será ignorado.
3	Configuração – Rede e Segurança do BMC	Um usuário pode modificar as configurações de Segurança, Protocolos de Rede, Interface de Rede, Designações de Porta e Porta Serial.
4	Gerenciamento de Contas do Usuário	Um usuário pode incluir, modificar ou excluir usuários e alterar as Configurações de Login Global na janela Perfis de Login.
5	Acesso ao Console Remoto	Um usuário pode acessar o console do servidor remoto.
6	Acesso ao Console Remoto e ao Disco Remoto	Um usuário pode acessar o console do servidor remoto e as funções de disco remoto para o servidor remoto.

Tabela 1. Bits de permissão (continuação)

Posição do Bit	Função	Explicação
7	Acesso para Ligar/ Reiniciar Servidor Remoto	Um usuário pode acessar as funções de ligação e reinicialização para o servidor remoto.
8	Configuração – Básica	Um usuário pode modificar parâmetros de configuração nas janelas Configurações do Sistema e Alertas.
9	Capacidade de Limpar Logs de Eventos	Um usuário pode limpar os logs de eventos. <b>Nota:</b> Todos os usuários podem visualizar os logs de eventos; mas, para limpar os logs, o usuário precisa ter esse nível de permissão.
10	Configuração – Avançada (Atualização de firmware, Reiniciar BMC, Restaurar configuração)	Um usuário não tem restrições ao configurar o XClarity Controller. Além disso, o usuário tem acesso administrativo ao XClarity Controller. O usuário pode executar as seguintes funções avançadas: atualizar o firmware, inicializar a rede PXE, restaurar os padrões de fábrica do adaptador, modificar e restaurar a configuração de adaptador a partir de um arquivo de configuração e reiniciar/reconfigurar o adaptador.
11	Configuração – Segurança do UEFI	Um usuário pode definir as configurações relacionadas à segurança UEFI, que também podem ser configuradas na página de configuração de segurança UEFI F1.
12	Reservado	Reservado para uso futuro e atualmente ignorado.

Se nenhum dos bits estiver definido, o usuário terá o acesso recusado

**Nota:** Observe que é dada prioridade às permissões de login recuperadas diretamente do registro do usuário. Se o usuário não tiver o atributo de permissão de login no registro, será feita uma tentativa de recuperar as permissões dos grupos aos quais o usuário pertence e, se configurado, que correspondem ao filtro de grupo. Nesse caso, será designado ao usuário o OR inclusivo de todos os bits para todos os grupos. De forma similar, o bit **Acesso Somente Leitura** será definido apenas se os demais bits forem zero. Além disso, observe que, se o bit **Negar Sempre** estiver definido para qualquer um dos grupos, o usuário terá o acesso recusado. O bit **Negar Sempre** tem sempre precedência sobre os demais bits.

**Importante:** Se você conceder a um usuário a capacidade de modificar os parâmetros básicos de configuração do adaptador relacionados à rede e/ou à segurança, você deverá conceder a esse mesmo usuário a capacidade de reiniciar o XClarity Controller (posição de bit 10). Caso contrário, sem essa capacidade, um usuário poderá alterar parâmetros (por exemplo, endereço IP do adaptador) mas essas alterações não terão efeito.

- Se o modo **Usar o servidor LDAP somente para autenticação (com autorização local)** for usado, configure os **Grupos para Autorização Local**. Nome do Grupo, Domínio do Grupo e Função são configurados para fornecer autorização local para grupos de usuários. Cada grupo pode ser atribuído com uma Função (permissões) que é a mesma configurada nas funções em Usuário Local. As contas de usuário são atribuídas a grupos diferentes no servidor LDAP. Uma conta de usuário será atribuída com a Função (permissões) do grupo ao qual essa conta de usuário pertence depois de fazer login no BMC. O Domínio de Grupo deve estar no mesmo formato que o Nome Distinto, como: dc=mycompany,dc=com, será usado como objeto base para pesquisas de grupo. Se o campo for deixado em branco, ele usará o mesmo valor que o campo "DN raiz". Grupos adicionais podem ser adicionados clicando no ícone "+" ou excluídos clicando no ícone "x".
- Selecione o atributo usado para exibir o nome do usuário no menu suspenso **Especificar o atributo usado para exibir nome do usuário**.

---

## Configurando protocolos de rede

Use as informações neste tópico para visualizar ou estabelecer as configurações de rede do XClarity Controller.

### Configurando as definições de Ethernet

Use as informações neste tópico para visualizar ou alterar como o XClarity Controller se comunica por uma conexão Ethernet.

**Nota:** Os servidores AMD não oferecem suporte à função de failover Ethernet.

O XClarity Controller usa dois controladores de rede. Um controlador de rede está conectado à porta de gerenciamento dedicada e o outro controlador de rede está conectado à porta compartilhada. Cada um dos controladores de rede recebe seu próprio endereço MAC gravado. Se o DHCP estiver sendo usado para atribuir um endereço IP ao XClarity Controller, quando um usuário alternar entre as portas de rede ou quando ocorrer um failover da porta de rede dedicada para a porta de rede compartilhada, um endereço IP diferente poderá ser atribuído ao XClarity Controller pelo servidor DHCP. É recomendado que, ao usar DHCP, os usuários utilizem o nome do host para acessar o XClarity Controller em vez de contar com um endereço IP. Mesmo se as portas de rede do XClarity Controller não forem alteradas, o servidor DHCP poderá atribuir um endereço IP diferente ao XClarity Controller quando a autorização do DHCP expirar ou o XClarity Controller for reinicializado. Se um usuário precisar acessar o XClarity Controller usando um endereço IP que não será alterado, o XClarity Controller deverá ser configurado para um endereço IP estático em vez de DHCP.

Clique em **Network** em **Configuração do BMC** para modificar as definições de Ethernet do XClarity Controller.

### Configurando o nome de host do XClarity Controller

O nome do host padrão do XClarity Controller é gerado usando uma combinação da cadeia de caracteres "XCC -" seguida pelo tipo de máquina do servidor e o número de série do servidor, por exemplo "XCC-7X03-1234567890"). É possível alterar o nome de host do XClarity Controller inserindo, no máximo, 63 caracteres nesse campo. O nome de host não deve incluir ponto (.) e pode conter apenas caracteres alfabéticos, numéricos, hifens e sublinhados.

### Portas Ethernet

Essa configuração controla a ativação de portas Ethernet usadas pelo controlador de gerenciamento, incluindo portas compartilhadas e dedicadas.

Depois de **desativadas**, nenhum endereço IPv4 ou IPv6 será atribuído às portas Ethernet e serão impedidas alterações adicionais em qualquer configuração de Ethernet.

**Nota:** Essa configuração não afeta a interface LAN USB ou a porta de gerenciamento USB na parte frontal do servidor. Essas interfaces têm suas próprias configurações de ativação dedicadas.

### Definindo configurações de rede IPv4

Para usar uma conexão de Ethernet IPv4, conclua as etapas a seguir:

1. Habilite a opção **IPv4**.

**Nota:** A desativação da interface Ethernet evita o acesso ao XClarity Controller a partir da rede externa.

2. No campo **Método**, selecione uma das opções a seguir:

- **Obter IP de DHCP:** o XClarity Controller obterá seu endereço IPv4 de um servidor DHCP.

- **Usar endereço IP estático:** o XClarity Controller usará o valor especificado pelo usuário para seu endereço IPv4.
  - **Primeiro DHCP, depois endereço IP estático:** o XClarity Controller tentará obter o endereço IPv4 de um servidor DHCP, mas se a tentativa falhar, o XClarity Controller usará o valor especificado pelo usuário para seu endereço IPv4.
3. No campo **Endereço IPv4 estático**, digite o endereço IP que você deseja atribuir ao XClarity Controller.

**Nota:** O endereço IP deve conter quatro números inteiros de 0 a 255 sem espaços e separados por pontos. Esse campo não será configurável se o método for definido como **Obter IP de DHCP**.

4. No campo **Máscara de rede**, digite a máscara de sub-rede que é usada pelo XClarity Controller.

**Nota:** A máscara de sub-rede deve conter quatro números inteiros de 0 a 255 sem espaços e pontos consecutivos e separados por pontos. A configuração padrão é 255.255.255.0. Esse campo não será configurável se o método for definido como **Obter IP de DHCP**.

5. No campo **Gateway Padrão**, digite seu roteador de gateway de rede.

**Nota:** O endereço do gateway deve conter quatro números inteiros de 0 a 255 sem espaços e pontos consecutivos e separados por pontos. Esse campo não será configurável se o método for definido como **Obter IP de DHCP**.

### Definindo as configurações avançadas de Ethernet

Clique na guia **Ethernet Avançada** para configurar definições de Ethernet adicionais.

Para ativar a identificação da LAN Virtual (VLAN), marque a caixa de seleção **Ativar VLAN**. Quando a VLAN está habilitada e um ID da VLAN é configurado, o XClarity Controller só aceita pacotes com os IDs de VLAN especificados. Os IDs de VLAN podem ser configuradas com valores numéricos entre 1 e 4094.

Na lista **Endereço MAC**, escolha uma das seguintes seleções:

- **Usar endereço MAC gravado**

A opção Endereço MAC Gravado é um endereço físico exclusivo designado a este XClarity Controller pelo fabricante. O endereço é um campo somente leitura.

- **Usar endereço MAC personalizado**

Se um valor for especificado, o endereço localmente administrado substituirá o endereço MAC gravado. O endereço localmente administrado deve ser um valor hexadecimal de 000000000000 por meio de FFFFFFFF. Esse valor deve estar em formato **xx:xx:xx:xx:xx:xx** em que **x** é um número hexadecimal de 0 a 9 ou a "a" a "f". O XClarity Controller não oferece suporte ao uso de um endereço multicast. O primeiro byte de um endereço multicast é um número ímpar (o bit menos significativo é configurado como 1); portanto, o primeiro byte deve ser um número par.

No campo **Taxa de dados e duplex**, selecione **negociação automática** ou **personalizada** para especificar a taxa de dados e o duplex.

No campo **MTU (Unidade de Transmissão Máxima)**, especifique a unidade máxima de transmissão de um pacote (em bytes) para sua interface de rede. A intervalo de unidade de transmissão máxima é de 1.000 a 1.500. O valor padrão para esse campo é 1.500.

### Definindo configurações de rede IPv6

1. Habilite a opção **IPv6**.
2. Atribua um endereço IPv6 à interface usando um destes métodos de atribuição:
  - Usar configuração automática de endereço sem estado

- Usar configuração automática de endereço com estado (DHCPv6)
- Usar endereço IP designado estaticamente

**Notas:** Quando **Usar endereço IP atribuído estaticamente** é escolhido, será solicitado que você digite as seguintes informações:

- Endereço IPv6
- Comprimento do prefixo
- Gateway

## Configurando o DNS

Use as informações neste tópico para exibir ou alterar as configurações de DNS do XClarity Controller.

Clique em **Network** em **Configuração do BMC** para visualizar ou modificar as definições do DNS do XClarity Controller.

Se você clicar na caixa de seleção **Usar servidores de endereço DNS adicionais**, especifique os endereços IP de até três servidores do Sistema de Nomes de Domínio em sua rede. Cada endereço IP deve conter quatro números inteiros de 0 a 255 separados por pontos. Esses servidores DNS são incluídos no início da lista de pesquisa, para que a consulta de nome do host seja feita nesses servidores antes de ocorrer em um designado automaticamente por um servidor DHCP.

Se você clicar na caixa de seleção **Usar DNS para descobrir o Lenovo XClarity Administrator**, o XClarity Manager deverá ser selecionado.

## Configurando o DDNS

Use as informações neste tópico para habilitar ou desabilitar o protocolo DDNS do XClarity Controller.

Clique em **Network** em **Configuração do BMC** para visualizar ou modificar as definições do DDNS do XClarity Controller.

Clique na caixa de seleção **Ativar DDNS** para ativar o DDNS. Quando o DDNS é habilitado, o XClarity Controller notifica um servidor de nome de domínio para alterar, em tempo real, a configuração do servidor de nomes de domínio ativo dos nomes de host configurados do XClarity Controller, endereços ou outras informações armazenadas no servidor de nomes de domínio.

Escolha uma opção na lista de itens para decidir como você deseja que o nome de domínio do XClarity Controller seja selecionado.

- **Usar nome de domínio personalizado:** é possível especificar o nome do domínio ao qual pertence o XClarity Controller.
- **Usar nome de domínio obtido do servidor DHCP:** o nome do domínio ao qual pertence o XClarity Controller é especificado pelo servidor DHCP.

## Configurando Ethernet sobre USB

Use as informações neste tópico para controlar a interface de Ethernet sobre USB usada para comunicação dentro da banda entre o servidor e o XClarity Controller.

Clique em **Network** em **Configuração do BMC** para visualizar ou modificar as configurações de Ethernet sobre USB do XClarity Controller.

A Ethernet sobre USB é usada para comunicação dentro da banda do XClarity Controller. Clique na caixa de seleção para habilitar ou desabilitar a interface Ethernet sobre USB.

#### Importante:

- Se você desabilitar **Ethernet sobre USB**, não será possível executar uma atualização dentro da banda do firmware do XClarity Controller nem do firmware do servidor usando o utilitário de atualização dentro da banda do XClarity Essentials. Use a opção Atualização de firmware na interface da Web do XClarity Controller ou no utilitário de atualização fora de banda do XClarity Essentials para atualizar o firmware.
- É importante desativar o tempo limite de watchdog para impedir que o servidor seja reiniciado inesperadamente quando a interface em banda USB estiver desativada.
- Para usar essa interface, os drivers do sistema operacional que suportam essa função (RNDIS para Windows, cdc\_ether e usbnet para Linux) devem ser instalados. O XClarity Controller fornece um arquivo INF para Windows que permite que o Windows reconheça o dispositivo USB do XClarity Controller como um dispositivo RNDIS.

Selecione o método que o XClarity Controller usa para atribuir endereços para os terminais da interface Ethernet sobre USB.

- **Usar endereço local de link IPv6 para Ethernet sobre USB:** Esse método usa endereços IPv6 com base no endereço MAC aos quais foram alocados os terminais da interface Ethernet sobre USB. Geralmente, o endereço local de link IPv6 é gerado usando o endereço MAC (RFC 4862), mas o Windows 2008 e sistemas operacionais 2016 mais recentes não oferecem suporte a um endereço IPv6 local de link na ponta estática da interface host. Em vez disso, o comportamento padrão do Windows gera novamente endereços de links locais aleatórios durante a execução. Se a interface de Ethernet sobre USB do XClarity Controller estiver configurada para usar o modo de endereço local de link IPv6, várias funções que utilizam essa interface não funcionarão porque o XClarity Controller não sabe qual endereço o Windows atribuiu à interface. Se o servidor estiver executando o Windows, use um dos outros métodos de configuração de endereço Ethernet sobre USB ou desabilite o comportamento padrão do Windows usando este comando:  

```
netsh interface ipv6 set global randomizeidentifiers=disabled
```
- **Configurar definição de IPv4 para Ethernet sobre USB:** Com esse método, especifique os endereços IP e a máscara de rede que têm o XClarity Controller e o lado de servidor da interface Ethernet sobre USB atribuídos.

#### Notas:

- Você precisa configurar manualmente o endereço IP da interface Ethernet sobre USB no sistema operacional local depois de configurar o endereço IP do XClarity Controller, o endereço IP do sistema operacional e a máscara de rede.
- A configuração de endereço IP do sistema operacional é usada para tornar o XClarity Controller ciente da extremidade oposta da rede Ethernet sobre USB (sistema operacional) para fins de comunicação, como o monitoramento de status do watchdog ou atualização de firmware em banda.

O mapeamento de números de porta Ethernet externas para números de porta Ethernet sobre USB é controlado clicando na caixa de seleção **Habilitar encaminhamento de porta de Ethernet externa para Ethernet sobre USB** e preenchendo as informações de mapeamento das portas que você deseja que sejam encaminhadas da interface de rede de gerenciamento para o servidor.

## Configurando o SNMP

Use as informações neste tópico para configurar os agentes SNMP.

Conclua as seguintes etapas para definir as configurações de alerta SNMP do XClarity Controller.

1. Clique em **Network** em **Configuração do BMC**.

2. Marque a caixa de seleção correspondente para ativar o **Agente SNMPv3**, **Trap SNMPv1**, **Trap SNMPv2** e/ou **Trap SNMPv3**.

**Notas:**

- Para ativar o **Agente SNMPv3**, um contato e um local do BMC devem ser especificados.
  - Depois que o **Agente SNMPv3** estiver Ativado, você poderá configurar o SNMPv3 para cada conta de usuário do XClarity Controller.
  - Para receber traps, os traps SNMP e o agente SNMPv3 devem ser ativados
3. Se ativar o **Trap SNMPv1** ou **Trap SNMPv2**, preencha os seguintes campos:
    - a. No campo **Nome da comunidade**, insira o nome da comunidade. Esse campo não pode estar vazio.
    - b. No campo **Host**, insira o endereço do host.
  4. Se ativar o **Trap SNMPv3**, preencha os seguintes campos:
    - a. No campo **ID do mecanismo**, insira o ID do mecanismo. O ID do mecanismo não pode estar vazio.
    - b. No campo **Porta do receptor de trap**, insira o número da porta. O número da porta padrão é 162.
  5. Se habilitar Traps SNMP, selecione os tipos de eventos sobre os quais deseja ser alertado:
    - **Crítico**
    - **Atenção**
    - **Sistema**

**Nota:** Clique em cada categoria principal para selecionar mais tipos de evento de subcategoria para os quais você deseja ser alertado.

6. Se ativar o **Agente SNMPv3**, conclua as seguintes etapas:
  - a. Clique em **Usuário/LDAP** na **Configuração do BMC**.
  - b. Clique no botão **Editar** ao lado do usuário correspondente e, em seguida, marque **SNMP** na lista suspensa da **Interface Acessível ao Usuário**.

**Nota:** Clique no botão **Enviar** ao lado de **Enviar um trap de teste** para verificar as configurações de SNMP.

## Ativando o acesso à rede IPMI

Use as informações neste tópico para controlar o acesso de rede à IPMI ao XClarity Controller.

Conclua as etapas a seguir para ativar o acesso IPMI via LAN.

1. Clique em **Network** em **Configuração do BMC** para visualizar ou modificar as definições da IPMI do XClarity Controller.
2. Clique no comutador **IPMI sobre LAN** em **Ativação de serviço e atribuição de porta** para ativar o acesso à rede IPMI para o XClarity Controller.
3. Clique em **Usuário/LDAP** na **Configuração do BMC**.
4. Clique no botão **Editar** ao lado do usuário correspondente e, em seguida, marque **IPMI sobre Lan** na lista suspensa da **Interface Acessível ao Usuário**.

**Importante:**

- Se não estiver usando nenhuma ferramenta nem aplicativos que acessem o XClarity Controller pela rede usando o protocolo IPMI, é altamente recomendável que você desabilite o acesso de rede da IPMI para obter segurança aprimorada.
- O IPMI sobre acesso via LAN ao XClarity Controller está desabilitado por padrão.

## Configurando definições de rede com comandos do IPMI

Use as informações neste tópico para configurar as definições de rede usando comandos do IPMI.

Como cada definição de rede do BMC é configurada usando solicitações do IPMI separadas e sem uma ordem específica, o BMC só tem a visualização completa de todas as definições de rede quando o BMC é reiniciado para aplicar as alterações de rede pendentes. A solicitação para alterar uma configuração de rede pode ser aceita no momento em que for feita, mas depois ser determinada como inválida quando alterações adicionais forem solicitadas. Se as configurações de rede pendentes forem incompatíveis quando o BMC for reiniciado, as novas configurações não serão aplicadas. Após reiniciar o BMC, você deve tentar acessar o BMC usando as novas configurações para verificar se elas foram aplicadas conforme esperado.

## Ativação de serviço e atribuição de porta

Use as informações neste tópico para visualizar ou alterar os números de porta usados por alguns serviços no XClarity Controller.

Clique em **Network** em **Configuração do BMC** para visualizar ou modificar as atribuições de porta do XClarity Controller. Conclua os campos a seguir para visualizar ou modificar designações de porta:

### HTTPS (Web/Redfish)

Este item é sempre Ativado. Nesse campo, especifique o número da porta para Web sobre HTTPS. O valor padrão é 443.

### Presença Remota

Este item é sempre Ativado. O número da porta é 443.

### IPMI sobre LAN

O número da porta é 623. Esse campo não é configurável pelo usuário.

**Nota:** Verifique se **IPMI sobre LAN** está selecionado e aplicado no campo **Interface Acessível ao Usuário** para o usuário correspondente na página Usuário/LDAP.

### SSDP

O número da porta é 1900. Esse campo não é configurável pelo usuário.

### SSH

Nesse campo, especifique o número da porta que é configurado para acessar a interface de linha de comando por meio do protocolo SSH. O valor padrão é 22.

### Agente do SNMP

Nesse campo, especifique o número da porta para o agente do SNMP que é executado no XClarity Controller. O valor padrão é 161. Os valores de números de porta válidos são de 1 a 65535.

**Nota:** Certifique-se de que o **SNMP** esteja selecionado e aplicado no campo **Interface Acessível ao Usuário** para o usuário correspondente na página Usuário/LDAP.

## Configurando a restrição de acesso

Use as informações neste tópico para exibir ou alterar as configurações que bloqueiam o acesso de endereços IP ou endereços MAC ao XClarity Controller.

Clique em **Network** em **Configuração do BMC** para exibir ou modificar as configurações de controle do acesso ao XClarity Controller.

## Lista de bloqueios e restrição de tempo

Essas opções permitem que você bloqueie endereços IP/Mac específicos por período específico.

### • Lista de endereços IP bloqueados

- Você pode inserir até três endereços IPv4 ou intervalos e três endereços IPv6 ou intervalos separados por vírgulas, que não podem acessar o XClarity Controller. Consulte os exemplos de IPv4 abaixo:
- Exemplo de endereço IPv4 exclusivo: 192.168.1.1
- Exemplo de endereço IPv4 de super-rede: 192.168.1.0/24
- Exemplo de intervalo IPv4: 192.168.1.1 – 192.168.1.5

### • Lista de endereços MAC bloqueados

- Você pode inserir até três endereços MAC separados por vírgulas, que não podem acessar o XClarity Controller. Por exemplo: 11:22:33:44:55:66.

### • Acesso restrito (único)

- É possível planejar um intervalo de tempo único durante o qual o XClarity Controller não possa ser acessado. Para o intervalo de tempo que você especificar:
- A data e a hora de início devem ser posteriores à hora atual do XCC.
- A data e a hora de término devem ser posteriores à hora e data de início.

### • Acesso restrito (diário)

- É possível planejar um ou mais intervalos de tempo diários durante os quais o XClarity Controller não possa ser acessado. Para cada intervalo de tempo que você especificar:
- A data e a hora de término devem ser posteriores à hora e data de início.

## Lista de bloqueios acionados externamente

Essas opções permitem configurar o bloqueio automático de endereços IP específicos (IPv4 e IPv6) a partir do qual o cliente tentou fazer login no XClarity Controller com um nome de usuário ou senha diferentes incorretos.

O bloqueio automático determinará dinamicamente quando ocorrerem falhas de login excessivas de um endereço IP específico e bloqueará o acesso do XClarity Controller por um período pré-determinado.

### • Número máximo de falhas de login de um determinado IP

- O número máximo de vezes indica o número de falhas de login permitidas para um usuário com uma senha incorreta de um endereço IP específico antes de se tornar bloqueado.
- Se for definido como 0, o endereço IP nunca será bloqueado devido a falhas de log.
- O contador de login com falha para o endereço IP específico será redefinido como zero após o login bem-sucedido do endereço IP.

### • Período para bloqueio de um IP

- O período mínimo (em minutos) que deve decorrer para que um usuário possa tentar fazer login novamente de um endereço IP bloqueado.
- Se for definido como 0, o acesso a partir do endereço IP bloqueado permanecerá bloqueado até que o administrador desbloqueie explicitamente.

### • Lista de bloqueios

- A tabela Lista de bloqueios exibe todos os endereços IP bloqueados. É possível desbloquear um ou todos os endereços IP da Lista de bloqueios.

## Configurando a porta USB do painel frontal para gerenciamento

Use as informações neste tópico para configurar a porta USB do painel frontal do XClarity Controller para gerenciamento.

A conexão com o XClarity Controller primeiro é destinada para uso com um dispositivo móvel que execute o aplicativo Lenovo XClarity Mobile. Quando um cabo USB estiver conectado entre o dispositivo móvel e o painel frontal do servidor, uma conexão Ethernet sobre USB será estabelecida entre a execução do aplicativo móvel no dispositivo e o XClarity Controller.

Em alguns servidores, a porta USB do painel frontal pode ser alternada para conectar ao servidor ou ao XClarity Controller.

**Nota:** Esse recurso será suportado em uma atualização futura.

---

## Configurando as definições de segurança

Use as informações neste tópico para configurar protocolos de segurança.

**Nota:** A configuração de versão mínima de TLS é TLS 1.2, mas você poderá configurar o XClarity Controller para usar outras versões de TLS se for necessário para o navegador ou aplicativos de gerenciamento. Para obter mais informações, consulte "[Comando tls](#)" na [página 134](#).

Clique em **Security** em **Configuração do BMC** para acessar e configurar as propriedades de segurança, status e configurações do XClarity Controller.

## Painel de segurança

Este tópico é uma visão geral do painel de segurança.

O painel de segurança fornece uma avaliação geral de segurança e status do sistema.

- **Eventos de segurança do BMC** relatam eventos declarados por problemas de segurança, como intrusão no chassi, corrupção detectada pelo PFR, inconsistência de hardware detectada pelo protetor do sistema, jumper de segurança aberto no planar etc.
- **Modo de segurança do BMC** fornece um status geral de conformidade do Modo de segurança.
- **Serviços e portas do BMC** enumeram todos os serviços/portas não protegidos ativados, mas não conformes com o Modo de segurança atual.
- **Certificados do BMC** todos os certificados não conformes usados pelo XCC.
- **Contas do usuário do BMC** fornecem sugestões gerais sobre como tornar o gerenciamento de conta e senha mais seguro.

**Nota:** O painel mostra um ícone de aviso se houver algum risco nessas áreas de segurança verificadas pelo XCC. O link **Detalhes** em cada categoria também leva o usuário à página de configuração para resolver os problemas.

## Modo de segurança

Este tópico é uma visão geral do modo de segurança.

A licença Padrão do XCC permite que os usuários configurem seus servidores em um dos dois Modos de segurança: Modo padrão e Modo de compatibilidade. Eles estão disponíveis em todos os servidores V4.

A licença de upgrade Premier do Lenovo XClarity Controller 3 vem com um terceiro modo de segurança: Modo estrito corporativo. Esse modo é mais adequado para requisitos de segurança de alto nível.

**Nota:** Por padrão, o XCC usa um certificado autoassinado ECDSA e apenas algoritmos baseados em ECDSA estão disponíveis. Para usar o certificado baseado em RSA, gere uma CSR e assine-a com uma CA interna ou externa e, em seguida, importe o certificado assinado para o XCC.

### Modo de segurança estrito corporativo

- O Modo de segurança estrito corporativo é o modo mais seguro.
- Todos os algoritmos criptográficos usados pelo BMC são compatíveis com CNSA 1.0.
- O BMC opera no modo validado FIPS 140-3.
- Requer certificados de classificação estrita corporativa.
- Somente os serviços que suportam criptografia CNSA 1.0 podem ser habilitados.
- Requer a Chave do Feature on Demand para habilitar.

### Modo de segurança padrão

- O modo padrão é o modo de segurança padrão.
- Todos os algoritmos criptográficos usados pelo BMC são compatíveis com FIPS 140-3.
- O BMC opera no modo validado FIPS 140-3 quando todos os serviços habilitados usam criptografia compatível com FIPS 140-3.
- Requer certificados de classificação padrão.
- Os serviços que requerem criptografia que não suporta criptografia compatível com FIPS 140-3 são desativados por padrão.

### Modo de compatibilidade

- O Modo de compatibilidade é o modo a ser usado quando os serviços e os clientes requerem criptografia que não seja compatível com o modo estrito corporativo/padrão.
- Um intervalo maior de algoritmos criptográficos é suportado.
- Quando esse modo estiver habilitado, o BMC **NÃO** está operando no modo validado pelo padrão.
- Permite que todos os serviços sejam habilitados.

### Conjuntos de criptografia TLS suportados

A Configuração de Criptografia TLS serve para restringir os conjuntos de criptografia TLS suportados em serviços do BMC.

Conjuntos de criptografia TLS	Modo de segurança	Versão do TLS
TLS_AES_256_GCM_SHA384	<ul style="list-style-type: none"> <li>• Estrito corporativo</li> <li>• Padrão*</li> <li>• Compatibilidade*</li> </ul>	TLS 1.3
TLS_CHACHA20_POLY1305_SHA256	<ul style="list-style-type: none"> <li>• Compatibilidade</li> </ul>	TLS 1.3
TLS_AES_128_GCM_SHA256	<ul style="list-style-type: none"> <li>• Padrão</li> <li>• Compatibilidade</li> </ul>	TLS 1.3
TLS_AES_128_CCM_SHA256	<ul style="list-style-type: none"> <li>• Padrão</li> <li>• Compatibilidade</li> </ul>	TLS 1.3
TLS_AES_128_CCM_8_SHA256	<ul style="list-style-type: none"> <li>• Padrão</li> <li>• Compatibilidade</li> </ul>	TLS 1.3

Conjuntos de criptografia TLS	Modo de segurança	Versão do TLS
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	<ul style="list-style-type: none"> <li>• Estrito corporativo</li> <li>• Padrão*</li> <li>• Compatibilidade*</li> </ul>	TLS 1.2
TLS_DHE_RSA_WITH_AES_256_GCM_SHA384	<ul style="list-style-type: none"> <li>• Estrito corporativo</li> <li>• Compatibilidade*</li> </ul>	TLS 1.2
TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384	<ul style="list-style-type: none"> <li>• Estrito corporativo</li> </ul>	TLS 1.2
TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	<ul style="list-style-type: none"> <li>• Padrão</li> <li>• Compatibilidade</li> </ul>	TLS 1.2
TLS_DHE_RSA_WITH_AES_128_GCM_SHA256	<ul style="list-style-type: none"> <li>• Padrão</li> <li>• Compatibilidade</li> </ul>	TLS 1.2
TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256	<ul style="list-style-type: none"> <li>• Padrão</li> <li>• Compatibilidade</li> </ul>	TLS 1.2
TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305	<ul style="list-style-type: none"> <li>• Compatibilidade</li> </ul>	TLS 1.2
TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305	<ul style="list-style-type: none"> <li>• Compatibilidade</li> </ul>	TLS 1.2
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384	<ul style="list-style-type: none"> <li>• Padrão</li> <li>• Compatibilidade</li> </ul>	TLS 1.2
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256	<ul style="list-style-type: none"> <li>• Padrão</li> <li>• Compatibilidade</li> </ul>	TLS 1.2
TLS_DHE_RSA_WITH_AES_256_CBC_SHA256	<ul style="list-style-type: none"> <li>• Padrão</li> <li>• Compatibilidade</li> </ul>	TLS 1.2
TLS_DHE_RSA_WITH_AES_128_CBC_SHA256	<ul style="list-style-type: none"> <li>• Padrão</li> <li>• Compatibilidade</li> </ul>	TLS 1.2
TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384	<ul style="list-style-type: none"> <li>• Padrão</li> <li>• Compatibilidade</li> </ul>	TLS 1.2
TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256	<ul style="list-style-type: none"> <li>• Padrão</li> <li>• Compatibilidade</li> </ul>	TLS 1.2
TLS_RSA_WITH_AES_256_GCM_SHA384	<ul style="list-style-type: none"> <li>• Padrão</li> <li>• Compatibilidade</li> </ul>	TLS 1.2
TLS_RSA_WITH_AES_128_GCM_SHA256	<ul style="list-style-type: none"> <li>• Padrão</li> <li>• Compatibilidade</li> </ul>	TLS 1.2
TLS_DHE_RSA_LATH_AES_256_GCM_SHA384	<ul style="list-style-type: none"> <li>• Padrão</li> </ul>	TLS 1.2

Conjuntos de criptografia TLS	Modo de segurança	Versão do TLS
TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384	• Padrão	TLS 1.2
TLS_RSA_WITH_AES_256_CBC_SHA256	• Padrão	TLS 1.2
TLS_RSA_WITH_AES_128_CBC_SHA256	• Padrão	TLS 1.2

**Nota:** Os modos de segurança com um asterisco (\*) listados na tabela requerem a licença de upgrade Premier do Lenovo XClarity Controller 3.

### Matriz de serviço em três Modos de segurança

Recurso/serviço	Usa criptografia	Estado padrão fora da caixa	Suportado no Modo Estrito	Suportado no Modo Padrão	Suportado no Modo de Compatibilidade
<b>IPMI sobre KCS</b>	Não	Habilitado	Sim	Sim	Sim
<b>IPMI sobre LAN</b>	Sim	Desabilitado	Não	Sim	Sim
<b>Traps SNMPv1</b>	Não	Não configurado	Não	Sim	Sim
<b>Traps SNMPv3</b>	Sim	Não configurado	Não	Sim Se ativado, alertará para o uso de criptografia não FIPS	Sim
<b>Agente do SNMPv3</b>	Sim	Não configurado	Não	Sim Se ativado, alertará para o uso de criptografia não FIPS	Sim
<b>Alertas de e-mail</b>	Sim	Não configurado	Sim Não é possível ativar com Autenticação CRAM-MD5	Sim Se CRAM-MD5 for necessário, alertará para o uso de criptografia não FIPS.	Sim
<b>Alertas do syslog</b>	Não	Não configurado	Não	Sim	Sim
<b>TLS 1.2</b>	Sim	Habilitado	Sim	Sim	Sim
<b>TLS 1.3</b>	Sim	Habilitado	Sim	Sim	Sim
<b>Web sobre HTTPS</b>	Sim	Habilitado	Sim	Sim	Sim
<b>Redfish sobre HTTPS</b>	Sim	Habilitado	Sim	Sim	Sim
<b>SSDP</b>	Não	Habilitado	Sim	Sim	Sim
<b>SSH-CLI</b>	Sim	Habilitado	Sim	Sim	Sim

Recurso/ serviço	Usa cripto- grafia	Estado padrão fora da caixa	Suportado no Modo Estrito	Suportado no Modo Padrão	Suportado no Modo de Compatibilidade
<b>SFTP</b>	Sim	Desabili- tado	Sim	Sim	Sim
<b>LDAP</b>	Não	Não configura- do	Não	Sim	Sim
<b>LDAP seguro</b>	Sim	Não configura- do	Sim	Sim	Sim
<b>Gerenciamen- to de chave de segurança</b>	Sim	Não configura- do	Sim	Sim	Sim
<b>Console Remoto</b>	Sim	Habilitado	Sim	Sim	Sim
<b>Mídia virtual – CIFS</b>	Sim	Não configura- do	Não	Sim	Sim
<b>Mídia virtual – NFS</b>	Não	Não configura- do	Não	Sim	Sim
<b>Mídia virtual - HTTPFS</b>	Sim	Não configura- do	Sim	Sim	Sim
<b>RDOC – Local</b>	Sim	Não configura- do	Sim	Sim	Sim
<b>RDOC – CIFS</b>	Sim	Não configura- do	Não	Sim	Sim
<b>RDOC – HTTP</b>	Não	Não configura- do	Não	Sim	Sim
<b>RDOC – HTTPS</b>	Sim	Não configura- do	Sim	Sim	Sim
<b>RDOC – FTP</b>	Não	Não configura- do	Não	Sim	Sim
<b>RDOC – SFTP</b>	Sim	Não configura- do	Sim	Sim	Sim
<b>Upload do FFDC (SFTP)</b>	Sim	Habilitado	Sim	Sim	Sim
<b>Upload do FFDC (TFTP)</b>	Não	Habilitado	Não	Sim	Sim
<b>Atualização do repositório – CIFS</b>	Sim	Não configura- do	Não	Sim	Sim

Recurso/serviço	Usa criptografia	Estado padrão fora da caixa	Suportado no Modo Estrito	Suportado no Modo Padrão	Suportado no Modo de Compatibilidade
Atualização do repositório – NFS	Não	Não configurado	Não	Sim	Sim
Atualização do repositório – HTTP	Não	Não configurado	Não	Sim	Sim
Atualização do repositório – HTTPS	Sim	Não configurado	Sim	Sim	Sim
Call home	Sim	Desabilitado	Sim	Sim	Sim
Senha de terceiros	Sim	Não configurado	Não	Sim	Sim
Encaminhamento de porta	N/D	Desabilitado	Sim	Sim	Sim

## Alternância do modo de segurança

Use as informações neste tópico para alternar e validar o modo de segurança.

O modo padrão é o modo de segurança padrão.

Em geral, se o XCC detectar alguma configuração não conforme com o Modo padrão, o XCC exibirá uma notificação, mas não exigirá que o usuário altere o modo. Nesse caso, o XCC entrará no modo de segurança padrão com substituição (não conformidade).

O usuário pode abrir o menu suspenso para selecionar outro modo e usar a função **Validar** para determinar quantos itens não conformes são detectados pelo XCC.

Quando o usuário clicar em **Aplicar**, o XCC também validará os itens em conformidade.

## Visão geral do SSL

Este tópico é uma visão geral do protocolo de segurança SSL.

SSL é um protocolo de segurança que fornece privacidade de comunicação. O SSL permite que aplicativos cliente/servidor se comuniquem de uma maneira que previna interceptações, violações e falsificações de mensagens. É possível configurar o XClarity Controller para usar suporte a SSL para diferentes tipos de conexões, como HTTPS, LDAPS, CIM sobre HTTPS e servidor SSH e para gerenciar os certificados necessários para SSL.

## Manipulação de certificado SSL

Este tópico fornece informações sobre a administração de certificados que podem ser usados com o protocolo de segurança SSL.

O cliente WEB, Redfish e LDAP usam a mesma configuração de certificado. A conexão SSL deve ser restabelecida sempre que você desejar alterar a configuração do certificado SSL. O SSL pode ser usado

com um certificado autoassinado ou com um certificado assinado por uma Autoridade de Certificação de terceiros. Usar um certificado autoassinado é o método mais simples para usar SSL, mas ao custo de um pequeno risco de segurança. O risco surge porque o cliente SSL não tem como validar a identidade do servidor SSL para a primeira tentativa de conexão entre o cliente e o servidor. É possível que um terceiro mal-intencionado possa se passar pelo servidor e interceptar os dados que fluem entre o XClarity Controller e o navegador. Se (no momento da conexão inicial entre o navegador e o XClarity Controller) o certificado autoassinado for importado para o armazenamento de certificados do navegador, todas as comunicações futuras serão seguras para esse navegador (supondo que a conexão inicial não foi comprometida por um ataque). Depois de usar a página Gerenciamento de certificados SSL para gerar um par de chaves e um certificado autoassinado, o SSL pode ser ativado.

Para uma segurança mais completa, use um certificado assinado por uma autoridade de certificação (CA). Para obter um certificado assinado:

- Selecione **Gerar CSR (solicitação de assinatura de certificado)** no ícone **Gerar** em **Gerenciamento de certificados SSL**.
- Preencha os campos obrigatórios e selecione **Gerar**.
- Depois que um certificado autoassinado for gerado, ele será mostrado no **Gerenciamento de certificados SSL**.
- Selecione **Baixar solicitação de assinatura de certificado (CSR)** no ícone **Download** para baixar o certificado assinado.
- Quando o certificado assinado for baixado, selecione o ícone **Importar certificado assinado** em **Gerenciamento de certificados de CA** para importá-lo no XClarity Controller.

A função da CA é verificar a identidade do XClarity Controller. Um certificado contém assinaturas digitais para a CA e o BMC. Se uma autoridade de certificação conhecida emitir o certificado ou se o certificado da autoridade de certificação já tiver sido importado no navegador da Web, o navegador poderá validar o certificado e identificar positivamente o servidor Web do BMC.

Observe que o SSL compara o nome de host do XClarity Controller (ou nome comum) no certificado com o nome do host, conforme observado pelo seu navegador da Web.

## Gerenciamento de certificado SSL

Este tópico fornece informações sobre algumas ações que podem ser selecionadas para gerenciamento de certificados com o protocolo de segurança SSL.

Clique em **Segurança** em **Configuração do BMC** para configurar o gerenciamento de certificados SSL.

Ao gerenciar certificados do XClarity Controller, são apresentadas as seguintes ações:

### Fazer download do certificado assinado

Use esse link para fazer uma cópia do certificado atualmente instalado. O certificado pode ser baixado em formato PEM ou DER. O conteúdo do certificado pode ser visualizado usando uma ferramenta de terceiros, como o OpenSSL (<http://www.openssl.org>). Um exemplo da linha de comandos para visualizar o conteúdo do certificado usando o OpenSSL teria a seguinte aparência:

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

### Fazer download da solicitação de assinatura de certificado (CSR)

Use esse link para baixar uma cópia da solicitação de assinatura de certificado. A CSR pode ser baixada em formato PEM ou DER.

### Gerar Certificado Assinado

gere um certificado autoassinado. Após o término da operação, o SSL poderá ser habilitado usando o novo certificado.

**Nota:** Ao executar a ação **Gerar certificado autoassinado**, a janela Gerar certificado autoassinado para HTTPS é aberta. Será solicitado que você preencha os campos obrigatórios e opcionais. Você **deve** concluir os campos obrigatórios. Depois de inserir suas informações, clique em **Gerar** para concluir a tarefa.

### **Gerar solicitação de assinatura de certificado (CSR)**

gere uma solicitação de assinatura de certificado (CSR). Após o término da operação, o arquivo CSR pode ser baixado e enviado para uma autoridade de certificação (CA) para assinatura.

**Nota:** Ao executar a ação **Gerar Solicitação de Assinatura de Certificado (CSR)**, a janela Gerar Solicitação de Assinatura de Certificado para HTTPS é aberta. Será solicitado que você preencha os campos obrigatórios e opcionais. Você **deve** concluir os campos obrigatórios. Depois de inserir suas informações, clique em **Gerar** para concluir a tarefa.

### **Importar um Certificado Assinado**

Use para importar um certificado assinado. Para obter um certificado assinado, é necessário primeiro gerar uma solicitação de assinatura de certificado (CSR) e enviá-la a uma autoridade de certificação (CA).

## **Configurando o servidor Shell Seguro**

Use as informações neste tópico para entender e habilitar o protocolo de segurança SSH.

Clique em **Network** em **Configuração do BMC** para configurar o servidor Shell Seguro.

Para usar o protocolo SSH, primeiro é necessário gerar a chave para habilitar o servidor SSH.

### **Notas:**

- Nenhum gerenciamento de certificado é necessário para usar essa opção.
- O XClarity Controller criará inicialmente uma chave do servidor SSH. Se você desejar gerar uma nova chave de servidor SSH, clique em **Rede** em **Configuração do BMC**; depois, clique em **Gerar chave** em **Servidor SSH**.
- Depois de concluir a ação, você deve reiniciar o XClarity Controller para que as alterações entrem em vigor.

## **Acesso da IPMI sobre Keyboard Controller Style (KCS)**

Use as informações neste tópico para controlar a IPMI sobre acesso via KCS ao XClarity Controller.

O XClarity Controller fornece uma interface IPMI através do canal de KCS que não requer autenticação.

Clique em **Segurança** em **Configuração do BMC** para ativar ou desativar **Acesso IPMI sobre KCS**.

### **Notas:**

- Depois de alterar as configurações, você deve reiniciar o XClarity Controller para que as alterações entrem em vigor.
- **Desativado (ativar sob demanda)** desativará o canal KCS na maior parte do tempo, mas permite que algumas ferramentas da Lenovo troquem informações com o XClarity Controller durante a janela de atualização de firmware do sistema. Quando isso ocorre, o canal KCS é ativado brevemente por alguns minutos e, em seguida, desativado após a conclusão ou após o tempo limite.

**Importante:** Se não estiver executando nenhuma ferramenta ou aplicativos no servidor que acessem o XClarity Controller pelo protocolo IPMI, é altamente recomendável que você desabilite a IPMI sobre acesso via KCS para obter segurança aprimorada. O XClarity Essentials usa a interface IPMI via KCS para o XClarity Controller. Se você desabilitar a interface IPMI via KCS, reabilite-a antes de executar o XClarity Essentials no servidor. Em seguida, desabilite a interface ao terminar.

## Evitar o rebaixamento do firmware do sistema

Use as informações neste tópico para evitar que o firmware do sistema seja alterado para níveis mais antigos de firmware.

Com esse recurso você decide se permite ou não que o firmware do sistema retorne a um nível anterior de firmware.

Clique em **Rede** em **Configuração do BMC** para ativar ou desativar **Evitar o rebaixamento do firmware do sistema**.

Todas as alterações que forem feitas entrarão em vigor imediatamente sem que o XClarity Controller exija uma reinicialização.

## Configurando o Gerenciamento de Chaves de Segurança (SKM)

Use as informações neste tópico para criar e gerenciar chaves de segurança.

Esse recurso usa o servidor Gerenciamento de Chaves centralizado para fornecer chaves que desbloqueiam o hardware de armazenamento, para obter acesso aos dados armazenados em SEDs em um servidor ThinkSystem. O servidor Gerenciamento de Chaves inclui servidores SKLM – Gerenciamento de Chaves IBM SED e servidores KMIP – Gerenciamento de Chaves Thales/Gemalto SED (KeySecure e CipherTrust).

**Nota:** Esse recurso será suportado em uma atualização futura.

## Security password manager

Use as informações neste tópico para permitir uma senha de terceiros.

Este recurso permite que o usuário decida se deve ou não permitir que uma senha de terceiros seja usada.

- **Senha de terceiros:** uma vez ativado, o BMC poderá usar um hash de senha fornecido pelo usuário para autenticação.
- **Permitir a recuperação de senha de terceiros:** O usuário também pode ativar ou desativar a recuperação do hash de senha de terceiros no BMC.

## Log de auditoria estendida

Use as informações neste tópico para controlar o log de auditoria estendida.

Esse recurso permite que você decida se incluirá ou não as entradas de log do comando de definição de IPMI (dados brutos) dos canais LAN e KCS no log de auditoria.

Clique em **Segurança** em **Configuração do BMC** no XCC Web para habilitar/desabilitar o log de auditoria estendida.

**Nota:** Se o comando de definição de IPMI for do canal de LAN, o nome do usuário e o endereço IP de origem serão incluídos na mensagem de log. E todos os comandos de IPMI com informações de segurança confidenciais (por exemplo, senha) serão excluídos.

## Limitar o login simultâneo por conta do usuário

Use as informações neste tópico para limitar as sessões simultâneas por conta do usuário.

Este recurso permite que o usuário decida quantas sessões simultâneas são permitidas por conta do usuário.

- **Número de sessões simultâneas da Web:** Pode ser definido de 1 a 10 sessões.
- **Número de sessões simultâneas da linha de comandos:** Pode ser definido a partir de 1 ou 2 sessões.
- **Número de sessões simultâneas da Redfish:** Pode ser definido de 1 a 16 sessões.

**Nota:** Se o número total de sessões exceder o número definido, o usuário não poderá mais criar uma nova sessão.

## Protetor do sistema

Este tópico é uma visão geral do protetor do sistema.

O recurso de protetor do sistema faz uma captura instantânea do inventário de componentes de hardware como referência confiável e, em seguida, monitora para qualquer desvio da captura instantânea de referência. Quando ocorre um desvio, ele pode relatar um evento ao usuário. Como opção, também pode impedir que o servidor seja inicializado no SO e solicitar uma resposta do usuário.

O usuário pode fazer uma captura instantânea a qualquer momento mesmo quando o recurso está desativado. A geração da captura instantânea leva cerca de um minuto. O usuário pode selecionar um subconjunto de componentes de hardware a ser aplicado e selecionar uma ação correspondente a ser tomada quando o desvio for detectado.

**Nota:** A detecção de desvio é executada na ativação do servidor (POST) ou na reinicialização do sistema. Por exemplo, enquanto o SO ainda estiver em execução, se uma unidade de disco estiver sendo retirada e, em seguida, conectada novamente em um momento posterior, o protetor do sistema não registrará o evento nem realizará alguma ação. Se a unidade de disco retirada permanecer ausente até a próxima reinicialização, o protetor do sistema entraria em ação.

**Notas:** Durante a restauração CA seguida pela primeira ativação, o XCC poderá não notificar a UEFI para evitar a inicialização do SO se as condições a seguir forem atendidas:

- Protetor do sistema ativado com:
  - Hardware de **CPU** ou **DIMM** selecionado
  - Opção **Impedir a inicialização do SO** selecionada
- Uma alteração de configuração de hardware que não corresponderá à captura instantânea confiável.

O XCC relatará uma incompatibilidade de configuração após o POST, e essa limitação não persistirá na reinicialização subsequente do SO.

## Ativando o protetor do sistema

Use as informações neste tópico para ativar o protetor do sistema.

O recurso de protetor do sistema é desativado por padrão. Ele é ativado antes da remessa conforme o requisito do usuário final.

A opção de redefinição para padrão do XCC também desativa o protetor do sistema e limpa as configurações, exceto o histórico de capturas instantâneas.

Ao ativar o protetor do sistema, o usuário deve confirmar as configurações, usar a captura instantânea confiável existente ou capturar o inventário como uma nova captura instantânea confiável antes de ativar o protetor do sistema. Uma vez ativado:

- Se a energia do sistema estiver desligada, o protetor do sistema começará a coletar o inventário de hardware imediatamente.
- Se a energia do sistema estiver ligada, o protetor do sistema comparará os dados do inventário do componente com a captura instantânea confiável.

Se o resultado da comparação indicar um desvio da captura instantânea confiável, o XCC exibirá um aviso de **Não conformidade devido à incompatibilidade de configuração de hardware**. Os detalhes da lista de incompatibilidade de cada componente de hardware ausente/alterado/novo com atributos local/identificador/descrição, em comparação com a captura instantânea confiável.

O usuário pode configurar o escopo e a ação do protetor do sistema e decidir qual ação realizar quando o sistema ficar não conforme por meio do painel Escopo e ação.

## Suporte da versão do TLS

Use as informações neste tópico para entender outra versão do TLS suportada.

A seguinte versão do TLS é suportada:

- TLS 1.2 e superior
- TLS 1.3

Para obter uma lista completa dos conjuntos de criptografia TLS suportados, consulte "[Conjuntos de criptografia TLS suportados](#)" na página 38

---

## Backup e restauração da configuração do BMC

As informações neste tópico descrevem como restaurar ou modificar a configuração do BMC.

Selecione **Fazer Backup e Restaurar** em **Configuração do BMC** para executar as seguintes ações:

- Visualizar um resumo de configuração do controlador de gerenciamento
- Fazer backup ou restaurar a configuração do controlador de gerenciamento
- Visualizar o status de backup ou restauração
- Redefinir a configuração do controlador de gerenciamento para suas configurações padrão de fábrica
- Acessar o assistente de configuração inicial do controlador de gerenciamento

## Backup da configuração do BMC

As informações neste tópico descrevem como fazer backup da configuração do BMC.

Selecione **Fazer backup e restaurar** em **Configuração do BMC**. No início se encontra a seção **Fazer backup da configuração do BMC**.

Se foi feito backup anteriormente, você verá os detalhes no campo **Último backup**.

Para fazer backup da configuração atual do BMC, siga as etapas mostradas abaixo:

1. Especifique a senha para o arquivo de backup do BMC.
2. Selecione se deseja criptografar o arquivo todo ou apenas os dados sigilosos.

3. Inicie o processo de backup clicando em **Iniciar backup**. Durante o processo, não é permitido executar nenhuma ação de restauração/redefinição.
4. Quando o processo estiver concluído, será exibido o botão para você baixar e salvar o arquivo.

**Nota:** Quando o usuário configura um novo usuário/senha do XClarity Controller e executa um backup da configuração, a senha/conta padrão (USERID/PASSWORD) também é incluída. Excluir subsequentemente a senha/conta padrão do backup resultará no sistema exibir uma mensagem notificando o usuário que há uma falha de restauração da senha/conta do XClarity Controller. Os usuários podem ignorar essa mensagem.

## Restaurando a configuração do BMC

As informações neste tópico descrevem como restaurar a configuração do BMC.

Selecione **Fazer backup e restaurar** em **Configuração do BMC**. Localizada abaixo de **Backup da configuração do BMC** está a seção **Restaurar BMC do arquivo de configuração**.

Para restaurar uma configuração do BMC salva anteriormente, siga as etapas mostradas abaixo:

1. Navegue para selecionar o arquivo de backup e inserir a senha quando solicitado. Depois, clique em **Avançar >**.
2. Verifique o arquivo clicando em **Exibir detalhes**.
3. Depois de verificar o conteúdo, clique em **Iniciar Restauração**.

## Redefinindo o BMC para o padrão de fábrica

As informações neste tópico descrevem como redefinir o BMC para as configurações padrão de fábrica.

Selecione **Fazer backup e restaurar** em **Configuração do BMC**. Localizada abaixo de **Restaurar BMC do arquivo de configuração** está a seção **Redefinir o BMC para o padrão de fábrica**.

Para redefinir o BMC para padrões de fábrica, siga as etapas mostradas abaixo:

1. Clique em **Iniciar para Redefinir o BMC para Padrões de Fábrica**.

### Notas:

- Apenas usuários com o nível de autoridade do usuário Supervisor podem executar essa ação.
- A conexão Ethernet será desconectada temporariamente. Você deve fazer login na interface da Web do XClarity Controller novamente após o término da operação de redefinição.
- Depois de clicar em **Iniciar para Redefinir o BMC para Padrões de Fábrica**, uma janela de confirmação será aberta e será possível marcar as caixas de seleção para reter as seguintes configurações:
  - **Retar Configurações do Usuário Local:** será feito backup da configuração atual de Usuário/Função/Global. Ele restaura o comando da CLI de conteúdo "users"/"roles"/"accesscfg". Por exemplo: Nome do usuário/Nome da função/Período de tempo de aviso de expiração da senha/Regras de complexidade da senha ativadas etc.
  - **Retar Configurações de Rede:** será feito backup da configuração de rede atual. Ele restaura a saída de rede do comando CLI "ifconfig". Por exemplo: Nome do host/endereço IPv4/endereço IPv6/gateway etc.
- Depois de clicar em **Ok**, todas as alterações de configuração anteriores serão perdidas, exceto as que você escolher reter.
- Se você deseja habilitar LDAP ao restaurar a configuração do BMC, será necessário primeiro importar um certificado de segurança confiável antes de fazer isso.

- Se estiver trabalhando no sistema local do BMC, como resultado, você perderá sua conexão TCP/IP. Será necessário reconfigurar a interface de rede do BMC para restaurar a conectividade.
- Após o término do processo, o XClarity Controller será reiniciado.
- A redefinição do BMC para o padrão de fábrica não afetará as configurações UEFI e o modo de acesso (usuário único/múltiplo) do Console Remoto (isso é salvo nos cookies do navegador).

---

## Reiniciando o XClarity Controller

As informações neste tópico explicam como reiniciar o XClarity Controller.

Para obter detalhes sobre como reiniciar o XClarity Controller, consulte ["Ações de energia" na página 62](#)



---

## Capítulo 4. Monitorando o status de servidor

Este as informações neste tópico para entender como visualizar e monitorar as informações para o servidor que você está acessando.

Depois que você fizer login no XClarity Controller, uma página status do sistema será exibida. Nesta página, é possível exibir o status de hardware do servidor, os logs de eventos e auditoria, o status do sistema, o histórico de manutenção e os destinatários de alerta.

---

### Exibindo o resumo de funcionamento/eventos ativos de sistema

Use as informações neste tópico para entender como visualizar o resumo de funcionamento/eventos ativos de sistema.

Ao acessar a página inicial do XClarity Controller, o **Resumo de funcionamento** é mostrado por padrão. Uma representação gráfica é fornecida, que mostra o número de componentes de hardware instalados e o respectivo status de integridade. Os componentes de hardware que estão sendo monitorados incluem os seguintes:

- CPU (processador)
- Memória
- Armazenamento Local
- Adaptadores PCI
- Fonte de Alimentação
- Ventilador
- Placa-mãe
- Outros
- Segurança

**Nota:** O **Armazenamento Local** pode mostrar **não disponível** no Ícone de Status nos sistemas com uma configuração de backplane simple-swap.

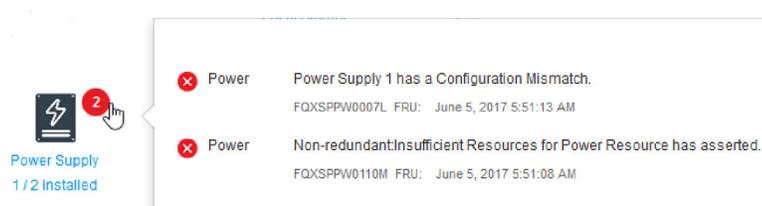
## Health Summary

Active System Events (0)



  <b>CPU</b> 1 / 2 installed	  <b>Memory</b> 1 / 32 installed	 <b>Local Storage</b> Not Found
 <b>PCI</b> Not Found	  <b>Power Supply</b> 2 / 2 installed	 <b>Fan</b> Not Found
  <b>System Board</b>	  <b>Others</b>	 <b>Security</b> Crypto:Standard

Se algum dos componentes de hardware não estiver funcionando normalmente, serão marcados por um ícone de crítico ou aviso. Um estado crítico será indicado por um ícone de círculo vermelho, enquanto uma condição de aviso estiver indicada por um ícone de triângulo amarelo. Ao passar o ponteiro do mouse sobre o sinal de crítico ou de aviso, até três eventos atualmente ativos para esse componente serão mostrados.



Power Supply  
1 / 2 installed

- Power Power Supply 1 has a Configuration Mismatch.  
FQXSPW0007L FRU: June 5, 2017 5:51:13 AM
- Power Non-redundant/Insufficient Resources for Power Resource has asserted.  
FQXSPW0110M FRU: June 5, 2017 5:51:08 AM

Para exibir os outros eventos, clique na guia **Eventos ativos de sistema**. Uma janela aparecerá mostrando os eventos que estão ativos atualmente no sistema. Clique em **Exibir todos os logs de eventos** para visualizar o histórico de eventos inteiro.

Se o componente de hardware estiver marcado por um visto verde, está funcionando normalmente e não há nenhum evento ativo.

O texto abaixo do componente de hardware indica o número de componentes instalados. Se você clicar no texto (link), será direcionado para a página **Inventário**.

**Nota:** Nos nós compatíveis com o chassi D3 V2, o link **Fonte de Alimentação** está disponível apenas no nó provisório.

---

## Exibindo as informações do sistema

Este tópico explica como obter um resumo de informações comuns do servidor.

O painel **Informações do Sistema e Configurações** localizado na parte direita da página inicial fornece um resumo das informações comuns do servidor, que incluem o seguinte:

- Nome da máquina, estado da energia e do sistema operacional
- Modelo/tipo de máquina
- Número de série
- Nome do sistema
- Gerenciamento da porta USB do painel frontal

**Nota:** Esse recurso será suportado em uma atualização futura.

- Licença do BMC
- Endereço IP do BMC
- Nome do host do BMC
- Chassi provisório ativo

**Nota:** Este item está disponível apenas em nós compatíveis com o chassi D3 V2.

- Versão do BMC
- Versão de UEFI
- Local

O servidor pode estar em um dos estados do sistema listados na tabela a seguir.

Tabela 2. *Descrições de Estados do Sistema*

Tabela de duas colunas com cabeçalhos documentando estados dos sistemas do servidor.

Estado	Descrição
Sistema desligado/Estado desconhecido	O servidor está desligado.
Sistema ligado/iniciando UEFI	O servidor está ligado, mas a UEFI não está em execução.
Sistema em execução na UEFI	O servidor está ligado e a UEFI está em execução.
Inicializando o sistema operacional ou em um sistema operacional não suportado (o sistema pode estar nesse estado se o sistema operacional não responder a pings)	O servidor pode estar nesse estado por um dos motivos a seguir: <ul style="list-style-type: none"><li>• O carregador do sistema operacional foi iniciado, mas o sistema operacional não está sendo executado</li><li>• A interface Ethernet sobre USB do BMC está desativada.</li><li>• O sistema operacional não possui os drivers carregados que suportam a interface Ethernet sobre USB.</li></ul>
Sistema operacional inicializado	O sistema operacional do servidor está em execução.
Sistema em execução no teste de memória	O servidor está ligado e executando ferramentas de diagnóstico de memória.

Tabela 2. Descrições de Estados do Sistema (continuação)

Estado	Descrição
Sistema em execução na configuração	O servidor está ligado e o sistema foi inicializado no menu de configuração UEFI F1 ou LXPM.
Sistema em execução no modo de manutenção LXPM	O servidor está ligado e o sistema foi inicializado no modo de manutenção de LXPM em que os usuários não podem navegar pelo menu LXPM.

Se desejar alterar o nome do sistema, clique no ícone de lápis. Digite o nome do sistema que você deseja usar; em seguida, clique no visto verde.

Se o servidor tiver uma licença que não seja a licença de nível Premier do XClarity Controller, talvez você possa comprar uma licença de atualização para habilitar recursos avançados. Para instalar uma licença de atualização depois de obtê-la, clique no ícone de seta para cima.



Para adicionar, excluir ou exportar uma licença, clique no ícone de seta para a direita.



Para alterar as configurações relevantes para o endereço IP do BMC, o nome do host do BMC, a versão do UEFI, a versão do BMC e os itens de local, clique na seta para a direita.

- Para o endereço IP e o nome do host, você será levado para a seção **Configuração Ethernet** em **Rede**.
- Para os itens de versão de UEFI e BMC, você será levado para a página **Atualização de firmware**.
- Para o item de local, você será levado para a seção **Propriedades do servidor** na página **Configuração do servidor**.



## Exibindo a utilização do sistema

Ao clicar em **Utilização** no painel esquerdo, um resumo das informações comuns de utilização do servidor é fornecido.

A utilização do sistema representa é uma medida composta com base na utilização em tempo real do processador, da memória e dos subsistemas E/S. Os dados de utilização podem ser exibidos na Exibição gráfica ou na Exibição da Tabela, que inclui o seguinte:

- **Temperatura**
  - Exibe a temperatura ambiente em tempo real e as temperaturas do componente-chave.
  - Passar o cursor do mouse sobre um módulo de memória mostrará sua temperatura atual.
- **Utilização de energia**
  - Exibe o gráfico de pizza de consumo de energia atual.

- Passar o cursor do mouse sobre o gráfico de pizza mostrará seu consumo de energia atual.
  - O gráfico de pizza de consumo de energia atual consiste em quatro categorias: CPU, Memória, Outro e Sobressalente. "Outro" significa o consumo total de energia do sistema menos o consumo de energia da CPU e da memória. "Sobressalente" significa o total de energia alocada disponível menos o consumo total de energia do sistema.
  - A guia Voltagem exibe as leituras de voltagem atuais e o status em todos os sensores de voltagem suportados pelo hardware.
- **Utilização do sistema**
    - Representa a captura instantânea de utilização atual dos subsistemas do sistema, do processador, da memória e E/S.

**Nota:** Esse recurso será suportado em uma atualização futura.
  - **Velocidade do ventilador (RPM)**
    - A seção de velocidade do ventilador mostra as velocidades do ventilador como porcentagem da velocidade máxima.
    - O usuário pode clicar no ícone de engrenagem para acessar as opções **Aumento de velocidade do ventilador**.
    - Essa configuração permite resfriamento adicional para o servidor com base na temperatura ambiente. Ela pode aumentar o ventilador acima da velocidade normal pelo algoritmo térmico controlado. Não haverá alteração se os ventiladores já estiverem funcionando a toda velocidade.

---

## Exibindo logs de eventos

O **Log de eventos** fornece uma lista histórica de todos os eventos de hardware e de gerenciamento.

Selecione a guia **Log de Eventos** em **Eventos** para exibir a página **Log de Eventos**. Todos os eventos no log são registrados com data e hora usando as configurações de data e hora do XClarity Controller. Alguns eventos também gerarão alertas quando ocorrerem, se estiverem configurados para isso em **Destinatários de alerta**. É possível classificar e filtrar eventos no log de eventos.

Leia a seguir uma descrição das ações que podem ser executadas na página **Log de Eventos**.

- **Personalizar tabela:** selecione esse item de ação para escolher o tipo de informações que deseja exibir na tabela. Um número de sequência pode ser exibido para auxiliar na determinação da ordem de eventos quando mais de um evento tiver o mesmo carimbo de data e hora.
- Nota:** Alguns números de sequência são usados por processos internos do BMC, portanto, é normal que haja intervalos de nos números da sequência quando os eventos são classificados por número de sequência.
- **Limpar logs:** selecione esse item de ação para excluir os logs de eventos.
  - **Atualizar:** selecione esse item de ação para atualizar a exibição com todas as entradas do log de eventos que possam ter ocorrido desde que a página foi exibida pela última vez.
  - **Tipo:** selecionar quais tipos de evento em mostrar. Os tipos de evento incluem o seguinte:



- Mostra entradas de erro no log



- Mostra entradas de aviso no log



- Mostra entradas informativas no log

Clique em cada ícone para desativar ou ativar a exibição dos tipos de erros. Clicar no ícone sucessivamente ativará e desativará a exibição dos eventos. Uma caixa preta ao redor do ícone indica que o tipo de evento será exibido.

- **Tipo de filtro de origem:** selecione um item no menu suspenso para exibir apenas o tipo de entrada desejado do log de eventos.
- **Filtro de tempo:** selecione esse item de ação para especificar o intervalo de eventos que você deseja exibir.
- **Pesquisar:** para procurar tipos específicos de eventos ou palavras-chave, clique no ícone de lupa e digite uma palavra para pesquisa na caixa **Pesquisar**. Observe que a entrada faz distinção entre maiúsculas e minúsculas.

**Nota:** O número máximo de registros de log de eventos é 1024. Quando os logs de eventos estiverem cheios, a nova entrada do log substituirá automaticamente a mais antiga.

---

## Exibindo logs de auditoria

O **Log de auditoria** fornece um registro histórico das ações do usuário, como fazer login no XClarity Controller, criar um novo usuário e alterar uma senha de usuário.

É possível usar o log de auditoria para acompanhar e documentar a autenticação, alterações e ações do sistema.

O log de eventos e o log de auditoria oferecem suporte a ações semelhantes de manutenção e visualização. Para ler a descrição das ações de exibição e filtragem que podem ser executadas na página Log de auditoria, consulte ["Exibindo logs de eventos" na página 55](#).

### Notas:

- Depois de executar as ferramentas da Lenovo no sistema operacional do servidor, o log de auditoria pode conter registros mostrando ações realizadas por um nome de usuário (por exemplo, usuário "20luN4SB") que você pode não reconhecer. Quando algumas ferramentas são executadas no sistema operacional do servidor, elas podem criar uma conta do usuário temporária para acessar o XClarity Controller. A conta é criada com um nome de usuário e senha aleatórios e só pode ser usada para acessar o XClarity Controller na Ethernet interna sobre interface USB. A conta pode ser usada apenas para acessar as interfaces Redfish e SFTP do XClarity Controller. A criação e a remoção dessa conta temporária são gravadas no log de auditoria, bem como as ações realizadas pela ferramenta com essas credenciais.
- O número máximo de registros de log de auditoria é 1024. Quando os logs de auditoria estiverem cheios, a nova entrada do log substituirá automaticamente a mais antiga.

---

## Exibindo o histórico de manutenção

A página **Histórico de manutenção** inclui informações sobre a atualização de firmware, configuração e histórico de substituição de hardware.

O conteúdo do histórico de manutenção pode ser filtrado para exibir determinados tipos de eventos ou intervalos de tempo.

**Nota:** O número máximo de registros de histórico de manutenção é 250. Quando os logs de histórico de manutenção estiverem cheios, a nova entrada do log substituirá automaticamente a mais antiga.

---

## Configurando destinatários de alertas

Use as informações neste tópico para incluir e modificar notificações por e-mail e syslog ou destinatários de SNMP TRAP.

**Nota:** Esse recurso será suportado em uma atualização futura.



---

## Capítulo 5. Configurando o servidor

Use as informações neste capítulo para entender as opções disponíveis para as configurações do servidor.

Ao configurar o servidor, as seguintes opções estão disponíveis:

- Adaptadores
- Opções de inicialização
- Política de energia
- Propriedades do servidor
- Chassi

**Nota:** Este item está disponível apenas em nós compatíveis com o chassi D3 V2.

---

### Exibindo as informações e as definições de configuração do adaptador

Use as informações neste tópico para visualizar informações sobre os adaptadores instalados no servidor.

Clique na opção **Adaptadores** em **Configuração do Servidor** para visualizar informações sobre os adaptadores instalados no servidor.

**Nota:** Se o adaptador não oferecer suporte ao monitoramento de status, ele não será visível para monitoramento nem configuração. Para obter informações relacionadas ao inventário de todos os adaptadores PCI instalados, consulte a página **Inventário**.

---

### Configurando o modo e a sequência de inicialização do sistema

Para configurar o modo e a sequência de inicialização do sistema, use as informações neste tópico.

Quando você seleciona **Opções de inicialização** em **Configuração do servidor**, é possível configurar a ordem de inicialização do sistema.

**Nota:** Nenhum método em banda não autenticado pode alterar as configurações do sistema relacionadas à segurança. Por exemplo, a inicialização segura NÃO deve ser configurada por APIs em banda não autenticadas do SO nem do shell de UEFI. Isso inclui OneCLI em execução em banda e obter credenciais temporárias usando IPMI ou qualquer ferramenta e APIs para configurar a inicialização segura, o TPM e a configuração relacionada à senha do UEFI. Todas as configurações relacionadas à segurança devem exigir autenticação adequada com privilégios suficientes.

Para configurar a sequência de inicialização do sistema, selecione um dispositivo da lista **Dispositivos disponíveis** e clique na seta para a direita para incluir o dispositivo na sequência de inicialização. Para remover um dispositivo da sequência de inicialização, selecione um dispositivo na lista Ordem de inicialização e clique na seta para a esquerda para mover o dispositivo de volta para a lista de dispositivos disponíveis. Para alterar a sequência de inicialização, selecione um dispositivo e clique na seta para cima ou para baixo para mover o dispositivo para cima ou para baixo em termos de prioridade.

Quando você faz uma alteração de sequência de inicialização, deve selecionar uma opção de reinicialização antes de aplicar a alteração. As opções a seguir estão disponíveis:

- **Reiniciar o servidor imediatamente:** as alterações de sequência de inicialização são salvas e o servidor é reiniciado imediatamente sem encerrar o sistema operacional.

- **Reiniciar o servidor normalmente:** as alterações da sequência de inicialização são salvas e o sistema operacional é encerrado antes de reiniciar o servidor.
- **Reinicialização manual posterior:** as alterações da sequência de inicialização serão salvas, mas não terão efeito até a próxima vez que o servidor for reinicializado.

---

## Configurando inicialização única

Para ignorar temporariamente a inicialização configurada e inicializar um dispositivo especificado uma única vez, use as informações neste tópico.

Clique em **Opções de inicialização** em **Configuração do servidor** e selecione um dispositivo no menu suspenso para configurar o dispositivo que o sistema iniciará uma única vez na próxima reinicialização de servidor. As opções a seguir estão disponíveis:

### Rede PXE

Configura seu servidor para tentar uma inicialização de rede de ambiente de execução pré-inicialização.

### Mídia removível primária

O servidor é inicializado no dispositivo USB padrão.

### CD/DVD padrão

O servidor é inicializado na unidade CD/DVD padrão.

### Configuração do sistema F1

O servidor é inicializado no Lenovo XClarity Provisioning Manager.

### Partição de diagnóstico

O servidor é inicializado na sessão Diagnóstico do Lenovo XClarity Provisioning Manager.

### Disco rígido padrão

O servidor é inicializado na unidade de disco padrão.

### Mídia remota primária

O servidor é inicializado a partir da mídia virtual montada.

### Montado

A sequência de inicialização configurada é utilizada. Não há nenhuma substituição de inicialização única da sequência de inicialização configurada.

### Sem inicialização única

A sequência de inicialização configurada é utilizada. Não há nenhuma substituição de inicialização única da sequência de inicialização configurada.

Quando você seleciona uma única alteração de sequência de inicialização, pode selecionar uma opção de reinicialização antes de aplicar a alteração.

- **Reiniciar o servidor imediatamente:** a alteração da sequência de inicialização é salva e o servidor é reiniciado imediatamente sem encerrar o sistema operacional.
- **Reiniciar o servidor normalmente:** a alteração da sequência de inicialização é salva e o sistema operacional é encerrado antes de reiniciar o servidor.
- **Reinicialização manual posterior:** a alteração da sequência de inicialização é salva, mas não terá efeito até a próxima vez que o servidor for reinicializado.

---

## Gerenciando a energia do servidor

Para visualizar informações de gerenciamento de energia e executar as funções de gerenciamento de energia, use as informações neste tópico.

Selecione **Política de energia** em **Configuração do servidor** para visualizar informações de gerenciamento de energia e executar funções de gerenciamento de energia.

**Nota:** Em um gabinete que contém nós de servidor de alta densidade, o resfriamento e a energia do chassi são controlados pelo SMM em vez do XClarity Controller. Consulte a interface da Web do SMM3 para obter mais detalhes do status de energia da solução.

## Configurando a redundância de energia

Para configurar a redundância de energia, use as informações neste tópico.

### Notas:

- Os servidores AMD não suportam a configuração da função de política de energia.
- Quando 2 unidades de fonte de alimentação estão instaladas, o modo de redundância é definido como Redundante (N+N). Com essa configuração de 2 unidades de fonte de alimentação, se uma das unidades de fonte de alimentação falhar, a CA for perdida ou removida, ela relatará evento de perda redundante no log de eventos do XCC.
- Quando apenas 1 unidade de fonte de alimentação estiver instalada após o envio, o modo de redundância será definido automaticamente como modo não redundante.

Os campos disponíveis na seção Redundância de energia incluem o seguinte:

- **Redundante (N+N):** Há duas ou mais fontes de alimentação independentes capazes de fornecer energia ao sistema simultaneamente. Isso significa que se uma ou mais fontes de alimentação falharem, as outras fontes poderão continuar fornecendo energia ao sistema sem interrupção. A redundância N+N fornece um alto nível de tolerância a falhas e garante que o sistema permaneça operacional mesmo no caso de várias falhas.
  - **Modo de saída zero:** uma vez ativado em Configuração redundante, algumas PSUs entrarão automaticamente no estado de espera em condições de carga baixa. Dessa forma, a PSU restante fornecerá a carga de energia inteira para aumentar a eficiência.
- **Modo não redundante:** neste modo, o servidor não tem a garantia de permanecer operacional se o fornecimento de energia for interrompido. O servidor será regulado se uma fonte de alimentação falhar em uma tentativa de permanecer em funcionamento.

Clique em **Aplicar** depois de fazer mudanças de configuração.

## Configurando a política de limitação de energia

Para configurar a política de limite de energia, use as informações neste tópico.

### Notas:

- Os servidores AMD não suportam a configuração da função de política de limitação de energia.
- Em um gabinete que contém nós de servidor de alta densidade, o resfriamento e a energia do chassi são controlados pelo SMM em vez do XClarity Controller. Consulte a interface da Web do SMM3 para obter mais detalhes do status de energia da solução.

É possível habilitar ou desabilitar a função de limitação de energia. Se a limitação de energia estiver ativada, uma seleção poderá ser feita para limitar a quantidade de energia usada pelo servidor. Se a limitação de energia estiver desabilitada, o limite máximo de energia será determinado pela política de redundância de energia. Para alterar a configuração, clique primeiro em **Redefinir**. Escolher sua configuração preferencial; em seguida, clique em **Aplicar**.

A capacidade total de energia está sendo calculada com base no modo de redundância de energia e no número de PSUs instaladas no sistema. A configuração manual do limite máximo de energia pode estar acima da capacidade energia real.

Quando a limitação de energia é ativada, o sistema pode ser regulado para manter o limite de energia.

**Nota:** Mesmo quando a limitação de energia é desativada, o sistema pode ser regulado sob determinadas condições de falha, como falha na fonte de alimentação, problema de resfriamento etc.

A limitação de energia pode ser ativada usando medições de **Entrada** ou medições de **Saída**. No menu suspenso, selecione o tipo das medidas que serão usadas para determinar a limitação de energia. Ao alternar entre as medições, o número no controle deslizante mudará conforme apropriado.

Existem duas maneiras de alterar o valor da limitação de energia:

- **Método 1:** mova a marca do controle deslizante para a voltagem desejada para definir o limite geral de energia do servidor.
- **Método 2:** insira o valor na caixa de entrada. A marca do controle deslizante irá se mover automaticamente para a posição correspondente.

Clique em **Aplicar** depois de fazer mudanças de configuração. As alterações entrarão em vigor imediatamente.

## Configurando a política de restauração de energia

Para configurar como o servidor reage quando a energia é restaurada após uma perda de energia, use as informações neste tópico.

Ao configurar a política de restauração de energia, as três opções a seguir estão disponíveis:

### Sempre Desligado

O servidor permanecerá desligado mesmo quando a energia for restaurada.

### Restaurar

O servidor será ligado automaticamente quando a energia for restaurada caso o servidor estivesse ligado no momento em que a falha de energia ocorreu. Caso contrário, o servidor permanecerá desligado quando a energia for restaurada.

**Nota:** Marque a caixa de seleção abaixo para definir um atraso aleatório entre 1 e 15 segundos para Ligar se o servidor estava ligado antes da falha de energia ocorrer.

### Sempre Ligado

O servidor será ligado automaticamente quando a energia for restaurada.

Clique em **Aplicar** depois de fazer mudanças de configuração.

## Ações de energia

Consulte as informações neste tópico para entender as ações de energia que podem ser executadas no servidor.

Clique em **Ação de energia** na seção **Ação rápida** na página inicial do XClarity Controller.

A tabela a seguir contém uma descrição das ações de energia e reinicialização que podem ser executadas no servidor.

Tabela 3. Ações de Energia e Descrições

Tabela de duas colunas que contém descrições das ações de energia e reinicialização de servidor.

Ação de Energia	Descrição
Ligar servidor	Selecione esse item de ação para ligar o servidor e inicializar o sistema operacional.
Desligar servidor normalmente	Selecione esse item de ação para encerrar o sistema operacional e desligar o servidor.
Desligar servidor imediatamente	Selecione esse item de ação para desligar o servidor sem primeiro encerrar o sistema operacional.
Reiniciar servidor normalmente	Selecione esse item de ação para encerrar o sistema operacional e desligar e ligar o servidor.
Reiniciar servidor imediatamente	Selecione esse item de ação para o efetuar o ciclo de ativação do servidor imediatamente sem primeiro encerrar o sistema operacional.
Inicializar servidor para configuração do sistema	Selecione esse item para ligar ou reinicializar o servidor e para inicializar automaticamente a configuração do sistema sem precisar pressionar F1 durante a inicialização.
Acionar NMI (interrupção não mascarável)	Selecione esse item de ação para forçar uma NMI em um sistema "travado". A seleção desse item de ação permite que o sistema operacional da plataforma execute um dump de memória que pode ser usado para propósitos de depuração da condição de interrupção do sistema. A reinicialização automática na configuração NMI no menu F1 de configuração do sistema determina se o XClarity Controller irá ou não reinicializar o servidor depois do NMI.
Programar ações de energia	Selecione esse item de ação para planejar ações de energia e reinicialização diárias e semanais para o servidor.
Reiniciar controlador de gerenciamento	Selecione esse item de ação para reiniciar o XClarity Controller
Servidor de ciclo de ativação CA	Selecione esta ação para efetuar um ciclo de ativação do servidor.
<p><b>Notas:</b></p> <ul style="list-style-type: none"> <li>• Se o sistema operacional estiver no protetor de tela ou no modo de bloqueio quando o encerramento do sistema operacional for tentado, o XClarity Controller talvez não consiga iniciar um encerramento normal. O XClarity Controller executará uma reinicialização ou um encerramento forçado após o intervalo de atraso de desligamento expirar, enquanto o sistema operacional ainda pode estar em execução.</li> <li>• Se o LED de energia no painel frontal estiver piscando rapidamente, o XClarity Controller pode não conseguir iniciar uma sequência de ativação normal. O XClarity Controller pode ligar o sistema quando o LED de energia começar a piscar lentamente.</li> </ul>	

## Gerenciando e monitorando o consumo de energia com os comandos da IPMI

Use as informações neste tópico para gerenciar e monitorar o consumo de energia usando comandos da IPMI.

Este tópico descreve como o Intel Intelligent Power Node Manager e a Data Center Manageability Interface (DCMI) podem ser usados para fornecer gerenciamento de energia e temperatura e gerenciamento de energia com base em política para um servidor usando comandos de gerenciamento de energia da Intelligent Platform Management Interface (IPMI).

Para servidores que usam o Intel Node Manager SPS 3.0, os usuários do XClarity Controller podem usar os comandos de gerenciamento de energia da IPMI fornecidos pelo mecanismo de gerenciamento (ME) da Intel para controlar os recursos do Node Manager e monitorar o consumo de energia do servidor. O gerenciamento de energia do servidor também pode ser realizado utilizando comandos de gerenciamento de energia de DCMI. Os comandos de gerenciamento de energia do Node Manager e de DCMI são fornecidos neste tópico.

## Gerenciando a energia do servidor usando comandos do Node Manager

Use as informações neste tópico para gerenciar a energia do servidor usando o Node Manager.

O firmware do Intel Node Manager não tem uma interface externa; portanto, os comandos do Node Manager devem primeiro ser recebidos pelo XClarity Controller e então enviados para o Intel Node Manager. O XClarity Controller funciona como um relé e um dispositivo de transporte para os comandos de IPMI usando uma ponte de IPMI padrão.

**Nota:** Alterar as políticas do Node usando comandos de IPMI do Node Manager pode criar conflitos com a funcionalidade de gerenciamento de energia do XClarity Controller. Por padrão, a ponte dos comandos do Node Manager é desativada para evitar qualquer conflito.

Para usuários que desejam gerenciar a energia do servidor usando o Node Manager em vez do XClarity Controller, um comando de IPMI OEM que consiste em (função de rede: **0x3A**) e (comando: **0xC7**) está disponível para uso.

Para ativar comandos de IPMI nativos do Node Manager, digite: `ipmitool -H <$XClarity_Controller_IP> -U <USERID> -P <PASSWORD> raw 0x3a 0xc7 0x01`

Para desativar comandos de IPMI nativos do Node Manager, digite: `ipmitool -H <$XClarity_Controller_IP> -U <USERID> -P <PASSWORD> raw 0x3a 0xc7 0x00`

As informações a seguir são exemplos de comandos de gerenciamento de energia do Node Manager.

### Notas:

- Especificando o **canal 0** de IPMI e um endereço de destino **0x2c**, você poderá usar o IPMITOOL para enviar comandos para o Intel Node Manager processar. Uma mensagem de solicitação é usada para inicializar uma ação e uma mensagem de resposta é retornada ao solicitante.
- Os comandos são exibidos no seguinte formato devido a limitações de espaço.

**Monitoramento de energia usando Obter estatísticas globais de energia do sistema (código de comando 0xC8):** Solicitação: `ipmitool -H <$XClarity_Controller_IP> -U <USERID> -P <PASSWORD> -b 0x00 -t 0x2c raw 0x2E 0xC8 0x57 0x01 0x00 0x01 0x00 0x00` Resposta: `57 01 00 38 00 04 00 41 00 39 00 ec 56 f7 53 5a 86 00 00 50`

**Limitação de energia usando Definir política do Intel Node Manager (código de comando 0xC1):** Solicitação: `ipmitool -H <$XClarity_Controller_IP> -U <USERID> -P <PASSWORD> -b 0x00 -t 0x2c raw 0x2e 0xC1 0x57 0x01 0x00 0x10 0x01 0xA0 0x00 0x00 0x00 0x60 0xea 0x00 0x00 0x00 0x00 0x1e 0x00` Resposta: `57 01 00`

### **Economia de energia usando Definir política do Intel Node Manager (código de comando 0xC1):**

Solicitação:ipmitool -H <\$XClarity\_Controller\_IP> -U <USERID> -P <PASSWORD> -b 0x00 -t 0x2c raw 0x2e 0xC1 0x57 0x01 0x00 0x10 0x01 0x00 0x00 0x00 0x00 0x60 0xea 0x00 0x00 0x00 0x00 0x1e 0x00

### **Função Obter ID do dispositivo usando Obter ID do dispositivo do mecanismo de gerenciamento da Intel:**

Solicitação:ipmitool -H <\$XClarity\_Controller\_IP> -U <USERID> -P <PASSWORD> -b 0x00 -t 0x2c raw 0x06 0x01 Resposta:50 01 03 05 02 21 57 01 00 05 0b 03 40 20 01

Para ver comandos adicionais do Intel Node Manager, consulte a última versão da **especificação de interface externa do Intel Intelligent Power Node Manager usando IPMI** em <https://businessportal.intel.com>.

## **Gerenciando a energia do servidor usando comandos do DCMI**

Use as informações neste tópico para gerenciar a energia do servidor usando comandos do DCMI.

O DCMI fornece funções de monitoramento e controle que podem ser expostas pelas interfaces padrão de software de gerenciamento. As funções de gerenciamento de energia do servidor também podem ser realizadas utilizando comandos de DCMI.

As informações a seguir são exemplos de funções e comandos comuns de gerenciamento de energia de DCMI. Uma mensagem de solicitação é usada para inicializar uma ação e uma mensagem de resposta é retornada ao solicitante.

**Nota:** Os comandos são exibidos nos seguintes formatos devido a limitações de espaço.

**Obter a leitura de energia:** Solicitação:ipmitool -H <\$XClarity\_Controller\_IP> -U <USERID> -P <PASSWORD> raw 0x2c 0x02 0xdc 0x01 0x00 0x00 Resposta:dc 39 00 38 00 3b 00 39 00 e3 6f 0a 39 e8 03 00 00 40

**Definir limite de energia:** Solicitação:ipmitool -H <\$XClarity\_Controller\_IP> -U <USERID> -P <PASSWORD> raw 0x2c 0x04 0xdc 0x00 0x00 0x00 0x00 0xA0 0x00 0xe8 0x03 0x00 0x00 0x00 0x00 0xe8 0x03 Resposta:dc

**Obter limite de energia:** Solicitação:ipmitool -H <\$XClarity\_Controller\_IP> -U <USERID> -P <PASSWORD> raw 0x2c 0x03 0xdc 0x00 0x00 Resposta:dc 00 00 00 a0 00 e8 03 00 00 00 00 01 00

**Ativar limite de energia:** Solicitação:ipmitool -H <\$XClarity\_Controller\_IP> -U <USERID> -P <PASSWORD> raw 0x2c 0x05 0xdc 0x01 0x00 0x00 Resposta:dc

**Desativar limite de energia:** Solicitação:ipmitool -H <\$XClarity\_Controller\_IP> -U <USERID> -P <PASSWORD> raw 0x2c 0x05 0xdc 0x00 0x00 0x00 Resposta:dc

**Nota:** Em alguns servidores, ações de exceção para o comando **Definir limite de energia** podem não ser suportadas. Por exemplo, o parâmetro **Desligamento forçado do sistema e log de eventos em SEL** talvez não seja suportado.

Para ver a lista completa dos comandos que são suportados pela especificação de DCMI, consulte a última versão da **especificação da interface de gerenciamento de data center** em <https://www.intel.com/content/dam/www/public/us/en/documents/technical-specifications/dcmi-v1-5-rev-spec.pdf>.

---

## **Baixando log de dados de serviço**

Use as informações neste tópico para coletar informações de serviço sobre o servidor. Esse processo geralmente é executado apenas a pedido da equipe de serviço para ajudar a resolver um problema do servidor.

Na página inicial do XClarity Controller, clique na opção **Log de serviço** na seção **Ação rápida** e selecione **Log de dados de serviço**.

Por padrão, o log de serviço conterá os seguintes dados: informações do sistema, inventário do sistema, utilização do sistema, tabela SMBIOS, leitura de sensores, log de eventos, chave FOD, chave SLP, configuração UEFI e configuração do XClarity Controller 3.

Passa o mouse sobre a opção Informações básicas e clique na janela flutuante para ver alguns dos dados reais que serão exportados.

Embora as Informações básicas sejam obrigatórias, as seguintes informações também podem ser exportadas:

- Informações de rede (IP, nome do host)
- Telemetria (dados de 24 horas)
- Log de auditoria (contém nome de usuário)
- Tela de Falha mais Recente

Clique em **Exportar** para baixar o log de dados de serviço.

O processo para coletar os dados de serviço e suporte pode demorar alguns minutos para ser concluído. O arquivo será salvo na pasta padrão de download. A convenção de nomenclatura para o arquivo de dados de serviço segue esta convenção: <machine type and model>\_<serial number>\_xcc3\_ServiceData\_<date>-<time>.zip

Por exemplo: 7X2106Z01A\_2345678\_xcc3\_ServiceData\_240517-112857.zip.

Além dos dados de serviço em formato .zip, o log de depuração também pode ser baixado no formato de arquivo .tar.zst via **Histórico de navegação...** A convenção de nomenclatura para o arquivo de depuração lddf segue esta convenção: <machine type and model>\_<serial number>\_xcc3\_DebugLog\_<date>-<time>.tar.zst

Por exemplo: 7X2106Z01A\_2345678\_xcc3\_DebugLog\_240517-112857.zip.

#### **Notas:**

- **Histórico de navegação...** também reterá logs de serviço exportados recentemente.
- O formato de arquivo .tar.zst usa um algoritmo de compactação diferente e pode ser extraído com o pacote "zstd". Por exemplo:  

```
tar --use-compress-program=unzstd -xvf <machine type and model>_<serial number>_xcc3_DebugLog_<date>-<time>.tar.zst
```

---

## **Propriedades do servidor**

Use as informações neste tópico para alterar ou visualizar as propriedades relevantes do servidor.

### **Definindo o local e o contato**

Use as informações neste tópico para definir vários parâmetros para ajudar a identificar o sistema para a equipe de operações e suporte.

Selecione **Propriedades do servidor** em **Configuração do servidor** para configurar as informações de **Local e contato**.

#### **Contato**

Permite que você especifique o nome e o número de telefone da pessoa que deve ser contatada se houver um problema com o sistema.

**Nota:** Este campo é o mesmo que o de contato na configuração SNMPv3 e é obrigatório para habilitar o SNMPv3.

#### **Nome do rack**

Permite que você localize o servidor mais facilmente especificando em qual rack ele está.

#### **Número da sala**

Permite que você localize o servidor mais facilmente especificando em qual sala ele está.

#### **Criando**

Permite que você localize o servidor mais facilmente especificando em qual prédio ele está.

#### **U mais baixo**

Permite que você localize o servidor mais facilmente especificando a posição do rack.

#### **Endereço**

Permite especificar o endereço postal completo no qual o servidor está localizado.

**Nota:** Quando as informações relevantes forem inseridas, elas aparecerão como uma única linha no campo **Local** na seção SNMPv3 e na página inicial do XClarity Controller.

## **Configurando tempos limites do servidor**

Use as informações neste tópico para definir os tempos limites para o servidor.

Esses tempos limite são usados para restaurar a operação de um servidor que travou.

Selecione **Propriedade do servidor** em **Configuração do servidor** para configurar os tempos limite do servidor. As seguintes opções de tempo limite do servidor são fornecidas:

#### **Ativar Atraso de Desligamento**

Use esse campo para especificar o número de minutos que o subsistema do BMC esperará até que o sistema operacional seja desativado antes de desligar o sistema.

Para configurar o valor de tempo limite de atraso de desligamento, selecione o intervalo de tempo no menu suspenso e clique em **Aplicar**. Para desativar o desligamento forçado do XClarity Controller, selecione **Nenhum** na seleção suspensa.

## **Mensagem de infração**

Para criar uma mensagem que é exibida quando um usuário faz login no XClarity Controller, use as informações neste tópico.

Selecione **Propriedades do servidor** em **Configuração do servidor**. Use a opção **Mensagem de Infração** para configurar uma mensagem que você deseja que seja exibida para o usuário. Clique em **Aplicar** quando terminar.

O texto da mensagem será exibido na área Mensagem da página de login do XClarity Controller quando um usuário fizer login.

## Serviço de soluções

Use as informações neste tópico para ativar ou desativar o serviço de solução.

**Nota:** Esse recurso será suportado em uma atualização futura.

---

## Definindo a data e a hora do XClarity Controller

Use as informações neste tópico para entender as configurações de data e hora do XClarity Controller. As instruções são fornecidas para configurar a data e hora do XClarity Controller. A data e hora do XClarity Controller são usadas para marcar data e hora de todos os eventos que são registrados no log de eventos e nos alertas que são enviados.

Na página inicial do XClarity Controller, clique em ícone de relógio no canto superior direito para visualizar ou alterar a data e hora do XClarity Controller. O XClarity Controller não tem seu próprio relógio em tempo real. É possível configurar o XClarity Controller para sincronizar sua data e hora com um servidor Network Time Protocol ou com o hardware de relógio em tempo real do servidor.

### Sincronização com NTP

Conclua as etapas a seguir para sincronizar o relógio do XClarity Controller com o servidor NTP:

- Selecione **Sincronizar hora com NTP** e especifique o endereço do servidor NTP.
- Servidores NTP adicionais podem ser especificados clicando no ícone "+".
- Especifique com que frequência você deseja que o XClarity Controller seja sincronizado com o servidor NTP.
- A hora obtida no servidor NTP está no formato Coordinated Universal Time (UTC).
  - Se quiser que o XClarity Controller ajuste data e hora para a sua região local, selecione o deslocamento do fuso horário de sua localidade no menu suspenso.
  - Se o seu local estiver em horário de verão, marque a caixa de seleção **Ajustar automaticamente para horário de verão (DST)**.
- Quando suas alterações de configuração estiverem completas, clique em **Aplicar**.

### Sincronização com o host

A hora mantida no hardware de relógio em tempo real do servidor pode estar no formato Coordinated Universal Time (UTC) ou pode já ter sido ajustada e armazenada no formato do horário local. Alguns sistemas operacionais armazenam o relógio em tempo real em formato UTC, enquanto outros armazenam a hora como hora local. O relógio em tempo real do servidor não indica em qual formato está a hora. Portanto, quando o XClarity Controller está configurado para sincronizar com o relógio em tempo real do host, o usuário pode escolher como o XClarity Controller usa a data e hora que é obtida do relógio em tempo real.

- Local (exemplo: Windows): Nesse modo, o XClarity Controller manipula a data e hora que é obtida do relógio em tempo real como hora local com o fuso horário e os deslocamentos de DST já aplicados. Se o seu local estiver em horário de verão, você também pode marcar a caixa de seleção **Ajustar automaticamente para horário de verão (DST)**.
- UTC (exemplo: Linux): Nesse modo, o XClarity Controller manipula a data e hora que é obtida do relógio em tempo real como Coordinated Universal Time, sem nenhum fuso horário ou deslocamento de DST já aplicado. Nesse modo, você pode optar por ajustar a data e hora para a sua região local selecionando o deslocamento de fuso horário da sua localização no menu suspenso. Se o seu local estiver em horário de verão, você também pode marcar a caixa de seleção **Ajustar automaticamente para horário de verão (DST)**.
- Quando suas alterações de configuração estiverem completas, clique em **Aplicar**.

**Nota:** Quando o horário de verão ocorrer, as ações que foram agendadas para o XClarity Controller executar durante o intervalo em que o relógio salta para a frente não serão executadas. Por exemplo, se o horário de início do horário de verão dos EUA 2 horas de 12 de março e uma ação de energia for planejada para 2<sup>h10</sup> de 12 de março, essa ação não ocorrerá. Quando for 2 horas, o XClarity Controller lerá a hora como 3 horas.

---

## Configurando o chassi D3 V2

Use as informações neste tópico para entender as configurações do chassi D3 V2.

Clique em **Chassi** na **Configuração do Servidor** para exibir informações sobre o chassi D3 V2.

### Informações do chassi

Esta seção exibe as informações do chassi, incluindo UUID, número de série, tipo de máquina e versão do firmware. Também mostra as informações dos nós, incluindo fator forma, status de energia e endereço IP.

#### Notas:

- Clique no botão **Redefinir/Reposicionar** ao lado do nó correspondente para reiniciar o nó ou simular um reposicionamento de nó físico.
- Apenas o nó provisório pode redefinir ou reposicionar outros nós.

### Função do chassi provisório

Esta seção exibe a preferência de seleção do chassi provisório.

#### Notas:

- Selecione **Participar para a função do chassi provisório** para permitir que um nó participe do processo de eleição de provisório. Se houver outro nó designado como provisório permanente, então nenhum processo de eleição ocorrerá, a menos que esse nó esteja ausente.
- Selecione **Designar esse nó como um chassi provisório permanente** se você quiser que apenas um nó seja o provisório. Nesse caso, não há alta disponibilidade para a função de provisório. Se o nó provisório permanente estiver ausente do chassi, então ocorrerá um processo de eleição de provisório para selecionar o próximo provisório adequado.

### Histórico de manutenção do chassi

O histórico de manutenção do chassi retém um registro de nós sendo adicionados ou removidos no chassi, bem como a função de provisório alterando de um nó para outro.



---

## Capítulo 6. Recurso de Console Remoto

Use as informações neste tópico para entender como visualizar e interagir remotamente com o console do servidor.

Você pode usar a função de console remoto na interface da Web do XClarity Controller para visualizar e interagir com o console do servidor. Você pode designar uma imagem de disco (arquivo ISO ou IMG) como uma unidade virtual no servidor. A funcionalidade de console remoto está disponível com os recursos de nível Premier do XClarity Controller e só está disponível por meio da interface da Web. Você deve fazer login no XClarity Controller com um ID do usuário que tenha privilégios de acesso de supervisor ou de console remoto para usar os recursos de console remoto. Para obter mais informações sobre como atualizar do nível padrão do XClarity Controller para o nível Premier do XClarity Controller, consulte ["Atualizando o XClarity Controller" na página 6](#).

Use os recursos de console remoto para fazer o seguinte:

- Visualize vídeo remotamente com resolução gráfica de até 1920x1200 32 bpp a 60 Hz, independentemente do estado do servidor.
- Acessar remotamente o servidor usando o teclado e mouse a partir de um cliente remoto.
- Montar arquivos ISO e IMG que estão localizados no seu sistema local ou em um sistema remoto como unidades virtuais que estão disponíveis para uso pelo servidor.
- Fazer upload de uma imagem IMG ou ISO para a memória do XClarity Controller e montá-la no servidor como uma unidade virtual. Até dois arquivos com um tamanho máximo total de 100 MB podem ser carregados na memória do XClarity Controller.

### Notas:

- Quando o recurso de console remoto é iniciado no modo multiusuário (o XClarity Controller com o conjunto de recursos de nível Premier do XClarity Controller suporta até seis sessões simultâneas), o recurso de disco remoto pode ser exercido por apenas uma sessão por vez.
- O console remoto é capaz de exibir apenas o vídeo gerado pelo controlador de vídeo na placa-mãe. Se um adaptador de controlador de vídeo separado estiver instalado e for usado no lugar do controlador de vídeo do sistema, o console remoto do XClarity Controller não poderá exibir o conteúdo de vídeo do adaptador adicionado.
- Se você tiver firewalls em sua rede, a porta de rede deve ficar aberta para suportar o recurso de console remoto. Para visualizar ou alterar o número de porta de rede utilizado pelo recurso de console remoto, consulte ["Ativação de serviço e atribuição de porta" na página 35](#).
- O recurso de console remoto usa HTML5 para exibir o vídeo do servidor em páginas da Web. Para usar esse recurso, seu navegador deve suportar exibição de conteúdo de vídeo usando elementos de HTML5.
- Se estiver usando certificados autoassinados e um endereço IPv6 para acessar o BMC com o navegador Internet Explorer, a sessão de console remoto pode não iniciar devido a um erro de certificado. Para evitar esse problema, o certificado autoassinado pode ser adicionado às autoridades de certificado raiz do Internet Explorer:
  - Selecione **Segurança** em **Configuração do BMC** e baixe o certificado autoassinado.
  - Altere a extensão do arquivo de certificado para \*.crt e clique duas vezes no arquivo de certificado da Web.
  - Limpe o cache do navegador IE11.
  - Clique em **Instalar certificado** para instalar o certificado para o armazenamento de certificados seguindo as etapas do assistente de importação de certificado.

---

## Habilitando o recurso de console remoto

Este tópico fornece informações sobre o recurso de console remoto.

A funcionalidade do console remoto do XClarity Controller está disponível apenas nos recursos de nível Premier do XClarity Controller. Se não tiver o privilégio para operar o console remoto, você verá um ícone de cadeado.

Depois de comprar e obter a chave de ativação para a atualização de nível do XClarity Controller Premier, instale-o usando as instruções em ["Instalando uma chave de ativação" na página 87](#).

Para usar a funcionalidade do console remoto, clique na imagem com uma seta branca apontando diagonalmente na seção **Visualização do console remoto** da página inicial do XClarity Controller ou na página da Web do **Console remoto**.

---

## Controle remoto de energia

Este tópico explica como enviar comandos para ligar e reiniciar o servidor a partir da janela do console remoto.

Você pode enviar comandos para ligar e reiniciar o servidor a partir da janela do console remoto sem retornar à página da Web principal. Para controlar a energia do servidor com o console remoto, clique em **Energia** e selecione um dos seguintes comandos:

### Ligar servidor

Selecione esse item de ação para ligar o servidor e inicializar o sistema operacional.

### Desligar servidor normalmente

Selecione esse item de ação para encerrar o sistema operacional e desligar o servidor.

### Desligar servidor imediatamente

Selecione esse item de ação para desligar o servidor sem primeiro encerrar o sistema operacional.

### Reiniciar servidor normalmente

Selecione esse item de ação para encerrar o sistema operacional e desligar e ligar o servidor.

### Reiniciar servidor imediatamente

Selecione esse item de ação para o efetuar o ciclo de ativação do servidor imediatamente sem primeiro encerrar o sistema operacional.

### Inicializar servidor para configuração do sistema

Selecione esse item para ligar ou reinicializar o servidor e para inicializar automaticamente a configuração do sistema sem precisar pressionar F1 durante a inicialização.

---

## Tela de captura do console remoto

Use as informações neste tópico para entender como usar o recurso de captura de tela do console remoto.

O recurso de captura de tela na janela do console remoto captura o conteúdo da exibição de vídeo do servidor. Para capturar e salvar uma imagem de tela, conclua as etapas a seguir:

Etapa 1. Na janela do console remoto, clique em **Capturar tela**.

Etapa 2. Na janela pop-up, clique em **Salvar arquivo** e pressione **OK**. O arquivo será salvo como rpviewer.png na sua pasta padrão de baixar arquivos.

**Nota:** A imagem de captura de tela é salva como um arquivo do tipo JPG.

---

## Suporte a teclado de console remoto

Na janela do console remoto, em **Teclado**, os seguintes itens de opção são fornecidos:

- Clique em **Teclado virtual** para ativar o teclado virtual. Esse recurso é útil quando você usa um tablet que não tem um teclado físico. As seguintes opções podem ser usadas para criar macros e combinações de teclas que podem ser enviadas ao servidor. O sistema operacional no sistema cliente que você está usando pode prender determinadas combinações de teclas (por exemplo, Ctrl+Alt+Del) em vez de transmiti-las para o servidor. Outras teclas, como F1 ou Esc, podem ser interceptadas pelo programa ou navegador que você está usando. As macros fornecem um mecanismo para envio de pressionamentos de teclas para o servidor que o usuário talvez não consiga enviar.
- Clique em **Macros de servidor** para usar macros definidas pelo servidor. Algumas macros de servidor são predefinidas pelo firmware do XClarity Controller.

---

## Modos de tela de console remoto

Use as informações neste tópico para configurar os modos de tela de console remoto.

Para configurar os modos de tela de console remoto, clique em **Modo de tela**.

As seguintes opções de menu estão disponíveis:

### Tela Cheia

Este modo preenche a área de trabalho do cliente com a exibição do vídeo. Pressionar a tecla Esc neste modo sairá do modo de tela cheia. Como o menu do console remoto não está visível no modo de tela cheia, você terá que sair do modo de tela cheia para usar qualquer um dos recursos fornecidos pelo console remoto, como as macros de teclado.

### Ajustar na tela

Essa é a configuração padrão quando o console remoto é ativado. Nessa configuração, a área de trabalho de destino é completamente exibida sem barras de rolagem. A proporção é mantida.

---

## Métodos de montagem de mídia

Use as informações neste tópico para entender como executar montagens de mídia.

Três mecanismos são fornecidos para montar arquivos ISO e IMG como unidades virtuais.

- Unidades virtuais podem ser adicionadas ao servidor na sessão de console remoto clicando em **Mídia**.
- Diretamente na página da Web do console remoto, sem estabelecer uma sessão de console remoto.
- Ferramenta independente.

Os usuários precisam dos privilégios de **Acesso de console remoto e disco remoto** para usar os recursos de mídia virtual.

Arquivos podem ser montados como mídia virtual do sistema local ou de um servidor remoto e podem ser acessados na rede ou carregados na memória do XClarity Controller, por meio do recurso RDOC. Esses mecanismos são descritos abaixo.

- Mídias locais são arquivos ISO ou IMG localizados no sistema que você está usando para acessar o XClarity Controller. Esse mecanismo está disponível apenas por meio da sessão do console remoto, não diretamente na página da Web do console remoto, e está disponível apenas com recursos de nível Premier do XClarity Controller. Para montar mídia local, clique em **Montar toda a mídia local** na seção **Montar arquivo de mídia local**. Até quatro arquivos podem ser montados simultaneamente no servidor.

- Os arquivos que estão localizados em um sistema remoto também podem ser montados como mídia virtual. Até quatro arquivos podem ser montados simultaneamente como unidades virtuais. O XClarity Controller oferece suporte aos protocolos de compartilhamento de arquivos a seguir:

- **CIFS - Common Internet File System:**

- Insira o URL que localiza o arquivo no sistema remoto.
- Se quiser que o arquivo seja apresentado ao servidor como mídia virtual somente leitura, marque a caixa de seleção.
- Insira as credenciais necessárias para o XClarity Controller acessar o arquivo no sistema remoto.

**Nota:** O XClarity Controller não suporta espaços no nome de usuário, na senha ou no URL. Certifique-se de que o servidor CIFS não tenha credenciais de login configuradas com um espaço no nome de usuário ou na senha e que o URL não contenha um espaço.

- As opções de montagem são opcionais e definidas pelo protocolo CIFS.
- Se o servidor remoto pertencer a uma coleção de servidores, em que a segurança será manipulada centralmente, insira o nome do domínio ao qual pertence o servidor remoto.

- **NFS - Network File System:**

- Insira o URL que localiza o arquivo no sistema remoto.
- Se quiser que o arquivo seja apresentado ao servidor como mídia virtual somente leitura, marque a caixa de seleção.
- As opções de montagem são opcionais e definidas pelo protocolo NFS. NFS v3 e NFS v4 têm suporte. Por exemplo, para usar NFS v3, você precisa especificar a opção 'nfsvers=3'. Se o servidor NFS usa o tipo de segurança AUTH\_SYS para autenticar operações NFS, será necessário especificar a opção 'sec=sys'.

- **HTTPFS - HTTP Fuse-based File System:**

- Insira o URL que localiza o arquivo no sistema remoto.
- Se quiser que o arquivo seja apresentado ao servidor como mídia virtual somente leitura, marque a caixa de seleção.

**Nota:** Erros podem ocorrer durante o processo de montagem para certificados de segurança gerados pelo Microsoft IIS. Se isso acontecer, consulte "[Problemas de erro de montagem de mídia](#)" na página 77.

Clique em **Montar todas as mídias remotas** para montar o arquivo como mídia virtual. Para remover a mídia virtual, clique no ícone de lixeira no lado direito da mídia montada.

- Até dois arquivos podem ser carregados na memória do XClarity Controller e montados como mídia virtual com o recurso RDOC do XClarity Controller. O tamanho total dos dois arquivos não deve ultrapassar 100 MB. Esses arquivos permanecerão na memória do XClarity Controller até que sejam removidos, mesmo se a sessão de console remoto for encerrada. O recurso RDOC oferece suporte aos seguintes mecanismos ao carregar os arquivos:

- **CIFS - Common Internet File System:** Consulte a descrição anterior para obter detalhes. **Exemplo:**

Para montar um arquivo ISO chamado account\_backup.iso que está localizado no diretório backup\_2016 de um servidor CIFS no endereço IP 192.168.0.100 como uma unidade virtual somente leitura no servidor, você deve preencher os campos conforme mostrado na figura a seguir. Nesse exemplo, o servidor localizado em 192.168.0.100 é membro de um conjunto de servidores no domínio "contabilidade". O nome do domínio é opcional. Se o seu servidor CIFS não fizer parte de um domínio, deixe o campo **Domínio** em branco. A opção de montagem CIFS "nocase" é especificada no campo **Opções de Montagem** neste exemplo, indicando para o servidor CIFS que a verificação de maiúsculas/minúsculas do nome do arquivo deve ser ignorada. O campo **Opções de Montagem** é opcional. As informações inseridas pelo usuário nesse campo não são usadas pelo BMC e são

simplesmente passadas para o servidor CIFS quando a solicitação de montagem é feita. Consulte a documentação para obter informações sobre a sua implementação do servidor CIFS a fim de determinar quais opções são compatíveis com o servidor CIFS.

Mount Media File from Network: 0 mounted

Mount an ISO or IMG image file from a file server to the host as a DVD or USB drive.  
Note: The client session could be closed without affecting mounted media.

CIFS Input URL: //192.168.0.100/backup\_2016/account\_backup.iso Read-only

User Name: mycifsname Password: \*\*\*\*\*

Mount Options: nocase Domain: accounting

Mount all remote media

O BMC fornece orientação ao especificar a URL. Se a URL que está sendo digitada não for válida, o botão de montagem ficará cinza, e um texto em vermelho será exibido no campo de URL mostrando o formato esperado para ela.

URL address in the form of //ipaddress/path/to/file or //domain-name/path/to/file. The domain-name can be alphanumeric characters, '.', '-' or '\_'. It must contain at least two domain items.

- **NFS - Network File System:** Consulte a descrição anterior para obter detalhes. **Exemplo:**

Para montar um arquivo ISO chamado US\_team.iso localizado no diretório "personnel" de um servidor NFS no endereço IP 10.243.28.77 como uma unidade virtual somente leitura no servidor, você deve preencher os campos conforme mostrado na figura a seguir. A opção de montagem NFS "porta = 2049" especifica que a porta de rede 2049 deve ser usada para transferir os dados. O campo **Opções de Montagem** é opcional. As informações inseridas pelo usuário nesse campo são passadas para o servidor NFS quando a solicitação de montagem é feita. Consulte a documentação para obter informações sobre a sua implementação do servidor NFS a fim de determinar quais opções são compatíveis com o servidor NFS.

Mount Media File from Network: 0 mounted

Mount an ISO or IMG image file from a file server to the host as a DVD or USB drive.  
Note: The client session could be closed without affecting mounted media.

NFS Input URL: 10.243.28.77/personnel/US\_team.iso Read-only

Mount Options: port=2049

Mount all remote media

O BMC fornece orientação ao especificar a URL. Se a URL que está sendo digitada não for válida, o botão de montagem ficará cinza, e um texto em vermelho será exibido no campo de URL mostrando o formato esperado para ela.

URL address in the form of ipaddress:/path/to/file or domain-name:/path/to/file. The domain-name can be alphanumeric characters, '.', '-' or '\_'. It must contain at least two domain items.

## – HTTPS – Protocolo de Transporte de Hipertexto Seguro:

- Insira o URL que localiza o arquivo no sistema remoto.
- Se quiser que o arquivo seja apresentado ao servidor como mídia virtual somente leitura, marque a caixa de seleção.
- Insira as credenciais necessárias para o XClarity Controller acessar o arquivo no sistema remoto.

### Notas:

- Erros podem ocorrer durante o processo de montagem para certificados de segurança gerados pelo Microsoft IIS. Se isso acontecer, consulte "[Problemas de erro de montagem de mídia](#)" na [página 77](#).
- O XClarity Controller não suporta espaços no nome de usuário, na senha ou no URL. Certifique-se de que o servidor CIFS não tenha credenciais de login configuradas com um espaço no nome de usuário ou na senha e que o URL não contenha um espaço. **Exemplo:**

Para montar um arquivo ISO chamado EthernetDrivers.ISO localizado no diretório "newdrivers" de um servidor HTTPS com o nome de domínio "mycompany.com" usando a porta de rede 8080 como uma unidade virtual somente leitura no servidor, você deve preencher os campos conforme mostrado na figura a seguir.

The screenshot shows a web interface for mounting a Remote Disc On Card (RDOC). At the top, it says "Remote Disc On Card (RDOC): 0 uploaded (50 MB available)". Below this, there is a note: "Upload an ISO or IMG image file to the BMC, then mount it to the host as a DVD or USB drive. The BMC storage space is restricted to 50 MB in total. Note: The client session could be closed without affecting the mounted media." The main form has a dropdown menu set to "HTTPS". The "Input URL:" field contains "HTTPS://mycompany.com:8080/newdrivers/EthernetDrivers.ISO" and has a "Read-only" checkbox checked. The "User Name:" field contains "test" and the "Password:" field is masked with asterisks. There is a "Mount all RDOC files" button at the bottom.

O BMC fornece orientação ao especificar a URL. Se a URL que está sendo digitada não for válida, o botão de montagem ficará cinza, e um texto em vermelho será exibido no campo de URL mostrando o formato esperado para ela.

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

## – SFTP – SSH File Transfer Protocol

- Insira o URL que localiza o arquivo no sistema remoto.
- Se quiser que o arquivo seja apresentado ao servidor como mídia virtual somente leitura, marque a caixa de seleção.
- Insira as credenciais necessárias para o XClarity Controller acessar o arquivo no sistema remoto.

### Notas:

- O XClarity Controller não suporta espaços no nome de usuário, na senha ou no URL. Certifique-se de que o servidor CIFS não tenha credenciais de login configuradas com um espaço no nome de usuário ou na senha e que o URL não contenha um espaço.
- Quando o XClarity Controller se conectar a um servidor HTTPS, uma janela pop-up aparecerá mostrando informações do certificado de segurança usado pelo servidor HTTPS. O XClarity Controller não conseguiu verificar a autenticação do certificado de segurança.

## – LOCAL - Common Internet File System:

- Procure no sistema o arquivo ISO ou IMG que deseja montar.

- Se quiser que o arquivo seja apresentado ao servidor como mídia virtual somente leitura, marque a caixa de seleção.

Clique em **Montar todos os arquivos RDOC** para montar o arquivo como mídia virtual. Para remover a mídia virtual, clique no ícone da lixeira no lado direito da mídia montada.

## Ferramenta independente

Para os usuários que precisam montar dispositivos ou imagens (.iso/.img) usando o XClarity Controller, os usuários podem usar a parte rdmount do código independente do pacote do OneCLI. Especificamente, rdmount abrirá uma conexão para XClarity Controller e montará o dispositivo ou imagens para o host.

rdmount tem a seguinte sintaxe:

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

Exemplo para montar um arquivo 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
```

---

## Problemas de erro de montagem de mídia

Use as informações neste tópico para solucionar problemas de erro de montagem de mídia.

Ao usar certificados de segurança gerados pelo Microsoft IIS, você pode encontrar erros durante o processo de montagem. Se isso ocorrer, substitua o certificado de segurança por um novo gerado pelo openssl. Especificamente, o arquivo pfx recém-gerado é carregado no servidor Microsoft IIS.

A seguir há um exemplo que mostra como o novo certificado de segurança é gerado pelo openssl no sistema operacional 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
```

---

## Saindo da sessão de console remoto

Este tópico explica como finalizar a sessão de console remoto.

Para sair da sessão de controle remoto, feche o console remoto e as janelas de sessão de mídia virtual.

---

## Capítulo 7. Configurando o armazenamento

Use as informações neste capítulo para entender as opções disponíveis para as configurações de armazenamento.

Ao configurar o armazenamento, as seguintes opções estão disponíveis:

- Detalhe do armazenamento
- Configuração de RAID

---

### Detalhe do armazenamento

Para usar a função de detalhe de armazenamento, use as informações neste tópico.

Essa função exibe a estrutura física dos dispositivos de armazenamento e a configuração de armazenamento junto com detalhes como local, fabricante, nome do produto, status, capacidade, interface, mídia, fator de forma e outras informações.

Um evento crítico ou de aviso será acionado quando o valor de vida útil restante da unidade SSD atingir o limite ou for inferior. O valor padrão de vida útil restante para evento de aviso e crítico é de 8% e 4%, respectivamente. Clique no ícone de engrenagem ao lado de **Detalhe do armazenamento** para definir o valor limite.

Para configurar backplanes SAS/SATA/NVMe (AnyBay) que oferecem suporte ao modo de **pista PCIe x1**, clique no ícone de engrenagem ao lado de **Backplane**, selecione o grupo de compartimentos de unidade e clique no botão **Aplicar** para salvar a configuração.

---

### Configuração de RAID

Para executar funções de configuração de RAID, use as informações neste tópico.

Use as informações neste tópico para visualizar e configurar conjuntos de armazenamento, discos virtuais associados e unidades para o adaptador RAID. Se o sistema estiver desligado, ligue-o para visualizar informações de RAID.

### Exibindo e configurando unidades virtuais

Use as informações neste tópico para exibir e configurar as unidades virtuais.

Quando você selecionar **Configurar RAID** em **Configuração do servidor**, a guia **Configuração da matriz** será escolhida e os discos virtuais existentes serão exibidos por padrão. As unidades lógicas são classificadas por matrizes de discos e controladores. São exibidas informações detalhadas sobre o disco virtual, como o tamanho da faixa e informações inicializáveis.

Para definir as configurações RAID, clique em **Habilitar modo de edição**.

No modo de edição, é possível clicar no menu de ação do controlador, visualizar os discos virtuais RAID existentes e criar novos discos virtuais RAID.

No menu Ações do controlador, você pode executar as seguintes ações:

#### Limpar configuração de RAID

Limpar todas as configurações e dados do controlador selecionado.

### Importar unidades estrangeiras

Importar as unidades estranhas que foram detectadas. Uma unidade estranha é uma unidade que foi movida de uma configuração do RAID diferente para o controlador RAID existente

**Nota:** Você será notificado se nenhuma unidade estranha for detectada.

### Gerenciar configuração externa

Importar as unidades estranhas que foram detectadas. Uma unidade estranha é uma unidade que foi movida de uma configuração do RAID diferente para o controlador RAID existente

**Nota:** Você será notificado se nenhuma unidade estranha for detectada.

Informações dos discos virtuais RAID existentes para um controlador específico são exibidas como as respectivas "placas de disco virtual". Cada placa exibe informações como nome do disco virtual, status, capacidade e ações. O ícone de lápis permite editar informações, o ícone de lixeira permite excluir as "placas de disco virtual".

**Nota:** A capacidade e o nível RAID não podem ser alterados.

Se você clicar no nome do disco virtual, aparecerá uma janela de propriedades de disco virtual.

### Criando um novo disco virtual RAID

Para criar um novo disco virtual RAID, siga as etapas mostradas abaixo:

**Nota:** Se não há capacidade de armazenamento disponível, não é possível criar um novo disco virtual.

#### 1. Selecione unidades ou uma matriz de disco que tenha capacidade de armazenamento livre

- a. Para criar um disco virtual em uma nova matriz de disco, é necessário especificar o nível RAID.

**Nota:** Se não houver unidades suficientes para selecionar e você clicar em **Avançar**, uma mensagem de erro aparecerá no campo de nível RAID.

- b. Para alguns níveis RAID, o intervalo é necessário. Há também uma quantidade mínima de unidades que precisam estar presentes no intervalo. Para esses tipos de situações, especifique o número da extensão no campo **Número da extensão**, selecione **Membro** ou **Hot Spare** no menu suspenso ao lado das unidades e, em seguida, marque a caixa de seleção ao lado das unidades que serão usadas para criar o disco virtual.
- c. Para criar discos virtuais em uma matriz de disco existente, você precisa selecionar uma matriz de disco que possui capacidade disponível.

#### 2. Criação de um disco virtual

- a. Por padrão, a criação de um disco virtual usará toda a capacidade de armazenamento. O ícone **Adicionar** é desabilitado quando toda a capacidade de armazenamento é usada. Você pode clicar no ícone de lápis para alterar a capacidade ou outras propriedades.
- b. Quando você editar o primeiro disco virtual para usar apenas alguma capacidade de armazenamento, o ícone **Adicionar** será habilitado. Clique no ícone para mostrar a janela **Adicionar disco virtual**.
- c. Clique no ícone **Remover** para Remover um disco virtual. Esse ícone não será mostrado se houver apenas um disco virtual. Quando você clicar no ícone **Remover**, a linha selecionada será excluída imediatamente. Não haverá nenhuma janela de confirmação porque o disco virtual não foi criado ainda.
- d. Clique em **Iniciar criação** para iniciar o processo.

**Nota:** Quando o controlador não for suportado, uma mensagem aparecerá.

## Exibindo e configurando o inventário de armazenamento

Use as informações neste tópico para exibir e configurar o inventário de armazenamento.

Na guia **Inventário de armazenamento**, você pode visualizar e configurar matrizes de disco, unidades virtuais associadas e unidades para o controlador RAID.

- **Para dispositivos de armazenamento que suportam a configuração do RAID:**

1. Se o controlador incluir matrizes de disco configuradas, isso exibirá as unidades instaladas com base na matriz de disco. O seguinte descreve os itens que aparecem na janela.
  - **Título da tabela:** mostra o ID da matriz de disco, o nível de RAID e o número total de unidades.
  - **Conteúdo da tabela:** lista propriedades básicas, como nome da unidade, estado da unidade, tipo, produto, fabricante, número de série e ações. Você pode acessar a página **Inventário** para exibir todas as propriedades que o XClarity Controller pode detectar.
  - **Ações:** o seguinte mostra os itens de ação que podem ser executados. Algumas ações não estarão disponíveis quando a unidade estiver em um estado diferente.
    - **Designar hot spare:** especifica a unidade como hot spare global ou uma hot spare dedicada.
    - **Remover hot spare:** remove a unidade da hot spare.
    - **Tornar a unidade de disco offline:** define a unidade como offline.
    - **Tornar a unidade de disco online:** define a unidade como online.
    - **Iniciar reconstrução:** reconstruir o RAID.
    - **Tornar a unidade de disco reutilizável:** define a unidade como reutilizável.
    - **Tornar a unidade de disco ausente:** define a unidade como ausente.
    - **Adequar unidade a JBOD:** adiciona a unidade à organização de disco JBOD.
    - **Adequar unidade não configurada:** disponibiliza a unidade para ser configurada em um arranjo ou para uso como hot spare de emergência.
    - **Inadequar unidade não configurada:** marca a unidade como defeituosa, impedindo sua utilização em uma matriz ou como uma hot spare de emergência.
    - **Tornar a unidade de disco como preparada para remoção:** define a unidade para remoção.
2. Se o controlador incluir unidades que ainda não foram configuradas, estas serão exibidas na tabela **Unidades de disco não RAID**. Clicando na opção **Converter JBOD em pronto para configurar**, uma janela será exibida mostrando todas as unidades que suportam esse item de ação. Você pode selecionar uma ou mais unidades para converter.

**Para dispositivos de armazenamento que não suportam a configuração do RAID:** o XClarity Controller não pode detectar as propriedades de algumas unidades.



---

## Capítulo 8. Atualizando o firmware de servidor

Para atualizar o firmware do servidor, use as informações neste tópico.

---

### Visão geral da atualização de firmware

Informações gerais sobre como atualizar o firmware do servidor.

Ao clicar em **Atualização de firmware** no painel esquerdo, é fornecida uma visão geral das informações de firmware.

- **Atualização do repositório:** sincroniza o firmware do servidor com o repositório CIFS/NFS remoto para atualização em lotes. Consulte "[Atualização do repositório](#)" na página 84.
- **Firmware do sistema:** visão geral do status do firmware do sistema, versão e atualização do firmware do sistema.

**Nota:** Clique em **Sincronização automática** para ativar ou desativar **Promoção automática do BMC primário para fazer o backup**. Quando essa configuração estiver habilitada, o firmware do banco de backup pendente será sincronizado do banco primário depois que o banco primário passar na medição ISM (Métrica de Estabilidade de Imagem).

- **Firmware do adaptador:** visão geral do firmware do adaptador instalado, status, versão e atualização de firmware do adaptador.
- **Firmware da unidade da fonte de alimentação:** visão geral da versão do firmware da unidade de fonte de alimentação e da atualização de firmware da PSU.
- **Firmware PSoc do backplane da unidade:** visão geral da versão do firmware do backplane. E para executar a atualização de firmware do sistema.

O status e as versões atuais de firmware para as unidades BMC, UEFI, LXPM, SO integrado, FPGA e adaptadores são exibidos, incluindo as versões primária e de backup do BMC. Há três categorias para o status de firmware:

- **Ativo:** O firmware está ativo.
- **Inativo:** O firmware não está ativo.
- **Reinicialização pendente:** a imagem de firmware foi atualizada e entrará em vigor depois que o servidor do BMC for reiniciado.
- **N/D:** nenhum firmware foi instalado para este componente.

#### Atenção:

- XCC e IMM devem ser atualizados para a versão mais recente antes de atualizar o UEFI. A atualização em ordem diferente pode resultar em comportamento incorreto.
- A instalação da atualização de firmware errada pode causar mau funcionamento do servidor. Antes de instalar um firmware ou atualizar o driver de dispositivo, leia qualquer leia-me e altere arquivos históricos que são fornecidos com a atualização transferida por download. Esses arquivos contêm informações importantes sobre a atualização e o procedimento para instalar a atualização, incluindo qualquer procedimento especial para atualização de um firmware inicial ou de uma versão do driver de dispositivo para a versão mais recente. Como o navegador da Web pode conter dados de cache do XCC, é recomendado recarregar a página da Web após o firmware do XCC ser atualizado.
- Com exceção do adaptador SATA M.2, os servidores do processador AMD não dão suporte à atualização de firmware do adaptador fora da banda.

- Algumas atualizações de firmware exigem a reinicialização do sistema, que executa ativação de firmware ou atualização interna. Esse processo na inicialização do sistema é chamado de "modo de manutenção do sistema", que não permite ações de energia do usuário temporariamente. O modo também é ativado durante a atualização de firmware. O usuário não deve desconectar a energia CA quando o sistema entrar no modo de manutenção.

---

## Atualização de firmware do sistema, adaptador e PSU

Etapas para atualizar o firmware do sistema, o firmware do adaptador e o firmware da PSU.

Para aplicar manualmente a atualização para o **Firmware do sistema**, **Firmware do adaptador** e o **Firmware da PSU**, conclua as etapas a seguir:

1. Clique em **Atualizar firmware** em cada recurso. A janela Atualizar Firmware do Servidor é aberta.
2. Clique em **Procurar...** para selecionar o arquivo de atualização de firmware que você deseja usar.
3. Navegue para o arquivo que você deseja selecionar e clique em **Abrir**. Você é retornado à janela Atualizar Firmware do Servidor com o arquivo selecionado exibido.
4. Clique em **Avançar** para começar a fazer upload e verificar o processo do arquivo selecionado. Um medidor de progresso será exibido enquanto o arquivo estiver sendo transferido por upload e verificado. É possível visualizar essa janela de status para verificar se o arquivo selecionado para atualização é o arquivo correto. Em **Firmware do sistema**, a janela de status terá informações sobre o tipo de arquivo de firmware que deve ser atualizado, como BMC, UEFI ou LXPM. Após o arquivo de firmware ser carregado e verificado com êxito, clique em **Próximo** para selecionar o dispositivo que você deseja atualizar.
5. Clique em **Atualizar** para iniciar a atualização do firmware. Um medidor de andamento mostra o andamento da atualização. Quando a atualização de firmware for concluída com sucesso, clique em **Concluir**. Se a atualização exigir que o XClarity Controller seja reiniciado para que tenha efeito, uma mensagem de aviso será exibida. Para obter detalhes sobre como reiniciar o XClarity Controller, consulte "[Ações de energia](#)" na [página 62](#).

---

## Atualização do repositório

Atualizar o firmware do servidor a partir de um repositório remoto

### Visão Geral

**Nota:** A funcionalidade CIFS/NFS/HTTPS/Onboard Firmware History requer a licença Premier do XCC.

O XCC introduziu a atualização de firmware em um servidor usando os Pacotes de atualização (Service Packs). Esse recurso simplifica o processo usando uma única ferramenta cliente de API ou Redfish para atualizar todo o firmware no sistema, incluindo pacotes de firmware OOB e IB. O processo envolve identificar pacotes de firmware aplicáveis, baixá-los e extraí-los de um servidor HTTP/HTTPS remoto ou fazer upload deles para o armazenamento interno do BMC por meio de um navegador da Web ou montá-los de um diretório compartilhado do CIFS ou NFS.

Os arquivos de metadados (formato JSON) precisam ser colocados no diretório raiz do sistema de arquivos compartilhado de rede se usar a montagem de CIFS ou NFS, com cargas de firmware especificadas nos metadados. O dispositivo microSD do servidor pode armazenar repositórios históricos, permitindo que os usuários recuperem os níveis de firmware.

Se os pacotes de firmware contiverem cargas que não suportam atualização de firmware fora da banda, o BMC iniciará o servidor e o configurará para ser inicializado a partir da imagem do SO integrada instalada no BMC antes de realizar a atualização.

## Pacote de atualização e metadados

O Pacote de atualização (Service Packs) é um arquivo compactado de um pacote de firmware. Ele contém um ou vários pacotes de firmware para os componentes em um sistema. O recurso Atualização do repositório do XCC consome o arquivo Pacote de atualização. O arquivo do pacote não compactado contém metadados e binários de carga. Arquivos de metadados JSON fornecem informações ao XCC sobre o tipo de imagens de firmware que o arquivo do pacote contém, e binários de carga fornecem as imagens de firmware.

## Repositório de firmware dentro do XCC

O Pacote de atualização pode conter vários pacotes de firmware, e o XCC reserva 2 GB de espaço em seu flash para novos recursos. Quando um novo pacote é recebido, o XCC limpa dados antigos. Algumas plataformas usam um cartão MicroSD para fornecer armazenamento adicional, e o XCC move o último Pacote atualizado para o repositório de histórico do cartão SD. O repositório de histórico de firmware pode armazenar até três pacotes, e os usuários podem usar o recurso Reversão de firmware para reverter para um pacote anterior.

### Notas:

- Se o Pacote de atualização incluir apenas o pacote de firmware OOB disponível para o sistema, o XCC não alterará o estado de energia do sistema. Para atualizar o firmware do dispositivo PCI, ele requer que o sistema seja ligado.
- Se o Pacote de atualização incluir o pacote de firmware IB disponível para o sistema, o XCC armazenará o estado de energia do sistema antes de atualizar e restaurar o estado de energia após o Pacote de atualização ser atualizado. Durante o processo de atualização, o XCC reinicializa o host no SO integrado.
- Se o Pacote de atualização incluir um nível de pré-requisito de firmware UEFI e a versão atual da UEFI instalada não atender a esse nível ou estiver atrás dele, o XCC desligará o sistema para executar uma atualização de firmware UEFI primeiro.
- Se o Pacote de atualização incluir um nível de pré-requisito de firmware do XCC e a versão atual do XCC instalada não atender a esse nível ou estiver atrás dele, o XCC será reinicializado primeiro após a atualização.

## Atualização com WebGUI

Com **Atualização do repositório**, o usuário pode configurar o XCC para sincronizar o firmware do servidor com um armazenamento interno. O repositório de firmware deve conter pacotes, incluindo arquivos binários e de metadados, ou JSON de metadados do Pacote de atualização e arquivos binários correspondentes. O XCC analisa os arquivos JSON de metadados para retirar os pacotes de firmware que dão suporte à atualização OOB para esse hardware do sistema específico e, em seguida, inicia uma atualização em lotes.

Para atualização do repositório, execute as etapas a seguir:

1. Ao usar o Armazenamento Interno, clique em **Importar Pacote de Firmware** e procure o pacote de firmware (formato .tgz ou zip).
2. Clique em **Atualizar sistema** para iniciar a atualização em lotes.
3. Clique em **Exibir detalhes** para ver o status de atualização.
  - **Marca de seleção verde**  : a atualização do firmware foi concluída com êxito.
  - **Marca X vermelha**  : a atualização do firmware falhou.
  - **Atualização**: o firmware está passando pelo processo de atualização.
  - **Cancelar**: a atualização do firmware foi cancelada.
  - **Aguardando**: o upgrade do firmware está aguardando para ser implantado.

**Nota:** Clicar em **Interromper atualização** cancelará as atualizações na fila após a atualização do pacote de instalação atual ser concluída.

4. Ao usar CIFS ou NFS, clique em **Desmontar** para desconectar do repositório remoto.
5. Se a atualização exigir que o XClarity Controller seja reiniciado para que tenha efeito, uma mensagem de aviso será exibida. Para obter detalhes sobre como reiniciar o XClarity Controller, consulte "[Ações de energia](#)" na página 62.

**Nota:** Se o sistema tiver um cartão MicroSD instalado, será possível ver o histórico de atualização do Pacote de atualização e selecionar o índice do Pacote de atualização para executar reversões de firmware. O processo é semelhante à atualização do repositório, exceto que o Pacote de atualização histórico é colocado dentro do MicroSD.

---

## Capítulo 9. Gerenciamento de licenças

O Gerenciamento de licenças do Lenovo XClarity Controller permite instalar e gerenciar recursos opcionais de gerenciamento do servidor e de sistemas.

Há vários níveis de funcionalidade e recursos do firmware do XClarity Controller disponíveis para seu servidor. O nível dos recursos do firmware instalados em seu servidor varia com base no tipo de hardware.

É possível atualizar a funcionalidade do XClarity Controller comprando e instalando uma chave de ativação.

Para solicitar uma chave de ativação, entre em contato com o representante de vendas ou o parceiro de negócios.

Use a interface da Web do XClarity Controller ou a CLI do XClarity Controller para instalar manualmente uma chave de ativação que permita usar um recurso opcional comprado. Antes de ativar uma chave:

- A chave de ativação deve estar no sistema que você está usando para fazer login no XClarity Controller.
- Você deve ter pedido a chave de licença e recebido seu código de autorização via correio ou e-mail.

Consulte "[Instalando uma chave de ativação](#)" na página 87, "[Removendo uma chave de ativação](#)" na página 87 ou "[Exportando uma chave de ativação](#)" na página 88 para obter informações sobre como gerenciar uma chave de ativação usando a interface da web do XClarity Controller. Consulte "[Comando keycfg](#)" na página 117 para obter informações sobre como gerenciar uma chave de ativação usando a CLI do XClarity Controller.

Para registrar um ID na administração da sua licença do XClarity Controller, clique no link a seguir: <https://fod.lenovo.com/lkms/angular/app/pages/index.htm#/welcome>

Informações adicionais sobre gerenciamento de licenças para servidores Lenovo estão disponíveis no seguinte site **Lenovo Press**:

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

---

### Instalando uma chave de ativação

Use as informações neste tópico para adicionar um recurso opcional ao seu servidor.

Para instalar uma chave de ativação, conclua as etapas a seguir:

- Etapa 1. Clique em **Licença** em **Configuração do BMC**.
- Etapa 2. Clique em **Atualizar Licença**.
- Etapa 3. Na janela **Adicionar uma nova licença**, clique em **Procurar**; em seguida, selecione o arquivo de chave de ativação para incluir na janela Upload de Arquivo e clique em **Abrir** para adicionar o arquivo. Para concluir a adição da chave, clique em **Importar** na janela Adicionar Chave de Ativação.

**Nota:** Se a chave de ativação não for válida, uma janela de erro será exibida.

---

### Removendo uma chave de ativação

Use as informações neste tópico para excluir um recurso opcional de seu servidor.

Para remover uma chave de ativação, conclua as etapas a seguir:

- Etapa 1. Clique em **Licença** em **Configuração do BMC**.
- Etapa 2. Selecione a chave de ativação a ser removida; em seguida, clique em **Excluir**.
- Etapa 3. Na janela Confirmar Exclusão de Chave de Ativação, clique em **OK** para confirmar a exclusão da chave de ativação. A chave de ativação selecionada será removida do servidor e não aparecerá mais na página Gerenciamento de licenças.

---

## Exportando uma chave de ativação

Use as informações neste tópico para exportar um recurso opcional de seu servidor.

Para exportar uma chave de ativação, conclua as etapas a seguir:

- Etapa 1. Clique em **Licença** em **Configuração do BMC**.
- Etapa 2. Na página Gerenciamento de Licenças, selecione a chave de ativação a ser exportada; em seguida, clique em **Exportar**.
- Etapa 3. Na janela **Exportar a licença selecionada**, clique em **Exportar** para confirmar a solicitação de exportação da chave de ativação.
- Etapa 4. Selecione o diretório para salvar o arquivo. A chave de ativação selecionada será exportada do servidor.

---

## Capítulo 10. Interface da linha de comandos

Use as informações neste tópico para inserir comandos que gerenciam e monitoram o XClarity Controller sem precisar usar a interface da Web do XClarity Controller.

Use a interface de linha de comando do XClarity Controller para acessar o XClarity Controller sem precisar usar a interface da Web. Ela fornece um subconjunto das funções de gerenciamento fornecidas pela interface da Web.

Você pode acessar a CLI por meio de uma **sessão SSH**. Você **deve** ser autenticado pelo XClarity Controller para poder emitir todos os comandos CLI.

---

### Acessando a interface da linha de comandos

Use as informações neste tópico para acessar a CLI.

Para acessar a CLI, inicie uma sessão SSH para o endereço IP do XClarity Controller (consulte "[Configurando o redirecionamento serial para SSH](#)" na página 89 para obter mais informações).

---

### Fazendo login na sessão de linha de comandos

Use as informações neste tópico para fazer login na sessão de linha de comandos.

Para efetuar login na linha de comandos, conclua as etapas a seguir:

- Etapa 1. Estabeleça uma conexão com o XClarity Controller.
- Etapa 2. No prompt de nome do usuário, digite o ID do usuário.
- Etapa 3. No prompt de senha, digite a senha que você usa para fazer login no XClarity Controller.

**Nota:** O prompt da linha de comandos é `system>`. A sessão de linha de comandos continua até que você digite `exit` na linha de comandos. Seu logoff é efetuado e a sessão é terminada.

---

### Configurando o redirecionamento serial para SSH

Este tópico fornece informações sobre como usar o XClarity Controller como um servidor de terminal serial.

O redirecionamento serial para SSH permite que um administrador do sistema use o XClarity Controller como um servidor de terminal serial. Uma porta serial do servidor pode ser acessada a partir de uma conexão SSH quando o redirecionamento serial é ativado.

**Nota:** O comando **console 1** da CLI é usado para iniciar uma sessão de redirecionamento serial com a porta COM.

#### Sessão de Exemplo

```
$ ssh USERID@10.240.1.12
Password:

system>
```

Todo o tráfego da sessão SSH é roteado para COM2.

ESC (

Digite a sequência de teclas de saída para retornar à CLI. Neste exemplo, pressione Esc e, em seguida, digite um parêntese esquerdo. O prompt da CLI é exibido para indicar o retorno à CLI do IMM.

system>

---

## Sintaxe do comando

Leia as diretrizes neste tópico para entender como inserir comandos na CLI.

Leia as seguintes diretrizes antes de usar os comandos:

- Cada comando tem o seguinte formato:  
`command [arguments] [-options]`
- A sintaxe de comando faz distinção entre maiúsculas e minúsculas.
- O nome do comando é todo em letras minúsculas.
- Todos os argumentos devem seguir imediatamente o comando. As opções seguem imediatamente os argumentos.
- Cada opção é sempre precedida por um hífen (-). Uma opção pode ser curta (uma única letra) ou longa (várias letras).
- Se uma opção tiver um argumento, ele será obrigatório, por exemplo:  
`ifconfig eth0 -i 192.168.70.34 -g 192.168.70.29 -s 255.255.255.0`  
Em que **ifconfig** é o comando, **eth0** é um argumento e -i, -g e -s são opções. Nesse exemplo, as três opções possuem argumentos.
- Os colchetes indicam que um argumento ou opção é opcional. Os colchetes não fazem parte do comando digitado.

---

## Recursos e limitações

Este tópico contém informações sobre recursos e limitações da CLI.

A CLI tem os seguintes recursos e limitações:

- São permitidas várias sessões de CLI simultâneas por SSH.
- É permitido um comando por linha (limite de 1024 caracteres, incluindo espaços).
- Não há caractere de continuação para comandos longos. A única função de edição é a tecla Backspace para apagar o caractere que você acabou de digitar.
- As teclas de Seta para Cima e Seta para Baixo podem ser usadas para percorrer os últimos oito comandos. O comando **history** exibe uma lista dos últimos oito comandos, que podem ser usados como um atalho para se executar um comando, como no seguinte exemplo:

```
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 >
```

- Na CLI, o limite de buffer de saída é 2 KB. Não há armazenamento em buffer. A saída de um comando individual não pode exceder 2048 caracteres. Esse limite não se aplica ao modo de redirecionamento serial (os dados são armazenados em buffer durante o redirecionamento serial).
- Mensagens de texto simples são usadas para indicar o status de execução do comando, como no exemplo a seguir:

```
system> power on
ok
system> power state
Power: On
State: System power off/State unknown
system>
```
- A sintaxe de comando faz distinção entre maiúsculas e minúsculas.
- Deve haver pelo menos um espaço entre uma opção e seu argumento. Por exemplo, `ifconfig eth0 -i192.168.70.133` é uma sintaxe incorreta. A sintaxe correta é `ifconfig eth0 -i 192.168.70.133`.
- Todos os comandos têm as opções `-h`, `-help` e `?`, que fornecem ajuda de sintaxe. Todos os exemplos a seguir produzirão o mesmo resultado:

```
system> power -h
system> power -help
system> power ?
```
- Alguns dos comandos descritos nas seções a seguir podem não estar disponíveis para a sua configuração do sistema. Para ver uma lista dos comandos suportados pela sua configuração, use a opção `help` ou `?`, como demonstrado nos exemplos abaixo:

```
system> help
system> ?
```

---

## Listagem alfabética de comandos

Este tópico contém uma lista de comandos CLI em ordem alfabética. Os links são fornecidos para tópicos de cada comando. Cada tópico de comando fornece informações sobre o comando, a função, a sintaxe e o uso.

A lista completa de todos os comandos CLI do XClarity Controller, em ordem alfabética, é a seguinte:

- ["Comando accseccfg" na página 105](#)
- ["Comando adapter" na página 151](#)
- ["Comando asu" na página 106](#)
- ["Comando backup" na página 109](#)
- ["Comando batch" na página 140](#)
- ["Comando clearlog" na página 94](#)
- ["Comando clock" na página 141](#)
- ["Comando dbgshbmc" na página 152](#)
- ["Comando dhcpinfo" na página 110](#)
- ["Comando dns" na página 110](#)
- ["Comando encaps" na página 111](#)
- ["Comando ethtousb" na página 112](#)

- "Comando exit" na página 93
- "Comando fans" na página 94
- "Comando firewall" na página 112
- "Comando fuelg" na página 104
- "Comando hashpw" na página 114
- "Comando help" na página 93
- "Comando history" na página 93
- "Comando ifconfig" na página 115
- "Comando info" na página 142
- "Comando keycfg" na página 117
- "Comando ldap" na página 117
- "Comando led" na página 95
- "Comando mhlog" na página 94
- "Comando ntp" na página 119
- "Comando portcontrol" na página 120
- "Comando ports" na página 121
- "Comando power" na página 102
- "Comando pxeboot" na página 105
- "Comando rdmount" na página 121
- "Comando readlog" na página 97
- "Comando reset" na página 103
- "Comando restore" na página 122
- "Comando roles" na página 123
- "Comando rtd" na página 123
- "Comando seccfg" na página 124
- "Comando securityinfo" na página 124
- "Comando securitymode" na página 125
- "Comando servicelog" na página 98
- "Comando snmp" na página 126
- "Comando snmpalerts" na página 128
- "Comando spreset" na página 142
- "Comando sshcfg" na página 129
- "Comando sslcfg" na página 130
- "Comando storage" na página 143
- "Comando syshealth" na página 99
- "Comando syslock" na página 132
- "Comando temps" na página 100
- "Comando thermal" na página 133
- "Comando tls" na página 134
- "Comando trespass" na página 135
- "Comando uefipw" na página 135

- ["Comando usbeth" na página 136](#)
- ["Comando users" na página 136](#)
- ["Comando volts" na página 101](#)
- ["Comando vpd" na página 101](#)

---

## Comandos de utilitário

Este tópico fornece uma lista alfabética de comandos CLI de utilitários.

Atualmente, há 3 comandos de utilitário:

### Comando exit

Use esse comando para fazer logoff na sessão da CLI,

Use o comando **exit** para efetuar logoff e terminar a sessão da CLI.

### Comando help

Esse comando exibe uma lista de todos os comandos.

Use o comando **help** para exibir uma lista de todos os comandos com uma descrição curta de cada um. Você também pode digitar ? no prompt de comando.

### Comando history

Esse comando fornece uma lista de comandos emitidos anteriormente.

Use o comando **history** para exibir uma lista de históricos indexada dos últimos oito comandos emitidos. Os índices podem ser utilizados como atalhos (precedidos por!) para emitir novamente os comandos dessa lista histórica.

Exemplo:

```
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>
```

---

## Comandos do monitor

Este tópico fornece uma lista alfabética de comandos de CLI do monitor.

Atualmente, há 11 comandos de monitor:

## Comando clearlog

Este comando é usado para limpar o log de eventos do IMM.

Use o comando **clearlog** para limpar o log de eventos do IMM. Para usar esse comando, você deve ter a autoridade para limpar logs de eventos.

**Nota:** Este comando destina-se apenas para uso pela equipe de suporte.

Sintaxe:

```
clearlog [-options]
```

Tabela 4. Opções clearlog

Opção	Descrição	Valores
-t	Tipo de evento, escolha o tipo de evento a ser limpo. Se não for especificado, todos os tipos de evento serão selecionados.	all, platform, audit <ul style="list-style-type: none"><li>• Todos: todos os tipo de evento, incluindo eventos de plataforma e eventos de auditoria.</li><li>• plataforma: tipo de evento de plataforma.</li><li>• auditoria: tipo de evento de auditoria.</li></ul>

Exemplo:

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

## Comando fans

Esse comando é usado para exibir a velocidade dos ventiladores do servidor.

Use o comando **fans** para exibir a velocidade de cada um dos ventiladores do servidor.

Exemplo:

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

## Comando mhlog

Use esse comando para exibir as entradas do log de atividade do histórico de manutenção.

Sintaxe:  
mhlog [-options]

Tabela 5. Opções mhlog

Opção	Descrição	Valores
-c	Exibir entradas count	Entre 1 e 250
-i	Exibir entradas que começam no índice	Entre 1 e 250
-f	Nome de arquivo remoto do arquivo de log	Nome de arquivo válido para nome de arquivo do arquivo de log
-ip	Endereço do servidor tftp/sftp	Endereço IP válido para o servidor TFTP/SFTP
-pn	Número da porta do servidor tftp/sftp	Número da porta válido para o servidor TFTP/SFTP (padrão 69/22)
-u	Nome de usuário para o servidor sftp	Nome de usuário válido para o servidor SFTP
-pw	Senha para o servidor sftp	Senha válida para o servidor SFTP

Exemplo:

```
system> mhlog
```

```
Type                Message                                     Time
-----
Hardware            SAS Backplane1(SN: XXXX9CE009L) is added.    05/08/2020,04:23:18
Hardware            CPU 1(SKU NO: 50844440) is added.            05/08/2020,04:23:22
Hardware            CPU 2(SKU NO: 50844440) is added.            05/08/2020,04:23:22
Hardware            M2 Card(SN: R1SH9AJ0037) is added.          05/08/2020,04:23:22
Firmware            Primary XCC firmware is updated to TGBT99T by XCC Web. 05/08/2020,06:40:37
Firmware            Primary XCC firmware is activated to TGBT99T. 05/08/2020,06:41:26
Hardware            PSU1(SN: D1D694C0075) is added.            05/08/2020,06:43:28
system>
```

## Comando led

Use esse comando para exibir e configurar estados de LED.

O comando **led** exibe e define os estados de LED do servidor.

- A execução do comando **led** sem opções exibe o status dos LEDs do painel frontal.
- A opção de comando **led -d** deve ser usada com a opção de comando **led -identify on**.

A tabela a seguir mostra os argumentos das opções.

Sintaxe:

```
led [-options]
```

Tabela 6. Opções led

Opção	Descrição	Valores
-l	Obtenha o status de todos os LEDs no sistema e seus subcomponentes	
-identify	Alterar o estado do LED de identificação de gabinete	off, on, blink
-d	Ativar o LED de identificação para o período de tempo especificado	Período de tempo (segundos)

Exemplo:

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

Esse comando exibe os logs de eventos do IMM.

Use o comando **readlog** para exibir as entradas de log de eventos do IMM. Cinco logs de eventos são exibidos por vez. As entradas são exibidas da mais recente para a mais antiga.

### Notas:

- R - inválido
- I - informação
- W - advertência
- E - crítico

### Sintaxe:

```
readlog [-options]
```

Tabela 7. Opções readlog

Opção	Descrição	Valores
-a	Exibe todas as entradas no log de eventos, começando com as mais recentes.	
-f	Redefine o contador e exibe as 5 primeiras entradas no log de eventos, começando com as mais recentes.	
-date	Exibe entradas de log de eventos para a data especificada	Use o seguinte formato: mm/dd/aaaa
-sev	Exibe entradas de log de eventos para o nível de gravidade especificado.	R, I, W, E
-i	Define o endereço IP IPv4 ou IPv6 do servidor TFTP ou SFTP onde o log de eventos é salvo. As opções de comando <b>-i</b> e <b>-I</b> são usadas juntas para especificar o local.	Endereço IP válido
-l	Define o nome do arquivo de log de eventos. As opções de comando <b>-i</b> e <b>-l</b> são usadas juntas para especificar o local.	Nome do arquivo válido
-pn	Exibe ou define o número da porta do servidor TFTP ou SFTP.	Número da porta válido (padrão 69/22)
-u	Especifica o nome de usuário para o servidor SFTP.	Nome de usuário válido
-pw	Especifica a senha para o servidor SFTP.	Senha válida
-di	Capacidade estendida de log de auditoria	none, ipmi

### Exemplo:

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

## Comando servicelog

Esse comando é usado para gerar um novo arquivo de dados de serviço.

**Nota:** Esse comando costumava ser o comando **ffdc**.

Use o comando **servicelog** para gerar e transferir dados de serviço para o Suporte.

A lista a seguir consiste em comandos a serem usados com o comando **servicelog**:

A tabela a seguir mostra os argumentos das opções.

### Sintaxe:

```
servicelog [subset_command] [-options]
```

Tabela 8. Comandos do subconjunto servicelog

Opção	Descrição
generate	Criar um novo arquivo de dados de serviço
status	Verificar o status do arquivo de dados de serviço
copy	Copiar dados de serviço existentes
delete	Excluir dados de serviço existentes

Tabela 9. Opções servicelog

Opção	Descrição	Valores
-t	Tipo de log de serviço	1, 2, 3 <ul style="list-style-type: none"><li>1: log de depuração (FFDC, padrão)</li><li>2: log de dados de serviço</li><li>3: log de depuração acoplado do log de dados de serviço, que só é válido ao copiar arquivos de log</li></ul>
<b>Opções adicionais do comando generate</b>		

Tabela 9. Opções servicelog (continuação)

Opção	Descrição	Valores
-c	Seleção de categoria de dados de despejo. A categoria de dados não estará contida se não for especificada com essa opção.	<ul style="list-style-type: none"> <li>Para o tipo 1 (ffdc): corefile</li> <li>Para o tipo 2 (log de dados de serviço): rede, auditoria, telemetria, osscreen</li> </ul>
<b>Opções adicionais dos comandos generate e copy</b>		
-f	Nome do arquivo remoto ou diretório de destino sftp.	Para sftp, use caminho completo ou / à direita no nome do diretório (~/ ou /tmp/). O valor padrão é o nome gerado pelo sistema.
-ip	Endereço do servidor tftp/sftp.	Endereço IP válido
-pn	Número da porta do servidor tftp/sftp.	Número da porta válido (padrão 69/22)
-u	Nome de usuário para o servidor sftp.	Nome de usuário válido
-pw	Senha para o servidor sftp.	Senha válida
-timeout	Minutos para permitir a cópia em primeiro plano.	Entre 1 e 5 (padrão 1)

**Exemplo:**

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

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

## Comando syshealth

Esse comando fornece um resumo dos eventos ativos ou de integridade.

Use o comando **syshealth** para exibir um resumo do funcionamento ou dos eventos ativos do servidor. O estado de energia, o estado do sistema, o estado de hardware (inclui ventilador, fonte de alimentação, armazenamento, processador, memória), a contagem de reinicializações e o status de software do IMM são exibidos.

Sintaxe:  
syshealth [arguments]

Tabela 10. Argumentos syshealth

Argumentos	Descrição
summary	Exiba o resumo do funcionamento do sistema.
activeevents	Exiba eventos ativos.
cooling	Exiba o status de funcionamento dos dispositivos de resfriamento.
power	Exiba o status de funcionamento dos módulos de energia.
storage	Exiba o status de funcionamento do armazenamento local.
processors	Exiba o status de funcionamento dos processadores.
memory	Exiba o status de funcionamento da memória.

Exemplo:  
system> syshealth summary  
Power On  
State OS booted  
Restarts 29

system> syshealth activeevents  
No Active Event Available!

## Comando temps

Esse comando exibe todas as informações de temperatura e limites de temperatura.

Use o comando **temps** para exibir todas as temperaturas e limites de temperatura. O mesmo conjunto de temperaturas é exibido como na interface da Web.

Sintaxe:  
temps

Exemplo:  
system> temps  
Temperatures are displayed in degrees Fahrenheit/Celsius

	WR	W	T	SS	HS
Ambient Temp	109.40/43	N/A	78.80/26.00	109.40/43.00	122.00/50.00
Exhaust Temp	N/A	N/A	32.00/0.00	116.60/47.00	N/A

system>

### Notas:

1. A saída tem os seguintes títulos de colunas:  
WR: redefinição de aviso (valor Positivo indo para histerese do limite)  
W: aviso (Limite superior não crítico)  
T: temperatura (valor atual)

SS: encerramento temporário (limite crítico superior)

HS: encerramento forçado (limite superior não recuperável)

2. Todos os valores de temperatura estão em graus Fahrenheit/Celsius.
3. N/A representa não aplicável.

## Comando volts

Use esse comando para exibir as informações de voltagem do servidor.

Use o comando **volts** para exibir todas as voltagens e limites de voltagem. O mesmo conjunto de voltagens é exibido como na interface da Web.

Sintaxe:

```
volts
```

Exemplo:

```
system> volts
-----
          HSL  SSL  WL   WRL  V   WRH  WH   SSH  HSH
-----
CMOS Battery N/A  2.25  2.39  0.03  3.12  0.03  N/A  N/A  N/A
system>
```

**Nota:** A saída tem os seguintes títulos de colunas:

HSL: encerramento permanente baixo (limite inferior não recuperável)

SSL: encerramento temporário baixo (limite crítico inferior)

WL: aviso baixo (limite inferior não crítico)

WRL: redefinição de aviso baixo (valor negativo indo para histerese do limite)

V: voltagem (valor atual)

WRH: redefinição de aviso alto (valor Positivo indo para histerese do limite)

WH: aviso alto (limite superior não crítico)

SSH: encerramento temporário alto (limite crítico superior)

HSH: encerramento permanente alto (limite superior não recuperável)

## Comando vpd

Esse comando exibe a configuração e dados informativos (dados vitais do produto) associados ao hardware e ao software do servidor.

Use o comando **vpd** para exibir dados vitais do produto para o sistema (sys), IMM (bmc), BIOS do servidor (uefi), Lenovo XClarity Provisioning Manager (lxpm), firmware do servidor (fw), componentes do servidor (comp) e dispositivos PCIe (pcie). As mesmas informações são exibidas como na interface da Web.

Sintaxe:

```
vpd [arguments]
```

Tabela 11. Argumentos vpd

Argumentos	Descrição
vpd sys	Exibe Dados Vitais do Produto para o sistema.
vpd bmc	Exibe Dados Vitais do Produto para o controlador de gerenciamento.

Tabela 11. Argumentos vpd (continuação)

Argumentos	Descrição
vpd uefi	Exibe Dados Vitais do Produto para o BIOS do sistema.
vpd lxpm	Exibe Dados Vitais do Produto para o LXPM do sistema.
vpd fw	Exibe Dados Vitais do Produto para o firmware do sistema.
vpd comp	Exibe Dados Vitais do Produto para componentes do sistema.
vpd pcie	Exibe Dados Vitais do Produto para dispositivos PCIe.

Exemplo:

```
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>
```

## Comandos de controle de energia e reinicialização do servidor

Este tópico fornece uma lista alfabética de comandos de CLI de energia e reinicialização.

Atualmente, há 4 comandos de energia e reinicialização do servidor:

### Comando power

Este comando descreve como controlar a energia do servidor.

Use o comando **power** para controlar a energia do sistema. Para emitir comandos **power**, você deve ter o nível de autoridade Acesso a Energia/Reinicialização do Servidor Remoto.

Sintaxe:

```
power on [-options]
power off [-options]
power cycle [-options]
power uefi
power state
```

Tabela 12. comandos power

Comando	Descrição
power on	Use este comando para ligar a energia do servidor.
power off	Use este comando para desligar o servidor.
power cycle	Use este comando para desligar o servidor e, em seguida, ligá-lo novamente.
power uefi	Use este comando para inicializar na Configuração F1 da UEFI.
power state	Use este comando para exibir o estado de energia do servidor e o estado atual do servidor.

Tabela 13. opções de energia

Opção	Descrição	Valores
-s	Use esta opção para encerrar o sistema operacional antes de desligar o servidor. <b>Nota:</b> A opção <b>-s</b> é indicada ao usar a opção <b>-every</b> para o <b>power off</b> e <b>power cycle</b> .	
-every	Use esta opção com os comandos <b>power on</b> , <b>power off</b> e <b>power cycle</b> para controlar a energia do servidor. É possível configurar datas, horários e frequência (diária ou semanal) para ligar, desligar o servidor ou executar um ciclo de ativação.	Dom, Seg, Ter, Qua, Qui, Sex, Sáb, Dia, claro
-t	Use esta opção para especificar o tempo, em horas e minutos, para ligar o servidor, encerrar o sistema operacional e desligar ou reiniciar o servidor.	Use o formato a seguir: hh:mm
-d	Use esta opção para especificar a data para ligar o servidor. Essa é uma opção adicional para o comando <b>power on</b> . <b>Nota:</b> As opções <b>-d</b> e <b>-every</b> não podem ser usadas juntas no mesmo comando.	Use o seguinte formato: mm/dd/aaaa
-clear	Use esta opção para limpar a data de ativação planejada. Essa é uma opção adicional para o comando <b>power on</b> .	

As informações a seguir são exemplos do comando **power**.

Para encerrar o sistema operacional e desligar o servidor todo domingo, às 1:30, insira o seguinte comando:  
system> power off -every Sun -t 01:30

Para encerrar o sistema operacional e reiniciar o servidor todo dia, às 1:30, insira o seguinte comando:  
system> power cycle -every Day -t 01:30

Para ligar o servidor toda segunda-feira às 1:30, insira o seguinte comando:  
system> power on -every Mon -t 1:30

Para ligar o servidor em 31/12/2013, às 23:30, insira o seguinte comando:  
system> power on -d 12/31/2013 -t 23:30

Para limpar um ciclo de ativação semanal, insira o seguinte comando:  
system> power cycle -every clear

## Comando reset

Este comando descreve como redefinir o servidor.

Use o comando **reset** para reiniciar o servidor. Para usar esse comando, você deve ter autoridade de acesso de energia e reinicialização.

Sintaxe:  
reset [-options]

Tabela 14. opções options

Opção	Descrição	Valores
-s	Desligue o sistema operacional antes do servidor ser reconfigurado.	
-d	Atraso na execução da redefinição para o número especificado de segundos.	0 - 120
-nmi	Gere um Non-Maskable Interrupt (NMI) no servidor.	

## Comando fuelg

Esse comando exibe informações sobre a energia do servidor.

Use o comando **fuelg** para exibir informações sobre o uso de energia do servidor e configure o gerenciamento de energia do servidor. Este comando também configura políticas para perda de redundância de energia.

Sintaxe:

fuelg [-options]

Tabela 15. Opções fuelg

Opção	Descrição	Valores
-pme	Habilite ou desabilite o gerenciamento de energia e o limite no servidor.	on, off
-pcapmode	Defina o modo de limite de energia para o servidor.	saída, entrada
-pcap	Um valor numérico que está no intervalo de valores máximos de energia exibido ao executar o comando fuelg no destino, sem quaisquer opções.	valor numérico da potência
-history	Exibe o consumo de energia ou o histórico de desempenho.	pc, perf
-period	Um valor numérico para exibir o histórico.	1, 6, 12, 24 horas
-pm	Defina o modo de política para perda de energia redundante.	<ul style="list-style-type: none"> <li>• <b>bt</b> - básico com limitação</li> <li>• <b>rt</b>- redundante com regulagem (padrão)</li> </ul>
-zm	Habilite ou desabilite o modo de saída zero. Essa configuração só pode ser definida quando o modo de política é definido como redundante com regulagem.	on, off

Tabela 15. Opções fuelg (continuação)

Opção	Descrição	Valores
-perf	Exibe a utilização de computação atual, incluindo sistema, processador, módulo de memória e E/S.	
-pc	Exibir consumo de energia atual	<ul style="list-style-type: none"> <li>• <b>saída</b> – Exibe a saída atual de consumo de energia do sistema, processador, módulo de memória e outros componentes.</li> <li>• <b>entrada</b> – exibe o consumo de energia de entrada atual, incluindo o consumo de energia do sistema.</li> </ul> <p><b>Nota:</b> Nos servidores AMD, a saída atual do consumo de energia não exibirá alguns dos componentes.</p>

## Comando pxeboot

Esse comando exibe e define a condição do Ambiente de Execução de Pré-inicialização.

Sintaxe:

pxeboot [-options]

Tabela 16. Opções pxeboot

Opção	Descrição	Valores
-en	Define a condição do Ambiente de Execução de Pré-inicialização para a próxima reinicialização do sistema.	habilitado, desabilitado

## Comandos de configuração

Este tópico fornece uma lista alfabética de comandos CLI de configuração.

Atualmente, há 41 comandos de configuração:

### Comando accsecfg

Use esse comando para exibir e definir configurações de segurança de conta.

Sintaxe:

accsecfg [-options]

Tabela 17. Opções accsecfg

Opção	Descrição	Valores
-am	Define o método de autenticação do usuário.	local, ldap, localldap, ldaplocal
-lp	Período de bloqueio após número máximo de falhas de login (minutos).	Entre 0 e 2880, 0 = período de bloqueio não expira

Tabela 17. Opções `accseccfg` (continuação)

Opção	Descrição	Valores
-pe	Período de tempo de expiração de senha (dias).	Entre 0 e 365, 0 = nunca expirará
-pew	Período de aviso de expiração da senha <b>Nota:</b> O período de aviso de expiração de senha deve ser menor que o período de expiração de senha.	Entre 0 e 30, 0 = nunca avisar
-pc	Regras de complexidade de senha habilitadas.	on, off
-pl	Comprimento da senha.	Se as regras de complexidade de senha estiverem habilitadas, o tamanho da senha estará entre 8 e 32. Caso contrário, ele estará entre 0 e 32.
-ci	Intervalo mínimo de alteração de senha (horas).	entre 0 e 240, 0 = alterar imediatamente
-lf	Número máximo de falhas de login.	Entre 0 e 10, 0 = nunca bloqueado
-chgnew	Alterar nova senha de usuário após primeiro login.	on, off
-rc	Ciclo de reutilização de senha.	Entre 0 e 10, 0 = reutilizar imediatamente
-wt	Tempo limite de inatividade da sessão da Web e Secure Shell (minutos).	Entre 0 e 1440

**Exemplo:**

```
system> accseccfg
-am: local
-lp: 60
-pe: none
-pew: 0
-pc: on
-pl: 10
-ci: 0
-lf: 5
-chgnew: on
-rc: 5
-wt: 20
system>
```

## Comando `asu`

Esse comando é usado para definir as configurações UEFI.

Os comandos do Utilitário de Configurações Avançadas (ASU) são usados para definir as configurações UEFI. O sistema host deve ser reinicializado para que quaisquer mudanças de configurações de UEFI entrem em vigor.

**Sintaxe:**

```
asu [subset_command]
```

Tabela 18. Comandos do subconjunto asu

Comando	Descrição	Valor
help	Use esse comando para exibir informações da ajuda para uma ou mais configurações.	<b>setting_name</b>
set	Use esse comando para alterar o valor de uma configuração. Configure a definição de UEFI para o valor de entrada. <b>Notas:</b> <ul style="list-style-type: none"> <li>• Configure um ou mais pares de configuração/valor.</li> <li>• A configuração poderá conter curingas se ela expandir para uma configuração única.</li> <li>• O valor deverá ser colocado entre aspas se ele contiver espaços.</li> <li>• Os valores de lista ordenada são separados pelo símbolo de igual (=). Por exemplo, configure B*. Bootorder "CD/DVD Rom=Hard Disk 0=PXE Network."</li> </ul>	<b>setting_name=valor</b>
show	Use esse comando para exibir o valor atual de uma ou mais configurações.	<b>setting_name</b>
showvalues	Use esse comando para exibir todos os valores possíveis para uma ou mais configurações. <b>Notas:</b> <ul style="list-style-type: none"> <li>• Esse comando exibirá informações sobre os valores permitidos para a configuração.</li> <li>• Os números mínimo e máximo de instâncias permitidos para a configuração são exibidos.</li> <li>• O valor padrão será exibido se disponível.</li> <li>• O valor padrão é colocado entre os sinais de maior e menor (&lt; e &gt;).</li> <li>• Os valores de texto mostram os comprimentos mínimo e máximo e a expressão regular.</li> </ul>	<b>setting_name</b>
showgroups	Use esse comando para exibir os grupos de configuração disponíveis. Esse comando exibe os nomes de grupos conhecidos. Os nomes dos grupos podem variar dependendo dos dispositivos instalados.	
<b>Notas:</b> <ul style="list-style-type: none"> <li>• Na sintaxe de comando, <b>setting_name</b> é o nome de uma configuração que você deseja visualizar ou alterar e <b>value</b> é o valor que está colocando na configuração.</li> <li>• <b>setting_name</b> pode ser mais que um nome, exceto ao usar o comando <b>set</b>.</li> <li>• <b>setting_name</b> pode conter caracteres curinga, por exemplo, um asterisco (*) ou um ponto de interrogação (?).</li> <li>• <b>setting_name</b> pode ser um grupo, um nome de configuração ou <b>tudo</b>.</li> </ul>		

Exemplos:

- Para exibir todas as opções de comando asu, insira asu help.
- Para exibir a ajuda para um comando, insira asu help setting\_name.
- Para alterar um valor, insira asu set setting\_name=value.
- Para exibir o valor atual, insira asu show setting\_name.

- Para exibir todos os valores possíveis para uma configuração, insira `asu showvalues setting_name`.  
Exemplo de comando `show values`:  

```
system> asu showvalues S*.POST*
SystemRecovery.POSTWatchdogTimer==<Disable>=Enable
SystemRecovery.POSTWatchdogTimerValue=numeric min=5 max=20 step=1 default=5
system>
```
- Para exibir os grupos de configurações disponíveis, insira `asu showgroups`.

A tabela a seguir mostra os argumentos das opções.

Tabela 19. Opções `asu`

A tabela a seguir é uma tabela de três colunas e várias linhas que consiste nas opções, descrições das opções e os valores associados das opções.

Opção	Descrição	Valores
-b	Exibir no formato de lote.	
-help <sup>1</sup>	Exibir uso e opções do comando. O ícone -help é colocado antes do comando, por exemplo, <b>asu -help show</b> .	
-l	Nome de configuração de formato longo (incluir o conjunto de configuração).	
-m	Nome de configuração de formato combinado (usar o ID de configuração).	
-v <sup>2</sup>	Saída detalhada.	
1. A opção -help pode ser usada com qualquer comando. 2. A opção -v é usada apenas entre <b>asu</b> e o comando.		

Sintaxe:

`asu [-options] command [cmdopts]`

options:

- v verbose output
- help display main help

cmdopts:

- help help for the command

**Nota:** Consulte comandos individuais para mais opções de comando.

Use os comandos de transação `asu` para configurar várias definições de UEFI e criar e executar comandos no modo em lote. Use os comandos **tropen** e **trset** para criar um arquivo de transação que contenha várias configurações para serem aplicadas. Uma transação com um ID fornecido é aberta usando o comando **tropen**. As configurações são incluídas no conjunto usando o comando **trset**. A transação concluída é confirmada usando o comando **trcommit**. Quando a transação for concluída, ela poderá ser excluída com o comando **trrm**.

**Nota:** A operação de restauração de configurações de UEFI criará uma transação com um ID usando um número aleatório de três dígitos.

A tabela a seguir contém comandos de transação que podem ser usados com o comando **asu**.

Tabela 20. Comandos de transação asu

A tabela a seguir é uma tabela de três colunas e várias linhas que consiste nos comandos de transação, nas descrições de comandos e nos valores associados dos comandos.

Comando	Descrição	Valor
tropen id	Esse comando cria um novo arquivo de transação contendo várias definições a serem configuradas.	Id é a sequência de identificação, 1 a 3 caracteres alfanuméricos.
trset id	Esse comando inclui uma ou mais configurações ou pares de valores em uma transação.	Id é a sequência de identificação, 1 a 3 caracteres alfanuméricos.
trlist id	Esse comando exibe o conteúdo do arquivo de transação primeiro. Isso pode ser útil quando o arquivo de transação é criado no shell da CLI.	Id é a sequência de identificação, 1 a 3 caracteres alfanuméricos.
trcommit id	Esse comando confirma e executa o conteúdo do arquivo de transação. Os resultados da execução e quaisquer erros serão exibidos.	Id é a sequência de identificação, 1 a 3 caracteres alfanuméricos.
trrm id	Esse comando remove o arquivo de transação após ele ter sido confirmado.	Id é a sequência de identificação, 1 a 3 caracteres alfanuméricos.

Exemplo de estabelecer várias configurações de UEFI:

```
asu tropen TR1
asu trset TR1 UEFI.BootModes.SystemBootMode "UEFI and Legacy"
asu trset TR1 BootOrder.BootOrder "CD/DVD Rom=Hard Disk 0=PXE Network"
asu trset TR1 BootOrder.WolBootOrder "CD/DVD Rom=Hard Disk 0=PXE Network"
asu trset TR1 UEFI.DevicesandIOPorts.Com1BaudRate 115200
asu trset TR1 UEFI.DevicesandIOPorts.Com1DataBits 8
asu trset TR1 UEFI.DevicesandIOPorts.Com1FlowControl Disable
asu trset TR1 UEFI.DevicesandIOPorts.Com1Parity None
asu trset TR1 UEFI.DevicesandIOPorts.Com1StopBits 1
asu trset TR1 UEFI.DevicesandIOPorts.COMPort1 Enable
asu trcommit TR1
```

## Comando backup

Use esse comando para criar um arquivo de backup que contenha as configurações de segurança do sistema atuais.

Sintaxe:

```
backup [-options]
```

Tabela 21. Opções backup

Opção	Descrição	Valores
-f	Nome do arquivo de backup	Nome do arquivo válido
-pp	Senha ou frase delimitada por aspas usada para criptografar as senhas no arquivo de backup	Senha ou passphrase delimitada por aspas válida
-ip	Endereço IP do servidor TFTP/SFTP	Endereço IP válido
-pn	Número da porta do servidor TFTP/SFTP	Número da porta válido (padrão 69/22)
-u	Nome de usuário para o servidor SFTP	Nome de usuário válido
-pw	Senha para o servidor SFTP	Senha válida
-fd	Nome do arquivo para descrição XML de comandos CLI de backup	Nome do arquivo válido

Exemplo:

```
system> backup -f xcc-back.cli -pp xxxxxx -ip 192.168.70.200
ok
system>
```

## Comando dhcpinfo

Use esse comando para exibir a configuração de IP atribuída ao servidor DHCP para eth0.

Use o comando **dhcpinfo** para visualizar a configuração de IP designada pelo servidor DHCP para eth0, se a interface for configurada automaticamente por um servidor DHCP. É possível usar o comando **ifconfig** para ativar ou desativar o DHCP.

Sintaxe:

```
dhcpinfo [ethernet_number]
```

Exemplo:

```
dhcpinfo eth1
```

A tabela a seguir descreve a saída do exemplo.

Tabela 22. Saída dhcpinfo

Campo	Descrição
-server	Servidor DHCP que designou a configuração
-n	Nome do host designado
-i	Endereço IPv4 designado
-i6	Endereço IPv6 designado
-g	Endereço de gateway designado
-s	Máscara de sub-rede designada
-d	Nome de domínio IPv4 designado
-d6	Nome de domínio IPv6 designado
-dns1	Endereço IP do servidor DNS IPv4 primário
-dns2	Endereço IP do servidor DNS IPv4 secundário
-dns3	Endereço IP do servidor DNS IPv4 terciário
-i6	Endereço IPv6
-d6	Nome de domínio IPv6
-dns61	Endereço IP do servidor DNS IPv6 primário
-dns62	Endereço IP do servidor DNS IPv6 secundário
-dns63	Endereço IP do servidor DNS IPv6 terciário

## Comando dns

Use este comando para visualizar e definir a configuração DNS do IMM.

Sintaxe:

```
dns [-options]
```

Tabela 23. Opções dns

Opção	Descrição	Valores
-state	Estado do DNS	on, off
-i1	Endereço IP do servidor DNS IPv4 primário	Endereço IP no formato de endereço IP decimal pontuado.
-i2	Endereço IP do servidor DNS IPv4 secundário	Endereço IP no formato de endereço IP decimal pontuado.
-i3	Endereço IP do servidor DNS IPv4 terciário	Endereço IP no formato de endereço IP decimal pontuado.
-i61	Endereço IP do servidor DNS IPv6 primário	Endereço IP no formato IPv6.
-i62	Endereço IP do servidor DNS IPv6 secundário	Endereço IP no formato IPv6.
-i63	Endereço IP do servidor DNS IPv6 terciário	Endereço IP no formato IPv6.
-ddns	Estado do DDNS	habilitado, desabilitado
-dnsrc	Nome de domínio DDNS preferencial	DHCP, Manual
-ddn	DDN especificado manualmente	
-ddncur	DDN atual (somente leitura)	
-p	Servidores DNS preferenciais (ipv4 ou ipv6)	ipv4, ipv6
-dscvry	descoberta de endereços do LXCA	habilitado, desabilitado
-dsclist	Lista LXCA de DNS SRV	
-dscxm	Configurar o XClarity Manager	

O exemplo a seguir mostra uma configuração do IMM em que o DNS está desabilitado:

```
system> dns
  -state   : disabled
  -i1      : 0.0.0.0
  -i2      : 0.0.0.0
  -i3      : 0.0.0.0
  -i61     : ::
  -i62     : ::
  -i63     : ::
  -ddns    : enabled
  -dnsrc   : DHCP
  -ddn     :
  -ddncur  : labs.lenovo.com
  -p       : ipv6
  -dscvry  : enabled
system>
```

## Comando encaps

Use este comando para deixar o BMC sair do modo de encapsulamento.

Sintaxe:

```
encaps [arguments]
```

Tabela 24. Argumentos encaps

Argumentos	Descrição
lite off	Deixar o BMC sair do modo de encapsulamento e abrir o acesso global a todos os usuários

## Comando ethtousb

Use o comando **ethtousb** para exibir e configurar o mapeamento de portas Ethernet para Ethernet-sobre-USB.

O comando permite mapear um número de porta Ethernet externa para um número de porta diferente para Ethernet-sobre-USB.

Sintaxe:

ethtousb [-options]

Tabela 25. Comando ethtousb

Opção	Descrição	Valores
-en	Estado de Ethernet sobre USB.	habilitado, desabilitado <b>Nota:</b> Ativar interface Ethernet sobre USB via <b>&lt;usbeth&gt;</b> para tornar o mapeamento de porta eficaz.
-m[x] <b>port1:port2</b>	Configurar mapeamento de portas para índice <b>x</b> .	Onde: <ul style="list-style-type: none"> <li>O número de índice de porta, <b>x</b>, é especificado como um número inteiro de 1 a 10 na opção de comando.</li> <li><b>port1</b> do par de portas é o número da porta Ethernet externa.</li> <li><b>port2</b> do par de portas é o número da porta Ethernet-sobre-USB.</li> </ul>
-rm <b>map_index</b>	Remova o mapeamento de portas para o índice especificado.	O número de índice de porta, <b>map_index</b> , é especificado como um número inteiro de 1 a 10 na opção de comando. <b>Nota:</b> Os índices de mapa de portas são exibidos usando o comando <b>ethtousb</b> sem opções.

Exemplo:

```
system> ethtousb -en enabled -m1 100:200 -m2 101:201
system> ethtousb
ethtousb : 0n
=====
1: 100: 200
2: 101: 201
system>
```

## Comando firewall

Use este comando para configurar o firewall para restringir o acesso de determinados endereços e, opcionalmente, limitar o período de acesso. Se nenhuma opção for especificada, as configurações atuais serão exibidas.

Sintaxe:

firewall [-options]

Tabela 26. Opções de firewall

Opção	Descrição	Valores
<b>A opção a seguir é para a lista de permissões de endereços IP</b>		
-wips	Mostrar/configurar os endereços IP da lista de permissões.	<p>&lt;Endereços IP válidos&gt;, clr</p> <ul style="list-style-type: none"> <li>• <b>Endereços IP válidos:</b> Permitir 1–3 endereços IP (separados por vírgula, CIDR ou intervalo)</li> </ul> <p><b>Nota:</b> Os endereços IPv4 e IPv6 podem usar o formato CIDR para bloquear um intervalo de endereços.</p> <ul style="list-style-type: none"> <li>• <b>-clr:</b> Limpar a lista branca</li> </ul>
<b>As opções a seguir são para Lista de Bloqueios e Restrição de Tempo</b>		
-bips	Bloquear endereços IP 1 a 3 (separados por vírgula, CIDR ou intervalo)	Endereços IP válidos <b>Nota:</b> Os endereços IPv4 e IPv6 podem usar o formato CIDR para bloquear um intervalo de endereços.
-bmacs	Bloquear endereços MAC 1-3 (separados por vírgula)	Endereços MAC válidos <b>Nota:</b> A filtragem de endereços MAC funciona apenas com endereços específicos.
-bbt	Hora de início de bloqueio, deve ser posterior à hora atual	Tempo com formato <AAAA-MM-DD HH:MM>
-bet	Hora de término do bloqueio, deve ser posterior à hora de início	Tempo com formato <AAAA-MM-DD HH:MM>
-bti	Bloquear 1 a 3 intervalos de tempo (separados por vírgula)  por exemplo, <b>firewall – bti 01:00 – 02:00,05:05 – 10:30</b> bloqueará o acesso durante 01:00-02:00 e 05:05-10:30 todos os dias	Intervalo de tempo com o formato <HH:MM-HH:MM>
-clr	Limpar a regra de firewall para um determinado tipo	ip, mac, datetime, intervalo, todos
<b>As opções a seguir são para o bloqueio de endereços IP</b>		
-iplp	Período de bloqueio de endereços IP em minutos.	Valor numérico entre 0 e 2880, 0 = nunca expirar

Tabela 26. Opções de firewall (continuação)

Opção	Descrição	Valores
-iplf	Número máximo de falhas de login antes que o endereço IP seja bloqueado.	Valor numérico entre 0 e 32, 0 = nunca bloquear <b>Nota:</b> Se esse valor não for 0, deverá ser maior ou igual a <Número máximo de falhas de login> que é definido por <accseccfg -lf>
-ipbl	Mostrar/configurar a lista de endereços IP que estão sendo bloqueados.	del, clrall, mostrar  <ul style="list-style-type: none"> <li>• <b>-del:</b> exclui um endereço IPv4 ou IPv6 da lista de bloqueios</li> <li>• <b>-clrall:</b> limpar todos os IP bloqueados</li> <li>• <b>-show:</b> mostrar todos os IPs bloqueados</li> </ul>

Exemplos da sintaxe do comando **firewall** são apresentados na lista a seguir:

- Para mostrar o valor de todas as opções e a lista de bloqueio de endereços IP, digite firewall.
- Para bloquear o acesso de vários IPs, digite firewall -bips 192.168.1.1,192.168.1.0/24,192.168.1.1-192.168.1.5.
- Para bloquear todos os acessos durante o 01:00-02:00,05:05-10:30,14:15-20:00 todos os dias, digite firewall -bti 01:00-02:00,05:05-10:30,14:15-20:00.
- Para limpar todas as regras de Lista de bloqueios e restrição de tempo, digite firewall -clr all.
- Para definir o período de bloqueio de endereço IP como 60 minutos, digite firewall -iplp 60.
- Para definir o número máximo de falhas de login como 5 vezes, digite firewall -iplf 5.
- Para excluir 192.168.100.1 da lista de bloqueio de endereços IP, digite firewall -ipbl -del 192.168.100.1.
- Para excluir 3fcc:1234::2 da lista de bloqueio de endereços IP, digite firewall -ipbl -del 3fcc:1234::2.
- Para excluir todos os endereços IP de bloqueio, digite firewall -ipbl -clrall.
- Para mostrar todos os endereços IP de bloqueio, digite firewall -ipbl -show.

## Comando hashpw

Use este comando com a opção -sw para habilitar/desabilitar a função de senha de terceiros ou com a opção -re para habilitar/desabilitar a permissão de recuperação de senha de terceiros.

Sintaxe:

hashpw [-options]

Tabela 27. Opções hashpw

Opção	Descrição	Valores
-sw	Status do comutador de senha de terceiros	habilitado, desabilitado
-re	Status de leitura de senha de terceiros  <b>Nota:</b> A leitura poderá ser definida se o comutador estiver habilitado.	habilitado, desabilitado

Exemplo:

```
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

Use esse comando para configurar a interface Ethernet.

Use o comando **ifconfig** para exibir a configuração atual da interface Ethernet. Para alterar a configuração da interface Ethernet, digite as opções, seguidas pelos valores. Para alterar a configuração da interface, você deve ter pelo menos autoridade de Configuração de Rede e Segurança do Adaptador.

Sintaxe:

```
ifconfig [ethernet_number] [-options]
```

Exemplo:

```
dhcpcfg eth1 -b
```

Tabela 28. Opções ifconfig

Opção	Descrição	Valores
-state	Estado da interface	habilitado, desabilitado
-c	Método de configuração	dhcp, static, dthens (dthens corresponde à opção <b>try dhcp server, if it fails use static config</b> na interface da Web)
-ghn	Obter nome do host do DHCP	habilitado, desabilitado
-i	Endereço IP estático	Endereço no formato válido.
-g	Endereços do gateway	Endereço no formato válido.
-s	Máscara de sub-rede	Endereço no formato válido.
-n	Nome do host	Sequência de até 63 caracteres. A sequência pode incluir letras, dígitos, pontos, sublinhados e hifens.
-auto	Configuração de negociação automática, que determina se as definições Taxa de dados e Rede duplex são configuráveis	true, false
-vlan	Ative ou desative a identificação de VLAN	habilitado, desabilitado
-vlanid	ID VLAN	Valor numérico entre 1 e 4094.
-r	Taxa de dados	10, 100, 1000
-d	Modo duplex	completo, metade
-m	MTU	Numérico entre 60 e 1500.
-l	LAA	Formato de endereço MAC. Endereços multicast não são permitidos (o primeiro byte deve ser par).
-b	Endereço MAC gravado (somente leitura)	

Tabela 28. Opções ifconfig (continuação)

Opção	Descrição	Valores
-dn	Nome de domínio (somente leitura)	
-ipv6	Estado do IPv6	habilitado, desabilitado
-ipv6static	Estado do IPv6 estático	habilitado, desabilitado
-i6	Endereço IP estático	Endereço IP estático para canal Ethernet 0 no formato IPv6.
-p6	Comprimento de prefixo de endereço	Valor numérico entre 1 e 128.
-g6	Gateway ou rota padrão	Endereço IP para o gateway ou a rota padrão do canal Ethernet 0 no IPv6.
-dhcp6	Modo DHCP IPv6	habilitado, desabilitado
-sa6	Modo sem estado IPv6	habilitado, desabilitado
-lla	Endereço local do link (somente leitura)	
-ncsi	Seleção de porta NCSI NIC	nic[x]:port[y] <b>Nota:</b> Use vírgula como delimitador se houver duas ou mais configurações.
-nic	Modo NIC de comutador <sup>1</sup>	shared, dedicated, shared:nic[x] <sup>2</sup>
-failover <sup>2</sup>	Modo de failover	none, shared, shared:nic[x]
-nssync <sup>3</sup>	Sincronização da configuração de rede	habilitado, desabilitado
-address_table	Tabela de endereços IPv6 gerados automaticamente e seus comprimentos de prefixo (somente leitura) <b>Nota:</b> A opção será visível somente se IPv6 e a configuração automática stateless estiverem habilitados.	

**Notas:**

1. -nic também mostrará o status da nic. [active] indica qual nic o XCC está usando atualmente.

Por exemplo:

```
-nic: shared:nic3
```

```
nic1: dedicate
```

```
nic2: ext card slot #3
```

```
nic3: ext card slot 5 [active]
```

Indica que nic3 está no modo compartilhado, no slot 5, nic2 está em slot3, nic1 é porta dedicada a XCC e XCC está usando nic3.

2. O valor shared:nic[x] está disponível em servidores que têm uma placa de rede de mezanino opcional instalada. Essa placa de rede tipo mezanino pode ser usada pelo IMM.
3. Se o IMM for configurado para usar a porta de rede de gerenciamento dedicada, a opção de failover direcionará o IMM para alternar para a porta de rede compartilhada se a porta dedicada estiver desconectada.
4. Se o modo de failover estiver habilitado, a opção -nssync direcionará o IMM para usar as mesmas configurações de rede que são usadas na porta de rede de gerenciamento dedicada para a porta de rede compartilhada.

**Exemplo:**

```
system> ifconfig eth0 -c static -i 192.168.70.133
```

These configuration changes will become active after the next reset of the IMM.

```
system>
```

## Comando keycfg

Use esse comando para exibir, incluir ou excluir chaves de ativação.

Acesso de controle de chaves de ativação para funcionalidade do IMM opcional.

### Notas:

- Inclua novas chaves de ativação por meio da transferência de arquivos.
- Exclua chaves antigas especificando número da chave ou o tipo de chave. Ao excluir chaves por tipo, apenas a primeira chave de um determinado tipo é excluída.

### Sintaxe:

```
keycfg [-options]
```

Tabela 29. Opções keycfg

Opção	Descrição	Valores
-add	Incluir chave de ativação	ip, pn, u, pw, f <ul style="list-style-type: none"><li>• <b>-ip</b>: endereço IP do servidor TFTP/SFTP com chave de ativação para adicionar</li><li>• <b>-pn</b>: número da porta do servidor TFTP/SFTP com a chave de ativação a ser incluída (padrão 69/22)</li><li>• <b>-u</b>: nome de usuário para o servidor SFTP com chave de ativação para adicionar</li><li>• <b>-pw</b>: senha para o servidor SFTP com chave de ativação a ser incluída</li><li>• <b>-f</b>: nome do arquivo da chave de ativação a ser adicionada</li></ul>
-del	Excluir chave de ativação por número de índice	Número de índice de chave de ativação válido a partir da listagem <b>keycfg</b>
-deltype	Excluir chave de ativação por tipo de chave	Valor de tipo de chave válido

Quando o comando **keycfg** é executado sem quaisquer opções, a lista de chaves de ativação instaladas é exibida. As informações chave exibidas incluem um número de índice para cada chave de ativação, o tipo de chave de ativação, a data até a qual a chave é válida, o número de usos restantes, o status da chave e uma descrição da chave.

### Exemplo:

```
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:** O campo **Descrição** para o número de ID 3 é exibido em linhas separadas devido a limitações de espaço.

## Comando ldap

Use esse comando para exibir e configurar os parâmetros de configuração do protocolo LDAP.

### Sintaxe:

ldap [-options]

Tabela 30. Opções ldap

Opção	Descrição	Valores
-aom	Modo somente de autenticação para usuários do Active Directory	habilitado, desabilitado
-a	Método de autenticação do usuário	<ul style="list-style-type: none"> <li>• <b>loc</b>: somente local</li> <li>• <b>ldap</b>: somente LDAP</li> <li>• <b>locl</b>: local primeiro e depois LDAP</li> <li>• <b>ldloc</b>: LDAP primeiro e depois local</li> </ul>
-b	Método de ligação	<ul style="list-style-type: none"> <li>• <b>anon</b>: anônimo</li> <li>• <b>client</b>: vincular com ClientDN e senha</li> <li>• <b>login</b>: vincular com Credencial de Login</li> </ul>
-c	Nome distinto do cliente	Sequência de até 127 caracteres para <b>client_dn</b>
-d	Domínio de procura	Sequência de até 63 caracteres para <b>search_domain</b>
-fn	Nome da floresta	Para ambientes do Active Directory. Sequência de até 127 caracteres.
-f	Filtro de grupo	Sequência de até 127 caracteres para <b>group_filter</b>
-g	Atributo de procura de grupo	Sequência de até 63 caracteres para <b>group_search_attr</b>
-l	Atributo de permissão de login	Sequência de até 63 caracteres para <b>string</b>
-p	Senha do cliente	Sequência de até 15 caracteres para <b>client_pw</b>
-pc	Confirmar senha do cliente	<p>Sequência de até 15 caracteres para <b>confirm_pw</b>  O uso do comando é: ldap -p <b>client_pw</b> -pc <b>confirm_pw</b></p> <p>Essa opção é necessária quando você altera a senha do cliente. Ela compara o argumento <b>confirm_pw</b> com o argumento <b>client_pw</b>. O comando falhará se os argumentos não corresponderem.</p>
-r	Nome distinto (DN) de entrada raiz	Sequência de até 127 caracteres para <b>root_dn</b>
-s1ip	Nome do host/endereço IP do servidor 1	Sequência de até 127 caracteres ou um endereço IP para <b>host name/ip_addr</b>
-s2ip	Nome do host/endereço IP do servidor 2	Sequência de até 127 caracteres ou um endereço IP para <b>host name/ip_addr</b>
-s3ip	Nome do host/endereço IP do servidor 3	Sequência de até 127 caracteres ou um endereço IP para <b>host name/ip_addr</b>
-s4ip	Nome do host/endereço IP do servidor 4	Sequência de até 127 caracteres ou um endereço IP para <b>host name/ip_addr</b>
-s1pn	Número da porta do servidor 1	Um número de porta com até 5 dígitos para <b>port_number</b>
-s2pn	Número da porta do servidor 2	Um número de porta com até 5 dígitos para <b>port_number</b>

Tabela 30. Opções ldap (continuação)

Opção	Descrição	Valores
-s3pn	Número da porta do servidor 3	Um número de porta com até 5 dígitos para <b>port_number</b>
-s4pn	Número da porta do servidor 4	Um número de porta com até 5 dígitos para <b>port_number</b>
-u	Atributo de pesquisa do nome de login do usuário	Sequência de até 63 caracteres para <b>search_attrib</b>
-v	Obter endereço do servidor LDAP por meio de DNS	off, on
-h	Exibe o uso e as opções do comando	

**Exemplo:**

```
system> ldap
  -aom enable
  -a loclld
  -b client
  -c cn=admin,dc=lenovo,dc=com
  -d
  -fn
  -f example.com
  -g cn
  -l XCC3RBSPermissions
  -r
  -s1ip 10.241.99.94
  -s2ip
  -s3ip
  -s4ip
  -s1pn 389
  -s2pn 389
  -s3pn 389
  -s4pn 389
  -u uid
  -v off
system>
```

## Comando ntp

Use esse comando para exibir e configurar o Network Time Protocol (NTP).

**Sintaxe:**

```
ntp [-options]
```

Tabela 31. Comando ntp

Opção	Descrição	Valores
-en	Habilita ou desabilita o Network Time Protocol.	habilitado, desabilitado
-i[x]	Nome ou endereço IP do servidor Network Time Protocol para o índice <b>x</b> .	O nome do servidor NTP a ser usado para a sincronização de clock. O intervalo do número de índice do servidor NTP é de -i1 a -i4. <b>Nota:</b> -i é igual a i1.

Tabela 31. Comando ntp (continuação)

Opção	Descrição	Valores
-f	A frequência (em minutos) com que o relógio do IMM é sincronizado com o servidor Network Time Protocol.	3 a 1440 minutos
-synch	Solicita uma sincronização imediata com o servidor Network Time Protocol.	Nenhum valor é usado com esse parâmetro.

Exemplo:

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

## Comando portcontrol

Use esse comando para ativar ou desativar uma porta de serviço de rede.

Sintaxe:

```
portcontrol [-options]
```

Tabela 32. Opções portcontrol

Opção	Descrição	Valores
-ipmi	Ative ou desative o acesso ao ipmi via LAN	on, off
-ipmi-kcs	Ativar sob demanda, ativar ou desativar acesso IPMI do servidor	auto, on, off
-rest	Ative ou desative a descoberta de REST	on, off
-snmp	Ative ou desative a descoberta de SNMP	on, off
-ssdp	Ative ou desative a descoberta de SSDP	on, off
-cli	Ative ou desative a descoberta de CLI	on, off
-web	Ative ou desative a descoberta de WEB	on, off
-all	Ative ou desative todas as interfaces e protocolos de descoberta	on, off

Exemplo:

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

```
web : on
system>
```

## Comando ports

Use esse comando para exibir e configurar as portas do IMM.

Sintaxe:

```
ports [-options]
```

Tabela 33. Opções ports

Opção	Descrição	Valores
-open	Exibir portas abertas (somente leitura)	
-reset	Redefinir portas para configurações padrão (somente leitura)	
-http	Número da porta HTTP	Número da porta padrão: 80
-https	Número da porta HTTPS	Número da porta padrão: 443
-ssh	Número da porta da CLI legada do SSH	Número da porta padrão: 22
-snmpa	Número da porta do agente SNMP	Número da porta padrão: 161
-snmpt	Número da porta de traps SNMP	Número da porta padrão: 162
-rp	Número da porta de presença remota	Número da porta padrão: 3900

Exemplo:

```
system> ports
  -http 80
  -https 443
  -rp 3900
  -snmpa 161
  -snmpt 162
  -ssh 22
system>
```

## Comando rdmount

Use esse comando para montar imagens de disco remoto ou compartilhamentos de rede

**Notas:**

- Até dois arquivos podem ser carregados na memória do XClarity Controller e montados como mídia virtual com o recurso RDOC do XClarity Controller. O tamanho total dos dois arquivos não deve ultrapassar 50 MB. As imagens transferidas por upload são somente leitura, a menos que a opção `-rw` seja usada.
- Ao usar os protocolos HTTP, SFTP ou FTP para montar ou mapear as imagens, o tamanho total de todas as imagens não deve exceder 50 MB. Não há nenhum limite se os protocolos NFS ou SAMBA forem usados.

Sintaxe:

```
rdmount [-options]
```

Tabela 34. Opções rdmount

Opção	Descrição
-r	Operação rdoc (se usada, deve ser primeira opção) -r -map: montar as imagens RDOC  -r -unmap<filename>: desmontar as imagens RDOC montadas  -r -maplist: mostra as imagens RDOC montadas por meio da interface CLI e do navegador da Web do XClarity Controller
-map	-t <samba nfs http sftp ftp> filesystem type  -ro read-only  -rw read-write  -u user  -p password  -l file location (formato do URL)  -o option (string de opção adicional para montagens samba e nfs)  -d domain (domínio para montagem samba)
-maplist	Mostra as imagens mapeadas
-unmap	<id fname> usar o id com imagens de rede, nome de arquivo com rdoc
-mount	Montar as imagens mapeadas
-unmount	Desmontar as imagens montadas

## Comando restore

Use esse comando para restaurar as configurações do sistema a partir de um arquivo de backup.

Sintaxe:

restore [-options]

Tabela 35. Opções restore

Opção	Descrição	Valores
-f	Nome do arquivo de backup	Nome do arquivo válido
-pp	Senha ou passphrase usada para criptografar senhas no arquivo de backup	Senha ou passphrase delimitada por aspas válida
-ip	Endereço IP do servidor TFTP/SFTP	Endereço IP válido
-pn	Número da porta do servidor TFTP/SFTP	Número da porta válido (padrão 69/22)
-u	Nome de usuário para o servidor SFTP	Nome de usuário válido
-pw	Senha para o servidor SFTP	Senha válida

Exemplo:

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

## Comando roles

Use esse comando para exibir ou configurar as funções.

Sintaxe:

```
roles role_account[3-31] [-options]
```

Tabela 36. Opções roles

Opção	Descrição	Valores
-n	Nome da função	Limitada a 32 caracteres
-p	Definir privilégios	personalizado: am, rca, rcvma, pr, cel, bc, nsc, ac, us <ul style="list-style-type: none"><li>• <b>am</b>: acesso de gerenciamento da conta do usuário</li><li>• <b>rca</b>: acesso ao console remoto</li><li>• <b>rcvma</b>: acesso ao console e ao disco remotos (mídia virtual)</li><li>• <b>pr</b>: acesso de energia/reinicialização do servidor remoto</li><li>• <b>cel</b>: capacidade para limpar logs de eventos</li><li>• <b>bc</b>: configuração de adaptador (básica)</li><li>• <b>nsc</b>: configuração de adaptador (rede e segurança)</li><li>• <b>ac</b>: configuração de adaptador (avançada)</li><li>• <b>us</b>: segurança do UEFI</li></ul> <b>Nota:</b> Os sinalizadores de permissão personalizada acima podem ser usados em qualquer combinação
-d	Excluir uma linha	

Exemplo:

```
system> roles -3 -n test1 -p custom:am|rca|rcvma
ok
```

```
system> roles
```

Account	Role	Privilege	Assigned To
0	Administrator	all	USERID
1	ReadOnly	none	
2	Operator	custom:pr cel bc nsc	
3	test1	custom:am rca rcvma	

## Comando rtd

Use esse comando para restaurar todas as configurações do BMC para o padrão de fábrica.

**Nota:** Esse comando costumava ser o comando **restoredefaults** e **clearcfg**.

Sintaxe:  
rtd [-options]

Tabela 37. Opções rtd

Opção	Descrição
-all	Redefina todas as configurações do BMC para os padrões de fábrica.
-eu	Redefina todas as configurações do BMC para os padrões de fábrica, exceto Configurações do usuário
-en	Redefina todas as configurações do BMC para os padrões de fábrica, exceto Configurações de rede.
-eun	Redefina todas as configurações do BMC para os padrões de fábrica, exceto Configurações de rede e do usuário.

Exemplo:  
system> rtd -all

This action will cause all IMM settings to be set to factory defaults.

If this is the local system, you will lose your TCP/IP connection as a result. You will need to reconfigure the IMM network interface to restore connectivity. After the IMM configuration is cleared, the IMM will be restarted.

Proceed? (y/n)  
Y  
Restoring defaults

## Comando seccfg

Use esse comando para executar uma reversão de firmware.

Sintaxe:  
seccfg [-options]

Tabela 38. Opções seccfg

Opção	Descrição	Valor
-fwr	Permite reverter o firmware para a versão anterior.	habilitado, desabilitado
-aubp	Habilitar ou desabilitar a função de backup automático para a promoção primária.	habilitado, desabilitado

## Comando securityinfo

Esse comando é usado para exibir informações relacionadas à segurança.

Sintaxe:  
securityinfo [-options]

Tabela 39. Opções securityinfo

Opção	Descrição
-event	Exibir eventos de segurança.
-cryptomode	Exibir status de cryptomode de segurança.
-service	Exibir o status de segurança de serviços e portas.
-cert	Exibir o status de segurança do certificado.
-account	Exibir o status de segurança das contas de usuário.

## Comando securitymode

Esse comando é usado para gerar um novo arquivo de dados de serviço.

Sintaxe:

securitymode [-options]

Tabela 40. Opções securitymode

Opção	Descrição	Valores
-mode	Seleciona o modo de segurança. <ul style="list-style-type: none"> <li>• CNSA – Estrito corporativo</li> <li>• FIPS – Padrão</li> <li>• COMPAT – Compatibilidade</li> </ul>	CNSA, FIPS, COMPAT <ul style="list-style-type: none"> <li>• <b>CNSA</b>: somente serviços que suportam criptografia de nível estrito corporativo são permitidos; requer a chave Feature on Demand para ativar.</li> <li>• <b>FIPS</b>: os serviços que requerem criptografia que não suportam criptografia de nível padrão são desativados por padrão.</li> <li>• <b>COMPAT</b>: quando esse modo é ativado, o XCC NÃO está operando no modo validado pelo padrão; permite que todos os serviços sejam ativados.</li> </ul>
-h	Listar uso e opções.	

## Comando set

Use esse comando para alterar algumas configurações do IMM.

- Algumas configurações do IMM podem ser alteradas com um simples comando **set**.
- Algumas dessas configurações, como variáveis de ambiente, são usadas pela CLI.

A tabela a seguir mostra os argumentos das opções.

Tabela 41. Comando set

A tabela a seguir é uma tabela de três colunas e uma linha que consiste na descrição do comando e informações associadas.

Opção	Descrição	Valores
value	Configurar valor para caminho ou configuração especificada	Valor apropriado para o caminho ou configuração especificada.

Sintaxe:

```
set [-options]
option:
  value
```

## Comando snmp

Use esse comando para exibir e configurar informações da interface SNMP.

Sintaxe:

```
snmp [-options]
```

Tabela 42. Opções snmp

Opção	Descrição	Valores
-a3	Agente do SNMPv3	on, off <b>Notas:</b> Para ativar o agente do SNMPv3, os critérios a seguir devem ser atendidos: <ul style="list-style-type: none"> <li>Contato do IMM especificado usando a opção de comando -cn.</li> <li>Local do IMM especificado usando a opção de comando -l.</li> </ul>
-t	Traps SNMPv3	on, off
-tn	Nome de usuário do trap SNMPv3	Nome de usuário válido
-tauth	Protocolo de autenticação do trap SNMPv3	nenhum, HMAC-SHA
-tapw	Senha de autenticação do trap SNMPv3	Senha válida
-tpriv	Protocolo de privacidade do trap SNMPv3	nenhum, CBC-DES, AES
-tppw	Senha de privacidade do trap SNMPv3	Senha válida
-tix	Endereço IP ou nome do host da comunidade x	Endereço IP válido ou nome do host (limitado a 63 caracteres, x pode variar de 1 a 3). <b>Notas:</b> <ul style="list-style-type: none"> <li>Um endereço IP ou nome do host só pode conter pontos, sublinhados, sinais de subtração, letras e dígitos. Não são permitidos espaços integrados ou pontos consecutivos.</li> <li>Limpe um endereço IP ou nome do host da comunidade não especificando um argumento.</li> </ul>
-l	Local do IMM	Sequência (limitada a 47 caracteres). <b>Notas:</b> <ul style="list-style-type: none"> <li>Argumentos que contêm espaços devem ser colocados entre aspas. Nenhum espaço à esquerda ou direita é permitido nos argumentos.</li> <li>Limpe o local do IMM sem especificar um argumento ou especificando uma string vazia como o argumento, como "".</li> </ul>
-cn	Nome do contato do IMM	Sequência (limitada a 47 caracteres). <b>Notas:</b> <ul style="list-style-type: none"> <li>Argumentos que contêm espaços devem ser colocados entre aspas. Nenhum espaço à esquerda ou direita é permitido nos argumentos.</li> <li>Limpe o nome do contato do IMM sem especificar um argumento ou especificando uma string vazia como o argumento, como "".</li> </ul>

Tabela 42. Opções snmp (continuação)

Opção	Descrição	Valores
-t1	Traps SNMPv1	on, off
-c	Nome da comunidade SNMP	Sequência (limitada a 15 caracteres). <b>Notas:</b> <ul style="list-style-type: none"> <li>Argumentos que contêm espaços devem ser colocados entre aspas. Nenhum espaço à esquerda ou direita é permitido nos argumentos.</li> <li>Limpe o nome da comunidade do SNMP não especificando um argumento ou especificando uma sequência vazia como o argumento, tal como "".</li> </ul>
-ci	Endereço IP/nome do host da comunidade 1	Endereço IP ou nome do host válido (limitado a 63 caracteres). <b>Notas:</b> <ul style="list-style-type: none"> <li>Um endereço IP ou nome do host só pode conter pontos, sublinhados, sinais de subtração, letras e dígitos. Não são permitidos espaços integrados ou pontos consecutivos.</li> <li>Limpe um endereço IP ou nome do host da comunidade não especificando um argumento.</li> </ul>
-c1iy	Endereço IP/nome do host da comunidade <b>y</b>	Endereço IP válido ou nome do host (limitado a 63 caracteres, <b>y</b> pode variar 2 ou 3). <b>Notas:</b> <ul style="list-style-type: none"> <li>Um endereço IP ou nome do host só pode conter pontos, sublinhados, sinais de subtração, letras e dígitos. Não são permitidos espaços integrados ou pontos consecutivos.</li> <li>Limpe um endereço IP ou nome do host da comunidade não especificando um argumento.</li> </ul>
-t2	Traps SNMPv2	on, off
-ct	Nome da comunidade do trap SNMPv2	Sequência (limitada a 15 caracteres). <b>Notas:</b> <ul style="list-style-type: none"> <li>Argumentos que contêm espaços devem ser colocados entre aspas. Nenhum espaço à esquerda ou direita é permitido nos argumentos.</li> <li>Limpe o nome do contato do IMM sem especificar um argumento ou especificando uma string vazia como o argumento, como "".</li> </ul>
-cti	Nome do host/endereço IP 1 da comunidade do trap SNMPv2	Endereço IP ou nome do host válido (limitado a 63 caracteres). <b>Notas:</b> <ul style="list-style-type: none"> <li>Um endereço IP ou nome do host só pode conter pontos, sublinhados, sinais de subtração, letras e dígitos. Não são permitidos espaços integrados ou pontos consecutivos.</li> <li>Limpe um endereço IP ou nome do host da comunidade SNMP não especificando um argumento.</li> </ul>
-eid	ID do mecanismo SNMP	String (limite de 1 a 27 caracteres)
-send	Enviar informações sobre um trap de teste	

**Exemplo:**

```
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

Use esse comando para gerenciar alertas enviados via SNMP.

Sintaxe:

```
snmpalerts [-options]
```

Tabela 43. Opções snmpalerts

Opção	Descrição	Valores
-status	Status de alerta de SNMP	on, off
-crt	Configura eventos críticos que enviam alertas	<p>todos, nenhum, personalizado:te vo po di fa cp me in re ot pc</p> <p>Configurações customizadas de alerta crítico são especificadas usando uma lista de valores separados por barra vertical no formato <b>snmpalerts -crt custom:te vo</b>, em que os valores customizados são:</p> <ul style="list-style-type: none"> <li>• te: limite de temperatura crítico excedido</li> <li>• vo: limite de voltagem crítico excedido</li> <li>• po: falha de energia crítica</li> <li>• di: falha da unidade de disco rígido</li> <li>• fa: falha do ventilador</li> <li>• cp: falha do microprocessador</li> <li>• me: falha de memória</li> <li>• in: incompatibilidade de hardware</li> <li>• re: falha de redundância de energia</li> <li>• ot: todos os outros eventos críticos</li> <li>• pc: eventos críticos PCIe</li> </ul>

Tabela 43. Opções snmpalerts (continuação)

Opção	Descrição	Valores
-wrn	Configura eventos de aviso que enviam alertas	<p>todos, nenhum, personalizado:rp te vo po fa cp me ot pw</p> <p>Configurações customizadas de alerta de aviso são especificadas usando uma lista de valores separados por barra vertical no formato <b>snmpalerts -wrn custom:rp te</b>, em que os valores customizados são:</p> <ul style="list-style-type: none"> <li>• rp: aviso de redundância de energia</li> <li>• te: aviso de limite de temperatura excedido</li> <li>• vo: aviso de limite de voltagem excedido</li> <li>• po: aviso de limite de energia excedido</li> <li>• fa: evento de ventilador não crítico</li> <li>• cp: microprocessador em estado degradado</li> <li>• me: aviso de memória</li> <li>• ot: todos os outros eventos de aviso</li> <li>• pw: eventos de aviso PCIe</li> </ul>
-sys	Configura eventos de rotina que enviam alertas	<p>todos, nenhum, personalizado:lo tio ot po bf til pf el ne nl dh oa</p> <p>Configurações customizadas de alerta de rotina são especificadas usando uma lista de valores separados por barra vertical no formato <b>snmpalerts -sys custom:lo tio</b>, em que os valores customizados são:</p> <ul style="list-style-type: none"> <li>• lo: login remoto bem-sucedido</li> <li>• tio: tempo limite do sistema operacional</li> <li>• ot: todos os outros eventos informativos e do sistema</li> <li>• po: ligar/desligar energia</li> <li>• bf: falha de inicialização do sistema operacional</li> <li>• til: tempo limite de watchdog do carregador do sistema operacional</li> <li>• pf: falha prevista (PFA)</li> <li>• el: log de eventos 75% cheio</li> <li>• ne: mudança de rede</li> <li>• nl: link NIC do host inativo/ativo</li> <li>• dh: hotplug da unidade</li> <li>• oa: todos os outros eventos de auditoria</li> </ul>

## Comando sshcfg

Use esse comando para exibir e configurar os parâmetros do SSH.

Sintaxe:

```
sshcfg [-options]
```

Tabela 44. Opções sshcfg

Opção	Descrição	Valores
-cstatus	Estado da CLI do SSH	habilitado, desabilitado
-hk	Chave do servidor	<p>gen, todos</p> <ul style="list-style-type: none"> <li>• <b>gen</b>: Gerar a chave privada do servidor SSH</li> <li>• <b>todos</b>: Exibir chave pública do servidor</li> </ul>

### Exemplo:

```
system> sshcfg
-cstatus enabled
CLI SSH port 22
ssh-rsa 2048 bit fingerprint: b4:a3:5d:df:0f:87:0a:95:f4:d4:7d:c1:8c:27:51:61
1 SSH public keys installed
system>
```

## Comando sslcfg

Use esse comando para exibir e configurar o SSL para o IMM e gerenciar certificados.

O comando **sslcfg** é usado para gerar uma nova chave de criptografia e certificado autoassinado ou solicitação de assinatura de certificado (CSR).

### Sintaxe:

```
sslcfg [-options]
```

Tabela 45. Opções sslcfg

Opção	Descrição	Valores
-server	Status da Web sobre HTTPS	habilitado, desabilitado <b>Notas:</b> <ul style="list-style-type: none"><li>A Web sobre HTTPS só pode ser ativada se um certificado estiver em vigor.</li><li>Use <b>-rm</b> para desativar completamente o certificado.</li></ul>
-client	Status LDAP seguro	habilitado, desabilitado <b>Nota:</b> O cliente SSL poderá ser habilitado apenas se houver um certificado de servidor ou cliente válido no local.
-cert	Gerar certificado autoassinado	server, client, sysdir, storekey <b>Notas:</b> <ul style="list-style-type: none"><li>Os valores para as opções de comando <b>-c</b>, <b>-sp</b>, <b>-cl</b>, <b>-on</b> e <b>-hn</b> são necessários ao gerar um certificado autoassinado.</li><li>Os valores para as opções de comando <b>-cp</b>, <b>-ea</b>, <b>-ou</b>, <b>-s</b>, <b>-gn</b>, <b>-in</b> e <b>-dq</b> são opcionais ao gerar um certificado autoassinado.</li></ul>
-csr	Gerar um CSR	server, client, sysdir, storekey <b>Notas:</b> <ul style="list-style-type: none"><li>Os valores para as opções de comando <b>-c</b>, <b>-sp</b>, <b>-cl</b>, <b>-on</b> e <b>-hn</b> são necessários ao gerar um CSR.</li><li>Os valores para as opções de comando <b>-cp</b>, <b>-ea</b>, <b>-ou</b>, <b>-s</b>, <b>-gn</b>, <b>-in</b>, <b>-dq</b>, <b>-cpwd</b> e <b>-un</b> são opcionais ao gerar um CSR.</li></ul>
-form	Formato da CSR ou do certificado que será exportado.	der, pem (padrão pem)
-algo	Algoritmo de CSR	p256, p384, rsa2048, rsa3072, rsa4096 <b>Nota:</b> Um valor padrão (p256) será definido se não houver uma opção <b>-algo</b> .
-rm	Remover o certificado	servidor, storekey <b>Nota:</b> Um certificado autoassinado padrão (servidor) seria gerado automaticamente depois que o atual fosse removido.

Tabela 45. Opções `sslcfg` (continuação)

Opção	Descrição	Valores
-i	Endereço IP para o servidor TFTP/SFTP	Endereço IP válido <b>Nota:</b> Um endereço IP para o servidor TFTP ou SFTP deve ser especificado ao fazer upload de um certificado ou ao fazer download de um certificado ou CSR.
-pn	Número da porta do servidor TFTP/SFTP	Número da porta válido (padrão 69/22)
-u	Nome de usuário para o servidor SFTP	Nome de usuário válido
-pw	Senha para o servidor SFTP	Senha válida
-l	Nome do arquivo de certificado	Nome do arquivo válido <b>Nota:</b> Um nome de arquivo é necessário ao fazer download ou fazer upload de um certificado ou CSR. Se nenhum nome de arquivo for especificado para um download, o nome padrão para o arquivo será usado e exibido.
-dnld	Exporta o arquivo especificado para o host remoto	Essa opção não usa argumentos; mas deve ser usada com <b>-cert</b> ou <b>-csr</b> ; bem como as opções de comando <b>-i</b> e <b>-l</b> .
-upld	Importa o arquivo de certificado	Essa opção não usa argumentos, porém também deve especificar valores para as opções de comando <b>-cert</b> , <b>-i</b> e <b>-l</b> .
-tcx	Certificado de confiança <b>x</b> para cliente SSL	import, download, remove <b>Nota:</b> O número do certificado de confiança, <b>x</b> , é especificado como um número inteiro de 1 a 4 na opção de comando.
<b>Opções necessárias para gerar um certificado autoassinado ou CSR</b> <b>Nota:</b> Necessário ao gerar um certificado autoassinado ou CSR.		
-c	País	Código do país (2 letras)
-sp	Estado ou município	Sequência delimitada por aspas (máximo 60 caracteres)
-cl	Cidade ou localidade	Sequência delimitada por aspas (máximo 50 caracteres)
-on	Nome da organização	Sequência delimitada por aspas (máximo 60 caracteres)
-hn	Nome do host do BMC	Sequência (máximo 60 caracteres)
<b>Opções opcionais para gerar um certificado autoassinado ou CSR</b> <b>Nota:</b> Opcional ao gerar um certificado autoassinado ou CSR.		
-cp	Pessoa de contato	Sequência delimitada por aspas (máximo 60 caracteres)
-ea	Endereço de email da pessoa de contato	Endereço de email válido (máximo 60 caracteres)
-ou	Unidade Organizacional	Sequência delimitada por aspas (máximo 60 caracteres)
-s	Sobrenome	Sequência delimitada por aspas (máximo 60 caracteres)
-gn	Nome	Sequência delimitada por aspas (máximo 60 caracteres)
-in	Iniciais	Sequência delimitada por aspas (máximo 20 caracteres)
-dq	Qualificador de nome de domínio	Sequência delimitada por aspas (máximo 60 caracteres)
<b>Opções opcionais para gerar uma CSR</b> <b>Nota:</b> Opcional ao gerar um CSR.		

Tabela 45. Opções sslcfg (continuação)

Opção	Descrição	Valores
-cpwd	Senha de desafio	Sequência (mínimo 6 caracteres, máximo 30 caracteres)
-un	Nome não estruturado	Sequência delimitada por aspas (máximo 60 caracteres)

#### Exemplos:

```
system> sslcfg
-server enabled
-client disabled
-sysdir enabled
SSL Server Certificate status:
A self-signed certificate is installed
SSL Client Certificate status:
A self-signed certificate is installed
SSL Client Trusted Certificate status:
Trusted Certificate 1: Not available
Trusted Certificate 2: Not available
Trusted Certificate 3: Not available
Trusted Certificate 4: Not available
```

#### Exemplos de certificado de cliente:

- Para gerar um CSR para uma chave de armazenamento, insira o seguinte comando:  

```
system> sslcfg -csr storekey -c US -sp NC -cl rtp -on LNV -hn XCC-5cf3fc -cp Contact -ea "" -ou ""
ok
```
- Para fazer download de um certificado do IMM para outro servidor, insira o seguinte comando:  

```
system> sslcfg -csr storekey -dnld -i 192.168.70.230 -l storekey.csr
ok
```
- Para carregar o certificado processado pela autoridade de certificação (CA), insira o seguinte comando:  

```
system> sslcfg -cert storekey -upld -i 192.168.70.230 -l tklm.der
```
- Para gerar um certificado autoassinado, insira o seguinte comando:  

```
system> sslcfg -cert storekey -c US -sp NC -cl rtp -on LNV -hn XCC-5cf3fc -cp Contact -ea "" -ou ""
ok
```

#### Exemplo de certificado do Servidor SKLM:

- Para importar o certificado do servidor SKLM, insira o seguinte comando:  

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

## Comando syslock

Use esse comando para exibir e definir configurações de bloqueio do sistema.

#### Sintaxe:

```
syslock [-options]
```

Tabela 46. Opções syslock

Opção	Descrição	Valores
-en	Ative ou desative a função de bloqueio de configuração do sistema. <b>Nota:</b> Ativar com a opção <b>-e</b> pode promover o estoque atual como captura instantânea confiável.	habilitado, desabilitado
-e	Ative as definições de bloqueio de configuração do sistema com ou sem impor o estoque atual em uma captura instantânea confiável. <b>Nota:</b> Um valor padrão será definido se não houver opção <b>-e</b> .	habilitado, desabilitado
-l [x]	Liste o estoque de captura instantânea específica no índice <b>x</b> .	O número de índice, <b>x</b> , é especificado como um inteiro na opção de comando.
-m	Tire uma captura instantânea manual.	
-d	Descrição para captura instantânea manual.	Sequência de até 32 caracteres.
-c	Liste a diferença de inventário da captura instantânea confiável.	
-po	Defina a política de bloqueio. <b>Nota:</b> A ação impedirá a inicialização do servidor se o protetor do sistema estiver em status não compatível.	nenhum, osboot, pperm
-cpu	Defina o bloqueio da CPU.	on, off
-dimm	Defina o bloqueio de dimm.	on, off
-pci	Definir bloqueio PCI.	on, off
-drive	Defina o bloqueio da unidade.	on, off
-riser	Defina o bloqueio da placa riser.	on, off
-bp	Definir bloqueio de bp.	on, off

## Comando thermal

Use esse comando para exibir e configurar a política de modo térmico do sistema host.

A execução do comando **thermal** sem opções exibe a política de modo térmico. A tabela a seguir mostra os argumentos das opções.

Sintaxe:  
thermal [-options]

Tabela 47. Opções thermal

Opção	Descrição	Valores
-mode	Exibe a política de modo térmico e configura a tabela térmica dos sistemas host (somente leitura)	<ul style="list-style-type: none"> <li>• Computação geral – Eficiência de energia</li> <li>• Computação geral – Frequência de pico</li> <li>• Computação geral – Desempenho máximo</li> <li>• Virtualização – Eficiência de energia</li> <li>• Virtualização – Desempenho máximo</li> <li>• Banco de Dados – Processamento de transações</li> <li>• Baixa latência</li> <li>• Computação de alto desempenho</li> <li>• Personalizar</li> <li>• Desconhecido</li> </ul>
-tabela <b>table_</b> <b>number</b>	<b>table_number</b> especifica a tabela térmica alternativa a ser usada.	<p>1 = Baixo: Leve aumento na velocidade do ventilador</p> <p>2 = Médio: Aumento moderado na velocidade do ventilador</p> <p>3 = Alto: Grande aumento na velocidade do ventilador</p> <p>0 = Normal: Nenhum aumento na velocidade do ventilador</p>

Exemplo:

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

## Comando tls

Use esse comando para definir o nível mínimo do TLS.

Sintaxe:

```
tls [-options]
```

Tabela 48. Opções tls

Opção	Descrição	Valores
-min	Selecione o nível mínimo de TLS	1.2, 1.3 <b>Nota:</b> Quando o modo de criptografia é configurado para o Modo de Conformidade NIST-800-131A, a versão TLS deve ser configurada para 1.2.
-h	Liste o uso e as opções	
<b>Notas:</b>		
1. Quando o modo de criptografia é configurado para o Modo de Conformidade NIST-800-131A, a versão TLS deve ser configurada para 1.2.		

Exemplos:

Para obter o uso para o comando tls, emita o seguinte comando:

```
system> tls
-h
```

```
system>
```

Para obter a versão tls atual, emita o seguinte comando:

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

Para alterar a versão tls atual para 1.2, emita o seguinte comando:

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

## Comando trespass

Use esse comando para configurar e exibir mas mensagens de infração.

O comando **trespass** pode ser usado para configurar e exibir as mensagens de infração. As mensagens de infração serão exibidas para qualquer login de usuário por meio da interface da WEB ou da CLI.

Sintaxe:

```
trespass [-options]
```

Tabela 49. Opções trespass

Opção	Descrição
-s	Configurar mensagens de infração
-h	Lista o uso e as opções

Exemplo:

```
system> trespass -s testingmessage
ok
system> trespass
testingmessage
system>
system> trespass -s "testing message"
ok
system> trespass
testing message
system>
```

## Comando uefipw

Use este comando para configurar senhas do administrador de UEFI. A senha é somente gravação.

O comando **uefipw** pode ser usado com a opção "-p" para configurar a senha do administrador de UEFI para XCC ou com a opção "-ep" para LXCA para configurar a senha do administrador de UEFI pela interface da CLI. A senha é somente gravação.

Sintaxe:

```
uefipw [-options]
```

Tabela 50. Opções uefipw

Opção	Descrição
-cp	Senha atual (limitada a 20 caracteres)
-p	Nova senha (limitada a 20 caracteres)

## Comando usbeth

Use esse comando para habilitar ou desabilitar a interface LAN sobre USB dentro da banda.

### Notas:

- As definições de configuração de IP do sistema operacional não são usadas para configurar o endereço IP do sistema operacional de interface Ethernet sobre USB, mas são usadas para notificar o BMC que o endereço IP do sistema operacional de Ethernet sobre USB foi alterado.
- Antes de definir três configurações de IP de Ethernet sobre USB, você precisa configurar manualmente o endereço IP do sistema operacional da interface Ethernet sobre USB em seu sistema operacional local.

Sintaxe:

usbeth [-options]

Tabela 51. Opções usbeth

Opção	Descrição	Valores
-en	Ative ou desative a interface em banda (Ethernet sobre USB).	habilitado, desabilitado
-am	Selecione o modo de endereço IPv4 ou IPv6 LLA.	ipv4, ipv6lla
<b>Nota:</b> As opções -ip, -sn e -ipos só são válidas quando o modo ipv4 -am está selecionado		
-ip	Endereço IP da interface Ethernet sobre USB para BMC.	Endereço IP válido
-sn	Máscara de sub-rede da interface Ethernet sobre USB para BMC.	Endereço IP válido
-ipos	Endereço IP da interface Ethernet sobre USB para sistema operacional.	Endereço IP válido

Exemplo:

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

## Comando users

Use esse comando para acessar todas as contas do usuário e seus níveis de autoridade.

O comando **users** também é usado para criar novas contas do usuário e modificar as contas existentes. A execução do comando **users** sem opções exibe uma lista de usuários e algumas informações básicas sobre o usuário.

Sintaxe:

users [-user\_index] [-options]

Tabela 52. Opções users

Opção	Descrição	Valores
-user_index	Número de índice da conta do usuário.	Em que <b>user_index</b> é 1 a 12 (inclusive) ou <b>todos</b> para todos os usuários.
-l	Exibir dias de expiração da senha	
-n	Nome da conta do usuário	Sequência exclusiva que contém apenas números, letras, pontos e sublinhados. Mínimo de 4 caracteres e máximo de 16 caracteres.
-p	Senha de conta do usuário	Sequência que contém pelo menos um caractere alfabético e um não alfabético. Mínimo de 6 caracteres e máximo de 255 caracteres. Null cria uma conta sem uma senha que o usuário deve configurar durante seu primeiro login.
-shp	Definir a senha com hash	Total de 64 caracteres
-ssalt	Definir salt	Limitada a 64 caracteres
-ghp	Obter hashpassword	
-gsalt	Obter salt	
-ep	Senha de criptografia (para backup/restauração)	Senha válida
-esalt	salt para senha criptografada	Somente para backup ou restauração
-r	Nome da função	Administrador, Operador, ReadOnly. Conforme listado no comando " <a href="#">Comando roles</a> " na página 123.
-clear	Apagar conta do usuário especificada	O número de índice da conta do usuário a ser apagado deve ser especificado, seguindo o formato: users -clear -user_index <b>Nota:</b> Se você estiver autorizado, poderá remover sua própria conta ou a conta de outros usuários, mesmo se eles se estiverem conectados, a menos que seja a única conta remanescente com privilégios de gerenciamento de contas de usuário. As sessões que já estiverem em andamento quando as contas de usuário forem excluídas não serão finalizadas automaticamente.
-curr	Exibir usuários atualmente com login efetuado	
-ai	Interface acessível ao usuário	web, ssh, redfish, ipmi, snmp, todos <b>Nota:</b> Um valor padrão (web ssh redfish) será definido se não houver nenhuma opção -ai.
-sauth	Protocolo de autenticação SNMPv3	Nenhum, HMAC_MD5, HMAC_SHA96, HMAC128_SHA224, HMAC192_SHA256, HMAC256_SHA384, HMAC384_SHA512
-spriv	Protocolo de privacidade do SNMPv3	Nenhum, CBC_DES, CFB128_AES128, AES192, AES256, AES192C, AES256C
-spw	Senha de privacidade do SNMPv3	Senha válida
-sepw	Senha de privacidade do SNMPv3 (criptografada)	Senha válida

Tabela 52. Opções users (continuação)

Opção	Descrição	Valores
-sacc	Tipo de acesso do SNMPv3	get
-strap1	Nome do host do trap SNMPv3 1	Nome do host válido
-strap2	Nome do host do trap SNMPv3 2	Nome do host válido
-strap3	Nome do host do trap SNMPv3 3	Nome do host válido
-pk	Exibir chave pública SSH para o usuário	Número de índice da conta do usuário. <b>Notas:</b> <ul style="list-style-type: none"> <li>• Cada chave SSH designada ao usuário é exibida, juntamente com um número de índice de chave de identificação.</li> <li>• Ao usar as opções de chave pública SSH, a opção -pk deve ser usada após o índice de usuário (opção -userindex), no formato: users -2 -pk.</li> <li>• Todas as chaves estão no formato OpenSSH.</li> </ul>
<b>As opções a seguir são usadas junto com -pk</b>		
-e	Exibir uma chave SSH inteira no formato OpenSSH <b>(opção de chave pública SSH)</b>	Essa opção não usa argumentos e deve ser usada exclusiva de todas as outras opções users -pk. <b>Nota:</b> Ao usar as opções de chave pública SSH, a opção -pk deve ser usada após o índice de usuário (opção -userindex), no formato: users -2 -pk -e.
-remove	Remover chave pública SSH do usuário <b>(opção de chave pública SSH)</b>	O número de índice de chave pública a ser removido deve ser fornecido como um -key_index ou -all específico para todas as chaves designadas ao usuário. <b>Nota:</b> Ao usar as opções de chave pública SSH, a opção -pk deve ser usada após o índice de usuário (opção -userindex), no formato: users -2 -pk -remove -1.
-add	Incluir chave pública SSH para o usuário <b>(opção de chave pública SSH)</b>	Chave delimitada por aspas no formato OpenSSH <b>Notas:</b> <ul style="list-style-type: none"> <li>• A opção -add é de uso exclusivo de todas as outras opções de comando users -pk.</li> <li>• Ao usar as opções de chave pública SSH, a opção -pk deve ser usada após o índice de usuário (opção -userindex), no formato: users -2 -pk -add "AAAAB3NzC1yc2EAAAABIwAAAQEAvgfTUzRF7pdBuaBy4d0/aIFasa/Gtc+o/wlZnuC4aDHMA1UmnMyLOCiIaN0y400ICEKcKjKEhrYymtAoVtFKApv Y39GpnSGRC/qcLGWLM4cmirKL5kxHNOqIcwbT1NPceoKH j46X7E+mqLfnAhhjDpcVFjagM3Ek2y7w/tBGwGgN7DPHJU1tzcJy68mEAnIrzjUoR98Q3/B9cJD77ydGKe8rPdI2hIEpXR5dNUiupA1Yd8PSSMgdukASKEd3eRRZTBL3SATMucUsTkYjLXcqex10Qz4+N5OR6MbNcwlx+mTEAvvcPjhuga70UNPGhLJML6k7jeJiQ8Xd2p Xb0ZQ=="</li> </ul>

Tabela 52. Opções users (continuação)

Opção	Descrição	Valores
-upld	Fazer upload de uma chave pública SSH no formato OpenSSH ou RFC4716 <b>(opção de chave pública SSH)</b>	Requer as opções -i e -l para especificar o local da chave. <b>Notas:</b> <ul style="list-style-type: none"> <li>A opção -upld é usada exclusiva de todas as outras opções de comando users -pk (exceto -i e -l).</li> <li>Para substituir por uma nova chave, você deve especificar um -key_index. Para incluir uma chave no final da lista de chaves atuais, não especifique um índice de chave.</li> <li>Ao usar as opções de chave pública SSH, a opção -pk deve ser usada após o índice de usuário (opção -userindex), no formato: users -2 -pk -upld -i tftp://9.72.216.40/ -l file.key.</li> </ul>
-dnld	Baixar a chave pública SSH especificada para um servidor TFTP/SFTP <b>(opção de chave pública SSH)</b>	Requer um -key_index para especificar a chave para baixar e as opções -i e -l para especificar o local de download em outro computador que esteja executando um servidor TFTP. <b>Notas:</b> <ul style="list-style-type: none"> <li>A opção -dnld é usada exclusiva de todas as outras opções de comando users -pk (exceto -i, -l e -key_index).</li> <li>Ao usar as opções de chave pública SSH, a opção -pk deve ser usada após o índice de usuário (opção -userindex), no formato: users -2 -pk -dnld -1 -i tftp://9.72.216.40/ -l file.key.</li> </ul>
-i	Endereço IP do servidor TFTP/SFTP para fazer upload ou fazer o downloading de um arquivo-chave <b>(opção de chave pública SSH)</b>	Endereço IP válido <b>Nota:</b> A opção -i é exigida pelas opções de comando users -pk -upld e users -pk -dnld.
-pn	Número da porta do servidor TFTP/SFTP <b>(opção de chave pública SSH)</b>	Número da porta válido (padrão 69/22) <b>Nota:</b> Um parâmetro opcional para as opções de comando users -pk -upld e users -pk -dnld.
-u	Nome de usuário para o servidor SFTP <b>(opção de chave pública SSH)</b>	Nome de usuário válido <b>Nota:</b> Um parâmetro opcional para as opções de comando users -pk -upld e users -pk -dnld.
-pw	Senha para o servidor SFTP <b>(opção de chave pública SSH)</b>	Senha válida <b>Nota:</b> Um parâmetro opcional para as opções de comando users -pk -upld e users -pk -dnld.
-l	Nome do arquivo para fazer upload ou fazer download de um arquivo-chave via TFTP ou SFTP <b>(opção de chave pública SSH)</b>	Nome do arquivo válido <b>Nota:</b> A opção -l é exigida pelas opções de comando users -pk -upld e users -pk -dnld.

Tabela 52. Opções users (continuação)

Opção	Descrição	Valores
-af	Aceitar conexões do host <b>(opção de chave pública SSH)</b>	Uma lista separada por vírgula de nomes de host e endereços IP, limitada a 511 caracteres. Os caracteres válidos incluem: alfanumérico, vírgula, asterisco, ponto de interrogação, ponto de exclamação, ponto, hífen dois-pontos e sinal de percentual.
-cm	Comentário <b>(opção de chave pública SSH)</b>	Sequência limitada por aspas de até 255 caracteres. <b>Nota:</b> Ao usar as opções de chave pública SSH, a opção -pk deve ser usada após o índice de usuário (opção -userindex), no formato: users -2 -pk -cm "This is my comment.".

**Exemplo:**

```
system> users
```

```
Login ID      Name      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
```

```
Login ID      Name      Advanced Attribute  Role      Password Expires
-----
1            USERID      Native      Administrator      90 day(s)
2            sptest      Native      Administrator      Password expired
```

```
system> hashpw -sw enabled -re enabled
```

```
system> users -5 -n guest5 -shp 292bcbc41bb078cf5bd258db60b63a4b337c8c954409442cfad7148bc6428fee --salt abc -r Administrator
```

```
system> users -5 ghp
```

```
292bcbc41bb078cf5bd258db60b63a4b337c8c954409442cfad7148bc6428fee
```

```
system> users -5 gsalt
```

```
abc
```

```
system>
```

## Comandos de controle do IMM

Este tópico fornece uma lista alfabética dos comandos CLI de controle do IMM.

Atualmente, há 7 comandos de controle do IMM:

### Comando batch

Use esse comando batch para executar um ou mais comandos CLI que estão contidos em um arquivo.

**Notas:**

- As linhas de comentário no arquivo em lote iniciam com um #.
- Ao executar um arquivo em lote, os comandos que falham são retornados juntamente com um código de retorno de falha.
- Os comandos de arquivo em lote que contêm opções de comando não reconhecidas podem gerar avisos.

**Sintaxe:**

```
batch [-options]
```

Tabela 53. Opções batch

Opção	Descrição	Valores
-f	Nome do arquivo em lote	Nome do arquivo válido
-ip	Endereço IP do servidor TFTP/SFTP	Endereço IP válido
-pn	Número da porta do servidor TFTP/SFTP	Número da porta válido (padrão 69/22)
-u	Nome de usuário para o servidor SFTP	Nome de usuário válido
-pw	Senha para o servidor SFTP	Senha válida

Exemplo:

```
system> batch -f sslcfg.cli -ip 192.168.70.200
1 : sslcfg client dnld ip 192.168.70.20
Command total/errors/warnings: 8 / 1 / 0
system>
```

## Comando clock

Use esse comando para exibir a data e hora atuais. Você pode definir as configurações de deslocamento UTC e horário de verão.

Sintaxe:

```
clock [-options]
```

Tabela 54. Opções clock

Opção	Descrição	Valores
-u	Deslocamento UTC	Configurações especiais de horário de verão com deslocamento UTC de +2, -7, -6, -5, -4 e -3 são necessárias. <ul style="list-style-type: none"> <li>Para +2, as opções de horário de verão são as seguintes: off, ee (Zona Oriental da Europa), tky (Turquia), bei (Beirute), amm (Amã), jem (Jerusalém).</li> <li>Para -7, as configurações de horário de verão são as seguintes: off, mtn (Montanhas), maz (Mazatlan).</li> <li>Para -6, as configurações de horário de verão são as seguintes: off, mex (México), cna (América do Norte Central).</li> <li>Para -5, as configurações de horário de verão são as seguintes: off, cub (Cuba), ena (Zona Oriental da América do Norte).</li> <li>Para -4, as configurações de horário de verão são as seguintes: off, asu (Assunção), cui (Cuiabá), san (Santiago), cat (Canadá - Atlântico).</li> <li>Para -3, as configurações de horário de verão são as seguintes: off, gtb (Godthab), bre (Brasil - Leste).</li> </ul>
-dst	Horário de verão	ligado, desligado, caso especial
-host	Formato de hora obtido do host (padrão: utc)	local, utc <b>Nota:</b> Sistemas Windows usam local; Linux usa utc

**Notas:**

- O BMC obtém a hora do servidor host ou do servidor NTP.

- A hora obtida do host pode ser a hora local ou a hora UTC. A opção host deve ser definida como UTC se o NTP não estiver sendo utilizado e o host usar o formato UTC.
- O deslocamento UTC pode estar no formato +0200, +2:00, +2 ou 2, para deslocamentos positivos, e -0500, -5:00 ou -5, para deslocamentos negativos.
- O deslocamento UTC e o horário de verão são usados com NTP ou quando o modo do host está em UTC.

Exemplo:

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

## Comando info

Use esse comando para exibir e configurar informações sobre o BMC.

Sintaxe:

```
info [-options]
```

Tabela 55. Opções info

Opção	Descrição	Valores
-name	Nome do BMC	Sequência
-contact	Nome da pessoa de contato do BMC	Sequência
-location	Local do BMC	Sequência
-postal	Endereço postal completo da BMC	Sequência
-room	Identificador de sala do BMC	Sequência
-rack	Identificador de rack do BMC	Sequência
-rup	Posição do BMC no rack	Sequência

Exemplo:

```
system> info
-name: BMCName
-location: location
-contact: contact
-rack: rack
-room: room
-postal: postal
-rup: 1
system>
```

## Comando spreset

Use esse comando para reiniciar o IMM.

Você deve ter pelo menos autoridade de Configuração de Adaptador Avançada para emitir esse comando.

Sintaxe:

```
spreset
```

---

## Comandos sem agente

Este tópico fornece uma lista alfabética dos comandos sem agente.

Atualmente, há três comandos sem agente:

## Comando storage

Use esse comando para exibir e configurar (se suportado pela plataforma) informações sobre os dispositivos de armazenamento do servidor que são gerenciados pelo IMM.

Sintaxe:

storage [-options]

Tabela 56. Opções storage

Opção	Descrição	Valores
-list	Lista os destinos de armazenamento gerenciados pelo IMM.	<b>controllers pools volumes drives</b> <ul style="list-style-type: none"> <li>• controllers: lista os controladores RAID suportados<sup>1</sup></li> <li>• pools: lista os conjuntos de armazenamentos associados ao controlador RAID<sup>1</sup></li> <li>• volumes: lista os volumes de armazenamento associados ao controlador RAID<sup>1</sup></li> <li>• drives: lista as unidades de armazenamento associadas ao controlador RAID<sup>1</sup></li> </ul>
-list storage targets -target target_id	Lista os <b>destinos</b> de armazenamento gerenciados pelo IMM de acordo com o <b>target_id</b> .	<b>pools volumes drives e ctrl[x] pool[x]</b> Em que <b>storage targets</b> e <b>target_id</b> são: <ul style="list-style-type: none"> <li>• <b>pools</b> e <b>ctrl[x]</b>: listam os conjuntos de armazenamentos associados ao controlador RAID, com base no target_id<sup>1</sup></li> <li>• <b>volumes</b> e <b>ctrl[x] pool[x]</b>: listam os volumes de armazenamento associados ao controlador RAID, com base no target_id<sup>1</sup></li> <li>• <b>drives</b> e <b>ctrl[x] pool[x]</b>: listam as unidades de armazenamento associadas ao controlador RAID, com base no target_id<sup>1</sup></li> </ul>
-list devices	Exibe o status de todos os discos gerenciados pelo IMM.	
-show target_id	Exibe informações para o destino selecionado que é gerenciado pelo IMM.	Em que <b>target_id</b> é <b>ctrl[x] vol[x] disk[x] pool[x]</b> <sup>3</sup>
-show target_id info	Exibe informações detalhadas para o destino selecionado que é gerenciado pelo IMM.	Em que <b>target_id</b> é <b>ctrl[x] vol[x] disk[x] pool[x]</b> <sup>3</sup>
-show target_id firmware <sup>3</sup>	Exibe as informações de firmware para o destino selecionado que é gerenciado pelo IMM.	Em que <b>target_id</b> é <b>ctrl[x] disk[x]</b> <sup>2</sup>
-showinfo nvme	Exibe informações de firmware do disco NVME.	
-wthre show	Exibe o limite de desgaste do SSD crítico e de aviso.	Valor limite (1 a 99)
-wthre -ct <b>valor limite</b>	Define o limite crítico de desgaste do SSD.	Valor limite (1 a 99)

Tabela 56. Opções storage (continuação)

Opção	Descrição	Valores
-wthre -wt <b>valor limite</b>	Define o limite de aviso de desgaste do SSD.	Valor limite (1 a 99) <b>Nota:</b> O valor de aviso precisa ser maior que o crítico.
-config ctrl -scanforgn -target <b>target_id</b> <sup>3</sup>	Detecta a configuração externa de RAID.	Em que <b>target_id</b> é <b>ctrl[x]</b> <sup>5</sup>
-config ctrl -imptforgn -target <b>target_id</b> <sup>3</sup>	Importa a configuração externa de RAID.	Em que <b>target_id</b> é <b>ctrl[x]</b> <sup>5</sup>
-config ctrl -clrforgn -target <b>target_id</b> <sup>3</sup>	Limpa a configuração externa de RAID.	Em que <b>target_id</b> é <b>ctrl[x]</b> <sup>5</sup>
-config ctrl -clrcfg -target <b>target_id</b> <sup>3</sup>	Limpa a configuração de RAID.	Em que <b>target_id</b> é <b>ctrl[x]</b> <sup>5</sup>
-config ctrl -bootdevice -vd <b>volume</b> -target <b>target_id</b>	Define o dispositivo de inicialização por volume.	Em que <b>target_id</b> é <b>ctrl[x]</b> e <b>volume</b> é um valor na primeira coluna de saída de "list volumes".
-config ctrl -bootdevice -pd <b>drive</b> -target <b>target_id</b>	Define o dispositivo de inicialização por unidade.	Em que <b>target_id</b> é <b>ctrl[x]</b> e <b>drive</b> é um valor na primeira coluna da saída "list drives".
-config ctrl -bootdevice -index <b>index</b> -target <b>target_id</b>	Define o dispositivo de inicialização por índice.	Em que <b>target_id</b> é <b>ctrl[x]</b> e <b>index</b> é um valor em "[]" que é a saída da opção "display".
-config ctrl -bootdevice -display -target <b>target_id</b>	Mostra o dispositivo inicializável.	
-config drv -mkoffline -target <b>target_id</b> <sup>3</sup>	Altera o estado da unidade de online para offline.	Em que <b>target_id</b> é <b>disk[x]</b> <sup>5</sup>
-config drv -mkonline -target <b>target_id</b> <sup>3</sup>	Altera o estado da unidade de offline para online.	Em que <b>target_id</b> é <b>disk[x]</b> <sup>5</sup>
-config drv -mkmissing -target <b>target_id</b> <sup>3</sup>	Marca a unidade offline como uma unidade válida não configurada.	Em que <b>target_id</b> é <b>disk[x]</b> <sup>5</sup>
-config drv -prprm -target <b>target_id</b> <sup>3</sup>	Prepara uma unidade válida não configurada para remoção.	Em que <b>target_id</b> é <b>disk[x]</b> <sup>5</sup>
-config drv -undoprprm -target <b>target_id</b> <sup>3</sup>	Cancela a preparação de uma unidade válida não configurado para operação de remoção.	Em que <b>target_id</b> é <b>disk[x]</b> <sup>5</sup>
-config drv -mkbad -target <b>target_id</b> <sup>3</sup>	Altera a unidade válida não configurada para uma unidade inválida não configurada.	Em que <b>target_id</b> é <b>disk[x]</b> <sup>5</sup>
-config drv -mkgood -target <b>target_id</b> <sup>3</sup>	Altera uma unidade inválida não configurada para uma unidade válida não configurada. ou Converte a unidade JBOD para uma unidade válida não configurada.	Em que <b>target_id</b> é <b>disk[x]</b> <sup>5</sup>
-config drv -mkjbod -target <b>target_id</b> <sup>3</sup>	Configure o válido não configurado como JBOD.	Em que <b>target_id</b> é <b>disk[x]</b> <sup>5</sup>

Tabela 56. Opções storage (continuação)

Opção	Descrição	Valores
-config drv -rebuild -target <b>target_id</b> <sup>3</sup>	Inicie a reconstrução da unidade.	Em que <b>target_id</b> é <b>disk[x]</b> <sup>5</sup>
-config drv -addhsp -target <b>target_id</b> <sup>3</sup>	Designa a unidade selecionada como hot spare a um controlador ou conjuntos de armazenamento existentes.	Em que <b>target_id</b> é <b>disk[x]</b> <sup>5</sup>
-config drv -dedicated pools -target <b>target_id</b> <sup>3</sup>	Atribua a unidade como hot spare dedicada aos pools de armazenamento selecionados.	Em que <b>target_id</b> é <b>disk[x]</b> <sup>5</sup>
-config drv -rmhsp -target <b>target_id</b> <sup>3</sup>	Remove a host spare.	Em que <b>target_id</b> é <b>disk[x]</b> <sup>5</sup>
-config vol -remove -target <b>target_id</b> <sup>3</sup>	Remove um volume.	Em que <b>target_id</b> é <b>vol[x]</b> <sup>5</sup>
-config vol -set [-N] [-w] [-r ] [-i] [-a] [-d] [-b] -target <b>target_id</b> <sup>3</sup>	Modifica as propriedades de um volume.	<ul style="list-style-type: none"> <li>• [-N <b>volume_name</b>] é o nome do volume</li> <li>• [-w &lt;0 1 2 3&gt;] é a política de gravação de cache: <ul style="list-style-type: none"> <li>– Digite <b>0</b> para a política de gravação de cache</li> <li>– Digite <b>1</b> para a política de write-back protegida</li> <li>– Digite <b>2</b> para a política de write-back não protegida</li> <li>– Digite <b>3</b> para nenhuma política</li> </ul> </li> <li>• [-r &lt;0 1&gt;] é a política de leitura de cache: <ul style="list-style-type: none"> <li>– Digite <b>0</b> para a política Nenhuma leitura antecipada</li> <li>– Digite <b>1</b> para a política Leitura antecipada</li> </ul> </li> <li>• [-i &lt;0 1&gt;] é a política de E/S de cache: <ul style="list-style-type: none"> <li>– Digite <b>0</b> para a política de E/S direta</li> <li>– Digite <b>1</b> para a política de E/S em cache</li> </ul> </li> <li>• [-a &lt;0 2 3&gt;] é a política de acesso: <ul style="list-style-type: none"> <li>– Digite <b>0</b> para a política Leitura e gravação</li> <li>– Digite <b>2</b> para a política Somente leitura</li> <li>– Digite <b>3</b> para a política Bloqueada</li> </ul> </li> <li>• [-d &lt;0 1 2&gt;] é a política de cache de disco: <ul style="list-style-type: none"> <li>– Digite <b>0</b> se a política estiver inalterada</li> <li>– Digite <b>1</b> para habilitar a política<sup>6</sup></li> <li>– Digite <b>2</b> para desabilitar a política</li> </ul> </li> <li>• [-b &lt;0 1&gt;] é a inicialização em segundo plano: <ul style="list-style-type: none"> <li>– Digite <b>0</b> para habilitar a inicialização</li> <li>– Digite <b>1</b> para desabilitar a inicialização</li> </ul> </li> <li>• <b>-target_id</b> é <b>vol[x]</b><sup>5</sup></li> </ul>

Tabela 56. Opções storage (continuação)

Opção	Descrição	Valores
-config vol -add [-R] [-D disk] [-H disk] [-1 hole] [-N] [-w] [-r] <sup>3, 7</sup>	<p>Cria um volume para um novo conjunto de armazenamento quando o destino é um controlador.</p> <p>ou</p> <p>Cria um volume com um conjunto de armazenamento existente quando o destino é um conjunto de armazenamento.</p>	<ul style="list-style-type: none"> <li>• [-R &lt;0 1 5 1E 6 10 50 60 00&gt;] Essa opção define o nível de RAID e só é usada com um novo conjunto de armazenamento</li> <li>• [-D disk [id11]:disk[id12]:...disk[id21]:disk[id22]:...] Essa opção define o grupo da unidade (incluindo distribuições) e é usada apenas com um novo conjunto de armazenamento</li> <li>• [-H disk [id1]:disk[id2]:...] Essa opção define o grupo de hot spare e é usada apenas com um novo conjunto de armazenamentos</li> <li>• [-1 hole] Essa opção define o número de índice do espaço livre para um conjunto de armazenamento existente</li> <li>• [-N volume_name] é o nome do volume</li> <li>• [-w &lt;0 1 2 3&gt;] é a política de gravação de cache: <ul style="list-style-type: none"> <li>– Digite 0 para a política de gravação de cache</li> <li>– Digite 1 para a política de write-back protegida</li> <li>– Digite 2 para a política de write-back não protegida</li> <li>– Digite 3 para nenhuma política</li> </ul> </li> <li>• [-r &lt;0 1&gt;] é a política de leitura de cache: <ul style="list-style-type: none"> <li>– Digite 0 para a política Nenhuma leitura antecipada</li> <li>– Digite 1 para a política Leitura antecipada</li> </ul> </li> </ul>
-config vol -add[-i] [-a] [-d] [-f] [-S] [-P] -target target_id <sup>3</sup>	<p>Cria um volume para um novo conjunto de armazenamento quando o destino é um controlador.</p> <p>ou</p> <p>Cria um volume com um conjunto de armazenamento existente quando o destino é um conjunto de armazenamento.</p>	<ul style="list-style-type: none"> <li>• [-i &lt;0 1&gt;] é a política de E/S de cache: <ul style="list-style-type: none"> <li>– Digite 0 para a política de E/S direta</li> <li>– Digite 1 para a política de E/S em cache</li> </ul> </li> <li>• [-a &lt;0 2 3&gt;] é a política de acesso: <ul style="list-style-type: none"> <li>– Digite 0 para a política Leitura e gravação</li> <li>– Digite 2 para a política Somente leitura</li> <li>– Digite 3 para a política Bloqueada</li> </ul> </li> <li>• [-d &lt;0 1 2&gt;] é a política de cache de disco: <ul style="list-style-type: none"> <li>– Digite 0 se a política permanecer inalterada</li> <li>– Digite 1 para habilitar a política<sup>6</sup></li> <li>– Digite 2 para desabilitar a política</li> </ul> </li> <li>• [-f &lt;0 1 2&gt;] é o tipo de inicialização: <ul style="list-style-type: none"> <li>– Digite 0 para nenhuma inicialização</li> <li>– Digite 1 para inicialização rápida</li> <li>– Digite 2 para inicialização completa</li> </ul> </li> <li>• [-S volume_size] é o tamanho do novo volume em MB</li> </ul>

Tabela 56. Opções storage (continuação)

Opção	Descrição	Valores
		<ul style="list-style-type: none"> <li>[-P <b>strip_size</b>] é o tamanho da faixa de volume, por exemplo, 512B, 4K, 128K, 1M e assim por diante</li> <li>-target <b>target_id</b> é: <ul style="list-style-type: none"> <li>- <b>ctrl[x]</b> (novo conjunto de armazenamentos)<sup>5</sup></li> <li>- <b>pool[x]</b> (conjunto de armazenamento existente)<sup>5</sup></li> </ul> </li> </ul>
-config vol -getfreecap [-R] [-D disk] [-H disk] -target <b>target_id</b> <sup>3</sup>	Obtém a quantidade livre de capacidade do grupo de unidades.	<ul style="list-style-type: none"> <li>[-R &lt;0 1 5 1E 6 10 50 60 00&gt;] Essa opção define o nível de RAID e só é usada com um novo conjunto de armazenamento</li> <li>[-D disk <b>[id1]:[id2]:...[id21]:[id22]:...</b>] Essa opção define o grupo da unidade (incluindo distribuições) e é usada apenas com um novo conjunto de armazenamento</li> <li>[-H disk <b>[id1]:[id2]:...</b>]Essa opção define o grupo de hot spare e é usada apenas com um novo conjunto de armazenamento</li> <li>-target <b>target_id</b> é <b>ctrl[x]</b><sup>5</sup></li> </ul>
-fgi vol[ <b>idx</b> ]	Inicializar rapidamente os volumes especificados	Em que vol[ <b>idx</b> ] é vol[ <b>id1</b> ],vol[ <b>id2</b> ]:...
-help	Exibir o uso e as opções do comando	
<p><b>Notas:</b></p> <ol style="list-style-type: none"> <li>1. Esse comando é suportado apenas em servidores nos quais o IMM pode acessar o controlador RAID.</li> <li>2. As informações de firmware são exibidas apenas para controladores associados, discos e Flash DIMMs. As informações de firmware para conjuntos e volumes associados não são exibidas.</li> <li>3. As informações são exibidas em várias linhas devido a limitações de espaço.</li> <li>4. Esse comando é suportado somente em servidores que oferecem suporte a logs RAID.</li> <li>5. Esse comando é suportado somente em servidores que oferecem suporte a configurações RAID.</li> <li>6. O valor <b>Enable</b> não oferece suporte a configurações de nível RAID 1.</li> <li>7. Uma lista parcial de opções disponíveis é fornecida aqui. As outras opções para o comando <b>storage -config vol -add</b> são listadas na linha a seguir.</li> </ol>		

**Exemplos:**

```

system> storage -config ctrl -clrcfg -target ctrl[0]
ok
system>
system> storage -config ctrl -clrforgn -target ctrl[0]
ok
system>
system> storage -config ctrl -imptforgn -target ctrl[0]
ok
system>
system> storage -config ctrl -scanforgn -target ctrl[0]
Detect 1 foreign configuration(s) on controller ctrl[0]
system>
system> storage -config drv -addhsp -dedicated pool[0-1] -target disk[0-0]
ok
system>
system> storage -config drv -addhsp -target disk[0-0]
ok

```

```

system>
system> storage -config drv -mkbad -target disk[0-0]
ok
system>
system> storage -config drv -mkgood -target disk[0-0]
ok
system>
system> storage -config drv -mkmissing -target disk[0-0]
ok
system>
system> storage -config drv -mkoffline -target disk[0-0]
ok
system>
system> storage -config drv -mkonline -target disk[0-0]
ok
system>
system> storage -config drv -prprm -target disk[0-0]
ok
system>
system> storage -config drv -rmhsp -target disk[0-0]
ok
system>
system> storage -config drv -undoprprm -target disk[0-0]
ok
system>
system> storage -config vol -add -1 1 -target pool[0-1]
ok
system>
system> storage -config vol -add -R 1 -D
disk[0-0]:disk[0-1] -w 1 -r 2 -i 0 -a 0 -d 0 -f 0
-N LD_volume -S 100000 -P 64K -H disk[0-2] -target ctrl[0]
ok
system>
system> storage -config vol -getfreecap -R 1 -D
disk[0-0]:disk[0-1] -H disk[0-2] -target ctrl[0]
The drive group configuration is good with free capacity 500000MB
system>
system> storage -config vol -remove -target vol[0-1]
ok
system>
system> storage -config vol -set -N LD_volume
-w 0 -target vol[0-0]
ok
system>
system> storage -list controllers
ctrl[0]    ServerRAID M5110e(Slot No. 0)
ctrl[1]    ServerRAID M5110f(Slot No. 1)
system>
system> storage -list drives
disk[0-0]  Drive 0
disk[0-1]  Drive 1
disk[0-2]  Drive 2
system>
system> storage -list pools
pool[0-0]  Storage Pool 0
pool[0-1]  Storage Pool 1
system>
system> storage -list volumes
vol[0-0]   Volume 0
vol[0-1]   Volume 1
Vol[0-2]   Volume 2

```

```

system>
system> storage -list drives -target ctrl[0]
disk[0-0]   Drive 0
disk[0-1]   Drive 1
disk[0-2]   Drive 2
system>
system> storage -list drives -target pool[0-0]
disk[0-0]   Drive 0
disk[0-1]   Drive 1
system>
system> storage -list pools -target ctrl[0]
pool[0-0]   Storage Pool 0
system>
system> storage -list volumes -target ctrl[0]
vol[0-0]    Volume 0
vol[0-1]    Volume 1
system>
system> storage -list volumes -target pool[0-0]
vol[0-0]    Volume 0
vol[0-1]    Volume 1
system>
system> storage -show ctrl[0] firmware
Total Firmware number: 2
Name: RAID Firmware1
Description: RAID Firmware
Manufacture: 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: HDD
Health Status: Normal
Capacity: 100.000GB
Speed: 6.0Gb/s
Current Temperature: 33C
Manufacture: ATA
Device ID: 5
Enclosure ID: 0x00FC
Machine Type:
Model:
Serial No.: 9XKJKL
FRU No.:
Part No.:
system>
system> storage -show pool[0-0]
RAID State: RAID 0
RAID Capacity: 67.000GB (0.000GB free)
Drives: 2
disk[0-0]    Drive 0
disk[0-1]    Drive 1
Volumes: 2
vol[0-0]     Volume 0
vol[0-1]     Volume 1
system>
system> storage -show pool[0-1] info
RAID State: RAID 1
RAID Capacity: 231.898GB (200.000GB free)
Holes: 2
#1 Free Capacity: 100.000GB
#2 Free Capacity: 100.000GB

Drives: 2
disk[0-1]    Drive 1
disk[0-2]    Drive 2

Volume: 1
vol[0-1]     LD_volume
system>
system> storage -show vol[0-0]
Name: Volume 0
Stripe Size: 64KB
Status: Offline
Capacity: 100.000GB
system>
system> storage -show vol[0-0] info
Name: LD_volume
Status: Optimal
Stripe Size: 64KB

```

```

Bootable: Not Bootable
Capacity: 231.898GB
Read Policy: No Read Ahead
Write Policy: Write Through
I/O Policy: Direct I/O
Access Policy: Read Write
Disk Cache Policy: Unchanged
Background Initialization: Enable
system>

```

## Comando adapter

Esse comando é usado para exibir informações sobre o inventário do adaptador PCIe.

Sintaxe:

```
adapter [-options]
```

Tabela 57. Opções adapter

Opção	Descrição	Valores
-list	Listar todos os adaptadores PCIe no servidor.	
-show <b>target_id</b>	Mostrar as informações detalhadas para o adaptador PCIe de destino.	<b>target_id [info firmware ports]</b> Onde: <ul style="list-style-type: none"> <li>• <b>info</b>: exibe as informações de hardware para o adaptador</li> <li>• <b>firmware</b>: exibe todas as informações de firmware para o adaptador</li> <li>• <b>ports</b>: exibe todas as informações da porta Ethernet para o adaptador</li> </ul>

Se o comando **adapter** não for suportado, o servidor responderá com a seguinte mensagem quando o comando for emitido:

```
Your platform does not support this command.
```

**Nota:** Se remover, substituir ou configurar qualquer adaptador, você deverá reiniciar o servidor (pelo menos uma vez) para visualizar as informações atualizadas do adaptador.

Exemplos:

```

system> adapter -list
ob-1    Flex System CN4054 10Gbps Virtual Fabric Adapter
ob-2    GPU Card 1
slot-1  Raid Controller 1
slot-2  Adapter 01:02:03
system>
system> adapter -show ob-1 info
Product Name: Flex System CN4054 10Gbps Virtual Fabric Adapter
Card Interface: PCIe x 16
Function Count: 2
Function Name: xxx Emulx xx component1
Segment Number: 2348
Bus Number: 23949
Device Number: 1334
Function Number: 21
Vendor Id: 12
Device Id: 33
Revision Id: 1

```

```
Class Code: 2
Sub Vendor: 334
Sub Device: 223
Slot Description: a slot
Slot Type: 23
Slot Data Bus Width: 0
Hot Plug: 12
PCI Type: 11
Blade Slot Port: xxx
UUID: 39302938485
Manufacturer: IBM
Serial Number: 998AAGG
Part Number: ADB233
Model: 345
Function Sku: 221
Fod Uid: 2355
Required Daughter: 0
Max Data Width: 0
Connector Layout: pci x
Package Type: dici
Function Name: xxx nVidia xx component2
Segment Number: 2348
Bus Number: 23949
Device Number: 1334
Function Number: 21
Vendor Id: 12
Device Id: 33
Revision Id: 1
Class Code: 2
Sub Vendor: 334
Sub Device: 223
Slot Description: a slot
Slot Type: 23
Slot Data Bus Width: 0
Hot Plug: 12
PCI Type: 11
Blade Slot Port: xxx
UUID: 39302938485
Manufacturer: IBM
Serial Number: 998AAGG
Part Number: ADB233
Model: 345
Function Sku: 221
Fod Uid: 2355
Required Daughter: 0
Max Data Width: 0
Connector Layout: pci x
Package Type: dici
system>
```

---

## Comandos de suporte

Este tópico fornece uma lista alfabética de comandos de suporte.

Existe apenas um comando de suporte: o "[Comando dbgshbmc](#)" na página 152.

## Comando dbgshbmc

Use esse comando para desbloquear o acesso à rede ao shell de depuração seguro.

**Nota:** Este comando costumava ser o comando **dbgshimm**.

**Importante:** Este comando destina-se apenas para uso pela equipe de suporte.

A tabela a seguir mostra os argumentos das opções.

Sintaxe:

```
dbgshbmc [subset_command]
```

*Tabela 58. Comandos de subconjunto dbgshbmc*

<b>Opção</b>	<b>Descrição</b>
status	Exibir status
enable	Habilitar acesso de depuração (padrão se nenhuma opção for especificada)
disable	Desabilitar acesso de depuração



---

## Capítulo 11. Interface IPMI

Este capítulo descreve a interface IPMI suportada pelo XClarity Controller.

Para obter detalhes dos comandos IPMI padrão, consulte o documento Especificação de Intelligent Platform Management Interface (IPMI) (versão 2.0 ou superior). Este documento fornece descrições dos parâmetros OEM usados com os comandos IPMI e OEM IPMI padrão suportados pelo firmware do XClarity Controller.

---

### Gerenciando o XClarity Controller com a IPMI

Use as informações neste tópico para gerenciar o XClarity Controller usando a Intelligent Platform Management Interface (IPMI).

O XClarity Controller é fornecido com o ID do usuário definido inicialmente como um nome de usuário USERID e uma senha PASSWORD (com um zero, não a letra O). Esse usuário tem acesso de Supervisor.

**Importante:** Altere esse nome de usuário e senha durante a configuração inicial para segurança aprimorada.

Em um Flex System, um usuário poderá configurar um Flex System CMM para gerenciar centralmente as contas de usuários ad IPMI do XClarity Controller. Nessa circunstância, você talvez não seja capaz de acessar o XClarity Controller usando o IPMI até que o CMM tenha configurado os IDs de usuário do IPMI.

**Nota:** As credenciais do ID do usuário configuradas pelo CMM podem ser diferentes da combinação USERID/PASSWORD descrita acima. Se nenhum ID de usuário do IPMI tiver sido configurado pelo CMM, a porta de rede associada ao protocolo IPMI será fechada.

O XClarity Controller também fornece os recursos de gerenciamento do servidor remoto IPMI a seguir:

#### Interfaces da linha de comandos IPMI

A interface de linha de comando IPMI fornece acesso direto às funções de gerenciamento do servidor por meio do protocolo IPMI 2.0. É possível usar o IPMItool para emitir comandos para controlar a energia do servidor, visualizar informações do servidor e identificar o servidor. Para obter mais informações sobre o IPMItool, consulte "[Usando o IPMItool](#)" na página 155.

#### Serial over LAN

Para gerenciar servidores a partir de um local remoto, use o IPMItool para estabelecer uma conexão Serial over LAN (SOL). Para obter mais informações sobre o IPMItool, consulte "[Usando o IPMItool](#)" na página 155.

---

### Usando o IPMItool

Use as informações neste tópico para acessar informações sobre o IPMItool.

O IPMItool fornece várias ferramentas que podem ser usadas para gerenciar e configurar um sistema IPMI. É possível usar o IPMItool dentro ou fora da faixa para gerenciar e configurar o XClarity Controller.

Para obter mais informações sobre o IPMItool ou baixá-lo, acesse <https://github.com/ipmitool/ipmitool>.

---

## Comandos IPMI com parâmetros OEM

### Obter/definir parâmetros de configuração LAN

Para refletir os recursos fornecidos pelo XCC para algumas das configurações de rede, os valores de alguns dos dados de parâmetro são definidos como mostrado a seguir.

#### DHCP

Além dos métodos comuns de obter um endereço IP, o XCC fornece um modo pelo qual ele tenta obter um endereço IP de um servidor DHCP por um determinado período e se houve falha ao usar um endereço IP estático.

A tabela a seguir é uma tabela de três colunas e várias linhas que consiste nas opções, descrições das opções e os valores associados das opções.

Parâmetro	#	Dados de parâmetro
Origem de endereço IP	4	<u>dados 1</u>  [7:4] – reservado  [3:0] – origem de endereço 0h = não especificado 1h = endereço estático (configurado manualmente) 2h = endereço obtido pelo XCC executando DHCP 3h = endereço obtido pelo BIOS ou pelo software do sistema 4h = endereço obtido pelo XCC executando outro protocolo de atribuição de endereço.  O XCC usa o valor 4h para indicar o modo de endereço do DHCP com failover para estático.

#### Seleção de interface Ethernet

O hardware XCC contém MACs duplos Ethernet 10/100 com interfaces RMII. O hardware XCC também contém MACs duplos Ethernet de 1 Gbps com interfaces RGMII. Um dos MACs normalmente é conectado à NIC do servidor compartilhado e o outro é usado como uma porta dedicada de gerenciamento do sistema. Apenas uma porta Ethernet em um servidor está ativa em um determinado momento. Ambas as portas não estarão habilitadas simultaneamente.

Em alguns servidores, os designers do sistema podem optar por conectar somente uma ou outra interface Ethernet no planar do sistema. Nesses sistemas, somente a interface Ethernet que está conectada no planar é suportada pelo XCC. Uma solicitação para usar a porta não conectada retorna um código de conclusão CCh.

Os IDS de pacote para todas as placas de rede opcionais são numerados da seguinte maneira:

- placa opcional N°1, ID do pacote = 03h (eth2),
- placa opcional N°2, ID do pacote = 04h (eth3),

A tabela a seguir é uma tabela de três colunas e várias linhas que consiste nas opções, descrições das opções e os valores associados das opções.

Parâmetro	#	Dados de parâmetro
<p>Parâmetro OEM</p> <p>Esse número de parâmetro é usado pelo XCC para indicar qual das possíveis portas Ethernet (pacotes lógicos) deve ser usada.</p> <p>Esse parâmetro no comando Obter/definir parâmetros de configuração LAN não usa um seletor de conjunto, nem requer um seletor de bloco, portanto, esses campos devem ser definidos como 00h.</p> <p>Os dados de resposta retornarão 3 bytes ou, opcionalmente, 4 bytes se o dispositivo estiver em um pacote NCSI.</p> <p>Byte 1 = código de conclusão  Byte 2 = revisão  Byte 3 = 00h para eth0 ou 01h para eth1 etc...  Byte 4 = (opcional) número do canal, se o dispositivo for um pacote NCSI</p>	C0h	<p><u>data1</u></p> <p>00h = eth0  01h = eth1  02h = eth2  etc...</p> <p>FFh = desabilitar todas as portas de rede externas</p> <p>O XCC oferece suporte a um segundo byte de dados opcional para especificar qual canal em um pacote é usado</p> <p><u>data2</u></p> <p>00h = canal 0  01h = canal 1  etc...</p> <p>Se data2 não for especificado na solicitação, o canal 0 será assumido</p>

O byte data1 é usado para especificar o pacote lógico. Pode ser uma NIC dedicada de gerenciamento de sistemas ou uma interface NCSI na NIC compartilhada com o servidor.

O byte data2 é usado para especificar o canal para o pacote lógico, se o pacote for um dispositivo NCSI. Se data2 não for especificado na solicitação e o pacote lógico for um dispositivo NCSI, o canal 0 será assumido. Se data2 não for especificado na solicitação mas o pacote lógico não for um dispositivo NCSI, as informações do canal serão ignoradas.

Exemplos:

Apêndice A. Se o canal 2 da NIC compartilhada no planar (ID do pacote = 0, eth0) for usado como a porta de gerenciamento, os dados de entrada serão: 0xC0 0x00 0x02

Apêndice B: se o primeiro canal da primeira placa de rede tipo mezanino for usado, a entrada será: 0xC0 0x02 0x0

### Ativação/desativação de Ethernet sobre USB

O parâmetro a seguir é usado para habilitar ou desabilitar a interface de banda do XCC.

A tabela a seguir é uma tabela de três colunas e várias linhas que consiste nas opções, descrições das opções e os valores associados das opções.

Parâmetro	#	Dados de parâmetro
<p>Parâmetro OEM</p> <p>(Esse número de parâmetro é usado pelo XCC para habilitar ou desabilitar a interface Ethernet sobre USB.)</p> <p>Esse parâmetro no comando Obter parâmetros de configuração LAN não usa um seletor de conjunto, nem requer um seletor de bloco, portanto, esses campos devem ser definidos como 00h.</p> <p>Os dados de resposta retornarão 3 bytes:</p> <p>Byte 1 = código de conclusão</p> <p>Byte 2 = revisão</p> <p>Byte 3 = 00h (desabilitado) ou 01h (habilitado)</p>	C1h	<p><u>dados 1</u></p> <p>0x00 = desabilitado</p> <p>0x01 = habilitado</p>

O byte data1 é usado para especificar o pacote lógico. Pode ser uma NIC dedicada de gerenciamento de sistemas ou uma interface NCSI na NIC compartilhada com o servidor.

O byte data2 é usado para especificar o canal para o pacote lógico, se o pacote for um dispositivo NCSI. Se data2 não for especificado na solicitação e o pacote lógico for um dispositivo NCSI, o canal 0 será assumido. Se data2 não for especificado na solicitação mas o pacote lógico não for um dispositivo NCSI, as informações do canal serão ignoradas.

Exemplos:

Apêndice A: Se o canal 2 da NIC compartilhada no planar (ID do pacote = 0, eth0) for usado como a porta de gerenciamento, os dados de entrada serão: 0xC0 0x00 0x02

Apêndice B: se o primeiro canal da primeira placa de rede tipo mezanino for usado, a entrada será: 0xC0 0x02 0x0

### Opção de IPMI para obter o DUID-LLT

Um valor somente leitura adicional que precisa ser exposto via IPMI é o DUID. De acordo com o RFC3315, esse formato de DUID é baseado no endereço da camada de link mais o tempo.

Parâmetro	#	Dados de parâmetro
<p>Parâmetro OEM</p> <p>(Esse número de parâmetro é usado pelo XCC para habilitar ou desabilitar a interface Ethernet sobre USB.)</p> <p>Esse parâmetro no comando Obter parâmetros de configuração LAN não usa um seletor de conjunto, nem requer um seletor de bloco, portanto, esses campos devem ser definidos como 00h.</p> <p>Os dados de resposta retornarão 3 bytes:</p> <ul style="list-style-type: none"> <li>Byte 1 = código de conclusão</li> <li>Byte 2 = Revisão de parâmetro (como na especificação de IPMI)</li> <li>Byte 3 = tamanho dos seguintes bytes de dados (16 bytes atualmente)</li> <li>Byte 4-n DUID_LLT</li> </ul>	C2h	

### Parâmetros de configuração Ethernet

Os parâmetros a seguir podem ser usados para definir configurações Ethernet específicas.

Parâmetro	#	Dados de parâmetro
<p>Parâmetro OEM</p> <p>(Esse número de parâmetro é usado pelo XCC para habilitar ou desabilitar a configuração de negociação automática para a interface Ethernet.)</p> <p>Os dados de resposta retornarão 3 bytes:</p> <p>Byte 1 = código de conclusão</p> <p>Byte 2 = revisão</p> <p>Byte 3 = 00h (desabilitado) ou 01h (habilitado)</p>	C3h	<p><u>dados 1</u></p> <p>0x00 = desabilitado</p> <p>0x01 = habilitado</p> <p>Nota: Nos sistemas Flex e Gabinete ThinkSystem D2 (Nó de cálculo ThinkSystem SD530), a configuração de negociação automática não é alterável porque pode interromper o caminho de comunicação de rede via CMM e SMM.</p>
<p>Parâmetro OEM</p> <p>(Esse número de parâmetro é usado pelo XCC para obter ou definir a taxa de dados da interface Ethernet.)</p> <p>Os dados de resposta retornarão 3 bytes:</p> <p>Byte 1 = código de conclusão</p> <p>Byte 2 = revisão</p> <p>Byte 3 = 00h (10 Mb) ou 01h (100 Mb)</p>	C4h	<p><u>dados 1</u></p> <p>0x00 = 10 Mbit</p> <p>0x01 = 100 Mbit</p>
<p>Parâmetro OEM</p> <p>(Esse número de parâmetro é usado pelo XCC para obter ou definir a configuração Duplex da interface Ethernet.)</p> <p>Os dados de resposta retornarão 3 bytes:</p> <p>Byte 1 = código de conclusão</p> <p>Byte 2 = revisão</p> <p>Byte 3 = 00h (Half Duplex) ou 01h (Full Duplex)</p>	C5h	<p><u>dados 1</u></p> <p>0x00 = Half Duplex</p> <p>0x01 = Full Duplex</p>

Parâmetro	#	Dados de parâmetro
<p>Parâmetro OEM</p> <p>(Esse número de parâmetro é usado pelo XCC para obter ou definir a Unidade de Transmissão Máxima (MTU) da interface Ethernet.)</p> <p>Os dados de resposta retornarão 3 bytes:</p> <p>Byte 1 = código de conclusão</p> <p>Byte 2 = revisão</p> <p>Byte 3-4 = tamanho da MTU</p>	C6h	<p><u>dados 1</u></p> <p>Tamanho da MTU</p>
<p>Parâmetro OEM</p> <p>(Esse número de parâmetro é usado pelo XCC para obter ou definir o endereço MAC administrado localmente.)</p> <p>Os dados de resposta retornarão 3 bytes:</p> <p>Byte 1 = código de conclusão</p> <p>Byte 2 = revisão</p> <p>Byte 3 – 8 = Endereço MAC</p>	C7h	<p><u>dados 1 - 6</u></p> <p>Endereço MAC</p>

### Opção IPMI para obter o endereço de link local

Este é um parâmetro somente leitura para recuperar o endereço de link local IPv6.

Parâmetro	#	Dados de parâmetro
<p>Parâmetro OEM</p> <p>Esse parâmetro é usado para obter o endereço de link local do XCC:</p> <p>Os dados de resposta retornarão o seguinte:</p> <p>Byte 1 = código de conclusão</p> <p>Byte 2 = Revisão de parâmetro (como na especificação de IPMI)</p> <p>Byte 3 = Comprimento do prefixo de endereço IPv6</p> <p>Byte 4-19 Endereço do link local em formato binário</p>	C8h	

### Opção IPMI para habilitar/desabilitar o IPv6

Esse é um parâmetro de leitura/gravação para habilitar/desabilitar o IPv6 no XCC.

Parâmetro	#	Dados de parâmetro
Parâmetro OEM  Esse parâmetro é usado para habilitar/desabilitar o IPv6 no XCC  Os dados de resposta retornarão o seguinte:  Byte 1 = código de conclusão Byte 2 = Revisão de parâmetro (como na especificação de IPMI) Byte 3 = 00h (desabilitado) ou 01h (habilitado)	C9h	<u>dados 1</u>  0x00 = desabilitado  0x01 = habilitado

### Passagem Ethernet sobre USB para rede externa

O parâmetro a seguir é usado para configurar o Ethernet sobre USB para passagem Ethernet externa.

Parâmetro	#	Dados de parâmetro
<p>Parâmetro OEM</p> <p>Esse parâmetro no comando Obter/definir parâmetros de configuração LAN não usa um seletor de conjunto, nem requer um seletor de bloco, portanto, esses campos devem ser definidos como 00h.</p> <p>Os dados Obter resposta retornarão o seguinte:</p> <p>Byte 1 = código de conclusão</p> <p>Byte 2 = revisão</p> <p>Byte 3 = reservado (00h)</p> <p>Bytes 4:5 = Número da porta Ethernet sobre USB (LSByte primeiro)</p> <p>Bytes 6:7 = Número da porta Ethernet externa (LSByte primeiro)</p> <p>O número de bytes a seguir pode variar (1, 4 ou 16 bytes) dependendo do modo de endereçamento:</p> <ul style="list-style-type: none"> <li>Byte 8 = modos predefinidos: <ul style="list-style-type: none"> <li>00h = a passagem está desabilitada</li> <li>01h = o endereço IP do CMM é usado</li> </ul> </li> </ul> <p>Bytes 8:11 = endereço IP de rede externa IPv4 em formato binário</p> <p>Bytes 8:23 = endereço IP de rede externa IPv6 em formato binário</p> <p>Códigos de conclusão:</p> <p>00h – sucesso</p> <p>80h – parâmetro não suportado</p> <p>C1h – comando não suportado</p> <p>C7h – comprimento dos dados da solicitação inválido</p>	CAh	<p>Definir parâmetros de configuração LAN:</p> <p><u>dados 1</u></p> <p>reservado (= 00h)</p> <p><u>dados 2:3</u></p> <p>Número da porta Ethernet sobre USB, LSByte primeiro</p> <p><u>dados 4:5</u></p> <p>Número da porta Ethernet externa, LSByte primeiro</p> <p>O número de bytes a seguir pode variar (1, 4 ou 16 bytes) dependendo do modo de endereçamento:</p> <p><u>dados 6</u></p> <p>00h = desabilitar a passagem</p> <p>01h = usar o endereço IP do CMM</p> <p><u>dados 6:9</u></p> <p>Endereço IP de rede externa IPv4 em formato binário</p> <p><u>dados 6:21</u></p> <p>Endereço IP de rede externa IPv6 em formato binário</p>
<p>Parâmetro OEM</p> <p>Esse parâmetro é usado para definir e obter o endereço IP de LAN sobre USB e a máscara de rede do XCC:</p> <p>Os dados de resposta retornarão o seguinte:</p> <p>Byte 1 = código de conclusão</p>	CBh	<p>Dados 1:4</p> <p>Endereço IP da interface LAN sobre USB do lado do XCC.</p> <p>Dados 5:8</p> <p>Máscara de rede da interface LAN sobre USB do lado do XCC</p>

Parâmetro	#	Dados de parâmetro
<p>Byte 2 = Revisão de parâmetro (como na especificação de IPMI)</p> <p>Byte 3:10 = Valor do endereço IP e da máscara de rede (MS-byte) primeiro</p>		
<p>Parâmetro OEM</p> <p>Esse parâmetro é usado para definir e obter o endereço IP de LAN sobre USB do SO do host:</p> <p>Os dados de resposta retornarão o seguinte:</p> <p>Byte 1 = código de conclusão</p> <p>Byte 2 = Revisão de parâmetro (como na especificação de IPMI)</p> <p>Byte 3:6 = Endereço IP (MS-byte) primeiro</p>	CCh	<p>Dados 1:4</p> <p>Endereço IP da interface LAN sobre USB do lado do host.</p>

### Consultar inventário do pacote lógico

O parâmetro a seguir é usado para consultar o inventário do pacote NCSI.

Parâmetro	#	Dados de parâmetro
<p>Parâmetro OEM</p> <p>Esse parâmetro no comando Obter/definir parâmetros de configuração LAN não usa um seletor de conjunto, nem requer um seletor de bloco, portanto, esses campos devem ser definidos como 00h.</p> <p>Consultar operação de inventário do pacote</p> <p>A operação de informação do pacote de consulta é executada emitindo a solicitação com dois bytes de dados 0x00 além do número do parâmetro D3h.</p> <p>Consultar inventário do pacote:</p> <p>--&gt; 0x0C 0x02 0x00 0xD3 0x00 0x00</p> <p>A resposta do XCC inclui um byte de informações para cada pacote presente:</p> <p>bits 7:4 = número de canais NCSI no pacote</p> <p>bits 3:0 = o número do pacote lógico</p> <p>Resposta</p> <p>--&gt; 0x00 0x00 0x40 0x01 0x32</p> <p>indica que há 3 pacotes lógicos presentes:</p> <ul style="list-style-type: none"> <li>o pacote 0 tem 4 canais NCSI</li> <li>o pacote 1 não é um NCSI NIC e, portanto, não é compatível a canais NCSI</li> <li>o pacote 2 tem 3 canais NCSI</li> </ul>	D3h	Obter/definir parâmetros de configuração LAN:

### Obter/definir dados do pacote lógico

O parâmetro a seguir é usado para ler e definir a prioridade atribuída a cada pacote.

Parâmetro	#	Dados de parâmetro
<p>Parâmetro OEM</p> <p>Esse parâmetro no comando Obter/definir parâmetros de configuração LAN não usa um seletor de conjunto, nem requer um seletor de bloco, portanto, esses campos devem ser definidos como 00h.</p> <p>O comando é compatível com 2 operações:</p> <ul style="list-style-type: none"> <li>• Ler prioridade do pacote</li> <li>• Definir prioridade do pacote</li> </ul> <p>Ler operação de prioridade do pacote</p> <p>A operação para ler a prioridade do pacote é executada emitindo a solicitação com dois bytes de dados 0x00 além do número do parâmetro D4h.</p> <p>Ler prioridade do pacote:</p> <p>--&gt; 0x0C 0x02 0x01 0xD4 0x00 0x00</p> <p>Resposta</p> <p>--&gt; 0x00 0x00 0x00 0x12 0x23</p> <p>pacote lógico 0 = prioridade 0 pacote lógico 2 = prioridade 1 pacote lógico 3 = prioridade 2</p> <p>Definir operação de prioridade do pacote</p> <p>A operação para definir a prioridade do pacote é executada emitindo a solicitação com um ou mais parâmetros além do número do parâmetro D4h.</p> <p>Definir prioridade do pacote:</p> <p>--&gt; 0x0C 0x01 0x01 0xD4 0x00 0x12 0x23</p> <p>definir pacote lógico 0 = prioridade 0 definir pacote lógico 2 = prioridade 1</p>	<p>D4</p>	<p>Obter/definir parâmetros de configuração LAN:</p> <p>Bit [7-4] = prioridade do pacote lógico (1 = maior, 15 = menor)</p> <p>Bit [3-0] = número do pacote lógico</p>

Parâmetro	#	Dados de parâmetro
definir pacote lógico 3 = prioridade 2  Resposta:  somente código de conclusão, sem dados adicionais		

#### Obter/definir status de sincronização de rede do XCC

Parâmetro	#	Dados de parâmetro
Parâmetro OEM  O byte é usado para definir para sincronizar a configuração de rede entre o modo NIC dedicado e compartilhado  Esse parâmetro no comando Obter parâmetros de configuração LAN não usa um seletor de conjunto, nem requer um seletor de bloco, portanto, esses campos devem ser definidos como 00h.  Os dados de resposta retornarão 3 bytes:  Byte 1 = código de conclusão Byte 2 = revisão Byte 3 = 00h (habilitado) ou 01h (desabilitado)	D5h	<u>dados 1</u>  0x00 = Sincronização  0x01 = Independência

O byte é usado para definir para sincronizar a configuração de rede entre o modo NIC dedicado e compartilhado, o valor padrão foi 0h aqui, significa que o XCC atualizará automaticamente a configuração de rede entre modos e alterará e usará a NIC compartilhada (integrada) como referência principal, se definido como 1h, cada configuração de rede será independente aqui, por esse motivo podemos definir configurações de rede diferentes entre modos, como VLAN habilitada em modo Dedicado e definir VLAN desabilitada no modo NIC compartilhada.

#### Obter/definir modo de rede do XCC

Parâmetro	#	Dados de parâmetro
<p>Parâmetro OEM</p> <p>Esse parâmetro é usado para obter/definir o modo de rede da NIC de gerenciamento do XCC.</p> <p>Os dados de resposta retornarão 4 bytes:</p> <p>Byte 1 = código de conclusão</p> <p>Byte 2 = revisão</p> <p>Byte 3 = aplicado/modo de rede especificado</p> <p>Byte 4 = ID do pacote do modo de rede aplicado</p> <p>Byte 5 = ID do canal do modo de rede aplicado</p>	D6h	<p>Definir parâmetros de configuração LAN:</p> <p><u>dados 1</u></p> <p>Modo de rede a ser definido</p> <p>Obter parâmetros de configuração LAN:</p> <p><u>dados 1</u></p> <p>Para obter o modo de rede, estes são dados opcionais, padrões para consultar o modo de rede atual</p>

## Comandos OEM IPMI

O XCC é compatível com os seguintes comandos OEM IPMI: Cada comando requer um nível de privilégio diferente, conforme listado a seguir.

Código	Comandos Netfn 0x2E	Privilégio
0xCC	Redefinir XCC como padrão	PRIV_USR

Código	Comandos Netfn 0x3A	Privilégio
0x00	Consultar versão de firmware	PRIV_USR
0x0D	Informações da placa	PRIV_USR
0x1E	Opções de atraso de restauração de energia do chassi	PRIV_USR
0x38	NMI e Redefinição	PRIV_USR
0x49	Iniciar coleta de dados	PRIV_USR
0x4A	Enviar arquivo	PRIV_USR
0x4D	Status da coleta de dados	PRIV_USR
0x50	Obter informações de construção	PRIV_USR
0x55	Obter/definir nome do host	PRIV_USR
0x6B	Consultar nível de revisão de firmware FPGA	PRIV_USR

<b>Código</b>	<b>Comandos Netfn 0x3A</b>	<b>Privilégio</b>
0x6C	Consultar nível de revisão de hardware de placa	PRIV_USR
0x6D	Consultar nível de revisão de firmware PSoC	PRIV_USR
0x98	Controle de porta USB FP	PRIV_USR
0xC7	Comutador de IPMI NM nativo	PRIV_ADM

### Reconfigurar XCC para comando padrão

Esse comando redefine a definição de configuração do XCC para os valores padrão.

<b>Função líquida = 0x2E</b>			
<b>Código</b>	<b>Comando</b>	<b>Solicitação, Dados de resposta</b>	<b>Descrição</b>
0xCC	Redefinir XCC como padrão	<p><b>Solicitação:</b></p> <p>Byte 1 – 0x5E Byte 2 – 0x2B</p> <p>Byte 3 – 0x00</p> <p>Byte 4 – 0x0A Byte 5 – 0x01</p> <p>Byte 6 – 0xFF</p> <p>Byte 7 – 0x00 Byte 8 – 0x00</p> <p>Byte 9 – 0x00</p> <p><b>Resposta:</b></p> <p>Byte 1 – Conclusão de Code Byte 2 – 0x5E Byte 3 – 0x2B</p> <p>Byte 4 – 0x00</p> <p>Byte 5 – 0x0A Byte 6 – 0x01</p> <p>Byte 7 – Dados de resposta</p> <p>0 = Sucesso diferente de zero = Falha</p>	Esse comando redefine as definições de configuração do XCC para os valores padrão.

### Comandos de informações de placa/firmware

Esta seção lista os comandos para consultar as informações de placa e firmware.

Função líquida = 0x3A			
Código	Comando	Solicitação, Dados de resposta	Descrição
0x00	Consultar versão de firmware	<p><b>Solicitação:</b></p> <p>Nenhum dado sobre a solicitação</p> <p><b>Resposta:</b></p> <p>Byte 1 – Código de conclusão</p> <p>Byte 2 - Versão principal</p> <p>Byte 3 - Versão secundária</p>	<p>Esse comando retorna os números de versão principal e secundária do firmware. Se o comando for feito com o 1 byte opcional de dados de solicitação, a resposta do XCC também retornará o terceiro campo (revisão) da versão.</p> <p>(Revisão, Principal, Secundária)</p>
0x0D	Consultar informações da placa	<p><b>Solicitação:</b> N/A</p> <p><b>Resposta:</b></p> <p>Byte 1 – ID do sistema</p> <p>Byte 2 – Revisão da placa</p>	<p>Esse comando retorna a revisão do planar e ID da placa.</p>
0x50	Consultar informações de construção	<p><b>Solicitação:</b> N/A</p> <p><b>Resposta:</b></p> <p>Byte 1 – Código de conclusão.</p> <p>Bytes 2:10 – Nome da construção ASCIIZ</p> <p>Bytes 11:23 – Data de construção ASCIIZ</p> <p>Bytes 24:31 – Tempo de construção ASCII</p>	<p>Esse comando retorna o nome, a data e o tempo de construção. As sequências de nome e data de construção têm uma finalização zero.</p> <p>O formato da data de construção é AAAA-MM-DD.</p> <p>por exemplo, "ZUBT99A"</p> <p>"2005-03-07"</p> <p>"23:59:59"</p>

Função líquida = 0x3A			
Código	Comando	Solicitação, Dados de resposta	Descrição
0x6B	Consultar nível de revisão de firmware FPGA	<p><b>Solicitação:</b></p> <p>Byte 1 – Tipo de dispositivo FPGA*</p> <p>Tipo de dispositivo FPGA</p> <p>0 = Local (nível ativo)</p> <p>1 = Placa de CPU 1 (nível ativo)</p> <p>2 = Placa de CPU 2 (nível ativo)</p> <p>3 = Placa de CPU 3 (nível ativo)</p> <p>4 = Placa de CPU 4 (nível ativo)</p> <p>5 = ROM primário local</p> <p>6 = ROM de recuperação local</p> <p><b>Resposta:</b></p> <p>Byte 1 – Código de conclusão</p> <p>Byte 2 – Nível de revisão principal</p> <p>Byte 3 – Nível de revisão menor</p> <p>Byte 4 – Nível de revisão subinferior</p> <p>(Byte de teste em plataformas do XCC)</p>	<p>Esse comando retorna o nível de revisão do firmware FPGA.</p> <p>Se o Byte 1 for omitido, o local (nível ativo) será selecionado</p>
0x6C	Consultar nível de revisão de hardware de placa	<p><b>Solicitação:</b></p> <p>Sem dados.</p> <p><b>Resposta:</b></p> <p>Byte 1 – Código de conclusão</p> <p>Byte 2 – Nível de revisão</p>	<p>Esse comando retorna o nível de revisão do hardware da placa onde o FPGA reside.</p>
0x6D	Consultar nível de revisão de firmware PSoC	<p><b>Solicitação:</b></p> <p>Nenhum(a)</p> <p><b>Resposta:</b></p> <p>Byte 1 – Código de conclusão</p> <p>Byte 2 – bin#</p> <p>Byte 3 – APID</p> <p>Byte 4 – Rev</p>	<p>Esse comando retorna o nível de revisão de todos os dispositivos PSoC detectados.</p> <p>Nota: bin# representa um local físico. Consulte as especificações do sistema para obter detalhes.</p>

Função líquida = 0x3A			
Código	Comando	Solicitação, Dados de resposta	Descrição
		Byte 5-6 – ID da FRU  Bytes 6:N – repetição de bytes 2-6 para cada PSoC detectado	

### Comandos de controle do sistema

A especificação IPMI fornece o controle básico de ativação e redefinição. A Lenovo adiciona funções de controle adicionais.

Função líquida = 0x2E							
Código	Comando	Solicitação, Dados de resposta	Descrição				
0x1E	Opções de atraso de restauração de energia do chassi	<p><b>Solicitação:</b></p> <table border="1"> <tr> <td>Byte 1</td> <td>           Tipo de solicitação:             0x00 = Definir opções de atraso             0x01 = Consultar opções de atraso         </td> </tr> <tr> <td>Byte 2</td> <td>           (se byte 1 = 0x00)             0x00 = Desabilitado (padrão)             0x01 = Aleatório             0x02 - 0xFF Reservado         </td> </tr> </table> <p><b>Resposta:</b></p> <p>Byte 1 – Código de conclusão</p> <p>Byte 2 – Opções de atraso (somente para solicitação de consulta)</p>	Byte 1	Tipo de solicitação:  0x00 = Definir opções de atraso  0x01 = Consultar opções de atraso	Byte 2	(se byte 1 = 0x00)  0x00 = Desabilitado (padrão)  0x01 = Aleatório  0x02 - 0xFF Reservado	<p>Essa configuração é usada quando a política de restauração de energia do chassi está configurada para ser sempre ligar ou restaurar para ser ligada (se anteriormente ativada), depois que a CA é aplicada/retorna. Há duas opções: Desabilitado (a configuração padrão, sem atraso quando habilitado) e Aleatório. A configuração de atraso aleatório fornece um atraso aleatório de 1 a 15 segundos, a partir da hora em que CA é aplicada/retorna e quando o servidor é ligado automaticamente.</p> <p>O comando é aceito pelo XCC apenas em servidores de rack.</p>
Byte 1	Tipo de solicitação:  0x00 = Definir opções de atraso  0x01 = Consultar opções de atraso						
Byte 2	(se byte 1 = 0x00)  0x00 = Desabilitado (padrão)  0x01 = Aleatório  0x02 - 0xFF Reservado						
0x38	NMI e redefinição	<p><b>Solicitação:</b></p> <p>Byte 1 – Número de segundos 0 = Apenas NMI</p> <p>Byte 2 – Tipo de redefinição 0 = redefinição flexível 1 = ciclo de ativação</p> <p><b>Resposta:</b></p> <p>Byte 1 – Código de conclusão</p>	<p>Esse comando é usado para executar um NMI do sistema. Opcionalmente, o sistema pode ser redefinido (reinicializado) ou o ciclo de ativação será executado após o NMI.</p> <p>Se o campo "Número de segundos" não for 0, o sistema será redefinido ou o ciclo de ativação será executado após o número especificado de segundos.</p> <p>O Byte 2 da solicitação é opcional. Se o byte 2 não for fornecido ou tiver um valor de 0x00, uma reinicialização flexível será executada. Se o byte 2 for 0x01, será executado o ciclo de ativação do sistema.</p>				

## **Comandos diversos**

Esta seção destina-se a comandos que não se encaixam em outra seção.

Função líquida = 0x3A											
Código	Comando	Solicitação, Dados de resposta	Descrição								
0x55	Obter/definir nome do host	<p><b>Tamanho da solicitação = 0:</b></p> <p>Dados da solicitação vazios</p> <p><b>Resposta:</b></p> <table border="1"> <tr> <td>Byte 1</td> <td>Código de conclusão</td> </tr> <tr> <td>Bytes 2-65</td> <td>Nome do host atual.  ASCIIZ, sequência terminada Null.</td> </tr> </table> <p><b>Tamanho da solicitação 1-64:</b></p> <table border="1"> <tr> <td>Bytes 1-64</td> <td>Nome do host do DHCP  ASCIIZ terminado com 00h</td> </tr> </table>	Byte 1	Código de conclusão	Bytes 2-65	Nome do host atual.  ASCIIZ, sequência terminada Null.	Bytes 1-64	Nome do host do DHCP  ASCIIZ terminado com 00h	<p>Use este comando para Obter/definir nome do host.</p> <p>Ao configurar o nome do host, o valor desejado deve ser terminado por um 00h. O nome do host está limitado a 63 caracteres mais o Null.</p>		
Byte 1	Código de conclusão										
Bytes 2-65	Nome do host atual.  ASCIIZ, sequência terminada Null.										
Bytes 1-64	Nome do host do DHCP  ASCIIZ terminado com 00h										
0x98	Controle de porta USB FP	<p><b>Solicitação:</b></p> <p>Byte 1</p> <table border="1"> <tr> <td>01h:</td> <td>Obter o proprietário atual da porta USB do painel frontal</td> </tr> </table> <p><b>Resposta:</b></p> <p>Byte 1 – Código de conclusão</p> <p>Byte 2</p> <table border="1"> <tr> <td>00h:</td> <td>Pertencente ao host</td> </tr> <tr> <td>01h:</td> <td>Pertencente ao BMC</td> </tr> </table> <p><b>Solicitação:</b></p> <p>Byte 1</p> <table border="1"> <tr> <td>02h:</td> <td>Obter a configuração da porta USB</td> </tr> </table>	01h:	Obter o proprietário atual da porta USB do painel frontal	00h:	Pertencente ao host	01h:	Pertencente ao BMC	02h:	Obter a configuração da porta USB	<p>Esse comando é usado para consultar o status/configuração da porta USB FP, configurar o modo/tempo limite da porta USB FP e alternar o proprietário da porta USB entre o host e o BMC.</p> <p>Na configuração, o USB FP pode ter 3 modos – dedicados ao host, pertencente exclusivamente ao BMC ou modo compartilhado que permite que o proprietário alterne entre o host e o BMC.</p> <p>Se o modo compartilhado estiver habilitado, a porta USB será conectada ao BMC quando o servidor for desligado e conectada ao servidor quando o servidor estiver ligado.</p> <p>Quando o modo compartilhado estiver habilitado e a energia do servidor estiver ativa, o BMC retornará a porta USB de volta para o servidor após decorrer o tempo limite de inatividade na configuração.</p> <p>Se o servidor tiver o botão de identificação, os usuários poderão</p>
01h:	Obter o proprietário atual da porta USB do painel frontal										
00h:	Pertencente ao host										
01h:	Pertencente ao BMC										
02h:	Obter a configuração da porta USB										

Função líquida = 0x3A																							
Código	Comando	Solicitação, Dados de resposta	Descrição																				
		<table border="1"> <tr> <td></td> <td>do painel frontal</td> </tr> </table> <p><b>Resposta:</b></p> <p>Byte 1 – Código de conclusão</p> <p>Byte 2</p> <table border="1"> <tr> <td>00h:</td> <td>Dedicado ao host</td> </tr> <tr> <td>01h:</td> <td>Dedicado ao BMC</td> </tr> <tr> <td>02h:</td> <td>Modo compartilhado</td> </tr> </table> <p>Byte 3:4 – Tempo limite de inatividade em minutos (MSB primeiro)</p> <p>Byte 5 – Habilitar botão de ID</p> <table border="1"> <tr> <td>00h:</td> <td>Desabilitado</td> </tr> <tr> <td>01h:</td> <td>Habilitado</td> </tr> </table> <p>Byte 6 – Histerese (opcional) em segundos</p> <p><b>Solicitação:</b></p> <p>Byte 1</p> <p>03h: definir a configuração da porta USB do painel frontal</p> <p>Byte 2</p> <table border="1"> <tr> <td>00h:</td> <td>Dedicado ao host</td> </tr> <tr> <td>01h:</td> <td>Dedicado ao BMC</td> </tr> <tr> <td>02h:</td> <td>Modo compartilhado</td> </tr> </table> <p>Byte 3:4 – Tempo limite de inatividade em minutos (MSB primeiro)</p> <p>Byte 5 – Habilitar botão de ID</p> <table border="1"> <tr> <td>00h:</td> <td>Desabilitado</td> </tr> </table>		do painel frontal	00h:	Dedicado ao host	01h:	Dedicado ao BMC	02h:	Modo compartilhado	00h:	Desabilitado	01h:	Habilitado	00h:	Dedicado ao host	01h:	Dedicado ao BMC	02h:	Modo compartilhado	00h:	Desabilitado	<p>habilitar/desabilitar o botão de ID para alternar o proprietário da porta USB FP segurando o botão de ID por mais de três segundos.</p> <p>Histerese em segundos serão configuradas quando a porta for alternada automaticamente durante o ciclo de ativação. Este é um parâmetro opcional.</p> <p>Servidores SD530</p> <p>Na plataforma SD530, a porta é opcional e, se presente, é conectada diretamente ao XCC e apenas ao XCC. Alternar a porta para o host não está disponível.</p> <ul style="list-style-type: none"> <li>Quando o comando é emitido com byte 1 = 1, o XCC sempre responderá que a porta pertence ao BMC.</li> <li>Quando o comando é emitido com byte 1 = 2, o XCC sempre responderá que a porta é dedicada ao BMC.</li> <li>Quando o comando é emitido com byte 1 = 3 ou byte 1 = 4, o XCC responderá com o código de conclusão D6h.</li> </ul> <p>Servidores não SD530</p> <p>Na plataforma não SD530, o uso do XCC da porta USB do painel frontal pode ser desabilitado alternando para o modo "Apenas host".</p> <p>Quando o comando é emitido com byte 1 = 5 ou byte 1 = 6, o XCC responderá com o código de conclusão D6h.</p>
	do painel frontal																						
00h:	Dedicado ao host																						
01h:	Dedicado ao BMC																						
02h:	Modo compartilhado																						
00h:	Desabilitado																						
01h:	Habilitado																						
00h:	Dedicado ao host																						
01h:	Dedicado ao BMC																						
02h:	Modo compartilhado																						
00h:	Desabilitado																						

Função líquida = 0x3A																	
Código	Comando	Solicitação, Dados de resposta	Descrição														
		<table border="1"> <tr> <td>01h:</td> <td>Habilitado</td> </tr> </table> <p>Byte 6 – Histerese (opcional) em segundos</p> <p><b>Resposta:</b></p> <p>Byte 1 - Código de conclusão de Byte 2</p> <table border="1"> <tr> <td>00h:</td> <td>Alternar para host</td> </tr> <tr> <td>01h:</td> <td>Alternar para BMC</td> </tr> </table> <p><b>Resposta:</b></p> <p>Byte 1 – Código de conclusão</p> <p>Byte 1</p> <table border="1"> <tr> <td>05h:</td> <td>Habilitar/ desabilitar a porta USB do painel frontal</td> </tr> </table> <p>Byte 2</p> <table border="1"> <tr> <td>00h:</td> <td>Desabilitar</td> </tr> <tr> <td>01h:</td> <td>Habilitar</td> </tr> </table> <p><b>Resposta:</b></p> <p>Byte 1 – Código de conclusão</p> <p><b>Solicitação:</b></p> <p>Byte 1</p> <table border="1"> <tr> <td>06h:</td> <td>Ler o estado de ativação/ desativação da porta USB do painel frontal</td> </tr> </table> <p><b>Resposta:</b></p> <p>Byte 1 - Código de conclusão</p> <p>Byte 2</p>	01h:	Habilitado	00h:	Alternar para host	01h:	Alternar para BMC	05h:	Habilitar/ desabilitar a porta USB do painel frontal	00h:	Desabilitar	01h:	Habilitar	06h:	Ler o estado de ativação/ desativação da porta USB do painel frontal	
01h:	Habilitado																
00h:	Alternar para host																
01h:	Alternar para BMC																
05h:	Habilitar/ desabilitar a porta USB do painel frontal																
00h:	Desabilitar																
01h:	Habilitar																
06h:	Ler o estado de ativação/ desativação da porta USB do painel frontal																

Função líquida = 0x3A															
Código	Comando	Solicitação, Dados de resposta	Descrição												
0xC7	Comutador de IPMI NM nativo	<p><b>Tamanho da solicitação = 0:</b></p> <p>Dados da solicitação vazios</p> <p><b>Resposta:</b></p> <table border="1"> <tr> <td>Byte 1</td> <td>Código de conclusão</td> </tr> <tr> <td>Bytes 2</td> <td>Status atual de ativação/desativação</td> </tr> </table> <p><b>Tamanho da solicitação= 1:</b></p> <table border="1"> <tr> <td>Byte 1</td> <td>Atributo de ativação/desativação da interface NM IPMI nativa</td> </tr> <tr> <td></td> <td>00h – Desabilitar</td> </tr> <tr> <td></td> <td>01h – Habilitar</td> </tr> </table> <p><b>Resposta:</b></p> <table border="1"> <tr> <td>Byte 1</td> <td>Código de conclusão</td> </tr> </table>	Byte 1	Código de conclusão	Bytes 2	Status atual de ativação/desativação	Byte 1	Atributo de ativação/desativação da interface NM IPMI nativa		00h – Desabilitar		01h – Habilitar	Byte 1	Código de conclusão	Esse comando é usado para habilitar/desabilitar a função de ponte do XCC para os comandos IPMI Intel nativos.
Byte 1	Código de conclusão														
Bytes 2	Status atual de ativação/desativação														
Byte 1	Atributo de ativação/desativação da interface NM IPMI nativa														
	00h – Desabilitar														
	01h – Habilitar														
Byte 1	Código de conclusão														

---

## Apêndice A. Obtendo ajuda e assistência técnica

Se precisar de ajuda, serviço ou assistência técnica ou apenas desejar mais informações sobre produtos Lenovo, você encontrará uma ampla variedade de fontes disponíveis da Lenovo para ajudá-lo.

Na Web, informações atualizadas sobre sistemas, dispositivos opcionais, serviços e suporte Lenovo estão disponíveis em:

<http://datacentersupport.lenovo.com>

**Nota:** Esta seção inclui referências aos Web sites da IBM e informações sobre como obter serviço. A IBM é o provedor de serviço preferencial da Lenovo para o ThinkSystem.

---

### Antes de Ligar

Antes de telefonar, há várias etapas que você pode realizar para tentar resolver o problema por conta própria. Se você decidir que realmente precisa ligar para obter assistência, colete todas as informações que serão necessárias para o técnico de serviço resolver mais rapidamente o problema.

#### Tente resolver o problema por conta própria

Você pode resolver muitos problemas sem assistência externa, seguindo os procedimentos de resolução de problemas que a Lenovo fornece na ajuda on-line ou na documentação fornecida com o produto Lenovo. A documentação fornecida com o produto Lenovo também descreve os testes de diagnóstico que podem ser executados. A documentação da maioria dos sistemas, sistemas operacionais e programas contém procedimentos de resolução de problemas e explicações de mensagens de erro e códigos de erro. Se suspeitar de um problema de software, consulte a documentação do sistema operacional ou do programa.

É possível encontrar a documentação dos seus produtos ThinkSystem no seguinte local:

<https://pubs.lenovo.com/>

Você pode realizar as seguintes etapas para tentar resolver o problema por conta própria:

- Verifique todos os cabos para certificar-se de que estejam conectados.
- Verifique os comutadores de energia para certificar-se de que o sistema e os dispositivos opcionais estejam ativados.
- Verifique se há software, firmware e drivers de dispositivo do sistema operacional atualizados para seu produto Lenovo. Os termos e condições da Lenovo Warranty indicam que você, o proprietário do produto Lenovo, é responsável pela manutenção e atualização de todos os softwares e firmwares do produto (a menos que ele seja coberto por um contrato de manutenção adicional). Seu técnico de serviço solicitará que você faça upgrade do software e firmware se o problema tiver uma solução documentada dentro de um upgrade do software.
- Se você tiver instalado um novo hardware ou software em seu ambiente, verifique o <http://www.lenovo.com/serverproven/> para se certificar de que o hardware e o software sejam suportados por seu produto.
- Acesse <http://datacentersupport.lenovo.com> e verifique as informações para ajudar a resolver o problema.
  - Verifique os fóruns da Lenovo em [https://forums.lenovo.com/t5/Datacenter-Systems/ct-p/sv\\_eg](https://forums.lenovo.com/t5/Datacenter-Systems/ct-p/sv_eg) para ver se alguém mais se deparou com um problema semelhante.

Você pode resolver muitos problemas sem assistência externa, seguindo os procedimentos de resolução de problemas que a Lenovo fornece na ajuda on-line ou na documentação fornecida com o produto Lenovo. A

documentação fornecida com o produto Lenovo também descreve os testes de diagnóstico que podem ser executados. A documentação da maioria dos sistemas, sistemas operacionais e programas contém procedimentos de resolução de problemas e explicações de mensagens de erro e códigos de erro. Se suspeitar de um problema de software, consulte a documentação do sistema operacional ou do programa.

### **Coletando as informações necessárias para chamar o suporte**

Se você achar que precisa de ajuda para executar serviço de garantia em seu produto Lenovo, os técnicos de serviço poderão auxiliá-lo com mais eficácia se você se preparar antes de ligar. Você também pode consultar <http://datacentersupport.lenovo.com/warrantylookup> para obter informações sobre a garantia do produto.

Reúna as informações a seguir para serem fornecidas ao técnico de serviço. Esses dados ajudarão o técnico a fornecer rapidamente uma solução para o seu problema e a assegurar que você receba o nível de serviço que contratou.

- Números de contrato do acordo de Manutenção de Hardware e Software, se aplicável
- Número de tipo de máquina (identificador de máquina com 4 dígitos da Lenovo)
- Número do modelo
- Número de série
- Níveis atuais de UEFI e de firmware do sistema
- Outras informações pertinentes, como mensagem de erro e logs

Em vez de chamar o Suporte Lenovo, você pode acessar <https://www-947.ibm.com/support/servicerequest/Home.action> para enviar uma Solicitação de serviço eletrônica. Submeter uma Solicitação Eletrônica de Serviço iniciará o processo de determinação de uma solução para o seu problema, tornando as informações pertinentes disponíveis para os técnicos de serviço. Os técnicos de serviço Lenovo podem começar a trabalhar na sua solução assim que você tiver concluído e enviado uma Solicitação de Serviço Eletrônico.

---

## **Coletando dados de serviço**

Para identificar claramente a causa raiz de um problema do servidor ou mediante solicitação do Suporte Lenovo, talvez seja necessário coletar dados de serviço que podem ser usados para realizar uma análise mais aprofundada. Os dados de serviço incluem informações como logs de eventos e inventário de hardware.

Os dados de serviço podem ser coletados pelas seguintes ferramentas:

- **Lenovo XClarity Controller**

É possível usar a interface da Web do Lenovo XClarity Controller ou a CLI para coletar dados de serviço do servidor. É possível salvar e enviar o arquivo salvo para o Suporte Lenovo.

- Para obter mais informações sobre como usar a interface da Web para coletar dados de serviço, consulte [https://pubs.lenovo.com/xcc3/nn1ia\\_c\\_servicesandsupport.html](https://pubs.lenovo.com/xcc3/nn1ia_c_servicesandsupport.html).
- Para obter mais informações sobre como usar a CLI para coletar dados de serviço, consulte [https://pubs.lenovo.com/xcc3/nn1ia\\_r\\_ffdcommand.html](https://pubs.lenovo.com/xcc3/nn1ia_r_ffdcommand.html).

- **Lenovo XClarity Administrator**

O Lenovo XClarity Administrator pode ser configurado para coletar e enviar arquivos de diagnóstico automaticamente para o Suporte Lenovo quando determinados eventos que podem ser reparados ocorrerem no Lenovo XClarity Administrator e nos terminais gerenciados. É possível optar por enviar arquivos de diagnóstico ao Suporte Lenovo utilizando Call Home ou outro provedor de serviço que usar SFTP. Também é possível coletar arquivos de diagnóstico manualmente, abrir um registro de problemas e enviar arquivos de diagnóstico ao Centro de Suporte Lenovo.

É possível obter mais informações sobre como configurar notificações automáticas de problemas no Lenovo XClarity Administrator em [https://pubs.lenovo.com/lxca/admin\\_setupcallhome.html](https://pubs.lenovo.com/lxca/admin_setupcallhome.html).

- **Lenovo XClarity Provisioning Manager**

Use a função Coletar dados de serviço do Lenovo XClarity Provisioning Manager para coletar dados de serviço do sistema. É possível coletar dados do log do sistema existente ou executar um novo diagnóstico para coletar novos dados.

- **Lenovo XClarity Essentials**

O Lenovo XClarity Essentials pode ser executado dentro da banda do sistema operacional. Além dos dados de serviço de hardware, o Lenovo XClarity Essentials pode coletar informações sobre o sistema operacional, como o log de eventos do sistema operacional.

Para obter dados de serviço, você pode executar o comando `getinfor`. Para obter mais informações sobre como executar o `getinfor`, consulte [https://pubs.lenovo.com/lxce-onecli/onecli\\_r\\_getinfor\\_command.html](https://pubs.lenovo.com/lxce-onecli/onecli_r_getinfor_command.html).

---

## Entrando em contato com o Suporte

É possível entrar em contato com o Suporte para obter ajuda para resolver seu problema.

Você pode receber serviço de hardware por meio de um Provedor de Serviços Autorizados Lenovo. Para localizar um provedor de serviços autorizado pela Lenovo para prestar serviço de garantia, acesse <https://datacentersupport.lenovo.com/us/en/serviceprovider> e use a pesquisa de filtro para países diferentes. Para consultar os números de telefone do Suporte Lenovo, consulte <https://datacentersupport.lenovo.com/us/en/supportphonenumber> para obter os detalhes de suporte da sua região.



---

## Apêndice B. Avisos

É possível que a Lenovo não ofereça os produtos, serviços ou recursos discutidos nesta publicação em todos os países. Consulte um representante Lenovo local para obter informações sobre os produtos e serviços disponíveis atualmente em sua área.

Qualquer referência a produtos, programas ou serviços Lenovo não significa que apenas produtos, programas ou serviços Lenovo possam ser utilizados. Qualquer produto, programa ou serviço funcionalmente equivalente, que não infrinja nenhum direito de propriedade intelectual da Lenovo, poderá ser utilizado em substituição a esse produto, programa ou serviço. Entretanto, a avaliação e verificação da operação de qualquer outro produto, programa ou serviço são de responsabilidade do Cliente.

A Lenovo pode ter patentes ou solicitações de patentes pendentes relativas a assuntos descritos nesta publicação. O fornecimento desta publicação não é uma oferta e não fornece uma licença em nenhuma patente ou solicitações de patente. Pedidos devem ser enviados, por escrito, para:

**Lenovo (United States), Inc.**  
**1009 Think Place**  
**Morrisville, NC 27560**  
**U.S.A.**  
**Attention: Lenovo VP of Intellectual Property**

A LENOVO FORNECE ESTA PUBLICAÇÃO "NO ESTADO EM QUE SE ENCONTRA", SEM GARANTIA DE NENHUM TIPO, SEJA EXPRESSA OU IMPLÍCITA, INCLUINDO, MAS A ELAS NÃO SE LIMITANDO, AS GARANTIAS IMPLÍCITAS DE NÃO INFRAÇÃO, COMERCIALIZAÇÃO OU ADEQUAÇÃO A UM DETERMINADO PROPÓSITO. Alguns países não permitem a exclusão de garantias expressas ou implícitas em certas transações; portanto, essa disposição pode não se aplicar ao Cliente.

Essas informações podem conter imprecisões técnicas ou erros tipográficos. São feitas alterações periódicas nas informações aqui contidas; tais alterações serão incorporadas em futuras edições desta publicação. A Lenovo pode fazer aperfeiçoamentos e/ou alterações nos produtos ou programas descritos nesta publicação a qualquer momento sem aviso prévio.

Os produtos descritos nesta publicação não são destinados para uso em implantações ou em outras aplicações de suporte à vida, nas quais o mau funcionamento pode resultar em ferimentos ou morte. As informações contidas nesta publicação não afetam nem alteram as especificações ou garantias do produto Lenovo. Nada nesta publicação deverá atuar como uma licença expressa ou implícita nem como indenização em relação aos direitos de propriedade intelectual da Lenovo ou de terceiros. Todas as informações contidas nesta publicação foram obtidas em ambientes específicos e representam apenas uma ilustração. O resultado obtido em outros ambientes operacionais pode variar.

A Lenovo pode utilizar ou distribuir as informações fornecidas, da forma que julgar apropriada, sem incorrer em qualquer obrigação para com o Cliente.

Referências nesta publicação a Web sites que não são da Lenovo são fornecidas apenas por conveniência e não representam de forma alguma um endosso a esses Web sites. Os materiais contidos nesses Web sites não fazem parte dos materiais desse produto Lenovo e a utilização desses Web sites é de inteira responsabilidade do Cliente.

Todos os dados de desempenho aqui contidos foram determinados em um ambiente controlado. Portanto, o resultado obtido em outros ambientes operacionais pode variar significativamente. Algumas medidas podem ter sido tomadas em sistemas em nível de desenvolvimento e não há garantia de que estas medidas serão as mesmas em sistemas disponíveis em geral. Além disso, algumas medidas podem ter sido

estimadas através de extrapolação. Os resultados atuais podem variar. Os usuários deste documento devem verificar os dados aplicáveis para seu ambiente específico.

---

## Marcas Registradas

Lenovo, o logotipo da Lenovo, ThinkSystem, Flex System, System x, NeXtScale System e x Architecture são marcas registradas da Lenovo nos Estados Unidos, em outros países e/ou em ambos.

Intel e Intel Xeon são marcas registradas da Intel Corporation nos Estados Unidos e/ou em outros países.

Internet Explorer, Microsoft e Windows são marcas registradas do grupo de empresas Microsoft.

Linux é uma marca registrada da Linus Torvalds.

Outros nomes de empresas, produtos ou serviços podem ser marcas registradas ou marcas de serviços de terceiros.

---

## Notas Importantes

A velocidade do processador indica a velocidade do relógio interno do microprocessador; outros fatores também afetam o desempenho do aplicativo.

A velocidade da unidade de CD ou DVD lista a taxa de leitura variável. As velocidades reais variam e frequentemente são menores que a velocidade máxima possível.

Ao consultar o armazenamento do processador, armazenamento real e virtual, ou o volume do canal, KB significa 1.024 bytes, MB significa 1.048.576 bytes e GB significa 1.073.741.824 bytes.

Ao consultar a capacidade da unidade de disco rígido ou o volume de comunicações, MB significa 1.000.000 bytes e GB significa 1.000.000.000 bytes. A capacidade total acessível pelo usuário pode variar, dependendo dos ambientes operacionais.

As capacidades máximas de unidades de disco rígido assumem a substituição de quaisquer unidades de disco rígido padrão e a população de todos os compartimentos de unidades de disco rígido com as maiores unidades com suporte disponibilizadas pela Lenovo.

A memória máxima pode requerer substituição da memória padrão com um módulo de memória opcional.

Cada célula da memória em estado sólido tem um número intrínseco, finito, de ciclos de gravação nos quais essa célula pode incorrer. Portanto, um dispositivo em estado sólido possui um número máximo de ciclos de gravação ao qual ele pode ser submetido, expressado como total bytes written (TBW). Um dispositivo que excedeu esse limite pode falhar ao responder a comandos gerados pelo sistema ou pode ser incapaz de receber gravação. A Lenovo não é responsável pela substituição de um dispositivo que excedeu seu número máximo garantido de ciclos de programas/exclusões, conforme documentado nas Especificações Oficiais Publicadas do dispositivo.

A Lenovo não representa ou garante produtos não Lenovo. O suporte (se disponível) a produtos não Lenovo é fornecido por terceiros, não pela Lenovo.

Alguns softwares podem ser diferentes de sua versão de varejo (se disponível) e podem não incluir manuais do usuário ou todos os recursos do programa.

---

## Contaminação por partículas

**Atenção:** Partículas do ar (incluindo flocos ou partículas de metal) e gases reativos agindo sozinhos ou em combinação com outros fatores ambientais, como umidade ou temperatura, podem impor risco ao dispositivo descrito neste documento.

Os riscos que são causados pela presença de níveis excessivos de substâncias particuladas ou as concentrações de gases nocivos incluem danos que podem causar o mau funcionamento ou a parada completa do dispositivo. Essa especificação define limites para substâncias particuladas e gases que são destinados a evitar tais danos. Os limites não devem ser vistos ou usados como definitivos, porque inúmeros outros fatores, como temperatura ou umidade do ar, podem influenciar o impacto de substâncias particuladas ou a transferência de contaminantes corrosivos e gasosos do ambiente. Na ausência de limites específicos definidos neste documento, adote práticas que mantenham os níveis de gás e substâncias particuladas consistentes com a proteção da saúde e segurança das pessoas. Se a Lenovo determinar que os níveis de substâncias particuladas ou gases em seu ambiente causaram dano ao dispositivo, a Lenovo pode condicionar a provisão de reparo ou substituição de dispositivos ou peças à implementação de medidas reparatórias apropriadas para mitigar essa contaminação ambiental. A implementação dessas medidas reparatórias é de responsabilidade do cliente.

Tabela 59. Limites para substâncias particuladas e gases

Contaminação	Limites
Particulada	<ul style="list-style-type: none"><li>• O ar do ambiente deve ser filtrado continuamente com uma eficiência de marca de poeira atmosférica de 40% (MERV 9) de acordo com o ASHRAE Standard 52.2<sup>1</sup>.</li><li>• O ar que entra em um datacenter deve ser filtrado a uma eficiência de 99,97% ou superior, usando filtros de ar particulado de alta eficiência (HEPA) que atendam ao MIL-STD-282.</li><li>• A umidade relativa deliquescente da contaminação por substância particulada deve ser superior a 60%<sup>2</sup>.</li><li>• O ambiente deve estar livre de contaminação condutora, como espanadores de zinco.</li></ul>
Gasosa	<ul style="list-style-type: none"><li>• Cobre: Classe G1 conforme ANSI/ISA 71.04-1985<sup>3</sup></li><li>• Prata: Taxa de corrosão de menos de 300 Å em 30 dias</li></ul>
<p><sup>1</sup> ASHRAE 52.2-2008 - <b>Método de Teste de Dispositivos Gerais de Limpeza de Renovação de Ar para Eficiência de Remoção por Tamanho de Partícula</b>. Atlanta: American Society of Heating, Refrigerating and Air-Conditioning Engineers, Inc.</p> <p><sup>2</sup> A umidade relativa deliquescente da contaminação por partículas é a umidade relativa na qual a poeira absorve água suficiente para ficar úmida e promover a condução iônica.</p> <p><sup>3</sup> ANSI/ISA-71.04-1985. <b>Environmental conditions for process measurement and control systems: Airborne contaminants</b>. Instrument Society of America, Research Triangle Park, Carolina do Norte, EUA.</p>	

---

## Declaração regulamentar de telecomunicação

Este produto pode não ser certificado em seu país para conexão por qualquer meio com interfaces de redes de telecomunicações públicas. Certificação adicional pode ser exigida por lei antes de fazer qualquer conexão desse tipo. Se tiver perguntas, entre em contato com o representante ou o revendedor da Lenovo.

---

## Avisos de Emissão Eletrônica

Ao conectar um monitor ao equipamento, você deve usar o cabo de monitor designado e quaisquer dispositivos de supressão de interferência fornecidos com o monitor.

Avisos de emissões eletrônicas adicionais estão disponíveis em:

<https://pubs.lenovo.com/>

## Declaração RoHS BSMI de 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 <sup>6+</sup> )	多溴聯苯 Polybrominated biphenyls (PBB)	多溴二苯醚 Polybrominated diphenyl ethers (PBDE)
機架	○	○	○	○	○	○
外部蓋板	○	○	○	○	○	○
機械組零件	-	○	○	○	○	○
空氣傳動設備	-	○	○	○	○	○
冷卻組零件	-	○	○	○	○	○
內存模塊	-	○	○	○	○	○
處理器模塊	-	○	○	○	○	○
鍵盤	-	○	○	○	○	○
調製解調器	-	○	○	○	○	○
監視器	-	○	○	○	○	○
滑鼠	-	○	○	○	○	○
電纜組零件	-	○	○	○	○	○
電源	-	○	○	○	○	○
儲備設備	-	○	○	○	○	○
電池匣組零件	-	○	○	○	○	○
有mech的電路卡	-	○	○	○	○	○
無mech的電路卡	-	○	○	○	○	○
雷射器	-	○	○	○	○	○
<p>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.</p> <p>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.</p> <p>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.</p>						

## Informações de contato de Taiwan para importação e exportação

Contatos estão disponíveis para informações de importação e exportação de 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



---

# Índice

## A

- a data e a hora, XClarity Controller
  - configurando 68
- a utilização do sistema
  - visualizando 54
- acesso remoto 2
- ajuda 179
- armazenamento
  - opções de configuração 79
- as informações do sistema
  - visualizando 53
- atributo de permissão de login
  - LDAP 117
- Atributo de pesquisa de UID
  - Servidor LDAP 117
- atributo de procura do grupo
  - LDAP 117
- autenticação de tentativa de login 17
- avisos 183
- avisos e instruções 8
- avisos importantes 184

## B

- Baseboard Management Controller (BMC) 1
- BIOS (sistema BIOS) 1
- BMC
  - configuração padrão 123
  - redefinir configuração 123

## C

- captura de tela azul 72
- captura de tela do sistema operacional 72
- Chassi D3 V2, XClarity Controller
  - configurando 69
- chave de ativação
  - exportação 88
  - gerenciar 117
  - instalar 87, 117
  - remover 87, 117
- chaves de criptografia
  - gerenciamento centralizado 45
- Chaves SSH
  - usuário 136
- CIM sobre HTTPS
  - gerenciamento de certificado 130
  - segurança 130
- coletando dados de serviço 180
- coletando log de dados de serviço 65
- Comando accsecfg 105
- Comando adapter 151
- Comando asu 106
- Comando backup 109
- Comando batch 140
- Comando clearlog 94
- Comando clock 141
- Comando dbgshbmc 152
- Comando dhcpinfo 110
- Comando dns 110
- Comando encaps 111
- Comando ethtousb 112
- Comando exit 93
- Comando fans 94
- Comando firewall 112

- Comando fuelg 104
- Comando hashpw 114
- Comando help 93
- Comando history 93
- Comando ifconfig 115
- Comando info 142
- Comando keycfg 117
- Comando ldap 117
- Comando led 95
- Comando mhlog 94
- Comando ntp 119
- Comando portcontrol 120
- Comando ports 121
- Comando power 102
- Comando pxeboot 105
- Comando rdmount 121
- Comando readlog 97
- Comando reset 103
- Comando restore 122
- Comando restoredefaults 123
- Comando roles 123
- Comando seccfg 124
- Comando securityinfo 124
- Comando securitymode 125
- Comando servicelog 98
- Comando set 125
- Comando snmp 126
- Comando snmpalerts 128
- Comando spreset 142
- Comando sshcfg 129
- Comando sslcfg 130
- Comando storage 143
  - dispositivos de armazenamento 143
- Comando syshealth 99
- Comando syslock 132
- Comando temps 100
- Comando thermal 133
- Comando TLS 134
- Comando trespass 135
- Comando uefiipw 135
- Comando usbeth 136
- Comando users 136
- Comando volts 101
- Comando vpd 101
- Comandos da ipmi
  - consumo de energia 63
- comandos de configuração 105
- Comandos de controle do IMM 140
- Comandos de suporte 152
- comandos de utilitário 93
- Comandos do
  - accsecfg 105
  - adaptador 151
  - armazenamento 143
  - asu 106
  - backup 109
  - clearlog 94
  - clock 141
  - configurar 125
  - dbgshbmc 152
  - dhcpinfo 110
  - dns 110
  - encaps 111
  - energia 102
  - ethtousb 112
  - firewall 112
  - fuelg 104
  - funções 123

- hashpw 114
- help 93
- histórico 93
- ifconfig 115
- informativo 142
- keycfg 117
- ldap 117
- led 95
- Lote 140
- mhlog 94
- ntp 119
- portas 121
- portcontrol 120
- pxeboot 105
- rdmount 121
- readlog 97
- redefinição 103
- restore 122
- restoredefaults 123
- sair 93
- seccfg 124
- securityinfo 124
- securitymode 125
- servicelog 98
- snmp 126
- snmpalerts 128
- sreset 142
- sshcfg 129
- sslcfg 130
- syshealth 99
- syslock 132
- temps 100
- térmica 133
- TLS 134
- trespass 135
- uefipw 135
- usbeth 136
- usuários 136
- ventiladores 94
- volts 101
- vpd 101
- comandos do monitor 93
- Comandos OEM IPMI 168
- Comandos sem agente 142
- comandos, lista alfabética 91
- comandos, tipos de
  - configuração 105
  - Controle do IMM 140
  - energia e reinicialização do servidor 102
  - monitor 93
  - Sem agente 142
  - Suporte 152
  - utilitário 93
- Comunidades de SNMPv1
  - gerenciar 126
- comutador
  - modo de segurança 42
- conexão de rede 10
  - endereço IP estático padrão 10
  - endereço IP estático, padrão 10
  - Endereço IP, estático padrão 10
- configuração do servidor
  - propriedade de servidor 66
- Configuração do Servidor
  - Configurar RAID 79
  - Detalhe do armazenamento 79
  - informações do adaptador 59
- configuração padrão
  - BMC 123
- configurações
  - Alerta SNMP 33
  - avançado 30, 46, 156
  - DDNS 32
  - designações de porta 35
  - DNS 32
  - Ethernet 30, 156
  - Ethernet sobre USB 32
  - LDAP 25
  - lista de bloqueios e restrição de tempo 35
  - login global 23
    - configurações de política de segurança da conta 24
  - Protetor do sistema 46
  - segurança 37
  - Servidor SSH 44
- configurações de rede
  - Comandos IPMI 35
- Configurações de SNMPv3
  - usuário 136
- configurações globais de login
  - configurações de política de segurança da conta 24
- configurando
  - a data e a hora do XClarity Controller 68
  - configurações globais de login 23
  - porta USB do painel frontal para gerenciamento 37
  - redirecionamento serial para SSH 89
- configurando o armazenamento
  - opções para configurar
    - o armazenamento 79
- configurando o servidor
  - opções para configurar
    - do servidor 59
- configurando o XClarity Controller
  - opções para configurar
    - o XClarity Controller 17
- configurando tempos limites do servidor 67
- configurar
  - Configurações de alerta SNMPv3 33
  - Configurações de Ethernet sobre USB 32
  - Configurações de LDAP 25
  - configurações de segurança 37
  - Configurações do DDNS 32
  - Configurações do DNS 32
  - Configurações Ethernet 30, 156
  - Contas de usuário de SNMPv3 136
  - Contato de SNMPv1 126
  - Contato de SNMPv3 126
  - data 141
  - DDNS 110
  - designações de porta 35
  - DNS 110
  - Ethernet 115
  - Ethernet sobre USB 112
  - evitar o rebaixamento do firmware do sistema 45
  - horário 141
  - IPMI 34
  - IPMI sobre acesso via KCS 44
  - IPv4 115
  - IPv6 115
  - LDAP 117
  - limitar o login simultâneo por conta do usuário 46
  - lista de bloqueios e restrição de tempo 35
  - Método de autenticação do usuário 105
  - MTU 115
  - negociação automática 115
  - níveis de segurança da conta do usuário 105
  - nome do host do 115
  - Porta da CLI SSH 121
  - porta de console remoto 121
  - porta de serviço de rede 120
  - Porta de Traps SNMP 121
  - Porta do agente do SNMP 121
  - Porta do CIM sobre HTTP 121
  - Porta do CIM sobre HTTPS 121
  - Porta do Servidor LDAP 117
  - Porta HTTP 121
  - Porta HTTPS 121
  - portas 121
  - Protetor do sistema 46
  - protocolos de rede 30
  - security password manager 45

- Servidor LDAP 117
- Servidor SSH 44
- SNMPv1 126
- tempo limite de inatividade da Web 105
- Traps SNMPv1 126
- unidade de transmissão máxima 115
- USB 112
- configurar números de porta 121
- Configurar RAID
  - Configuração do Servidor 79
- console remoto
  - captura de tela 72
  - comandos de energia e reinicialização 72
  - sessão de mídia virtual 71
  - suporte de teclado 73
  - visualizador de vídeo 71
- consumo de energia
  - Comandos da ipmi 63
- conta do usuário
  - criar 136
  - excluindo 21
- contaminação gasosa 185
- contaminação particulada 185
- contaminação, particulada e gasosa 185
- Contas de usuário de SNMPv3
  - configurar 136
- Contato de SNMPv1
  - configurar 126
- Contato de SNMPv3
  - configurar 126
- controle remoto de energia 72
- criando uma página da web de suporte personalizada 179
- criar
  - conta do usuário 136

## D

- dados de serviço 180
- data
  - configurar 141
- dcmi
  - funções e comandos 65
  - gerenciamento de energia 65
- DDNS
  - configurar 110
  - gerenciar 110
  - nome de domínio customizado 110
  - Nome de domínio especificado pelo servidor DHCP 110
  - origem de nome de domínio 110
- declaração regulamentar de telecomunicação 185
- Declaração RoHS BSMI de Taiwan 186
- definindo o local e o contato 66
- delete
  - usuário 136
- designações de porta
  - configurações 35
  - configurar 35
- Destinatários de SNMP TRAP 57
- Detalhe do armazenamento
  - Configuração do Servidor 79
- dispositivos de armazenamento
  - Comando storage 143
- DNS
  - configurar 110
  - endereçamento do servidor 110
  - Endereçamento IPv4 110
  - Endereçamento IPv6 110
  - Servidor LDAP 117
- domínio de procura
  - Servidor LDAP 117

## E

- encaminhamento de porta
  - Ethernet sobre USB 112
- endereçamento do servidor
  - DNS 110
- Endereçamento IPv4
  - DNS 110
- Endereçamento IPv6
  - DNS 110
- Endereço IP
  - configurando 9
  - IPv4 9
  - IPv6 9
  - Servidor LDAP 117
- endereço IP estático padrão 10
- endereço IP estático, padrão 10
- Endereço IP, estático padrão 10
- Endereço MAC
  - gerenciar 115
- energia
  - gerenciando com comandos da IPMI 63
  - monitorando com comandos da IPMI 63
- energia e reinicialização do servidor
  - Comandos do 102
- Ethernet
  - configurar 115
- Ethernet avançada
  - configurações 30, 156
- Ethernet sobre USB
  - configurar 112
  - encaminhamento de porta 112
- eventos ativos de sistema
  - visão geral 51
- evitar o rebaixamento do firmware do sistema
  - configurar 45
- exibir e configurar as unidades virtuais 79
- exportação
  - chave de ativação 88

## F

- Fazendo login no XClarity Controller 12
- Features on Demand
  - gerenciar 117
  - instalar recurso 117
  - remover recurso 117
- ferramentas
  - IPMItool 155
- filtro de grupo
  - LDAP 117
- firmware
  - servidor de visualização 101
- firmware do servidor
  - atualizando 83–84
- firmware, servidor
  - atualizando 83–84
- Flex System 1
- FoD
  - gerenciar 117
  - instalar recurso 117
  - remover recurso 117
- funcionamento do hardware 51
- Funções do XClarity Controller
  - na interface da Web 13
- funções e comandos
  - dcmi 65
  - node manager 64

## G

- gerenciamento centralizado

- chaves de criptografia 45
- Gerenciamento de BMC
  - Configuração do BMC
    - Fazer backup da configuração do BMC 47
    - fazer backup e restaurar a configuração do BMC 47
    - restaurar a configuração do BMC 48
    - restaurar para o padrão de fábrica 48
- gerenciamento de certificado
  - CIM sobre HTTPS 130
  - LDAP 130
  - Servidor HTTPS 130
  - Servidor SSH 129
- gerenciamento de energia
  - dcmi 65
  - ipmi bridging 64
- Gerenciamento de licenças 87
- gerenciamento do servidor
  - firmware do servidor 83–84
  - modo de inicialização do sistema 59
  - sequência de inicialização do sistema 59
  - tempos limites do servidor, configurando 67
  - única 60
- Gerenciamento do XClarity Controller
  - configurações de segurança 37
  - configurando contas de usuário 17
  - configurando o LDAP 17
  - criando um novo usuário local 19
  - criando uma função 18
  - exclusão de uma conta do usuário 21
  - Propriedades do XClarity Controller
    - Chassi D3 V2 69
    - data e hora 68
- gerenciando energia
  - usando comandos da IPMI 63
- gerenciar
  - chave de ativação 117
  - Comunidades de SNMPv1 126
  - DDNS 110
  - Endereço MAC 115
  - Features on Demand 117
  - FoD 117
  - usuário 136
- Guia Acesso a unidades
  - opção de segurança 45
- Guia Gerenciamento do Servidor
  - opção de gerenciamento de energia 60

## H

- histórico de manutenção 56
- horário
  - configurar 141

## I

- IMM
  - redefinição 142
  - restauração de configuração 122
  - restaurar configuração 122
  - spreset 142
- Informações de contato de Taiwan para importação e exportação 186
- informações do adaptador
  - Configuração do Servidor 59
- informações do sistema 53
- instalar
  - chave de ativação 87, 117
- instalar recurso
  - Features on Demand 117
  - FoD 117
- interface da linha de comandos (CLI)
  - acessando 89

- descrição 89
- efetuando login 89
- recursos e limitações 90
- sintaxe do comando 90
- interface da Web
  - fazendo login na interface da Web 12
- interface da Web, abrindo e usando 9
- Interface IPMI
  - descrição 155
- Introdução a MIBs 7
- inventário de armazenamento 81
- IPMI
  - configurar 34
  - gerenciamento de servidor remoto 155
- ipmi bridging
  - gerenciamento de energia 64
  - por meio do XClarity Controller 64
- IPMI sobre acesso via KCS
  - configurar 44
- IPMItool 155
- IPv4
  - configurar 115
- IPv6 9
  - configurar 115

## J

- janela de evento
  - log 55–56

## L

- LDAP
  - atributo de permissão de login 117
  - atributo de procura do grupo 117
  - configurando 17
  - configurar 117
  - filtro de grupo 117
  - gerenciamento de certificado 130
  - nome de destino do servidor 117
  - segurança 130
  - segurança aprimorada baseada em função 136
  - segurança baseada em função, aprimorada 136
  - Usuários do Active Directory 136
- limitar o login simultâneo por conta do usuário
  - configurar 46
  - limitar o login simultâneo por conta do usuário 46
- lista alfabética de comandos 91
- lista de bloqueios e restrição de tempo
  - configurações 35
- log de auditoria 56
- Log de auditoria estendida
  - log de auditoria estendida 45
- log de dados de serviço
  - coletando 65
  - fazendo download 65
- Log de eventos do 55
- login global
  - configurações 23

## M

- marcas registradas 184
- Método de autenticação do usuário 17
  - configurar 105
- método de ligação
  - Servidor LDAP 117
- métodos de montagem de mídia 73
- mínimos, níveis
  - TLS 134

modos de tela de console remoto 73  
módulo de gerenciamento avançado 1  
monitorando a energia  
usando comandos da IPMI 63  
monitorando o status de servidor 51  
MTU  
configurar 115

## N

negociação automática  
configurar 115  
níveis de segurança da conta do usuário  
configurar 105  
node manager  
funções e comandos 64  
nome de destino do servidor  
LDAP 117  
nome de destino, servidor  
LDAP 117  
nome de domínio, customizado  
DDNS 110  
nome de domínio, especificado pelo servidor DHCP  
DDNS 110  
nome distinto do cliente  
Servidor LDAP 117  
nome distinto raiz  
Servidor LDAP 117  
nome distinto, cliente  
Servidor LDAP 117  
nome distinto, raiz  
Servidor LDAP 117  
nome do host do  
configurar 115  
Servidor LDAP 117  
notas, importantes 184  
notificações por email e syslog 57  
nova conta local  
criando 19  
nova função  
criando 18  
número de porta  
Servidor LDAP 117  
números de portas  
configurar 121  
números de telefone 181  
números de telefone de serviço e suporte para hardware 181  
números de telefone de serviço e suporte para software 181

## O

Obtendo ajuda 179  
OneCLI 1  
opção  
SKM 45  
opção de gerenciamento de energia  
ações de energia 62  
Guia Gerenciamento do Servidor 60  
política de limitação de energia 61  
política de restauração de energia 62  
redundância de energia 61  
opção de mensagem de infração 67  
opção de segurança  
Guia Acesso a unidades 45  
origem de nome de domínio  
DDNS 110

## P

página da web de suporte personalizada 179

página da web de suporte, personalizar 179  
Porta da CLI SSH  
configurar 121  
porta de console remoto  
configurar 121  
porta de serviço de rede  
configurar 120  
Porta de Traps SNMP  
configurar 121  
Porta do agente do SNMP  
configurar 121  
Porta do CIM sobre HTTP  
configurar 121  
Porta do CIM sobre HTTPS  
configurar 121  
Porta do Servidor LDAP  
configurar 117  
Porta HTTP  
configurar 121  
Porta HTTPS  
configurar 121  
portas  
configurar 121  
configurar números 121  
visualizar abertas 121  
pré-configurado  
Servidor LDAP 117  
problemas de erro de montagem de mídia 77  
propriedade de servidor  
configuração do servidor 66  
definindo o local e o contato 66  
propriedades do protocolo de rede  
Configurações de alerta SNMP 33  
Configurações Ethernet 30, 156  
DDNS 32  
designações de porta 35  
DNS 32  
Ethernet sobre USB 32  
evitar o rebaixamento do firmware do sistema 45  
IPMI 34  
IPMI sobre acesso via KCS 44  
lista de bloqueios e restrição de tempo 35  
protetor do sistema  
Protetor do sistema 46  
Protetor do sistema  
configurações 46  
publicações online  
informações de atualização da documentação 1  
informações de atualização de firmware 1  
informações de código de erro 1

## R

recurso de console remoto 71  
ativando 72  
recursos de nível padrão 2  
recursos do XClarity Controller 2  
Recursos do XClarity Controller  
nível padrão 2  
Recursos do XClarity Controller recursos de nível platinum  
nível platinum 5  
redefinição  
IMM 142  
redefinir configuração  
BMC 123  
redirecionamento serial para SSH 89  
reiniciar o XClarity Controller 49  
remover  
chave de ativação 87, 117  
remover recurso  
Features on Demand 117  
FoD 117  
requisitos

- navegador da Web 6
- sistema operacional 6
- requisitos de navegador 6
- Requisitos de navegador da Web 6
- requisitos de sistema operacional 6
- restauração de configuração
  - IMM 122
- restaurar configuração
  - IMM 122

## S

- saindo da sessão de console remoto 78
- security password manager
  - configurar 45
  - security password manager 45
- segurança
  - alternar modo de segurança 42
  - CIM sobre HTTPS 130
  - Gerenciamento de certificado SSL 43
  - LDAP 130
  - manipulação de certificado ssl 42
  - Servidor HTTPS 130
  - Servidor SSH 44, 129
  - visão geral do modo de segurança 37
  - visão geral do painel de segurança 37
  - Visão geral do protetor do sistema 46
  - visão geral do ssl 42
- segurança aprimorada baseada em função
  - LDAP 136
- segurança baseada em função, aprimorada
  - LDAP 136
- senha
  - Servidor LDAP 117
  - usuário 136
- senha com hash 21
- Serial over LAN 155
- Serviço de soluções 68
- serviço e suporte
  - antes de fazer uma chamada 179
  - hardware 181
  - software 181
- Servidor
  - opções de configuração 59
- Servidor HTTPS
  - gerenciamento de certificado 130
  - segurança 130
- Servidor LDAP
  - Atributo de pesquisa de UID 117
  - configurar 117
  - DNS 117
  - domínio de procura 117
  - Endereço IP 117
  - método de ligação 117
  - nome distinto do cliente 117
  - nome distinto raiz 117
  - nome do host do 117
  - número de porta 117
  - pré-configurado 117
  - senha 117
- Servidor SSH
  - gerenciamento de certificado 129
  - segurança 129
- Servidores Flex 1
- SKM
  - opção 45
- SNMPv1
  - configurar 126
- SSL
  - gerenciamento de certificado 43
  - manipulação de certificado 42
- status de servidor
  - monitorar 51

- suporte a teclado no console remoto 73
- suporte a vários idiomas 7
- Suporte da versão do TLS
  - Suporte da versão do TLS 47

## T

- tempo limite de inatividade da sessão da Web 23
- tempo limite de inatividade da Web
  - configurar 105
- tempo limite do servidor
  - seleções 67
- ThinkSystem Server Firmware
  - descrição 1
- TLS
  - nível mínimo 134
- trabalhando com
  - eventos no log de auditoria 56
  - eventos no log de eventos 55
- Traps SNMPv1
  - configurar 126

## U

- única
  - configuração 60
- unidade de transmissão máxima
  - configurar 115
- usando
  - função do console remoto 71
  - recurso de console remoto 71
- USB
  - configurar 112
- usuário
  - Chaves SSH 136
  - Configurações de SNMPv3 136
  - delete 136
  - gerenciar 136
  - senha 136
- usuários
  - visualizar atuais 136
- Usuários do Active Directory
  - LDAP 136
- utilização do sistema 54

## V

- visão geral 51
  - modo de segurança 37
  - painel de segurança 37
  - protetor do sistema 46
  - ssl 42
- Visualizador de Vídeo
  - captura de tela 72
  - comandos de energia e reinicialização 72
  - modo de cor de vídeo 73
- visualizar atuais
  - usuários 136
- visualizar informações do firmware
  - Servidor 101
- visualizar portas abertas 121

## X

- XClarity Controller
  - conexão de rede 10
  - configurar o protocolo de rede 30
  - descrição 1
  - interface da Web 9

ipmi bridging 64  
Nível padrão do XClarity Controller 2  
Nível platinum do XClarity Controller 2  
novas funções 1  
opções de configuração 17

recursos 2  
redirecionamento serial 89  
XClarity Provisioning Manager  
Utilitário de configuração 10





**Lenovo**