Lenovo

Guia do usuário do XClarity Controller com Intel Xeon SP (1ª, 2ª geração)

Nota: Antes de usar estas informações, leia as informações gerais em Apêndice B "Avisos" na página 215.

Décima quinta edição (Maio de 2021)

© Copyright Lenovo 2017, 2022.
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 Nº GS-35F-05925.

Conteúdo

Conteúdo i

Capítulo 1. Introdução 1

Recursos de nível padrão, avançado e corporativo do XClarity Controller 2

- Recursos de nível padrão do XClarity Controller 2
- Recursos de nível avançado do XClarity Controller 5
- Recursos de nível corporativo 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 nova conta do usuário 18
- Exclusão de uma conta do usuário 20
- Usando as senhas com hash para autenticação 20
- 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 33
- Configurando o SNMP 34
- Habilitando ou desabilitando o acesso de rede à IPMI 34
- Configurando definições de rede com comandos do IPMI 34
- Ativação de serviço e atribuição de porta . . . 35
- Configurando a restrição de acesso 36
- Configurando a porta USB do painel frontal para gerenciamento 37

Configurando as definições de segurança 38

- Visão geral do SSL 38
- Manipulação de certificado SSL 38
- Gerenciamento de certificado SSL 39
- Configurando o servidor Shell Seguro 39
- Acesso da IPMI sobre Keyboard Controller Style (KCS) 40
- Evitar o rebaixamento do firmware do sistema 40
- Declarar Presença Física 40
- Configurando o Gerenciamento de Chaves de Segurança (SKM) 40
- Log de auditoria estendida 45
- Configuração de criptografia 45

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 48

Capítulo 4. Monitorando o status de servidor 49

Exibindo o resumo de funcionamento/eventos ativos de sistema 49

Exibindo as informações do sistema 50

Exibindo a utilização do sistema 52

Exibindo logs de eventos 53

Exibindo logs de auditoria 54

Exibindo o histórico de manutenção 54

Configurando destinatários de alertas 54

Capturando os dados da tela de falha mais recente do SO 56

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 61

- Configurando a redundância de energia . . . 61

© Copyright Lenovo 2017, 2022

Configurando a política de limitação de energia 61
Configurando a política de restauração de energia 62
Ações de energia 62
Gerenciando e monitorando o consumo de energia com os comandos da IPMI 63
Recurso de Console Remoto 65
Habilitando o recurso de console remoto . . . 66
Controle remoto de energia 67
Tela de captura do console remoto 67
Suporte a teclado de console remoto 68
Suporte a mouse de console remoto 68
Gravação/reprodução de tela de vídeo 69
Modos de tela de console remoto 69
Métodos de montagem de mídia 70
Disco remoto usando cliente Java 74
Problemas de erro de montagem de mídia . . 78
Saindo da sessão de console remoto 80
Baixando dados de serviço 80
Propriedades do servidor 80
Definindo o local e o contato 80
Configurando tempos limites do servidor . . . 81
Mensagem de infração 82
Definindo a data e a hora do XClarity Controller . . 82

Capítulo 6. Configurando o armazenamento 85
Detalhe de RAID 85
Configuração de RAID 85
Exibindo e configurando unidades virtuais . . 85
Exibindo e configurando o inventário de armazenamento 86

Capítulo 7. Atualizando o firmware de servidor 89
Visão Geral 89
Atualização de firmware do sistema, adaptador e PSU 89

Capítulo 8. Gerenciamento de licenças 91
Instalando uma chave de ativação 91
Removendo uma chave de ativação 92
Exportando uma chave de ativação 92

Capítulo 9. API REST do Redfish do Lenovo XClarity Controller. 93

Capítulo 10. Interface da linha de comandos 95
Acessando a interface da linha de comandos . . . 95
Fazendo login na sessão de linha de comandos . . 95
Configurando o redirecionamento serial para SSH 95
Sintaxe do comando 96
Recursos e limitações 96
Listagem alfabética de comandos 97
Comandos de utilitário 99
Comando exit 99
Comando help 99
Comando history 99
Comandos do monitor 100
Comando clearlog 100
Comando fans 101
Comando ffdc 101
Comando hreport 102
Comando mhlog. 103
Comando led 104
Comando readlog 105
Comando syshealth 106
Comando temps. 107
Comando volts 107
Comando vpd. 108
Comandos de controle de energia e reinicialização do servidor. 109
Comando power. 109
Comando reset 111
Comando fuelg 111
Comando pxeboot 112
Comando serial redirect 113
Comando console 113
Comandos de configuração 113
Comando accseccfg 113
Comando alertcfg 115
Comando asu 116
Comando backup 119
Comando dhcpinfo 120
Comando dns. 121
Comando encaps 123
Comando ethtousb 123
Comando firewall 124
Comando gprofile 125
Comando hashpw 126
Comando ifconfig 126
Comando keycfg 129
Comando ldap 130
Comando ntp 132
Comando portcfg 133
Comando portcontrol 134
Comando ports 135
Comando rdmount 136

Comando restore 137
Comando restoredefaults 138
comando roles 138
Comando seccfg 140
Comando set 140
Comando smtp 140
Comando snmp 141
Comando snmpalerts 143
Comando srcfg 145
Comando sshcfg 146
Comando ssl 147
Comando sslcfg 148
Comando storekeycfg 151
Comando syncrep 153
Comando thermal 154
Comando timeouts 154
Comando tls 155
Comando trespass 156
Comando uefipw 157
Comando usbeth 157
Comando usbfp 157
Comando users 158
Comandos de controle IMM 162
Comando alertentries 163
Comando batch 166
Comando clearcfg 166
Comando clock 167
Comando identify 167
Comando info 168
Comando spreset 168
Comandos sem agente 168
Comando storage 169
Comando adapter 178
Comando m2raid 180
Comandos de suporte 181
Comando dbgshimm 181

Capítulo 11. Interface IPMI 183
Gerenciando o XClarity Controller com a IPMI . . . 183
Usando o IPMItool 183
Comandos IPMI com parâmetros OEM 184
Obter/definir parâmetros de configuração LAN 184
Comandos OEM IPMI 196

Capítulo 12. Servidores Edge 207
Modo de bloqueio do sistema 207
Gerenciador da SED AK 208
Rede Edge 209

Apêndice A. Obtendo ajuda e assistência técnica 211
Antes de Ligar 211
Coletando dados de serviço 212
Entrando em contato com o Suporte 213

Apêndice B. Avisos 215
Marcas Registradas 216
Notas Importantes 216
Contaminação por partículas 217
Declaração regulamentar de telecomunicação . . . 217
Avisos de Emissão Eletrônica 217
Declaração RoHS BSMI de Taiwan 218
Informações de contato de Taiwan para importação e exportação 218

Índice 221

© Copyright Lenovo 2017, 2022

Capítulo 1. Introdução

O Lenovo XClarity Controller (XCC) é o controlador de gerenciamento da próxima geração que substitui o Baseboard Management Controller (BMC) para servidores Lenovo ThinkSystem.

Ele é a continuação do processador de serviços Integrated Management Module II (IMM2), que consolida os recursos de funcionalidade de processador de serviços, Super E/S, controlador de vídeo e 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 para os aplicativos de software e serviços adicionais relacionados à Web.

  Nota: O XClarity Controller oferece suporte à API do Redfish Scalable Platforms Management, especificação 1.0.2, e ao esquema 2016.2

Notas:

- 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.
- Para servidores Flex, o Chassis Management Module (CMM) é o módulo de gerenciamento primário para funções de gerenciamento de sistemas. O acesso ao XClarity Controller está disponível através da porta de rede no CMM.

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.

© Copyright Lenovo 2017, 2022

Recursos de nível padrão, avançado e corporativo do XClarity Controller

Com o XClarity Controller, são oferecidos os níveis padrão, avançado e corporativo da funcionalidade do produto. 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

Nota: Alguns recursos podem não se aplicar a servidores Flex System.

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

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
- CIM-XML
- DCMI 1.5
- SNMPv3
- SNMPv1 (apenas traps) requer atualizações de firmware do XCC mínimas v2.10 ou v2.12 dependendo do tipo de servidor. Consulte o arquivo Alteração de atualização de firmware do XCC para obter detalhes.

Outras interfaces de gerenciamento

- Web
- CLI legada
- 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

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
- Captura de tela azul (falha do SO)
- Ferramentas de diagnóstico integradas

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
- SNMPv1 (apenas traps)
- SSL
- SSH
- SMTP
- Cliente LDAP
- NTP
- SLP
- SSDP

Alertas

- Traps PET
- Indicação do CIM
- TRAPs SNMP
- E-mail
- Eventos Redfish

Redirecionamento serial

- IPMI SOL
- Configuração da porta serial

Segurança

- XClarity Controller Core Root of Trust for Measurement (CRTM)
- Atualizações de firmware assinado digitalmente
- Role Based Access Control (RBAC)
- Contas de usuários locais
- Contas do usuário LDAP/AD
- Retrocesso seguro do firmware
- Detecção de invasões do chassi (disponível somente em alguns módulos do servidor)
- Asserção remota XCC de Presença Física do UEFI TPM
- Criação de logs de auditoria das alterações de configuração e ações do servidor
- Autenticação de chave pública (PK)
- Desativação/realocação do sistema

Presença Remota

- Disco remoto na placa (RDOC): montagem de mídia virtual de arquivos ISO/IMG remotos por meio de CIFS, NFS, HTTP, HTTPS, FTP, SFTP e LOCAL

Gerenciamento de Energia

- Medidor de energia em tempo real

Gerenciamento de licenças

- Validação e repositório de chaves de ativação

Implantação e configuração

- Configuração remota
- Ferramentas de implantação e configuração e pacotes de Driver usando o XClarity Provisioning Manager integrado
- Backup e restauração da configuração

Atualizações de firmware

- Atualização livre de agente
- Atualização remota

Recursos de nível avançado do XClarity Controller

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

Todos os recursos do XClarity Controller Standard, além de:

Alertas

- Syslog

Presença Remota

- KVM remoto

Redirecionamento serial

- Redirecionamento serial via SSH

Segurança

- Security Key Lifecycle Manager (SKLM)
- Bloqueio de endereços IP

Gerenciamento de Energia

- Gráficos de energia em tempo real
- Contadores históricos de energia
- Gráficos de temperatura

Implantação e configuração

- Implantação remota do SO usando o XClarity Provisioning Manager integrado com o recurso KVM remoto do XClarity Controller

Recursos de nível corporativo do XClarity Controller

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

Todos os recursos do XClarity Controller Standard e Advanced, além de:

RAS

- Captura de inicialização

Presença Remota

- Controle de qualidade/largura da banda
- Colaboração de console virtual (seis usuários)
- Bate-papo de console virtual
- Mídia Virtual
  - Montagem de arquivos ISO/IMG remotos via console remoto
  - Montando arquivo da rede: - Montar um arquivo de imagem ISO ou IMG de um servidor de arquivos (HTTPS, CIFS, NFS) para o host como uma unidade de DVD ou USB

Gerenciamento de Energia

- Limitação de energia

- Monitoramento de desempenho OOB - medidas de desempenho do sistema

Implantação e configuração

- Implementação Remota usando o Lenovo XClarity Administrator. Ao usar o Lenovo XClarity Administrator para a implantação do sistema operacional, consulte https://pubs.lenovo.com/lxca/supported_operating_system_images para obter detalhes sobre os sistemas operacionais com suporte.

Atualizando o XClarity Controller

Se o seu servidor foi fornecido com o nível padrão ou avançado da funcionalidade de firmware do XClarity Controller, é provável que você consiga atualizar a funcionalidade do XClarity Controller em seu servidor. Para obter informações adicionais, sobre níveis de upgrade disponíveis e como pedi-los, consulte Capítulo 8 "Gerenciamento de licenças" na página 91.

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 48.0 ou superior (55.0 ou superior para o console remoto)
- Firefox ESR 38.6.0 ou acima
- Microsoft Edge
- Safari 9.0.2 ou acima (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:

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

- ECDHE-RSA-AES128-SHA256

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. Para acessar o XClarity Controller remotamente usando a interface da Web do XClarity Controller, você deve fazer login primeiro. 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:efff: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.

© Copyright Lenovo 2017, 2022

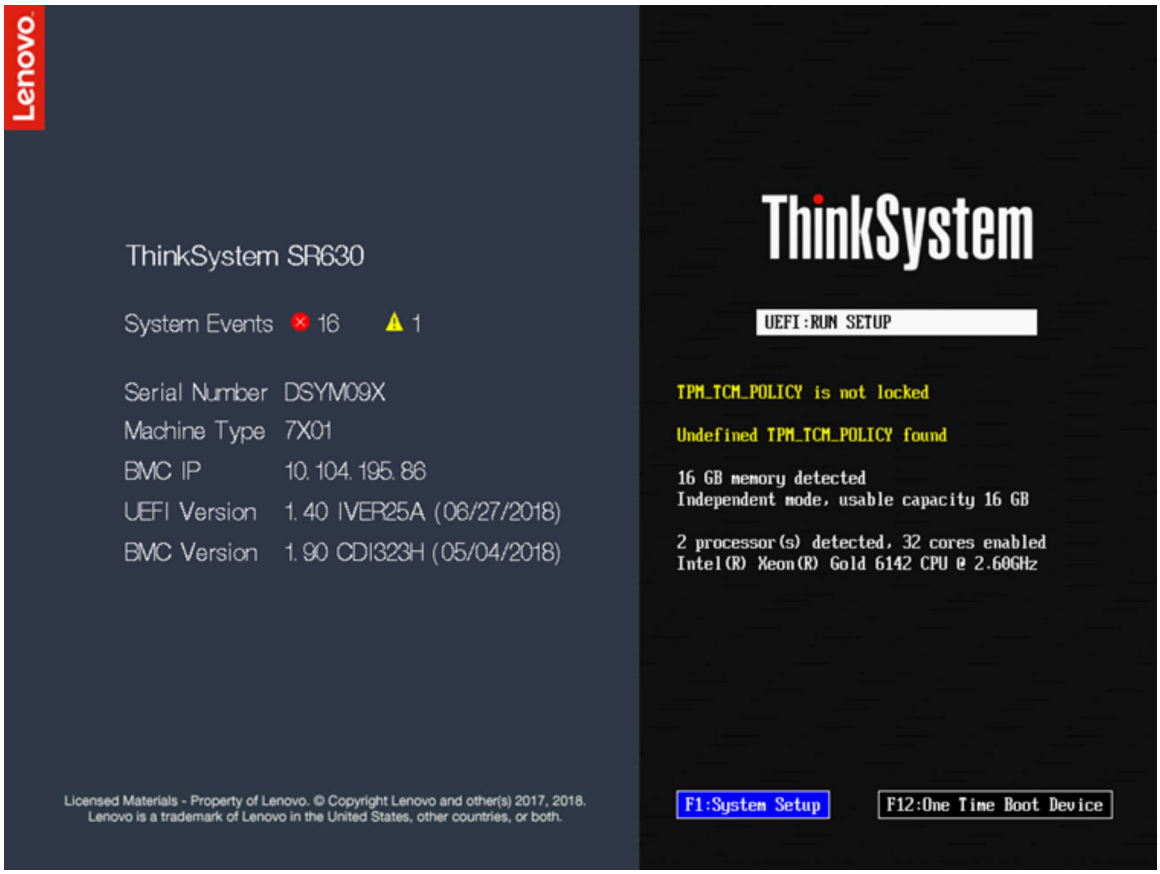
Configurando a conexão de rede do XClarity Controller por meio do XClarity Provisioning Manager

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.



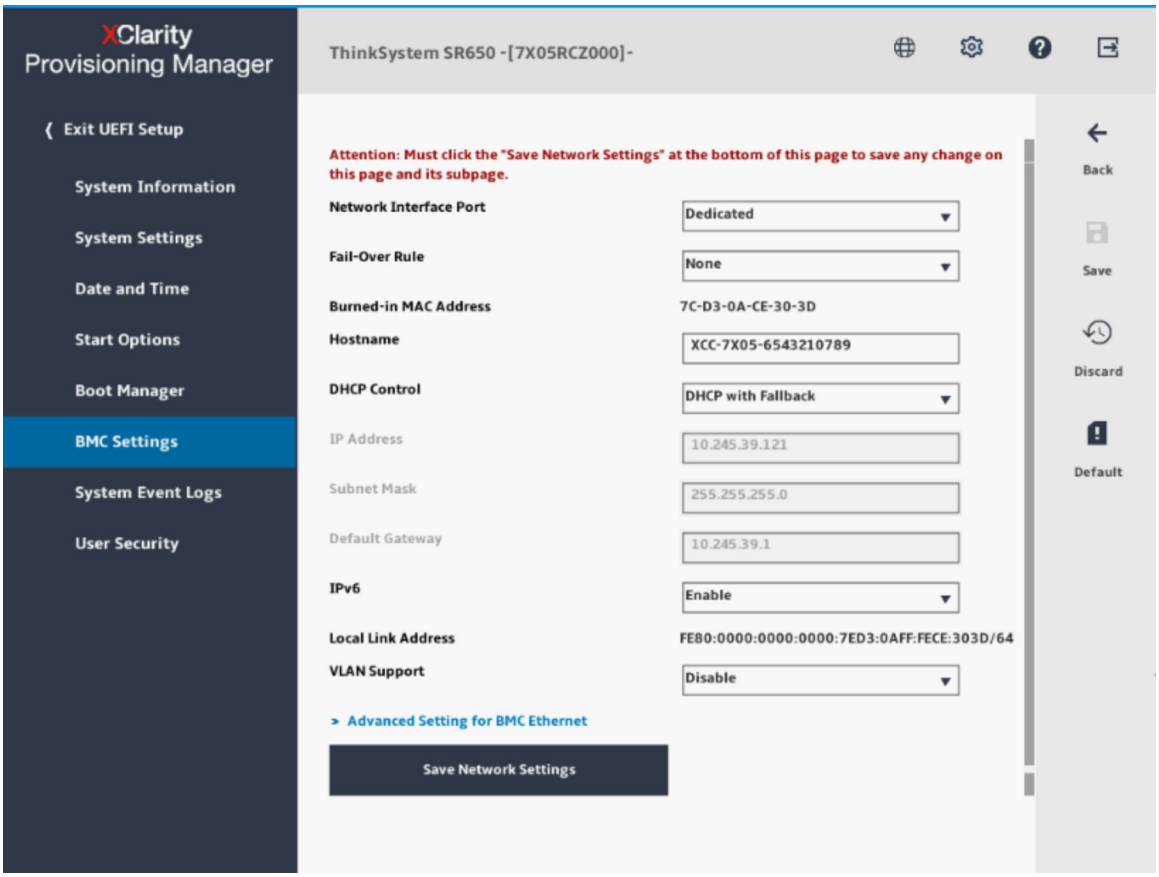
Etapa 2. Quando o prompt `<F1> System Setup` for exibido, pressione F1. Se tiver configurado uma senha de inicialização e uma senha de administrador, será necessário digitar a senha de administrador para acessar o XClarity Provisioning Manager.

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



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.

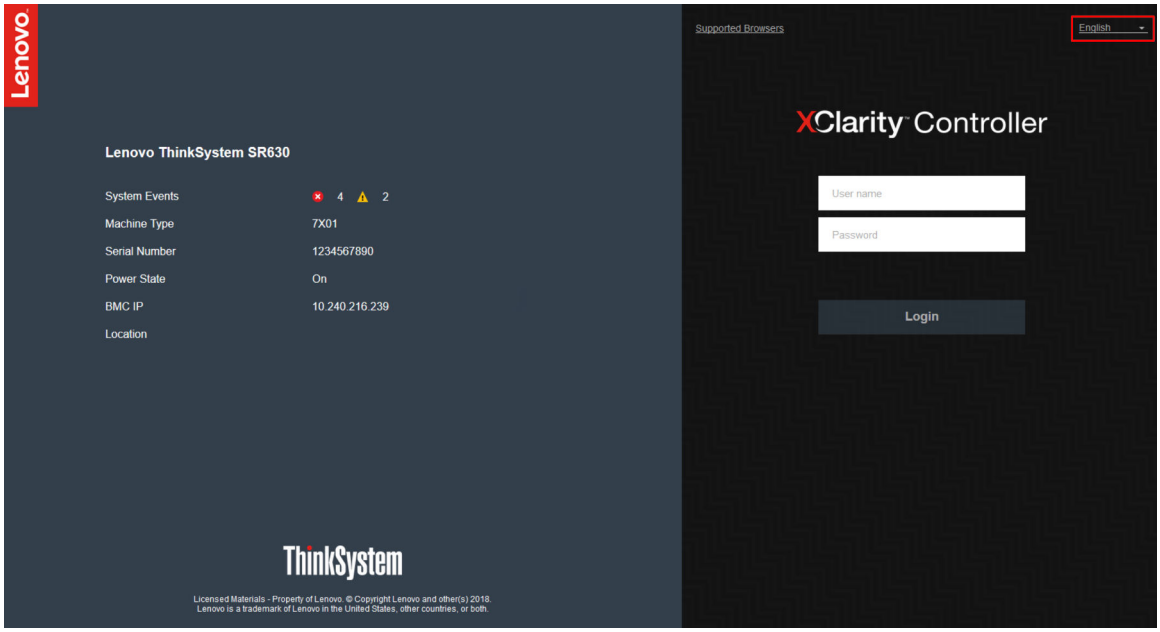
Nota: Em um Flex System, as contas de usuário do XClarity Controller podem ser gerenciadas por um Flex System Chassis Management Module (CMM) e podem ser diferentes da combinação USERID/PASSW0RD descrita acima.

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 o 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.

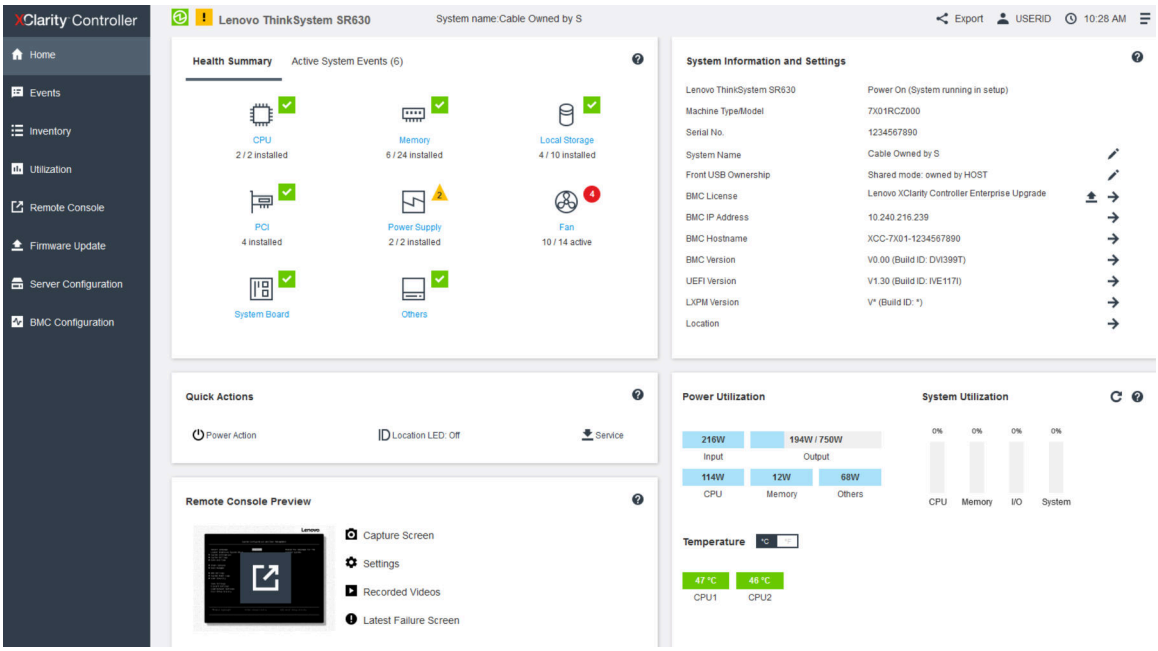
A janela Login é mostrada na ilustração a seguir.



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 **Log In** 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.



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 formatos 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

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.

Tabela 1. Funções do XClarity Controller

Tabela de três colunas contendo descrições das ações que podem ser realizadas na interface da Web do XClarity Controller.

Tab	Seleção	Descrição
Início	Resumo do funcionamento/ Eventos de sistema ativos	Mostra o status atual dos principais componentes de hardware no sistema.
	Informações e configurações do sistema	Fornece um resumo de informações comuns do sistema.

Tabela 1. Funções do XClarity Controller (continuação)

Tab	Seleção	Descrição
	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.
	Consumo de energia/ Utilização do sistema/ Temperatura	Fornece uma visão geral rápida da utilização de energia atual, da utilização do sistema e da temperatura geral do servidor.
	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. A barra de ferramentas direita inclui as seguintes ações rápidas: • Capturar tela • Configurações • Vídeos gravados • Tela de Falha mais Recente
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, como fazer login no Lenovo 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 e os controles em sistemas de TI.
	Histórico de manutenção	Exibe todo o histórico de atualização de firmware, configuração e substituição de hardware.
	Destinatários de alertas	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. **Nota:** Consulte a interface da Web do SMM2 para obter mais detalhes do status de energia da solução.
Utilização		Exibe a temperatura ambiente/do componente, a utilização de energia, os níveis de voltagem, a utilização de subsistema do sistema e as informações de velocidade do ventilador do servidor e seus componentes em formatos gráficos ou tabulares.
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.

Tabela 1. Funções do XClarity Controller (continuação)

Tab	Seleção	Descrição
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 conectada ao servidor.
Atualização de firmware		• Exibe níveis de firmware. • Atualiza o firmware do XClarity Controller e o firmware do servidor.
Configuração do Servidor	Adaptadores	Exibe informações dos adaptadores de rede instalados e as configurações que podem ser definidas por meio do XClarity Controller.
	Opções de inicialização	• Selecione o dispositivo de inicialização para inicialização única durante a próxima reinicialização do servidor. • Altere o modo de inicialização e as configurações de ordem de inicialização.
	Política de energia	• Configura a redundância de energia durante o evento de uma falha de fonte de alimentação. • Configura a política do limitação de energia. • Configure a política de restauração de energia. **Nota:** Consulte a interface da Web do SMM2 para obter mais detalhes do status de energia da solução.
	Propriedades do servidor	• Monitora várias propriedades, condições de status e configurações de seu servidor. • Gerencia tempos limite de início do servidor para detectar e fazer a recuperação de interrupções do servidor. • 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.
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.

Tabela 1. Funções do XClarity Controller (continuação)

Tab	Seleção	Descrição
	Usuário/LDAP	• Configura os perfis de login do XClarity Controller e as definições globais de login. • Exibe as contas do usuário que estão atualmente conectadas ao XClarity Controller. • 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.

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 em **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**.

© Copyright Lenovo 2017, 2022

Criando uma nova conta do usuário

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

Criar Usuário

Clique em **Criar** para criar uma nova conta do usuário.

Preencha os campos a seguir: **Nome do usuário**, **Senha**, **Confirmar Senha** e **Nível de Autoridade**. Para obter mais detalhes sobre o nível de autoridade, consulte esta seção.

Nível de autoridade do usuário

Os níveis de autoridade do usuário a seguir estão disponíveis:

Supervisor
O nível de autoridade do usuário Supervisor não possui restrições.

Somente Leitura
O nível de autoridade do usuário Somente Leitura tem acesso somente leitura e não executam ações como transferências de arquivo, ações de energia e reinicialização, ou funções de presença remota.

Personalizar
O nível de autoridade de usuário Customizado permite um perfil mais customizado para autoridade de usuário com configurações para as ações que o usuário tem permissão para executar.

Selecione um ou mais dos seguintes níveis de autoridade de usuário Customizados:

Configuração de Adaptador - Rede e Segurança
Um usuário pode modificar parâmetros de configuração nas páginas Segurança, Rede e Porta Serial.

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 de Adaptador - 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 de Adaptador - Avançado (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.

Quando um usuário define o nível de autoridade de um ID de login do XClarity Controller, o nível de privilégio da IPMI resultante do ID de Usuário da IPMI é definido de acordo com as seguintes prioridades:

- Se um usuário definir o nível de autoridade do ID de login do XClarity Controller como **Supervisor**, o nível de privilégio da IPMI será definido como Administrador.
- Se um usuário configurar o nível de autoridade do ID de login do XClarity Controller como **Somente Leitura**, o nível de privilégio da IPMI será definido como Usuário.
- Se um usuário definir o nível de autoridade do ID de login do XClarity Controller como qualquer um dos seguintes tipos de acesso, o nível de privilégio da IPMI será definido como Administrador:
  - Acesso ao Gerenciamento de Conta do Usuário
  - Acesso ao Console Remoto
  - Acesso ao Console Remoto e ao Disco Remoto
  - Configuração de Adaptador - Rede e Segurança
  - Configuração de Adaptador - Avançada
- Se um usuário definir o nível de autoridade do ID de login do XClarity Controller como **Acesso para Ligar/Reiniciar Servidor Remoto** ou **Capacidade para Limpar Logs de Eventos**, o nível de privilégio da IPMI será definido como Operador.
- Se um usuário configurar o nível de autoridade do ID de login do XClarity Controller como **Configuração de Adaptador - Básica**, o nível de privilégio da IPMI será definido como Usuário.

Configurações de SNMPv3

Para habilitar o acesso SNMPv3 para um usuário, marque a caixa de seleção ao lado de **Configurações de SNMPv3**. 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.

Endereço de traps
Especifique o destino do trap para o usuário. Esse pode ser um endereço IP ou nome de host. Usando traps, o agente do SNMP notifica a estação de gerenciamento sobre eventos (por exemplo, quando a temperatura de um processador excede o limite).

Protocolo de autenticação
Apenas **HMAC-SHA** tem suporte como o protocolo de autenticação. Esse algoritmo é usado pelo modelo de segurança SNMPv3 para autenticação.

Protocolo de privacidade
A transferência de dados entre o cliente SNMP e o agente pode ser protegida usando criptografia. Os métodos com suporte são **CBC-DES** e **AES**.

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 a página 72 no documento Padrão de Internet 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 incluir uma chave SSH na conta do usuário local, marque a caixa de seleção ao lado de **Chave SSH**. 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 CIM-XML 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 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.

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 seção **Security Password Manager** 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 292bcbc41bb078cf5bd258db60b63a4b337c8c954409442cfad7148bc6428fee

  $ sudo OneCli config set IMM.Loginid.3 Admin

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

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

- 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 292bcbc41bb078cf5bd258db60b63a4b337c8c954409442cfad7148bc6428fee

  > users -3 -n Admin -shp 292bcbc41bb078cf5bd258db60b63a4b337c8c954409442cfad7148bc6428fee
  -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.

Notas: Em um Flex System, as configurações de política de segurança da conta são gerenciadas pelo Flex System Chassis Management Module (CMM) e não podem ser modificadas no XCC. Quando o CMM é usado para configurar a política de segurança de conta, observe o seguinte:

- Diferente do XCC, o CMM não tem a configuração **Período de aviso de expiração da senha (dias)**. Quando o **Período de expiração da senha** estiver configurado como mais de 5 dias no CMM, a XCC definirá o período de aviso de expiração da senha como 5 dias. Por outro lado, se a configuração for menor que 5 dias, o período de aviso de expiração da senha será igual ao valor inserido no **Período de expiração da senha**.
- Para a configuração **Número máximo de falhas de login (vezes)**, o intervalo definido estabelecido no CMM é 0-100 vezes. No entanto, o intervalo definido no XCC é 0-10 vezes. Assim, quando o usuário selecionar um valor que excede 10 vezes no CMM, o XCC ainda definirá o número máximo de falhas de login como 10 vezes.
- Para a configuração **Intervalo mínimo de alteração de senha (horas)**, o intervalo definido estabelecido no CMM é 0-1440 horas. No entanto, o intervalo definido no XCC é 0-240 horas. Assim, quando o usuário selecionar um valor que excede 240 horas no CMM, o XCC ainda definirá o intervalo mínimo de alteração de senha como 240 horas.

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 ele efetuar login. O valor padrão para esse campo é ter a caixa de seleção habilitada.

Forçar que a senha da conta padrão seja alterada no próximo login
Uma opção de manufatura é fornecida para reconfigurar o perfil USERID padrão após o primeiro login bem-sucedido. Quando essa caixa de seleção é habilitada, a senha padrão deve ser alterada para que a conta possa ser usada. A nova senha está sujeita a todas as regras de cumprimento de senha ativas. 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 32 caracteres

Se a caixa de opção não estiver marcada, o número especificado no comprimento mínimo da senha poderá ser configurado como 0 – 32 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. Um valor de 0 a 30 dias é suportado. O valor padrão para esse campo é 14 dias.

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 expirar. Se for configurado como 0, nenhum aviso será enviado. Um valor de 0 a 30 dias é suportado. O valor padrão para esse campo é 14 dias.

Tamanho mínimo de senha

Esse campo contém o comprimento mínimo da senha. 8 a 32 caracteres são suportados para esse campo. O valor padrão para esse campo é 10.

Ciclo mínimo de reutilização de senha

Esse campo contém o número de senhas anteriores que não podem ser reutilizadas. Até 10 senhas anteriores podem ser comparadas. Selecione 0 para permitir a reutilização de todas as senhas anteriores. Um valor de 0 a 10 é suportado. O valor padrão para esse campo é 5.

Intervalo Mínimo de Mudança de Senha (Horas)

Esse campo contém quanto tempo um usuário deve aguardar entre as mudanças de senha. Um valor de 0 a 240 horas é suportado. O valor padrão para esse campo é 1 hora.

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. Um valor de 0 a 10 é suportado. O valor padrão para esse campo é cinco falhas de login.

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. Um valor de 0 a 2.880 minutos é suportado. O valor padrão para esse campo é 60 minutos.

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 Server)
- Serviço de diretório Microsoft Lightweight (Windows 2008, Windows 2012)
- Novell eDirectory Server, versões 8.7, 8.8 e 9.4
- Servidor OpenLDAP 2.1, 2.2, 2.3 e 2.4

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. Privilégios podem ser designadas a cada conta do usuário usando a sequência IBMRBSPermissions. 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 de grupos e privilégios podem ser configurados na seção Configurações do Active Directory.
   - **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 quatro 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 38.

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

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:

- **Nenhuma credencial é necessária**

  Use esse método para ligação sem um nome distinto (DN) ou senha. Esse método é altamente desencorajado porque a maioria dos servidores é configurada para não permitir solicitações de procura em registros de usuário específicos.

- **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, uma procura será executada para localizar uma entrada no servidor LDAP que pertence ao usuário que está efetuando login. Se necessário, será feita uma segunda tentativa de ligação, desta vez com o DN que é recuperado do registro LDAP do usuário e a senha que foi inserida durante o processo de login. Se a segunda tentativa de ligação falhar, o usuário terá o acesso negado. A segunda ligação só será executada quando os métodos de ligação **Nenhuma Credencial Necessária** ou **Usar Credenciais Configuradas** forem usados.

Nome distinto raiz (DN)

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 de UID

Quando o método de ligação é configurado para **Nenhuma Credencial Necessária** ou **Usar Credenciais Configuradas**, a ligação inicial para o servidor LDAP é seguida por uma solicitação de pesquisa que recupera informações específicas sobre o usuário, incluindo o DN do usuário, as permissões de login e a associação ao 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 **sAMAccountName**. Em servidores Novell eDirectory e OpenLDAP, o nome do atributo é **uid**. Se esse campo for deixado em branco, o padrão é **uid**.

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 logon 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.

A associação de grupo aninhado é suportada apenas em ambientes do Active Directory. Por exemplo, se um usuário for um membro de GroupA e GroupB, e GroupA também for um membro de GroupC, o usuário será considerado um membro de GroupC também. As procuras aninhadas serão paradas se 128 grupos tiverem sido procurados. Os grupos em um nível são procurados antes dos grupos em um nível inferior. Os loops não são detectados.

Atributo de Procura de Grupo

Em um ambiente Active Directory ou Novell eDirectory, o campo **Atributo de Procura de Grupo** especifica o nome do atributo que é usado para identificar os grupos aos quais um usuário pertence. Em um ambiente Active Directory, o nome do atributo é **memberOf**. Em um ambiente eDirectory, o nome do atributo é **groupMembership**. Em um ambiente do servidor OpenLDAP, os usuários geralmente são designados a grupos cujo objectClass equivale 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 o campo for deixado em branco, o usuário será designado a um padrão de permissões somente leitura, supondo que o usuário passe pela autenticação de usuário e de grupo.

O valor de atributo que é retornado pelo servidor LDAP procura a sequência de palavra-chave IBMRBSPermissions=. Essa sequência de palavra-chave deve ser seguida imediatamente por uma sequência de bits que é inserida como 12 0s ou 1s consecutivos. Cada bit representa um conjunto de funções. Os bits são numerados de acordo com suas posições. O bit mais à esquerda corresponde à posição de bit 0, e o bit mais à direita corresponde à posição de bit 11. Um valor 1 em uma posição de bit habilita a função que está associada a essa posição de bit. Um valor de 0 em uma posição de bit desativa a função que está associada a essa posição de bit.
A sequência IBMRBSPermissions=010000000000 é um exemplo válido. A palavra-chave IBMRBSPermissions= é usada para permitir que ela seja colocada em qualquer lugar nesse campo. Isso permite que o administrador de LDAP reutilize um atributo existente; portanto, evitando uma extensão para o esquema LDAP. Isso também permite que o atributo seja usado para seu propósito original. É possível incluir a sequência de palavra-chave em qualquer lugar nesse 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 2. 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) ou 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	Rede e Segurança	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.
7	Acesso para Ligar/ Reiniciar Servidor Remoto	Um usuário pode acessar as funções de ligação e reinicialização para o servidor remoto.
8	Configuração de Adaptador 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. **Nota:** Todos os usuários podem visualizar os logs de eventos; mas, para limpar os logs, o usuário precisa ter esse nível de permissão.

Tabela 2. Bits de permissão (continuação)

Posição do Bit	Função	Explicação
10	Configuração de Adaptador Avançada	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 XClarity Controller, modificar e restaurar a configuração de adaptador a partir de um arquivo de configuração e reiniciar/ reconfigurar o XClarity Controller.
11	Reservado	Essa posição de bit está reservada para uso futuro. Se nenhum dos bits for configurado, o usuário terá autoridade somente leitura. É dada prioridade às permissões de login que são recuperadas diretamente do registro do usuário. Se o atributo de permissão de login não estiver no registro do usuário, será feita uma tentativa de recuperar as permissões dos grupos aos quais o usuário pertence. Isso é executado como parte da fase de autenticação do grupo. É designado ao usuário o OR inclusivo de todos os bits para todos os grupos. O bit Acesso Somente Leitura (posição 2) será configurado apenas se todos os outros bits forem configurados para zero. Se o bit Negar Sempre (posição 0) for configurado para qualquer um dos grupos, o usuário terá o acesso recusado. O bit Negar Sempre (posição 0) sempre tem precedência sobre todos os outros bits.

Se nenhum desses bits for configurado, o padrão será configurado como **Somente leitura** para o usuário.

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.

Nota: 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.

3. Escolha se deverá ou não **Habilitar a segurança aprimorada baseada em funções para usuários do Active Directory** em **Configurações do Active Directory** (se o modo **Usar servidor LDAP para Autenticação e Autorização** for usado), ou configure os **Grupos para Autorização Local** (se **Usar o servidor LDAP apenas para Autenticação** (**com autorização local**) for usado).

   - **Ativar segurança aprimorada baseada em função para Usuários do Active Directory**

     Se a configuração de segurança aprimorada baseada em função estiver habilitada, um nome de servidor de formatação livre deverá ser configurado para atuar como o nome de destino para este XClarity Controller específico. O nome de destino pode ser associado a uma ou mais funções no servidor do Active Directory por meio de um Snap-RBS (Role Based Security). Isso é feito criando destinos gerenciados, dando nomes específicos a eles e associando-os às funções apropriadas. Se houver um nome configurado nesse campo, ele fornecerá a capacidade de definir funções

específicas para usuários e XClarity Controllers (destinos) que forem membros da mesma função. Quando um usuário faz login no XClarity Controller e é autenticado por meio do Active Directory, as funções das quais o usuário é membro são recuperadas do diretório. As permissões designadas ao usuário são extraídas das funções que também têm como membro um destino cujo nome corresponde ao nome do servidor configurado aqui ou um destino que corresponda a qualquer XClarity Controller. Vários XClarity Controllers podem compartilhar o mesmo nome de destino. Esse nome pode ser usado, por exemplo, para agrupar vários XClarity Controllers e atribuir a eles as mesmas funções usando um único destino gerenciado. Em contrapartida, cada XClarity Controller pode receber um nome exclusivo.

- **Grupos para Autorização Local**

  Os nomes de grupos são configurados para fornecer especificações de autorização local para grupos de usuários. Cada nome de grupo pode receber permissões (funções) que são as mesmas conforme descrito na tabela acima. O servidor LDAP associa usuários com um nome de grupo. Quando o usuário faz login, ele recebe as permissões associadas a um grupo ao qual ele pertence. Grupos adicionais podem ser configurados clicando no ícone "+" ou excluídos clicando no ícone "x".

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.

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 USB LAN nem 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 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.

Nota: Em um Flex System, as configurações de VLAN são gerenciadas pelo CMM do Flex System e não podem ser modificadas no XClarity Controller.

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 **Seleção de MAC**, escolha uma das seleções a seguir:

- 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

FFFFFFFFFFFF. 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 **Unidade Máxima de Transmissão**, especifique a unidade máxima de transmissão de um pacote (em bytes) para sua interface de rede. O intervalo de unidade de transmissão máxima é de 60 a 1500. O valor padrão para esse campo é 1500.

Para usar uma conexão de Ethernet IPv6, conclua as etapas a seguir:

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.

Nota: Em um Flex System, as configurações do DNS não podem ser modificadas no XClarity Controller. As configurações do DNS são gerenciadas pelo CMM.

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.

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 **Habilitar DDNS** para habilitar 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 a Ethernet sobre USB, não será possível executar uma atualização dentro da banda do firmware do XClarity Controller nem do firmware do servidor usando os utilitários de atualização do Linux ou do Windows.

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 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**
- **Usar endereço local de link IPv4 para Ethernet sobre USB**: Um endereço IP no intervalo 169.254.0.0/16 é atribuído ao XClarity Controller e ao lado de servidor da rede.
- **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:

1. 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.
2. 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.

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 **Trap SNMPv1**, **Trap SNMPv2** e/ou **Trap SNMPv3**.
3. Se ativar o **Trap SNMPv1** ou **Trap SNMPv2**, preencha os seguintes campos:
   a. No campo **Nome da comunidade**, insira o nome da comunidade; o nome 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.

Habilitando ou desabilitando o acesso de rede à IPMI

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

Clique em **Network** em **Configuração do BMC** para visualizar ou modificar as definições da IPMI do XClarity Controller. Conclua os campos a seguir para visualizar ou modificar configurações de IPMI:

IPMI sobre acesso via LAN
Clique no comutador para habilitar ou desabilitar o acesso de rede da IPIMI ao XClarity Controller.

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:

Web
O número da porta é 80. Esse campo não é configurável pelo usuário.

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

REST sobre HTTPS
O número da porta será alterado automaticamente para o especificado no campo Web sobre HTTPS. Esse campo não é configurável pelo usuário.

CIM sobre HTTP
Nesse campo, especifique o número da porta para o CIM sobre HTTP. O valor padrão é 5989.

Nota: O CIM permanece desabilitado por padrão.

Presença Remota
Nesse campo, especifique o número da porta para Presença Remota. O valor padrão é 3900.

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

Nota: O IPMI permanece desabilitado por padrão.

SFTP
Nesse campo, especifique o número da porta usado para o Protocolo de Transferência de Arquivos SSH (SFTP). O número da porta é 115. Esse campo não é configurável pelo usuário.

Nota: IMM.SFTPPortControl=open é necessário para atualizações dentro da banda do OneCLI.

SLP
Nesse campo, especifique o número da porta usado para o SLP. O número da porta é 427. Esse campo não é configurável pelo usuário.

Notas: Há dois tipos de serviço que o XClarity Controller relata:

- serviço: management-hardware.Lenovo:lenovo-xclarity-controller
- serviço: wbem

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.

Traps SNMP

Nesse campo, especifique o número da porta usado para traps SNMP. O valor padrão é 162. Os valores de números de porta válidos são de 1 a 65535.

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 deve ser posteriores à hora atual do XCC.
  - A data e a hora de término devem deve 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 deve 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.

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

Clique em **Network** em **Configuração do BMC** para visualizar ou alterar a porta USB do painel frontal do XClarity Controller para configurações de gerenciamento.

Existem quatro tipos de configurações para escolha:

Modo apenas host
A porta USB do painel frontal sempre é conectada apenas ao servidor.

Modo apenas BMC
A porta USB do painel frontal sempre é conectada apenas ao XClarity Controller.

Modo compartilhado: pertencente ao BMC
A porta USB do painel frontal é compartilhada pelo servidor e o XClarity Controller, mas a porta é alternada para o XClarity Controller.

Modo compartilhado: pertencente ao host
A porta USB do painel frontal é compartilhada pelo servidor e o XClarity Controller, mas a porta é alternada para o host.

Para obter informações adicionais sobre o aplicativo móvel, consulte o site a seguir:

https://pubs.lenovo.com/lxca/lxca_usemobileapp.html

Notas:

- Se a porta USB do painel frontal estiver configurada para o Modo Compartilhado, ela será conectada ao XClarity Controller quando hão houver energia e será conectada ao servidor quando houver energia. Quando houver energia, o controle da porta USB do painel frontal poderá ser alterada entre o servidor e o XClarity Controller. No modo compartilhado, a porta também pode ser alternada entre o host e o XClarity Controller pressionando e segurando o botão de identificação do painel frontal (para nós de cálculo, pode ser o botão de gerenciamento USB) por mais de 3 segundos.
- Quando configurado em modo compartilhado e a porta USB estiver conectada ao servidor, o XClarity Controller poderá oferecer suporte a uma solicitação para alternar a porta USB do painel frontal de volta para o XClarity Controller. Quando essa solicitação for executada, a porta USB frontal permanecerá conectada ao XClarity Controller até que não haja nenhuma atividade USB para o XClarity Controller durante o período especificado pelo tempo limite de inatividade.

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 155.

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

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.

É possível usar o SSL com um certificado autoassinado ou com um certificado assinado por uma autoridade de certificação de terceiros. O uso de um certificado autoassinado é o método mais simples para usar SSL, mas cria um risco de segurança pequeno. O risco existe porque o cliente SSL não tem uma maneira de validar a identidade do servidor SSL para a primeira tentativa de conexão entre o cliente e o servidor. Por exemplo, é possível que um terceiro possa personificar o servidor da Web do XClarity Controller e interceptar os dados que fluem entre o servidor da Web real do XClarity Controller e o navegador da Web do usuário. 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).

Para obter segurança mais completa, é possível usar um certificado assinado por uma autoridade de certificação (CA). Para obter um certificado assinado, você precisará selecionar **Gerar Solicitação de Assinatura de Certificado (CSR)**. Selecione **Baixar Solicitação de Assinatura de Certificado (CSR)** e envie a Solicitação de Assinatura de Certificado (CSR) para uma CA para obter um certificado assinado. Quando o certificado assinado for recebido, selecione **Importar Certificado Assinado** para importá-lo para o XClarity Controller.

A função da CA é verificar a identidade do XClarity Controller. Um certificado contém assinaturas digitais da CA e do XClarity Controller. Se uma CA reconhecida emitir o certificado ou se o certificado da CA já tiver sido importado para o navegador da Web, o navegador poderá validar o certificado e identificar positivamente o servidor da Web do XClarity Controller.

O XClarity Controller requer um certificado para usar com o Servidor HTTPS, o CIM sobre HTTPS e o cliente LDAP seguro. Além disso, o cliente LDAP seguro também requer que um ou mais certificados de confiança sejam importados. O certificado confiável é usado pelo cliente LDAP seguro para identificar positivamente o servidor LDAP. O certificado de confiança é o certificado da CA que assinou o certificado do servidor LDAP. Se o servidor LDAP usar certificados autoassinados, o certificado confiável poderá ser o certificado do

próprio servidor LDAP. Certificados confiáveis adicionais deverão ser importados se mais de um servidor LDAP for usado em sua configuração.

Gerenciamento de certificado SSL

Este tópico fornece informações sobre algumas ações que podem ser selecionados 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 dos certificados pode ser visualizado usando uma ferramenta de terceiros, como o OpenSSL (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 novamente**.
- 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 habilitar ou desabilitar o acesso IPMI sobre KCS.

Nota: Depois de alterar as configurações, você deve reiniciar o XClarity Controller para que as alterações entrem em vigor.

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 **Network** em **Configuração do BMC** para evitar o rebaixamento do firmware do sistema

Para habilitar ou desabilitar esse recurso, clique em **Network** em **Configuração do BMC**. Todas as alterações que forem feitas entrarão em vigor imediatamente sem que o XClarity Controller exija uma reinicialização.

Declarar Presença Física

Use as informações neste tópico para declarar e desativar a presença física na página da Web do XClarity Controller sem estar fisicamente presente no servidor.

Esse recurso estará disponível apenas se a **Política de Presença Física** for habilitada por UEFI. Uma vez habilitada, você pode acessar o recurso de presença física clicando em **Segurança** em **Configuração do BMC**.

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).

O XClarity Controller usa a rede para recuperar chaves do servidor Gerenciamento de Chaves; portanto, o servidor Gerenciamento de Chaves deve estar acessível ao XClarity Controller. O XClarity Controller fornece o canal de comunicação entre o servidor Gerenciamento de Chaves e o servidor ThinkSystem de solicitação. O firmware do XClarity Controller tenta se conectar com cada servidor Gerenciamento de Chaves configurado, parando quando uma conexão é estabelecida com êxito.

O XClarity Controller estabelecerá a comunicação com o servidor Gerenciamento de Chaves se as condições a seguir forem atendidas:

- Um ou mais endereços IP/nomes de host do servidor Gerenciamento de Chaves são configurados no XClarity Controller.
- Dois certificados (cliente e servidor) para comunicação com o servidor Gerenciamento de Chaves são instalados no XClarity Controller.

Nota: Configure pelo menos dois servidores Gerenciamento de Chaves (primário e secundário) com o mesmo protocolo para seu dispositivo. Se o servidor Gerenciamento de Chaves principal não responder à tentativa de conexão do XClarity Controller, tentativas de conexão serão iniciadas com os servidores Gerenciamento de Chaves adicionais até uma conexão bem-sucedida ser estabelecida.

Uma conexão TLS deverá ser estabelecida entre o XClarity Controller e o servidor Gerenciamento de Chaves. O XClarity Controller autentica o servidor Gerenciamento de Chaves comparando o certificado do servidor enviado pelo servidor Gerenciamento de Chaves, com o certificado do servidor Gerenciamento de Chaves importado anteriormente para o armazenamento confiável do XClarity Controller. O servidor Gerenciamento de Chaves autentica cada XClarity Controller que se comunica com ele e verifica se o XClarity Controller pode acessar o servidor Gerenciamento de Chaves. Essa autenticação é mantida comparando o certificado de cliente que o XClarity Controller envia com uma lista de certificados confiáveis armazenada no servidor Gerenciamento de Chaves.

Pelo menos, um servidor Gerenciamento de Chaves será conectado, e o grupo de dispositivos será considerado opcional. Será necessário importar o certificado do servidor Gerenciamento de Chaves e especificar o certificado de cliente. Por padrão, o certificado HTTPS é usado. Se desejar substituí-lo, poderá gerar um novo.

Nota: Para conectar o servidor KMIP (KeySecure e CipherTrust), é necessário gerar uma solicitação de assinatura de certificado (CSR), e seu nome comum deve ser corresponder ao nome do usuário definido no servidor KMIP e, em seguida, importar um certificado que foi assinado pela Autoridade de Certificação (CA) confiável pelo servidor KMIP para a CSR.

Configurando os servidores Gerenciamento de Chaves

Use as informações neste tópico para criar o nome do host ou o endereço IP e as informações de porta associadas do servidor Gerenciamento de Chaves.

A seção de configuração dos servidores Gerenciamento de Chaves consiste nos seguintes campos:

Nome do host ou endereço IP
Digite o nome do host (se o DNS estiver habilitado e configurado) ou o endereço IP do servidor Gerenciamento de Chaves nesse campo. É possível adicionar até 4 servidores.

Porta
Digite o número da porta para o servidor Gerenciamento de Chaves nesse campo. Se esse campo for deixado em branco, o valor padrão 5696 será usado. Os valores de números de porta válidos são de 1 a 65535.

Configurando o grupo de dispositivos

Use as informações neste tópico para configurar o grupo de dispositivos usados no servidor SKLM.

No servidor SKLM, um grupo de dispositivos permite que os usuários gerenciem as chaves de unidade autocriptografadas (SED) em vários servidores como um grupo. Um grupo de dispositivos com o mesmo nome também deve ser criado no servidor SKLM.

A seção Grupo de dispositivos contém o seguinte campo:

Grupo de dispositivos
Um grupo de dispositivos permite que os usuários gerenciem as SEDs em vários servidores como um grupo. Um grupo de dispositivos com o mesmo nome também deve ser criado no servidor SKLM. O valor padrão para esse campo é IBM_SYSTEM_X_SED.

Estabelecendo o gerenciamento de certificados

Este tópico fornece informações sobre o gerenciamento de certificados de cliente e servidor.

Certificados de cliente e servidor são usados para autenticar a comunicação entre o servidor SKLM e o XClarity Controller localizados no servidor ThinkSystem. O gerenciamento de certificados de cliente e servidor é abordado nesta seção.

Gerenciamento de certificado de cliente

Este tópico fornece informações sobre o gerenciamento de certificado de cliente.

Os certificados de cliente têm uma das seguintes classificações:

- Um certificado autoassinado do XClarity Controller.
- Um certificado gerado a partir de uma solicitação de assinatura de certificado (CSR) do XClarity Controller (externamente) por uma CA de terceiros.

Um certificado de cliente é necessário para comunicação com o servidor SKLM. O certificado de cliente contém assinaturas digitais para a CA e o XClarity Controller.

Notas:

- Os certificados são preservados entre as atualizações de firmware.
- Se um certificado de cliente não for criado para comunicação com o servidor SKLM, o certificado do servidor HTTPS do XClarity Controller será usado.
- A função da CA é verificar a identidade do XClarity Controller.

Para criar um certificado de cliente, clique no ícone de adição ( ) e selecione um dos seguintes itens:

- Gerar uma nova chave e um certificado autoassinado
- Gerar uma nova chave e uma solicitação de assinatura de certificado (CSR)

O item de ação **Gerar uma nova chave e um certificado autoassinado** gera uma nova chave de criptografia e um certificado autoassinado. Na janela Gerar nova chave e certificado autoassinado, digite ou selecione as informações nos campos obrigatórios e em todos os campos opcionais que se aplicam à sua configuração, (consulte a tabela a seguir). Clique em **OK** para gerar sua chave de criptografia e certificado. Uma janela de andamento será exibida enquanto o certificado autoassinado estiver sendo gerado. Uma janela de confirmação será exibida quando o certificado for instalado com êxito.

Nota: A nova chave de criptografia e certificado substituem qualquer certificado e chave existentes.

Tabela 3. Gerar uma nova chave e um certificado autoassinado

Tabela de duas colunas com cabeçalhos que documenta os campos obrigatórios e opcionais para a ação Gerar uma nova chave e um certificado autoassinado. A linha inferior se estende pelas duas colunas.

Tabela 3. Gerar uma nova chave e um certificado autoassinado (continuação)

Campo	Descrição
País[1]	No item de lista, selecione o país onde reside o BMC fisicamente.
Estado ou região[1]	Digite o estado ou a região onde reside o BMC fisicamente.
Cidade ou localidade[1]	Digite a cidade ou a localidade onde reside o BMC fisicamente.
Nome da organização[1]	Digite o nome da empresa ou da organização à qual pertence o BMC.
Nome do host do BMC[1]	Digite o nome do host do BMC que aparece na barra de endereços da Web.
Pessoa de Contato	Digite o nome da pessoa de contato responsável pelo BMC.
Endereço de e-mail	Digite o endereço de email da pessoa de contato responsável pelo BMC.
Unidade Organizacional	Digite a unidade na empresa à qual pertence o BMC.
Sobrenome	Digite o endereço da pessoa de contato responsável pelo BMC. Esse campo pode conter no máximo 60 caracteres.
Nome	Digite o nome da pessoa de contato responsável pelo BMC. Esse campo pode conter no máximo 60 caracteres.
Iniciais	Digite as iniciais da pessoa responsável pelo BMC. Esse campo pode conter no máximo 20 caracteres.
Qualificador de DN	Digite o qualificador de nome distinto para o BMC. Esse campo pode conter no máximo 60 caracteres.

1. Esse campo é obrigatório.

Quando o certificado do cliente for gerado será possível baixar o certificado para o armazenamento no XClarity Controller selecionando item de ação **Baixar Certificado**.

O item de ação **Gerar uma nova chave e uma solicitação de assinatura de certificado (CSR)** gera uma nova chave de criptografia e uma CSR. Na janela Gerar uma nova chave e uma solicitação de assinatura de certificado, digite ou selecione as informações nos campos obrigatórios e em todos os campos opcionais que se aplicam à sua configuração, (consulte a tabela a seguir). Clique em **OK** para gerar sua nova chave de criptografia e CSR.

É exibida uma janela de andamento enquanto a CSR é gerada, e uma janela de confirmação é exibida após a conclusão bem-sucedida. Após a geração da CSR, você deve enviá-la a uma CA para assinatura digital. Selecione o item de ação **Baixar solicitação de assinatura de certificado (CSR)** e clique em **OK** para salvar a CSR no servidor. É possível enviar a CSR para a CA para assinatura.

Tabela 4. Gerar uma nova chave e uma solicitação de assinatura de certificado

Tabela de duas colunas com cabeçalhos que documenta os campos obrigatórios e opcionais para a ação Gerar uma nova chave e uma ação de solicitação de assinatura de certificado. A linha inferior se estende pelas duas colunas.

Campo	Descrição
País[1]	No item de lista, selecione o país onde reside o BMC fisicamente.
Estado ou região[1]	Digite o estado ou a região onde reside o BMC fisicamente.
Cidade ou localidade[1]	Digite a cidade ou a localidade onde reside o BMC fisicamente.

Tabela 4. Gerar uma nova chave e uma solicitação de assinatura de certificado (continuação)

Campo	Descrição
Nome da organização[1]	Digite o nome da empresa ou da organização à qual pertence o BMC.
Nome do host do BMC[1]	Digite o nome do host do BMC que aparece na barra de endereços da Web.
Pessoa de Contato	Digite o nome da pessoa de contato responsável pelo BMC.
Endereço de e-mail	Digite o endereço de email da pessoa de contato responsável pelo BMC.
Unidade Organizacional	Digite a unidade na empresa à qual pertence o BMC.
Sobrenome	Digite o endereço da pessoa de contato responsável pelo BMC. Esse campo pode conter no máximo 60 caracteres.
Nome	Digite o nome da pessoa de contato responsável pelo BMC. Esse campo pode conter no máximo 60 caracteres.
Iniciais	Digite as iniciais da pessoa responsável pelo BMC. Esse campo pode conter no máximo 20 caracteres.
Qualificador de DN	Digite o qualificador de nome distinto para o BMC. Esse campo pode conter no máximo 60 caracteres.
Senha do Desafio	Digite a senha para a CSR. Esse campo pode conter no máximo 30 caracteres.
Nome Não Estruturado	Digite as informações adicionais, como um nome não estruturado que é designado ao BMC. Esse campo pode conter no máximo 60 caracteres.
1. Esse campo é obrigatório.	

A CSR é assinada digitalmente pela CA usando a ferramenta de processamento de certificado do usuário, como a ferramenta de linha de comando **OpenSSL** ou **Certutil**. Todos os certificados de cliente que são assinados usando a ferramenta de processamento de certificado do usuário têm o mesmo certificado **base**. Esse certificado **base** também deve ser importado para o servidor SKLM para que todos os servidores digitalmente assinados pelo usuário sejam aceitos pelo servidor SKLM.

Quando o certificado foi assinado pela CA, você deverá importá-lo para o BMC. Selecione o item de ação **Importar um certificado assinado** e selecione o arquivo para upload como o certificado do cliente; em seguida, clique em **OK**. Uma janela de progresso será exibida durante o upload do certificado assinado pela CA. Uma janela Upload de certificado será exibida se o andamento do upload for bem-sucedido. Uma janela Erro de upload de certificado será exibida se o andamento do upload não for bem-sucedido.

Notas:

- Para aumentar a segurança, use um certificado assinado digitalmente por uma CA.
- O certificado que foi importado para o XClarity Controller deve corresponder à CSR que foi gerada anteriormente.

Depois de importar um certificado assinado por uma CA para o BMC, selecione o item de ação **Baixar Certificado**. Quando você seleciona esse item de ação, o certificado assinado pela CA é baixado do XClarity Controller para armazenar em seu sistema.

Gerenciamento de certificados do servidor

Este tópico fornece informações sobre o gerenciamento de certificados do servidor.

O certificado de servidor é gerado no servidor SKLM e deve ser importado para o XClarity Controller para que a funcionalidade de acesso seguro a unidades funcione. Para importar o certificado que autentica o servidor SKLM para o BMC, clique em **Importar um Certificado** da seção Status de certificado do servidor da página Acesso a unidades. Um indicador de progresso é exibido conforme o arquivo é transferido para armazenamento no XClarity Controller.

Quando o certificado de servidor é transferido com êxito para o XClarity Controller, a área Status de certificado do servidor exibe o conteúdo a seguir: `A server certificate is installed.`

Caso deseje remover um certificado confiável, clique no botão **Remover** correspondente.

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.

Configuração de criptografia

Use as informações neste tópico para entender diferentes configurações de criptografia.

Modo de segurança alta

- Suporta apenas criptografias modernas e fortes.
- Compatível com NIST.
- Compatível com PFS (Perfect Forward Secrecy).

Modo de compatibilidade

- Dá suporte a uma ampla variedade de conjuntos de criptografia para máxima compatibilidade.
- Não compatível com PFS nem com NIST.

Modo compatível com NIST

- Dá suporte a uma ampla variedade de conjuntos de criptografia para máxima compatibilidade.
- Compatível com NIST.
- Compatível com PFS.

Suporte da versão do TLS

- TLS 1.0 e superior
- TLS 1.1 e superior
- TLS 1.2 e superior
- TLS 1.3

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

Consulte a tabela a seguir para ver os diferentes conjuntos de criptografia TLS suportados

Modo de segurança	**Versão TLS**	**Conjuntos de criptografia TLS**
Modo de segurança alta	TLS 1.3 e inferior	• TLS_AES_256_GCM_SHA384
Modo de segurança alta	TLS 1.2 e inferior	• TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 • TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 • TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
Modo compatível com NIST	TLS 1.3 e inferior	• TLS_AES_256_GCM_SHA384 • TLS_AES_128_GCM_SHA256
Modo compatível com NIST	TLS 1.2 e inferior	• TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 • TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 • TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 • TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 • TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 • TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 • TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 • TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 • TLS_DHE_RSA_WITH_AES_128_CBC_SHA256 • TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 • TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 • TLS_RSA_WITH_AES_256_GCM_SHA384 • TLS_RSA_WITH_AES_128_GCM_SHA256 • TLS_RSA_WITH_AES_256_CBC_SHA256 • TLS_RSA_WITH_AES_128_CBC_SHA256
Modo de compatibili-dade	TLS 1.3 e inferior	• TLS_AES_256_GCM_SHA384 • TLS_AES_128_GCM_SHA256 • TLS_CHACHA20_POLY1305_SHA256

Modo de segurança	Versão TLS	Conjuntos de criptografia TLS
Modo de compatibilidade	TLS 1.2 e inferior	• TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 • TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 • TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 • TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 • TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 • TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 • TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 • TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 • TLS_DHE_RSA_WITH_AES_128_CBC_SHA256 • TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384 • TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256 • TLS_RSA_WITH_AES_256_GCM_SHA384 • TLS_RSA_WITH_AES_128_GCM_SHA256 • TLS_RSA_WITH_AES_256_CBC_SHA256 • TLS_RSA_WITH_AES_128_CBC_SHA256
Modo de compatibilidade	TLS 1.1 e inferior	• TLS_RSA_WITH_AES_256_CBC_SHA256 • TLS_RSA_WITH_AES_128_CBC_SHA256

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.
2. Verifique o arquivo clicando em **Exibir conteúdo** para visualizar os 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**, todas as alterações de configuração anteriores serão perdidas. Se você deseja habilitar LDAP ao restaurar a configuração do BMC, será necessário primeiro importar um certificado de segurança confiável antes de fazer isso.
   - Após o término do processo, o XClarity Controller será reiniciado. Se este for um servidor local, a conexão TCP/IP será perdida, e talvez você precise reconfigurar a interface de rede para restaurar a conectividade.
   - A redefinição do BMC para o padrão de fábrica não está afetando as configurações de UEFI.

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

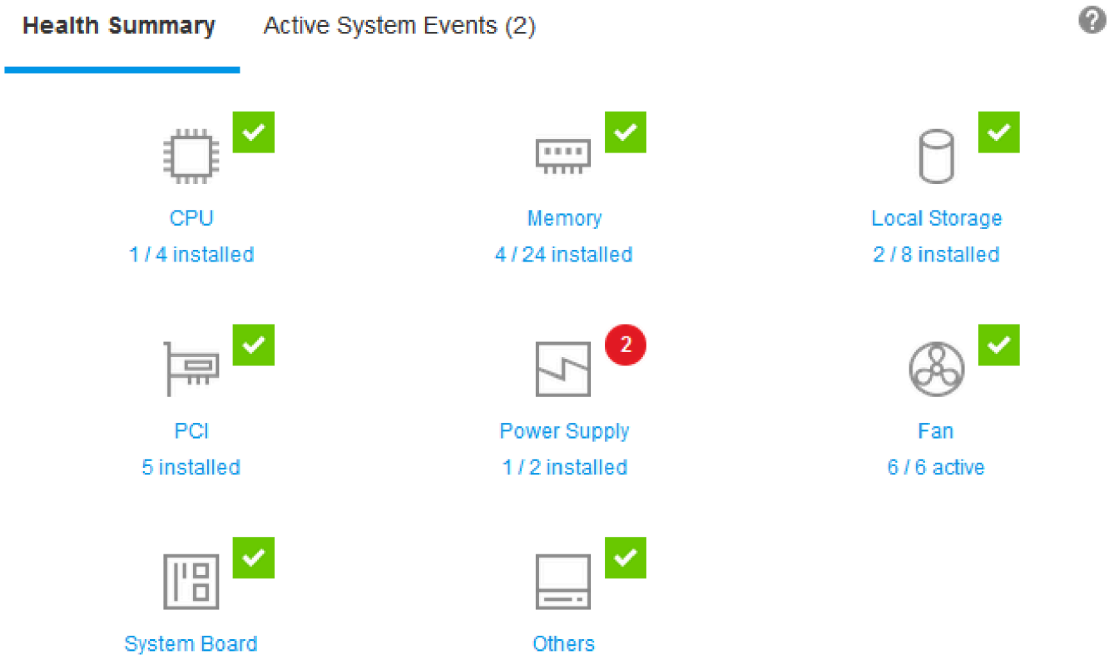
Use as informações neste tópico para entender como visualizar o resumo de funcionamento/eventos ativos de sistema.

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:

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

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

© Copyright Lenovo 2017, 2022



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.

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, você será direcionado para a página **Inventário**.

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 esquerda 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 do tipo de máquina
- Número de série
- Nome do sistema
- Propriedade do USB frontal
- Licença do BMC
- Endereço IP do BMC
- Nome do host do BMC
- Versão de UEFI
- Versão do BMC
- Versão de LXPM
- Local

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

Tabela 5. 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.
Sistema interrompido na UEFI	O servidor está ligado; a UEFI detectou um problema e parou de executar.
Inicializando o sistema operacional ou sistema operacional não suportado	O servidor pode estar nesse estado por um dos motivos a seguir: • O carregador do sistema operacional foi iniciado, mas o sistema operacional não está sendo executado • A interface Ethernet sobre USB do BMC está desativada. • O sistema operacional não possui os drivers carregados que suportam a interface Ethernet sobre USB.
Sistema operacional inicializado	O sistema operacional do servidor está em execução.
Suspender para RAM	O servidor foi colocado no estado de espera ou de suspensão.
Sistema em execução no teste de memória	O servidor está ligado e executando ferramentas de diagnóstico de memória.
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 desejar alterar a propriedade do USB frontal, clique no ícone de lápis e selecione o modo **Propriedade do USB frontal** desejado no menu suspenso. Em seguida, clique no visto verde.

Se o servidor tiver uma licença que não seja a licença corporativa 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 são todos provenientes do lado do ME (Gerenciador de nó), que incluem o seguinte:

- **Utilização da CPU**
  - Residência agregada do estado C
  - Tempo medido em C0 como porcentagem da residência de C0 usada e máxima (por segundo).
- **Utilização da Memória**
  - Volume R/W agregado de todos os canais de memória.
  - Largura de banda medida calculada como porcentagem da largura de banda de memória usada e máxima disponível (por segundo).

- **Utilização de E/S**
  - Volume R/W agregado das portas raiz no barramento PCIe *.
  - Largura de banda medida calculada como porcentagem da largura de banda de E/S usada e máxima disponível (por segundo).

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 azul que circunda o ícone indica que o tipo de evento em questão 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 53.

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 CIM-XML 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

Para incluir e modificar notificações por email e syslog ou destinatários de SNMP TRAP, use as informações neste tópico.

Leia a seguir uma descrição das ações que podem ser executadas na guia **Destinatários de Alertas**.

Os seguintes itens de ação podem ser executados na seção de destinatários de **E-mail/Syslog**.

- **Criar**: selecione esse item de ação para criar novos destinatários adicionais de email e Syslog. Até 12 destinatários de email e Syslog podem ser configurados.
  - **Criar destinatário de e-mail**: selecione esse item de ação para criar um destinatário de e-mail.
    - Insira o nome e o endereço de email do destinatário.
    - Selecione habilitar ou desabilitar a notificação de eventos. Se desabilitar for selecionado, a conta permanecerá configurada, mas nenhum email será enviado.

  - Selecione os tipos de eventos dos quais o destinatário será notificado. Se você clicar no menu suspenso ao lado dos rótulos das categorias Crítico, Atenção ou Sistema, poderá selecionar ou desmarcar notificações para componentes específicos na categoria.
  - Você pode escolher se deseja que o conteúdo do log de eventos seja ou não incluído nos alertas de email.
  - O índice especifica qual dos 12 slots de destinatários foi designado.
  - É possível configurar o servidor de emails para o qual os eventos serão encaminhados aqui ou clicando na ação do Servidor SMTP no início da seção. Consulte Servidor SMTP abaixo para obter detalhes de configuração.
- **Criar Destinatário de Syslog**: selecione esse item de ação para criar destinatários de syslog.
  - Insira o nome e o endereço IP ou o nome do host do servidor Syslog.
  - Selecione habilitar ou desabilitar a notificação de eventos. Se desabilitar for selecionado, a conta permanecerá configurada, mas nenhum email será enviado.
  - O índice especifica qual dos 12 slots de destinatários foi designado.
  - Selecione os tipos de eventos que serão enviados ao servidor Syslog. Se você clicar no menu suspenso ao lado dos rótulos das categorias Crítico, Atenção ou Sistema, poderá selecionar ou desmarcar notificações para componentes específicos na categoria.

- **Servidor SMTP**: selecione esse item de ação para definir as configurações relevantes para o servidor de email SMTP. Somente um servidor de email poderá ser configurado. A mesma configuração de email é usada ao enviar alertas para todos os destinatários de email configurados. O BMC alterna automaticamente de uma conexão segura para uma conexão criptografada para transferência de e-mail usando o comando STARTTLS uniformemente pela porta 587, se o servidor de e-mail de destino oferecer suporte a ele.
  - Insira o nome do host ou o endereço IP e o número de porta de rede do servidor de e-mail.
  - Se o servidor de email exigir autenticação, marque a caixa de seleção **Requerer Autenticação** e insira o nome de usuário e a senha. Selecione o tipo de autenticação necessária pelo servidor de Email, um método de resposta de desafio (**CRAM-MD5**) ou credenciais simples (**LOGIN**).
  - Algumas redes podem bloquear e-mails de saída se o valor de caminho inverso não for o esperado. Por padrão, o XClarity Controller usará alertmgr@domain, em que domain é o nome de domínio como especificado na seção DDNS de página da Web de rede do XClarity Controller. É possível especificar suas próprias informações de remetente em vez das informações padrão.
  - É possível testar a conexão com o servidor de e-mail para garantir que as configurações estejam corretas. O XClarity Controller exibirá uma mensagem que indica se a conexão foi ou não bem-sucedida.
- **Nova Tentativa e Atraso**: selecione esse item de ação para definir as configurações relevantes para as opções de nova tentativa e atraso.
  - O limite de nova tentativa especifica o número de vezes que o XClarity Controller tentará enviar um alerta se a tentativa inicial não for bem-sucedida.
  - O atraso entre entradas especifica o tempo que o XClarity Controller aguardará depois de enviar um alerta para um destinatário antes de enviar um alerta para o próximo destinatário.
  - O atraso entre tentativas especifica o tempo que o XClarity Controller aguardará após uma tentativa com falha antes de tentar novamente enviar o alerta.
- **Protocolo**: selecione esse item de ação para definir as configurações relevantes para o protocolo de conexão.
  - É possível escolher entre **Protocolo TCP** ou **Protocolo UDP**. Observe que essa configuração será aplicada a todos os destinatários do syslog.
- Se destinatários de Email ou Syslog forem criados, eles serão indicados nesta seção.

  - Para editar as configurações para um destinatário de Email ou Syslog, clique no ícone de lápis abaixo do cabeçalho de ação na linha ao lado do destinatário que você deseja configurar.
  - Para excluir um destinatário de Email ou Syslog, clique no ícone de lixeira.
  - Para enviar um alerta de teste para um destinatário de E-mail ou Syslog, clique no ícone de avião de papel.

As seguintes ações podem ser executadas no segmento de usuário de **SNMPv3**.

- **Criar**: selecione esse item de ação para criar destinatários de SNMPv3 TRAP.
  - Selecione a conta de usuário que deve estar associada às SNMPv3 TRAPs. A conta de usuário deve ser uma das doze contas de usuário locais.
  - Especifique o nome do host ou o endereço IP do gerenciador de SNMPv3 que receberá os TRAPs SNMPv3.
  - O XClarity Controller usa o algoritmo hash HMAC-SHA para fazer a autenticação com o gerenciador de SNMPv3. Este é o único algoritmo suportado.
  - A senha de privacidade será usada com o protocolo de privacidade para criptografar os dados SNMP.
  - A **configuração global SNMPv3** se aplica a todos os destinatários de SNMPv3 TRAP. Essas configurações podem ser definidas ao criar um destinatário de SNMPv3 TRAP ou clicando na ação Configurações SNMPv3 na parte superior do segmento de usuário **SNMPv3**.
    - Selecione habilitar ou desabilitar SNMPv3 TRAPs. Se não forem habilitadas, as configurações permanecerão definidas, mas nenhum TRAP SNMPv3 será enviado.
    - O contato e informações de local do BMC são necessários e são configurados na página da Web Propriedades do Servidor. Consulte "Definindo o local e o contato" na página 80 para obter mais informações.
    - Selecione os tipos de eventos que farão com que TRAPs sejam enviadas ao gerenciador de SNMPv3. Se você clicar no menu suspenso ao lado dos rótulos das categorias Crítico, Atenção ou Sistema, poderá selecionar ou desmarcar notificações para componentes específicos na categoria.

  Nota: A transferência de dados entre o cliente SNMP e o agente pode ser protegida usando criptografia. Os métodos suportados para o **protocolo de privacidade** são CBC-DES e AES.
- Se destinatários de TRAP SNMPv3 forem criados, eles serão indicados nesta seção.
  - Para editar as configurações para um destinatário de TRAP SNMPv3, clique no ícone de lápis abaixo do cabeçalho de ação na linha ao lado do destinatário que você deseja configurar.
  - Para excluir um destinatário de SNMPv3, clique no ícone de lixeira.

Capturando os dados da tela de falha mais recente do SO

Use as informações neste tópico para visualizar e capturar uma tela de falha do sistema operacional.

A tela do sistema operacional é capturada automaticamente quando ocorre o tempo limite de watchdog do SO. Se ocorrer um evento que faça com que o SO pare a execução, o recurso Watchdog do SO será acionado e o conteúdo da tela será capturado. O XClarity Controller armazena apenas uma captura de tela. Quando ocorre o limite de watchdog do SO, uma nova captura de tela substitui a captura de tela anterior. O recurso Watchdog do S.O. deve ser habilitado para capturar a tela de falha do S.O. Para definir o horário de watchdog do SO, consulte "Configurando tempos limites do servidor" na página 81 para obter mais informações. O recurso de captura de tela de falha do SO está disponível apenas com a funcionalidade Avançada do XClarity Controller ou o Nível Corporativo. Consulte a documentação de seu servidor para obter informações sobre o nível de funcionalidade do XClarity Controller instalada em seu servidor.

Clique na ação **Tela de Falha Mais Recente** na seção **Console Remoto** da página inicial do XClarity Controller para exibir uma imagem da exibição do sistema operacional que foi capturada quando ocorreu o limite de watchdog do SO. A captura também pode ser exibida clicando em **Serviço** e, em seguida, em **Tela de Falha Mais Recente** na seção **Ação Rápida** da página inicial. Se o sistema não passou por um tempo limite de watchdog do SO e não capturou a tela de SO, uma mensagem indicando que a tela de falha não foi criada será exibida.

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

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.

Notas:

- 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 o modo e a sequência 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 o modo de inicialização do sistema, as duas opções a seguir estão disponíveis:

Inicialização de UEFI
Selecione esta opção para configurar um servidor que seja compatível com Unified Extensible Firmware Interface (UEFI). Se estiver inicializando sistemas operacionais habilitados para UEFI, essa opção poderá diminuir o tempo de inicialização desativando ROMs opcionais herdadas.

Inicialização legada
Selecione essa opção se você estiver configurando um servidor para inicializar um sistema operacional que requer o firmware legado (BIOS). Selecione essa opção apenas se estiver inicializando sistemas operacionais não habilitados para UEFI.

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

© Copyright Lenovo 2017, 2022

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.

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

Quando você altera o tipo de inicialização a ser executada com o dispositivo de inicialização única, também pode especificar a inicialização como legada ou UEFI. Clique na caixa de seleção **Preferir inicialização legada** se você desejar que a inicialização seja de BIOS legado. Desmarque a caixa se desejar uma inicialização UEFI. 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 chassi que contém nós de servidor blade ou de alta densidade, o resfriamento e a energia do chassi são controlados pelo controlador de gerenciamento de chassi em vez do XClarity Controller.

Configurando a redundância de energia

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

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

- **Redundante (N+N)**: neste modo, o servidor não permanecerá operacional caso ocorra perda de uma fonte de alimentação.
  - **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.
- **Redundante (N+1)**: neste modo, o servidor não permanecerá operacional caso ocorra perda de uma fonte de alimentação quando quatro fontes de alimentação estão instaladas.
- **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.

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 quantia 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 limitação de energia pode ser ativada usando medidas de consumo de energia CA ou CC. No menu suspenso, selecione o tipo das medidas que serão usadas para determinar a limitação de energia. Ao alternar entre CA e CC, 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.

Nota: A opção **Políticas de energia** não está disponível quando o XClarity Controller está em um chassi que contém nós de servidor blade ou de alta densidade. A política de energia é controlada pelo controlador de gerenciamento de chassi em vez do XClarity Controller.

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.

Sempre Ligado
O servidor será ligado automaticamente quando a energia for restaurada.

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

Nota: A opção **Políticas de restauração de energia** não está disponível em um chassi que contém nós de servidor blade ou de alta densidade. A política de restauração de energia é controlada pelo controlador de gerenciamento de chassi em vez do XClarity Controller.

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 6. 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.
Desligue o 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.

Tabela 6. Ações de Energia e Descrições (continuação)

Ação de Energia	Descrição
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 non-maskable interrupt (NMI)	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.
Nota: 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.	

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` **<PASSW0RD>** `raw` **0x3a 0xc7 0x01**

Para desativar comandos de IPMI nativos do Node Manager, digite:`ipmitool -H` **<$XClarity_Controller_IP>** `-U` **<USERID>** `-P` **<PASSW0RD>** `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 comando0xC8): Solicitação:`ipmitool -H` **<$XClarity_Controller_IP>** `-U` **<USERID>** `-P` **<PASSW0RD>** `-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` **<PASSW0RD>** `-b` **0x00** `-t` **0x2c** `raw` **0x2e 0xC1 0x57 0x01 0x00 0x10 0x01 0xA0 0x00 0x00 0x00 0x60 0xea 0x00 0x00 0x00 0x00 0x1e 0x00**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` **<PASSW0RD>** `-b` **0x00** `-t` **0x2c** `raw` **0x2e 0xC1 0x57 0x01 0x00 0x10 0x01 0x00 0x00 0x00 0x00 0x60 0xea 0x00 0x00 0x00 0x00 0x1e 0x00**

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` **<PASSW0RD>** `-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` **<PASSW0RD>** `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` **PASSW0RD** `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` **<PASSW0RD>** `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` **<PASSW0RD>** `raw` **0x2c 0x05 0xdc 0x01 0x00 0x00** Resposta:`dc`

Desativar limite de energia: Solicitação:`ipmitool -H` **<$XClarity_Controller_IP>** `-U` **<USERID>** `-P` **<PASSW0RD>** `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.

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 do XClarity Controller Advanced e do XClarity Controller Enterprise e apenas pela 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 informações adicionais sobre upgrade do XClarity Controller Standard para o XClarity Controller Advanced ou XClarity Controller Enterprise, consulte "Atualizando o XClarity Controller" na página 6.

Use os recursos de console remoto para fazer o seguinte:

- Visualizar remotamente o vídeo com resolução gráfica de até 1280 x 1024 em 72 ou 75 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 50 MB podem ser carregados na memória de XClarity Controller.

Notas:

- Quando o recurso de console remoto é iniciado no modo multiusuário (o XClarity Controller com o conjunto de recursos do XClarity Controller Enterprise 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.

Como mencionado antes, a funcionalidade de console remoto do XClarity Controller está disponível apenas nos recursos do XClarity Controller Advanced e do XClarity Controller Enterprise. 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 do XClarity Controller Advanced, instale-o usando as instruções em "Instalando uma chave de ativação" na página 91.

Para usar a funcionalidade do console remoto, conclua estas etapas:

1. Clique na imagem com uma seta branca apontando na diagonal na seção Console Remoto da página inicial do XClarity Controller ou na página da Web do console remoto.
2. Selecione um dos modos a seguir:
   - Iniciar o console remoto no modo de usuário único
   - Iniciar o console remoto no modo multiusuário

   Nota: O conjunto de recursos do XClarity Controller com XClarity Controller Enterprise suporta até seis sessões de vídeo simultâneas no modo multiusuário.

3. Especifique se você permite ou não que outros peçam para enviar uma solicitação de desconexão para um usuário de console remoto quando alguém desejar usar o recurso do console remoto e o recurso já estiver em uso no modo de usuário único, ou quando o número máximo de usuários estiver usando o recurso do console remoto no modo multiusuário. **Nenhum intervalo de tempo de resposta** especifica quanto tempo o XClarity Controller aguardará antes de desconectar automaticamente o usuário se nenhuma resposta de solicitação de desconexão for recebida.
4. Especifique se você permite ou não o registro dos três últimos vídeos de inicialização de servidor.
5. Especifique se você permite ou não o registro dos três últimos vídeos de falha de servidor.
6. Selecione se deve ou não permitir a captura de tela de falha do SO com erro de HW.
7. Clique em **Iniciar o console remoto** para abrir a página do console remoto em outra guia. Quando todas as possíveis sessões de console remoto estiverem em uso, uma caixa de diálogo aparecerá. Nessa caixa de diálogo, o usuário pode enviar uma solicitação de desconexão para um usuário do console remoto que habilitou a configuração **Permitir que outros solicitem minha desconexão de sessão remota**. O usuário pode aceitar ou negar a solicitação de desconexão. Se o usuário não responder no intervalo especificado pela configuração **Nenhum intervalo de tempo de resposta**, a sessão do usuário será finalizada automaticamente pelo XClarity Controller.

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 PNG.

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. Outras macros definidas pelo servidor podem ser definidas usando o Lenovo XClarity Essentials e baixadas a partir do XClarity Controller. Essas macros são definidas para todos os usuários do recurso do console remoto.
- Clique em **Configurar** para adicionar ou remover macros definidas pelo usuário. As macros definidas pelo usuário são definidas apenas para o usuário atual do console remoto. Outros usuários do console remoto não verão as macros definidas pelo usuário uns dos outros.
  - Clique no ícone Adicionar macros e pressione as sequências de teclas desejadas. Em seguida, clique em **Adicionar** para adicionar uma nova macro.
  - Para remover uma macro definida pelo usuário, selecione a macro na lista e clique no ícone de lixeira.
  - Para enviar uma macro definida pelo usuário para o servidor, selecione a opção **Macros definidas pelo usuário** e clique na macro que deseja enviar.

Suporte a mouse de console remoto

Use estas informações para entender as opções de controle de mouse remoto.

A janela do console remoto oferece diversas opções para controle de mouse, incluindo controle absoluto de mouse, controle relativo de mouse (sem aceleração) e controle de mouse (RHEL, versão anterior de Linux).

Controle de mouse absoluto e relativo

Use estas informações para acessar as opções absoluto e relativo para controlar o mouse.

Para acessar as opções de controle absoluto e relativo do mouse, conclua as etapas a seguir:

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

Etapa 2. Clique em **Configurações do mouse** no menu suspenso.

Etapa 3. Selecione um dos modos de **Aceleração de mouse** a seguir:

Posicionamento absoluto (Windows, Linux mais recente e Mac OS X)
O cliente envia mensagens de localização do mouse para o servidor que são sempre relativas à origem (área superior esquerda) da área de visualização.

Posicionamento relativo, sem aceleração
O cliente envia a localização do mouse como um deslocamento da localização anterior.

Posicionamento relativo (Linux mais antigo)

Este modo aplica um fator de aceleração para alinhar melhor o mouse em alguns destinos Linux. As configurações de aceleração foram selecionadas para maximizar a compatibilidade com distribuições de Linux mais antigas.

Gravação/reprodução de tela de vídeo

Use as informações neste tópico para gravar ou reproduzir vídeos de tela de presença remota.

A interface da Web do XClarity Controller fornece um recurso parecido com DVR para suportar a gravação e reprodução de vídeos de tela de presença remota. Essa função oferece suporte apenas à gravação de vídeo em uma pasta da rede. Atualmente, os protocolos NFS e CIFS são compatíveis. A seguir estão as etapas para usar a função de gravação e reprodução.

1. Na página da Web do console remoto, clique me **Gravação de tela** para abrir a janela de configurações.
2. Na janela de configurações, as informações a seguir podem precisar ser especificadas.
   - Se o tipo de montagem "CIFS" estiver selecionado, especifique os parâmetros **Pasta remota**, **Nome do usuário** e **Senha**. O formato da pasta remota CIFS é "**//<endereço IP remoto>/<nome da pasta>**". Por exemplo: //xxx.xxx.xxx.xxx/folder.
   - Se o tipo de montagem "NFS" estiver selecionado, especifique os parâmetro **Pasta remota**. O formato da pasta remota NFS é "**<endereço IP remoto>:/<nome da pasta>**". Por exemplo: xxx.xxx.xxx.xxx:/folder.
   - Especifique o nome do arquivo de vídeo, se necessário. Se um nome de arquivo já foi fornecido, uma caixa de mensagem de erro será exibida. Para substituir o nome do arquivo existente, escolha "Substituir nome do arquivo". Se a caixa "Automático" estiver marcada, o nome do arquivo de vídeo será gerado automaticamente.
   - O "Tamanho de arquivo máximo" indica o tamanho máximo do arquivo de vídeo antes que a gravação de vídeo seja interrompida automaticamente.
   - A "Duração de gravação máxima" indica a duração máxima da gravação de vídeo antes que a gravação seja interrompida automaticamente.
3. Clique em **Iniciar gravação** para iniciar a gravação de vídeo.
4. Clique em **Interromper gravação** para interromper a gravação de vídeo. Uma janela pop com a mensagem "Gravação de vídeo concluída" será exibida, mostrando informações relevantes sobre a gravação de vídeo.
5. Baixe os vídeos gravados do NFS ou CIFS para a pasta local. Na seção Visualização do console remoto da página inicial do XClarity Controller, clique em **Vídeos gravados** e selecione o arquivo de vídeo a ser reproduzido.

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.

Dimensionamento da tela
Com a escala ativada, a imagem de vídeo é dimensionada para que a imagem completa fique proporcional para preencher a janela do console.

Tela de origem
A imagem de vídeo possui as mesmas dimensões que a extremidade do servidor. As barras de rolagem são exibidas, se necessário, permitindo visualizar as áreas de imagem de vídeo que não cabem na janela.

Modo de cor
Ajusta a profundidade da cor da janela do console remoto. Existem duas opções de modo de cor:

- Cor: 7, 9, 12, 15 e 23 bits
- Escala de cinza: 16, 32, 64 e 128 sombras

Nota: Os ajustes de modo de cor geralmente serão feitos se sua conexão com o servidor remoto tiver largura de banda limitada e você quiser reduzir a demanda de largura de banda.

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 do XClarity Controller Enterprise. Para montar a mídia local, clique em **Ativar** na seção **Montar mídia local**. Até quatro arquivos podem ser montados simultaneamente no servidor.

  Notas:

  – Ao usar o navegador Google Chrome, uma opção de montagem adicional chamada **Montar arquivos/pastas** fica disponível para permitir que você arraste e solte arquivo(s)/pasta(s).
  – Se diversas sessões de controle remoto simultâneas estiverem em andamento com um XClarity Controller, esse recurso poderá ser ativado apenas por uma das sessões.
- 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.

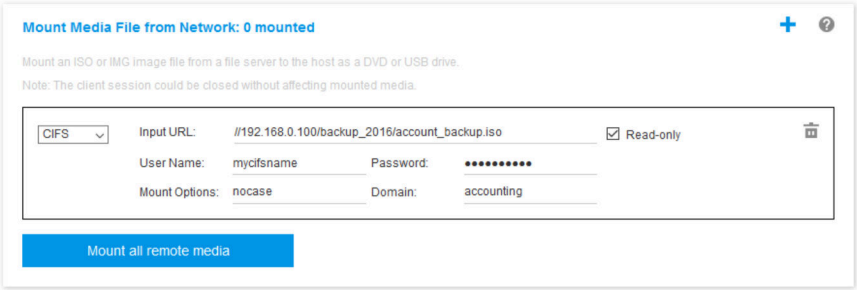
    Nota: Erros podem ocorrer durante o processo de montagem para certificados de segurança gerados pelo Microsoft IIS. Se isso acontecer, consulte "Problemas de erro de montagem de mídia" na página 78.

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.

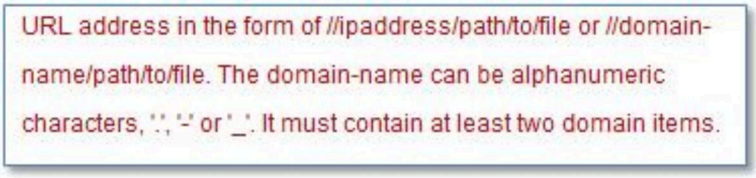
- Até dois arquivos podem ser carregados na memória do XClarity Controller e montados como mídia virtual com o recurso RDOC do XClarity Controller. O tamanho total dos dois arquivos não deve ultrapassar 50 MB. Esses arquivos permanecerão na memória do XClarity Controller até que sejam removidos, mesmo 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.



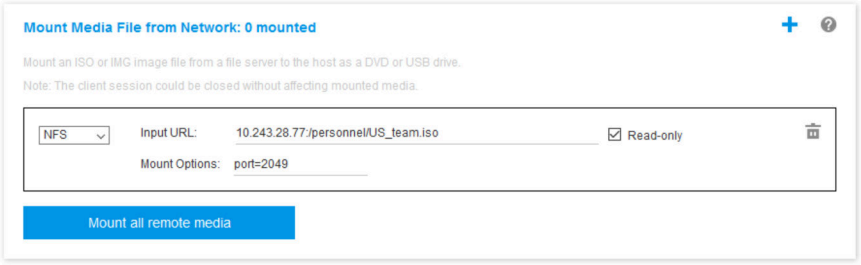
O BMC fornece orientação ao especificar a URL. Se a URL que está sendo digitada não for válida, o botão de montagem ficará cinza, e um texto em vermelho será exibido no campo de URL mostrando o formato esperado para ela.



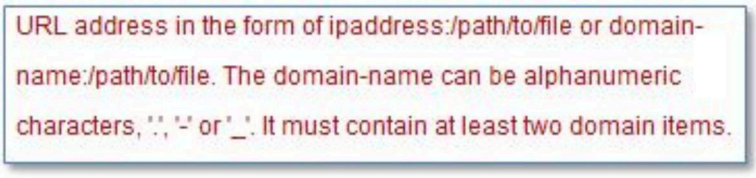
– **NFS - Network File System**: Consulte a descrição anterior para obter detalhes.

  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.



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.



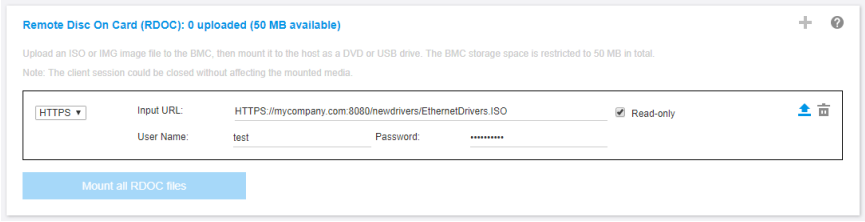
– **HTTPS – Protocolo de Transporte de Hipertexto Seguro**:
  – Insira o URL que localiza o arquivo no sistema remoto.

- 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 78.
- 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.



  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 images (.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
```

Disco remoto usando cliente Java

Estas seções descrevem como montar a mídia local usando cliente Java.

É possível usar cliente Java para designar ao servidor uma unidade de CD ou DVD, uma unidade de disquete, uma unidade flash USB que está em seu computador, ou especificar uma imagem de disco em seu computador para que o servidor use. É possível usar a unidade para funções como reiniciar (inicializar) o servidor, atualizar código, instalar um novo software no servidor e instalar ou atualizar o sistema operacional no servidor. É possível acessar o disco remoto. As unidades e imagens de disco são exibidas como unidades USB no servidor.

Notas: O Java do Console Remoto oferece suporte a um dos seguintes ambientes Java e ele só poderá ser aberto se o cliente HTML5 não estiver em execução.

1. Oracle Java Runtime Environment 1.8/Java SE 8 ou versões mais recentes
2. A distribuição OpenJDK 8. do AdoptOpenJDK com HotSpot JVM é suportada.

Se você usar o AdoptOpenJDK, deverá usar https://openwebstart.com/ em OSX, Windows e Linux.

Criando um arquivo de imagem

Para criar um novo arquivo de imagem a partir de uma pasta de origem especificada, conclua as etapas a seguir:

1. Clique na opção **Criar imagem** na guia **Mídia Virtual** na janela Cliente Java de mídia virtual. A janela Criar imagem da pasta será exibida.
2. Clique no botão **Procurar** associado ao campo **Pasta de origem** para selecionar a pasta de origem específica.
3. Clique no botão **Procurar** associado ao campo **Novo arquivo de imagem** para selecionar o arquivo de imagem a ser usado.
4. Clique no botão **Criar imagem** .

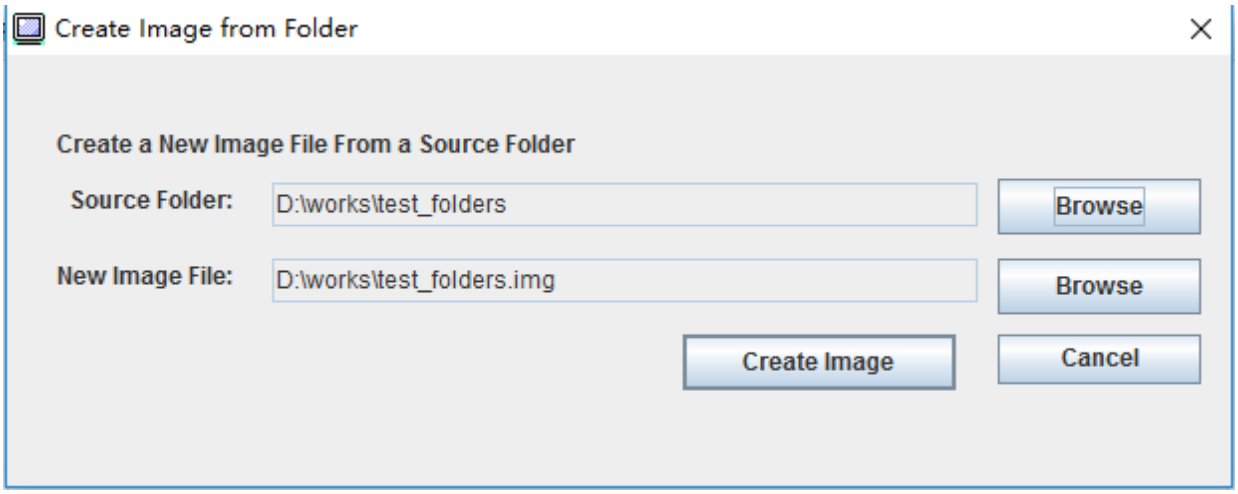


Figura 1. Criando um arquivo de imagem

Selecionando dispositivos a serem montados

Para montar a imagem local, pasta e unidade de CD/DVD/USB, conclua as etapas a seguir:

Clique na opção **Selecionar dispositivos a serem montados** na guia **Mídia Virtual** na janela Cliente Java de mídia virtual. A janela Selecionar dispositivos a serem montados será exibida.

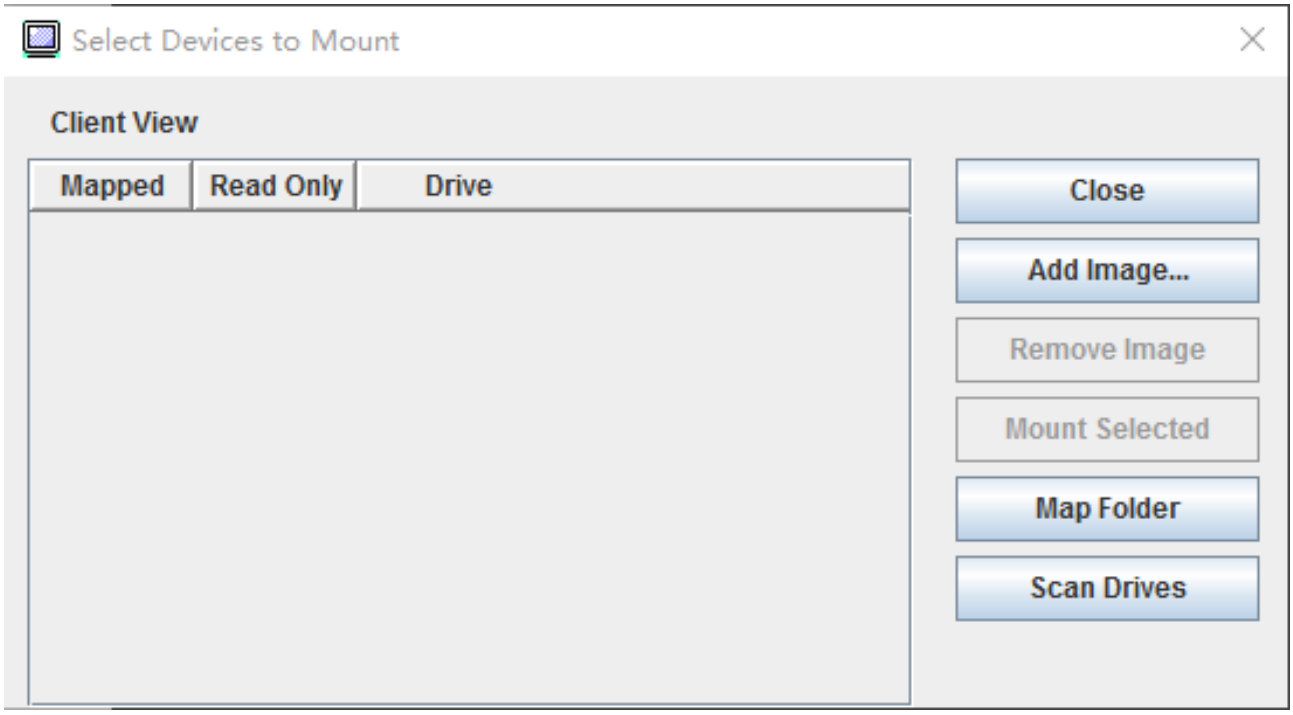


Figura 2. Janela Selecionar dispositivos a serem montados

É possível montar a imagem local, pasta e unidade de CD/DVD/USB executando as etapas a seguir:

- **Montar imagem local**:
  1. Clique no botão **Adicionar imagem** para selecionar a imagem que deseja montar.
  2. Marque a opção **Mapeado**.

3. Marque a opção **Somente leitura** para habilitar a função, se necessário.
4. Clique no botão **Montagem selecionada** e você poderá montar a imagem local com êxito.

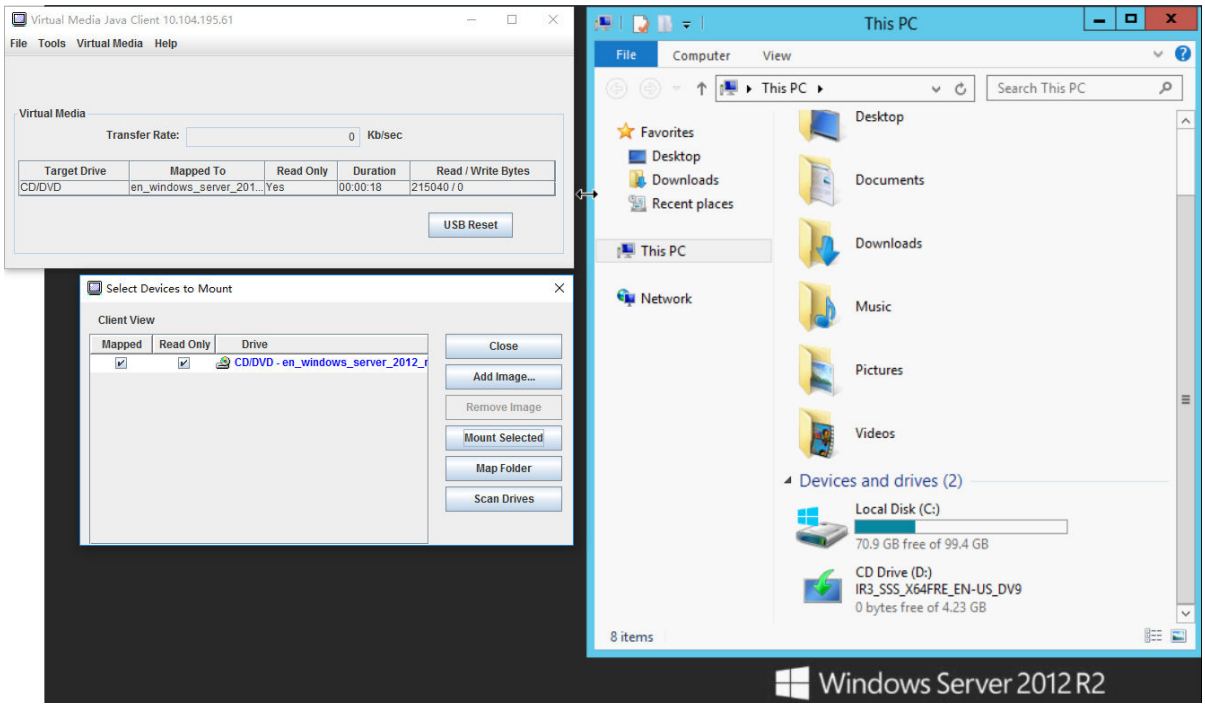


Figura 3. Montar imagem local

- **Pasta montagem local**:
  1. Clique no botão **Pasta do mapa** para selecionar a pasta local que deseja montar.
  2. Clique no botão **Montagem selecionada** e você poderá montar a pasta local com êxito.

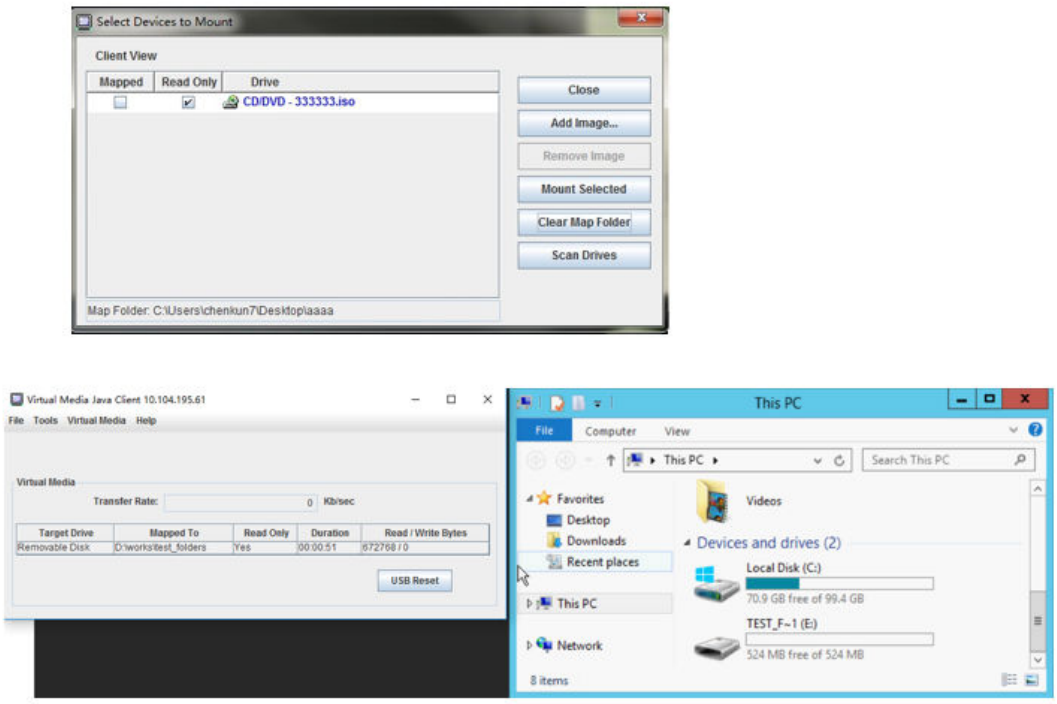


Figura 4. Pasta montagem local

- **Montar CD/DVD ou unidade USB**:
  1. Clique no botão **Verificar unidades** para detectar uma unidade USB ou um CD/DVD conectado.
  2. Marque a opção **Mapeado**.
  3. Marque a opção **Somente leitura** para habilitar a função, se necessário.
  4. Clique no botão **Montagem selecionada** e você poderá montar a imagem local com êxito.

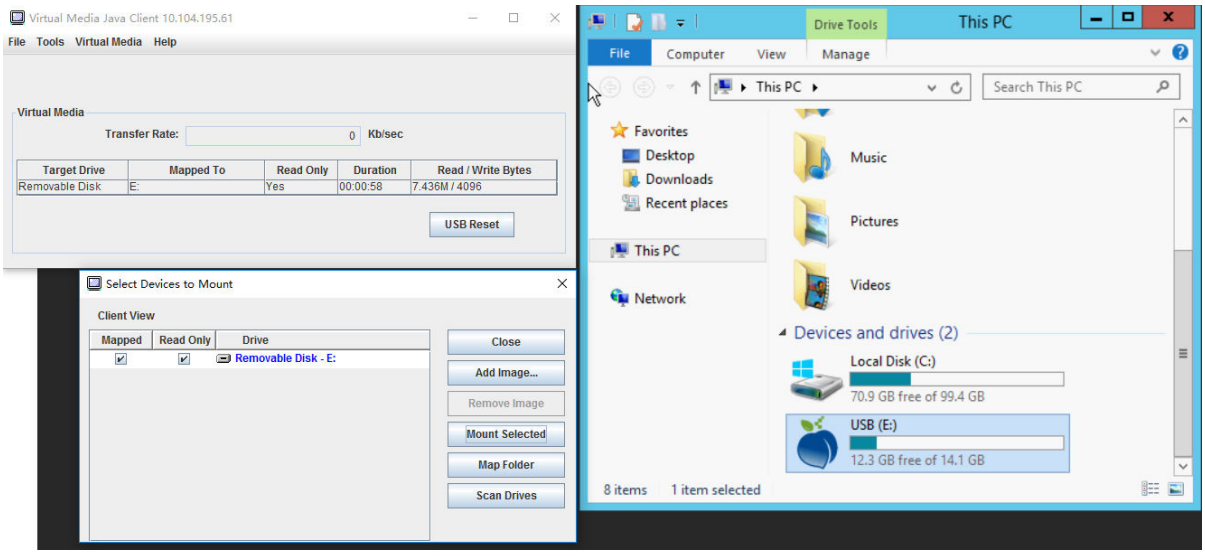


Figura 5. Montar CD/DVD ou unidade USB

A janela Selecionar dispositivos a serem montado contém uma lista de dispositivos locais atuais que estão disponíveis para montagem. Essa janela contém os seguintes campos e botões:

- O campo **Mapeado** contém a caixa de seleção que permite selecionar os dispositivos a serem montados ou mapeados.
- O campo **Somente leitura** contém a caixa de seleção que permite selecionar os dispositivos mapeados ou montados que serão **somente leitura** no servidor host.
- O campo **Unidade** contém o caminho do dispositivo na máquina local.
- Clique no botão **Fechar** para fechar a janela Selecionar dispositivos a serem montados.
- Clique no botão **Adicionar imagem** para procurar a imagem de disquete e o arquivo de imagem ISO no sistema de arquivos local que deseja adicionar à lista de dispositivos.
- Clique no botão **Remover imagem** para remover uma imagem que foi adicionada à lista de dispositivos.
- Clique no botão **Montagem selecionada** para montar ou mapear todos os dispositivos que são marcados para montagem ou mapeamento no campo **Mapeado**.

  Nota: A pasta será montada como somente leitura.
- Clique no botão **Verificar unidades** para atualizar a lista de dispositivos locais.

Selecionando dispositivos a serem desmontados

Para desmontar os dispositivos do servidor host, conclua as etapas a seguir:

1. Clique na opção **Desmontar tudo** na guia **Mídia Virtual** na janela Cliente Java de mídia virtual.
2. Depois de selecionar a opção **Desmontar tudo** uma janela de confirmação Desmontar tudo será apresentada. Se você aceitar, **todos** os dispositivos do servidor host no servidor serão desmontados.

   Nota: Não é possível desmontar as unidades individualmente.

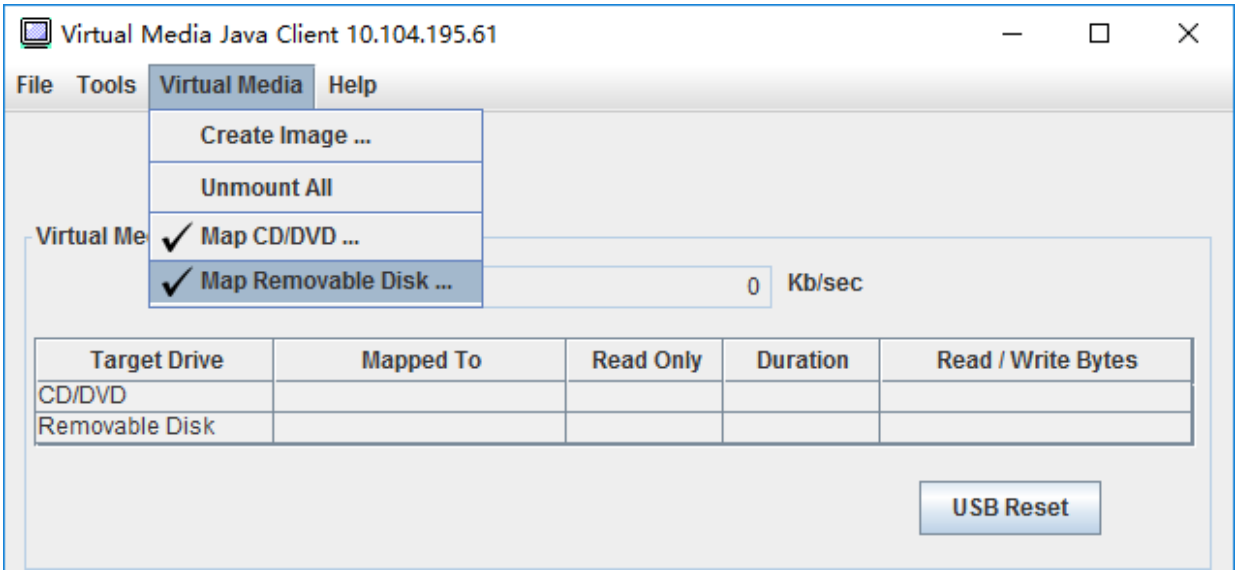


Figura 6. Desmontar tudo

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.

Baixando 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 **Serviço** na seção **Ação rápida** e selecione **Baixar dados de serviço**. Clique em **OK** para baixar os dados de serviço.

O processo para coletar os dados de serviço e suporte demora alguns minutos para gerar os dados de serviço. 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>_xcc_<date>-<time>.tgz

Por exemplo: 7X2106Z01A_2345678_xcc_170511-175656.tgz.

Além formato tgz, os dados de serviço também podem ser baixados usando o formato tzz. Tzz usa um algoritmo de compactação diferente e pode ser extraído com um utilitário como "lzop".

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.

Nota: O campo é opcional e não é configurável em um nó Flex.

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.

Nota: O campo é opcional e não é configurável em um nó Flex.

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:

Watchdog de SO
O watchdog de SO é usado para monitorar o sistema operacional e garantir que não seja travado. A interface Ethernet sobre USB deve ser ativada para esse recurso. Consulte a "Configurando Ethernet sobre USB" na página 33 para obter detalhes. O XClarity Controller se comunica com o sistema operacional em um intervalo configurado na seleção **Tempo de watchdog de SO**. Se o sistema operacional não responder antes da próxima verificação, o XClarity Controller presumirá que o sistema operacional travou. O XClarity Controller capturará o conteúdo do vídeo do servidor e reinicializará o servidor na tentativa de restaurar a operação. O XClarity Controller reinicializará o servidor apenas uma vez. Se o sistema operacional continuar travado após a reinicialização, em vez de reinicializar o servidor continuamente, o servidor ficará travado para que o problema possa ser investigado e corrigido. Para reacionar o watchdog de SO, desligue e ligue o servidor. Para habilitar o watchdog de SO, selecione um intervalo no menu suspenso Tempo de watchdog de SO e clique em **Aplicar**. Para desabilitar o watchdog de SO, selecione **Nenhum** no menu suspenso Tempo de watchdog de SO.

Watchdog do carregador
O watchdog do carregador monitora o intervalo entre a conclusão do POST e quando o sistema operacional começa a ser executado. A interface Ethernet sobre USB deve ser ativada para esse recurso. Consulte a "Configurando Ethernet sobre USB" na página 33 para obter detalhes. Quando o POST é concluído, o XClarity Controller inicia um cronômetro e começa a se comunicar com o sistema operacional. Se o sistema operacional não responder no tempo configurado na opção Watchdog do carregador, o XClarity Controller presumirá que a inicialização do sistema operacional travou. O XClarity Controller irá então reinicializar o servidor na tentativa de restaurar a operação. O XClarity Controller reinicializará o servidor apenas uma vez. Se a inicialização do sistema operacional continuar travada após a reinicialização, em vez de reinicializar o servidor continuamente, o servidor ficará travado para que o problema possa ser investigado e corrigido. O watchdog do carregador é reacionado quando o servidor é desligado e ligado ou quando o servidor é inicializado com sucesso no sistema operacional. Para habilitar o watchdog do carregador, selecione um intervalo no menu suspenso Watchdog do carregador e clique em **Aplicar**. Para desabilitar o watchdog do carregador, selecione **Nenhum** no menu suspenso Watchdog do carregador.

Ativar Atraso de Desligamento
Use o campo Atraso de desligamento para especificar o número de minutos que o subsistema do XClarity Controller esperará até que o sistema operacional seja desativado antes de forçar o desligamento. 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.

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 a hora está. 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.
- 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**.

Notas:

- 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^{h10} de 12 de março, essa ação não ocorrerá. Quando for 2 horas, o XClarity Controller lerá a hora como 3 horas.
- As configurações de data e hora do XClarity Controller não podem ser modificadas em um Flex System.

Capítulo 6. 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
- Configurar RAID

Detalhe de RAID

Para usar a função de detalhe de RAID, 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.

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.

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,

© Copyright Lenovo 2017, 2022

capacidade e ações. O ícone de lápis permite editar informações, o ícone de lixeira permite excluir a "placa 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.

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

      Para alguns níveis RAID, o intervalo é necessário. Há também uma quantidade mínima de unidades que precisam estar presentes no intervalo.
      1) Para esses tipos de situações, a interface da Web exibirá **Intervalo 1** por padrão.
      2) Selecione as unidades e clique em **Adicionar membro** para adicionar as unidades no **Intervalo 1**. Quando **Intervalo 1** não tiver unidades suficientes, desabilite o link **Adicionar intervalo**.
      3) Clique em **Adicionar intervalo** para adicionar o **Intervalo 2**. Selecione as unidades e clique em **Adicionar membro** para adicionar ao **Intervalo 2**.
      4) Clique em **Adicionar membro** para adicionar unidades ao último intervalo. Se desejar adicionar unidades ao **Intervalo 1** novamente, será necessário clicar em Intervalo 1 e selecionar as unidades para adicionar ao **Intervalo 1**.
      5) Se o número de intervalos atingir a quantia máxima, desabilite **Adicionar intervalo**.
   b. 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, cria um disco virtual que usa 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. Se houver mais de um disco virtual, o ícone **Remover** será habilitado. 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 a criação do disco virtual** 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 as propriedades básicas - nome da unidade, estado do RAID, número de série, número de peça, número de FRU 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.
  - **Tornar unidade de disco como reutilizável**: Define a unidade como reutilizável.
  - **Tornar a unidade de disco como ausente**: Define a unidade como ausente.
  - **Adequar unidade a JBOD**: Inclui a unidade na organização de discos JBOD.
  - **Adequar unidade não configurada**: Torna a unidade disponível para ser configurada em uma matriz 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**: Configura a unidade para remoção.

2. Se o controlador incluir unidades que ainda não foram configuradas, estas serão exibidas na tabela **Unidades 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 7. Atualizando o firmware de servidor

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

Visão Geral

Informações gerais sobre como atualizar o firmware do servidor.

A opção **Atualização de firmware** no painel de navegação tem 4 características:

- **Firmware do sistema:** visão geral do status e da versão do firmware do sistema. E para executar a atualização de firmware do sistema.
- **Promoção automática do XCC primário para fazer o backup:** uma vez habilitado, o firmware do banco de backup pendente será sincronizado do banco primário após o banco primário passar a medida Métrica de Estabilidade de Imagem (ISM).
- **Firmware do adaptador:** visão geral do firmware do adaptador instalado, seus status e versão. E para executar a atualização de firmware do adaptador.

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

- **Ativo:** O firmware está ativo.
- **Inativo:** O firmware não está ativo.
- **Pendente:** O firmware está aguardando para tornar-se ativo.
- **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 estranho ou 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.
- 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.

© Copyright Lenovo 2017, 2022

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.

Capítulo 8. 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 email.

Consulte "Instalando uma chave de ativação" na página 91, "Removendo uma chave de ativação" na página 92 ou "Exportando uma chave de ativação" na página 92 para obter informações sobre como gerenciar uma chave de ativação usando a interface da web do XClarity Controller. Consulte "Comando keycfg" na página 129 para obter informações sobre como gerenciar uma chave de ativação usando a CLI do XClarity Controller.

Para registrar um ID para administrar 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

Atenção: Não é possível atualizar diretamente do Standard XClarity Controller para a funcionalidade de nível Enterprise. Você precisará atualizar primeiro para o nível Advanced antes que a funcionalidade do nível Enterprise possa ser ativada.

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 incluir o arquivo ou clique em **Cancelar** para parar a instalação. Para concluir a inclusão da chave, clique em **OK**, na janela Incluir Chave de Ativação, ou clique em **Cancelar** para parar a instalação.

A janela Sucesso indica que a chave de ativação está instalada.

Notas:

© Copyright Lenovo 2017, 2022

- Se a chave de ativação não for válida, uma janela de erro será exibida.

Etapa 4. Clique em **OK** para fechar a janela Sucesso.

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 ou clique em **Cancelar** para manter o arquivo-chave.
A chave de ativação selecionada é removida do servidor e não aparece 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 exportação da chave de ativação ou clique em **Cancelar** para cancelar a solicitação de exportação de chave.

Etapa 4. Selecione o diretório para salvar o arquivo.
A chave de ativação selecionada é exportada do servidor.

Capítulo 9. API REST do Redfish do Lenovo XClarity Controller

O Lenovo XClarity Controller fornece um conjunto compatível com Redfish de APIs REST fáceis de usar que podem ser usadas para acessar os dados do Lenovo XClarity Controller e os serviços de aplicativos em execução fora da estrutura do Lenovo XClarity Controller.

Isso permite a fácil integração de recursos do Lenovo XClarity Controller em outro software, esteja o software em execução no mesmo sistema que o servidor do Lenovo XClarity Controller ou em um sistema remoto dentro da mesma rede. Essas APIs são baseadas em API REST do REDFISH de padrão do setor e são acessados pelo protocolo HTTPS.

O guia do usuário da API REST do Redfish do XClarity Controller pode ser encontrado aqui: https://pubs.lenovo.com/xcc-restapi/xcc_restapi_book.pdf.

A Lenovo fornece scripts Redfish de amostra de software livre que podem ser usados como referência para o desenvolvimento de software que se comunique com API REST do Redfish da Lenovo. Esses scripts de amostra podem ser encontrados aqui:

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

Especificações DMTF relacionadas à API do Redfish estão disponíveis em: https://redfish.dmtf.org/. Este site fornece especificações gerais e outro material de referência sobre API REST do Redfish.

© Copyright Lenovo 2017, 2022

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 95 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.

Seu login é efetuado na linha de comandos. 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.

© Copyright Lenovo 2017, 2022

```
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> ?
```
- Em um Flex System, algumas configurações são gerenciadas pelo CMM e não podem ser modificadas no XClarity Controller.

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 113
- "Comando adapter" na página 178
- "Comando alertcfg" na página 115
- "Comando alertentries" na página 163
- "Comando asu" na página 116
- "Comando backup" na página 119
- "Comando batch" na página 166
- "Comando clearcfg" na página 166
- "Comando clearlog" na página 100
- "Comando clock" na página 167

- "Comando console" na página 113
- "Comando dbgshimm" na página 181
- "Comando dhcpinfo" na página 120
- "Comando dns" na página 121
- "Comando encaps" na página 123
- "Comando ethtousb" na página 123
- "Comando exit" na página 99
- "Comando fans" na página 101
- "Comando ffdc" na página 101
- "Comando firewall" na página 124
- "Comando fuelg" na página 111
- "Comando gprofile" na página 125
- "Comando hashpw" na página 126
- "Comando help" na página 99
- "Comando history" na página 99
- "Comando hreport" na página 102
- "Comando identify" na página 167
- "Comando ifconfig" na página 126
- "Comando info" na página 168
- "Comando keycfg" na página 129
- "Comando ldap" na página 130
- "Comando led" na página 104
- "Comando mhlog" na página 103
- "Comando m2raid" na página 180
- "Comando ntp" na página 132
- "Comando portcfg" na página 133
- "Comando portcontrol" na página 134
- "Comando ports" na página 135
- "Comando power" na página 109
- "Comando pxeboot" na página 112
- "Comando rdmount" na página 136
- "Comando readlog" na página 105
- "Comando reset" na página 111
- "Comando restore" na página 137
- "Comando restoredefaults" na página 138
- "comando roles" na página 138
- "Comando seccfg" na página 140
- "Comando set" na página 140
- "Comando smtp" na página 140
- "Comando snmp" na página 141
- "Comando snmpalerts" na página 143

- "Comando spreset" na página 168
- "Comando srcfg" na página 145
- "Comando sshcfg" na página 146
- "Comando ssl" na página 147
- "Comando sslcfg" na página 148
- "Comando storage" na página 169
- "Comando storekeycfg" na página 151
- "Comando syncrep" na página 153
- "Comando syshealth" na página 106
- "Comando temps" na página 107
- "Comando thermal" na página 154
- "Comando timeouts" na página 154
- "Comando tls" na página 155
- "Comando trespass" na página 156
- "Comando uefipw" na página 157
- "Comando usbeth" na página 157
- "Comando usbfp" na página 157
- "Comando users" na página 158
- "Comando volts" na página 107
- "Comando vpd" na página 108

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

Esse 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.

A tabela a seguir mostra os argumentos das opções.

Tabela 7. Comando clearlog

A tabela a seguir é uma tabela de duas colunas e uma linha que consiste na opção e na descrição da opção.

Opção	Descrição
-t <all | platform | audit>	Tipo de evento, escolha o tipo de evento a ser limpo. Se não for especificado, todos os tipos de evento serão selecionados.

Descrição do tipo de evento

- Todos: todos os tipo de evento, incluindo eventos de plataforma e eventos de auditoria.
- plataforma: tipo de evento de plataforma.
- auditoria: tipo de evento de auditoria.

Exemplo:

```
system> clearlog
All event log cleared successfully
system> clearlog -t all
All event log cleared successfully
```

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

Comando fans

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 ffdc

Esse comando é usado para gerar um novo arquivo de dados de serviço.

Use o comando first failure data capture (**ffdc**) para gerar e transferir dados de serviço para o Suporte.

A lista a seguir consiste em comandos a serem usados com o comando **ffdc**:

- **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

A tabela a seguir mostra os argumentos das opções.

Tabela 8. Comando ffdc

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
-t	Número de tipo	1 (dump do processador) e 4 (dados de serviço). O despejo de processador contém todos os logs e arquivos disponíveis. Os dados de serviço contêm apenas um subconjunto dos logs e arquivos. O valor padrão é 1.
-f [1]	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 [1]	Endereço do servidor tftp/ sftp	
-pn [1]	Número da porta do servidor tftp/sftp	O valor padrão é 69/22.
-u [1]	Nome de usuário para o servidor sftp	
-pw [1]	Senha para o servidor sftp	

1. Argumento adicional para os comandos **generate** e **copy**

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

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


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

Comando hreport

Use esse comando para exibir o relatório de funcionamento incorporado.

A tabela a seguir exibe os comandos hreport.

Tabela 9. Comandos hreport

A tabela a seguir é uma tabela de duas colunas e várias linhas que consiste em diferentes descrições do comando hreport.

Opção	Descrição
gerar	Criar novo relatório de funcionamento
status	Verificar status
copiar	Copiar o relatório de funcionamento existente
delete	Excluir o relatório de funcionamento existente

A tabela a seguir mostra os argumentos para as opções de generate e copy.

Tabela 10. Comando generate e copy

A tabela a seguir é uma tabela de duas colunas e várias linhas que consiste em opções de comando generate e copy e descrições de opção.

Opção	Descrição
-f	Nome do arquivo remoto ou diretório de destino sftp (o padrão é o nome gerado pelo sistema ((para sftp, use o caminho completo ou barra / no nome do diretório (~/ ou /tmp/))
-ip	Endereço do servidor tftp/sftp
-pn	Número da porta do servidor tftp/sftp (padrão 69/22)
-u	Nome de usuário para o servidor sftp
-pw	Senha para o servidor sftp

Comando mhlog

Use esse comando para exibir as entradas do log de atividade do histórico de manutenção.

A tabela a seguir mostra os argumentos das opções.

Tabela 11. Comando mhlog

A tabela a seguir é uma tabela de duas colunas e várias linhas que consiste em opções e descrições de opção.

Opção	Descrição
-c <count>	Exibir entradas "count" (1-250)
-i <index>	Exibir entradas que começam no índice (1-250)
-f	Nome de arquivo remoto do arquivo de log
-ip	Endereço do servidor tftp/sftp
-pn	Número da porta do servidor tftp/sftp (padrão 69/22)
-u	Nome de usuário para o servidor sftp
-pw	Senha para o servidor sftp

Exemplo

A exibição será assim:

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

Comando led

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.

Tabela 12. Comando led

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
-l	Obtenha o status de todos os LEDs no sistema e seus subcomponentes	
-chklog	Desligar o LED de log de verificação	desligado
-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)

Sintaxe:

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

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.

readlog exibe as cinco primeiras entradas no log de eventos, iniciando com a mais recente, em sua primeira execução, depois as próximas cinco para cada chamada subsequente.

readlog -a exibe todas as entradas no log de eventos, iniciando com a mais recente.

readlog -f reconfigura o contador e exibe as 5 primeiras entradas no log de eventos, iniciando com a mais recente.

readlog -date date exibe entradas de log de eventos para a data especificada, especificada no formato mm/dd/aa. Pode ser um lista de datas separadas por barra vertical (|).

readlog -sev severity exibe entradas de log de eventos para o nível de severidade especificado (E, W, I). Pode ser um lista de níveis de severidade separados por barra vertical (|).

readlog -i ip_address configura o endereço IP IPv4 ou IPv6 do servidor TFTP ou SFTP no qual o log de eventos é salvo. As opções de comando **-i** e **-l** são usadas juntas para especificar o local.

readlog -l filename configura o nome de arquivo do log de eventos. As opções de comando **-i** e **-l** são usadas juntas para especificar o local.

readlog -pn port_number exibe ou configura o número da porta do servidor TFTP ou SFTP (padrão 69/22).

readlog -u username especifica o nome de usuário para o servidor SFTP.

readlog -pw password especifica a senha para o servidor SFTP.

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

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 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 [argument]
argument:
  summary      -display the system health summary
  activeevents -display active events
  cooling - display cooling devices health status
```

```
  power - display power modules health status
  storage - display local storage health status
  processors - display processors health status
  memory - display memory health status
```

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.

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

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

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.

```
Example:
system> volts

      i HSL    SSL    WL     WRL    V      WRH    WH    SSH     HSH
-------------------------------------------------------------------
5v    5.02  4.00  4.15  4.50  4.60  5.25  5.50  5.75   6.00
3.3v  3.35  2.80  2.95  3.05  3.10  3.50  3.65  3.70   3.85
12v   12.25 11.10 11.30 11.50 11.85 12.15 12.25 12.40  12.65
-5v   -5.10 -5.85 -5.65 -5.40 -5.20 -4.85 -4.65 -4.40  -4.20
-3.3v -3.35 -4.10 -3.95 -3.65 -3.50 -3.10 -2.95 -2.80  -2.70
VRM1                          3.45
VRM2                          5.45
system>
```

Nota: 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 sys  - displays Vital Product Data for the system
vpd bmc  - displays Vital Product Data for the management controller
vpd uefi - displays Vital Product Data for system BIOS
vpd lxpm  - displays Vital Product Data for system LXPM
vpd fw   - displays Vital Product Data for the system firmware
vpd comp - displays Vital Product Data for the system components
vpd pmem - displays Vital Product Data for Intel Optane PMem
vpd pcie - displays Vital Product Data for PCIe devices
```

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.

A tabela a seguir contém um subconjunto de comandos que pode ser usado com o comando **power**.

Tabela 13. Comando power

A tabela a seguir é uma tabela de três colunas e várias linhas que consiste em comandos power, descrições de comando e os valores associados dos comandos.

Comando	**Descrição**	**Valor**
ligado	Use este comando para ligar a energia do servidor.	ligar, desligar
desligar	Use este comando para desligar o servidor. **Nota:** A opção **-s** encerra o sistema operacional antes de desligar o servidor.	ligar, desligar
ciclo de energia	Use este comando para desligar o servidor e, em seguida, ligá-lo novamente. **Nota:** A opção **-s** encerra o sistema operacional antes de desligar o servidor.	
power enterS3	Use este comando para colocar o sistema operacional no modo S3 (hibernação). **Nota:** Este comando é usado apenas quando o sistema operacional está ligado. O modo S3 não é suportado em todos os servidores.	
power rp	Use esta opção para especificar a política de restauração de energia do host.	alwayson|alwaysoff|restore
power S3resume	Use este comando para ativar o sistema operacional do modo S3 (hibernação). **Nota:** Este comando é usado apenas quando o sistema operacional está ligado. O modo S3 não é suportado em todos os servidores.	
estado de energia	Use este comando para exibir o estado de energia do servidor e o estado atual do servidor.	ligar, desligar

A tabela a seguir contém as opções dos comandos **power on**, **power off** e **power cycle**.

Tabela 14. Comando power

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.

Tabela 14. Comando power (continuação)

Opção	Descrição	Valores
-s	Use esta opção para encerrar o sistema operacional antes de desligar o servidor. **Nota:** A opção **-s** é indicada ao usar a opção **-every** para o **power off** e **power cycle**.	
-every	Use esta opção com os comandos **power on**, **power off** e **power cycle** 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.	**Nota:** Os valores para essa opção são apresentados em linhas separadas devido a limitações de espaço. Sun|Mon|Tue|Wed|Thu| Fri|Sat|Day|clear
-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 **power on**. **Nota:** As opções **-d** e **-every** 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 **power on**.	

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

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 13:00
```

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.

A tabela a seguir mostra os argumentos das opções.

Tabela 15. Comando reset

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
-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.	

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

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. A tabela a seguir mostra os argumentos das opções.

Tabela 16. Comando fuelg

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
-pme	Habilite ou desabilite o gerenciamento de energia e o limite no servidor.	ligar, desligar
-pcapmode	Defina o modo de limite de energia para o servidor.	entrada, saída
-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)	valor numérico em horas

Tabela 16. Comando fuelg (continuação)

Opção	Descrição	Valores
-pm	Defina o modo de política para perda de energia redundante.	• **bt** - básico com limitação • **rt**- redundante com regulagem (padrão) • **ort**- N_1 redundante com regulagem
-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.	ligar, desligar
-perf	Exibe a utilização de computação atual, incluindo o sistema, o microprocessador e E/S.	porcentagem
-pc	Exibir consumo de energia atual	• **saída** – exibir consumo de energia CC atual. Para servidores de rack e em torre, incluirá o consumo de energia do sistema, CPU, memória e outros componentes, para servidores blade ITE, incluirá apenas o consumo de energia do sistema. • **entrada** – exibe o consumo de energia de entrada atual, incluindo o consumo de energia do sistema.

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

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

Comando pxeboot

Esse comando exibe e define a condição do Ambiente de Execução de Pré-inicialização.

A execução de **pxeboot** sem opções retorna a configuração do Ambiente de Execução de Pré-inicialização atual. A tabela a seguir mostra os argumentos das opções.

Tabela 17. Comando pxeboot

A tabela a seguir é uma tabela de três colunas e uma linha que consiste na opção, na descrição da opção e nos valores associados da opção.

Tabela 17. Comando pxeboot (continuação)

Opção	Descrição	Valores
-en	Define a condição do Ambiente de Execução de Pré-inicialização para a próxima reinicialização do sistema.	habilitado, desabilitado

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

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

Comando serial redirect

Este tópico contém o comando serial redirect.

Existe apenas um comando de redirecionamento serial: o "Comando console" na página 113.

Comando console

Esse comando é usado para iniciar uma sessão do console de redirecionamento serial.

Use o comando **console** para iniciar uma sessão de console de redirecionamento serial para a porta serial designada do IMM.

Sintaxe:
```
console 1
```

Comandos de configuração

Este tópico fornece uma lista alfabética de comandos CLI de configuração.

Atualmente, há 41 comandos de configuração:

Comando accseccfg

Use esse comando para exibir e definir configurações de segurança de conta.

A execução do comando **accseccfg** sem opções exibe todas as informações de segurança de conta. A tabela a seguir mostra os argumentos das opções.

Tabela 18. Comando accseccfg

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.

Tabela 18. Comando accseccfg (continuação)

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
-pe	Período de tempo de expiração de senha (dias).	Entre 0 e 365, 0 = nunca expirará
-pew	Período de aviso de expiração da senha **Nota:** 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.	ligar, desligar
-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
-chgdft	Alterar senha padrão após primeiro login.	ligar, desligar
-chgnew	Alterar nova senha de usuário após primeiro login.	ligar, desligar
-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

Syntax:

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

Exemplo:

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

Comando alertcfg

Use este comando para exibir e configurar os parâmetros globais de alerta remoto IMM.

A execução do comando **alertcfg** sem opções exibe todos os parâmetros de alerta remoto global. A tabela a seguir mostra os argumentos das opções.

Tabela 19. Comando alertcfg

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
-dr	Define o tempo de espera entre as repetições antes de IMM reenviar um alerta.	0 a 4,0 minutos, em incrementos de 0,5 minuto
-da	Define o tempo de espera antes de IMM enviar um alerta para o próximo destinatário na lista.	0 a 4,0 minutos, em incrementos de 0,5 minuto
-rl	Define a quantidade de vezes adicionais que o IMM tenta enviar um alerta, se as tentativas anteriores tiverem falhado.	0 a 8

Sintaxe:

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

Exemplo:

```
system>alertcfg
-dr 1.0
-da 2.5
-rl 5
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.

A tabela a seguir contém um subconjunto de comandos que podem ser usado com o comando **asu**.

Tabela 20. Comando asu

A tabela a seguir é uma de três colunas e várias linhas que consiste em um subconjunto de comandos que podem ser usados em conjunto com o comando **asu**. Informações descritivas e valores associados para os comandos são fornecidos.

Comando	Descrição	Valor
delete	Use esse comando para excluir uma instância ou registro de uma configuração. A configuração deve ser uma instância que permita exclusão, por exemplo, iSCSI. AttemptName.1.	**setting_instance**
ajuda	Use esse comando para exibir informações da ajuda para uma ou mais configurações.	**configuração**
configurar	Use esse comando para alterar o valor de uma configuração. Configure a definição de UEFI para o valor de entrada. **Notas:** • Configure um ou mais pares de configuração/valor. • A configuração poderá conter curingas se ela expandir para uma configuração única. • O valor deverá ser colocado entre aspas se ele contiver espaços. • Os valores de lista ordenada são separados pelo símbolo de igual (=). Por exemplo, configure B*. Bootorder "CD/DVD Rom=Hard Disk 0=PXE Network."	**setting value**
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.	**configurando**
show	Use esse comando para exibir o valor atual de uma ou mais configurações.	**configurando**

Tabela 20. Comando asu (continuação)

Comando	Descrição	Valor
showvalues	Use esse comando para exibir todos os valores possíveis para uma ou mais configurações. **Notas:** • Esse comando exibirá informações sobre os valores permitidos para a configuração. • Os números mínimo e máximo de instâncias permitidos para a configuração são exibidos. • O valor padrão será exibido se disponível. • O valor padrão é colocado entre os sinais de maior e menor (< e >). • Os valores de texto mostram os comprimentos mínimo e máximo e a expressão regular.	**configurando**
Notas: • Na sintaxe de comando, **setting** é o nome de uma configuração que você deseja visualizar ou alterar e **value** é o valor que está colocando na configuração. • **Setting** pode ser mais que um nome, exceto ao usar o comando **set**. • **Setting** pode conter curingas, por exemplo, um asterisco (*) ou um ponto de interrogação (?). • **Setting** pode ser um grupo, um nome de configuração ou **all**.		

Exemplos da sintaxe do comando **asu** são apresentados na lista a seguir:

- Para exibir todas as opções de comando asu, insira `asu --help`.
- Para exibir a ajuda detalhada para todos os comandos, insira `asu -v --help`.
- Para exibir a ajuda detalhada para um comando, insira `asu -v set --help`.
- Para alterar um valor, insira `asu set` **setting value**.
- Para exibir o valor atual, insira `asu show` **setting**.
- Para exibir configurações no formato de lote longo, insira `asu show -l -b all`
- Para exibir todos os valores possíveis para uma configuração, insira `asu showvalues` **setting**. 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>
```

A tabela a seguir mostra os argumentos das opções.

Tabela 21. 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[1]	Exibir uso e opções do comando. O ícone --help é colocado antes do comando, por exemplo, **asu --help show**.	

Tabela 21. Opções asu (continuação)

Opção	Descrição	Valores
--help[1]	Exibir ajuda para o comando. A opção --help é colocada após o comando, por exemplo, **asu show --help**.	
-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[2]	Saída detalhada.	

1. A opção --help pode ser usada com qualquer comando.
2. A opção -v é usada apenas entre **asu** 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 22. 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.

Tabela 22. Comandos de transação asu (continuação)

Comando	Descrição	Valor
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.

A tabela a seguir mostra os argumentos das opções.

Tabela 23. Comando backup

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
-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
-fd	Nome do arquivo para descrição XML de comandos CLI de backup	Nome do arquivo válido

Sintaxe:

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

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 eth0
```

Example:

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

A tabela a seguir descreve a saída do exemplo.

Tabela 24. Comando dhcpinfo

A tabela a seguir é uma tabela de duas colunas e várias linhas que descreve as opções usadas no exemplo anterior.

Opção	Descrição
-server	Servidor DHCP que designou a configuração
-n	Nome do host designado
-i	Endereço IPv4 designado

Tabela 24. Comando dhcpinfo (continuação)

Opção	Descrição
-g	Endereço de gateway designado
-s	Máscara de sub-rede designada
-d	Nome de domínio 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 esse comando para visualizar e definir a configuração DNS do IMM.

Nota: Em um Flex System, as configurações DNS não podem ser modificadas no IMM. As configurações do DNS são gerenciadas pelo CMM.

A execução do comando **dns** sem opções exibe todas as informações de configuração do DNS. A tabela a seguir mostra os argumentos das opções.

Tabela 25. Comando dns

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
-state	Estado do DNS	ligar, desligar
-ddns	Estado do DDNS	habilitado, desabilitado
-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.
-p	Prioridade de IPv4/IPv6	ipv4, ipv6

Sintaxe:

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

Nota: O exemplo a seguir mostra uma configuração do IMM em que o DNS está desabilitado.

Exemplo:

```
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>
```

A seguinte tabela descreve as opções usadas no exemplo anterior.

Tabela 26. Saída do comando dns

A tabela a seguir é uma tabela de duas colunas e várias linhas que descreve as opções usadas no exemplo anterior.

Opção	Descrição
-state	Estado do DNS (`on` ou `off`)
-i1	Endereço IP do servidor DNS IPv4 primário
-i2	Endereço IP do servidor DNS IPv4 secundário
-i3	Endereço IP do servidor DNS IPv4 terciário
-i61	Endereço IP do servidor DNS IPv6 primário
-i62	Endereço IP do servidor DNS IPv6 secundário
-i63	Endereço IP do servidor DNS IPv6 terciário
-ddns	Estado do DDNS (`enabled` ou `disabled`)
-dnsrc	Nome de domínio DDNS preferencial (`dhcp` ou `manual`)
-ddn	DDN especificado manualmente
-ddncur	DDN atual (somente leitura)
-p	Servidores DNS preferenciais (`ipv4` ou `ipv6`)

Comando encaps

Use este comando para deixar o BMC sair do modo de encapsulamento.

A tabela a seguir mostra os argumentos das opções.

Tabela 27. Comando encaps

A tabela a seguir é uma tabela de duas colunas e uma linha que consiste em opções e descrições de opção.

Opção	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.

A execução do comando **ethtousb** sem opções exibe informações de Ethernet-sobre-USB. A tabela a seguir mostra os argumentos das opções.

Tabela 28. Comando ethtousb

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
-en	Estado de Ethernet-sobre-USB	habilitado, desabilitado
-m**x**	Configurar mapeamento de portas para índice **x**	O par de portas, separadas por dois-pontos (:), no formato **port1:port2** Onde: • O número de índice de porta, **x**, é especificado como um número inteiro de 1 a 10 na opção de comando. • **port1** do par de portas é o número da porta Ethernet externa. • **port2** do par de portas é o número da porta Ethernet-sobre-USB.
-rm	Remover mapeamento de portas para índice especificado	1 a 10 Os índices de mapa de portas são exibidos usando o comando **ethtousb** sem opções.

Sintaxe:

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

Exemplo:

```
system> ethtousb  -en enabled -m1 100:200 -m2 101:201
system> ethtousb
 -en enabled
```

```
 -m1 100:200
 -m2 101:201
system> ethtousb -rm 1
system>
```

Comando firewall

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.

A tabela a seguir mostra os argumentos das opções.

Tabela 29. Comando firewall

A tabela a seguir é uma tabela de três colunas e várias linhas que consiste em opções e descrições de opção.

Opção	Descrição	Valores
-bips	Bloquear endereços IP 1 a 3 (separados por vírgula, CIDR ou intervalo)	Endereços IP válidos **Nota:** 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 **Nota:** A filtragem de endereços MAC funciona apenas com endereços específicos.
-bbd	Data de início de bloqueio	Data com o formato <AAAA-MM-DD>
-bed	Data de término do bloqueio	Data com o formato <AAAA-MM-DD>
-bbt	Hora de início de bloqueio	Hora com o formato <HH:MM>
-bet	Hora de término do bloqueio	Hora com o formato <HH:MM>
-bti	Bloquear 1 a 3 intervalos de tempo (separados por vírgula) por exemplo, **firewall – bti 01:00 – 02:00,05:05 – 10:30** 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
As opções a seguir são para o bloqueio de endereços IP		
-iplp	Período de bloqueio de endereços IP em minutos.	Valor numérico entre 0 e 2880, 0 = nunca expirar

Tabela 29. Comando firewall (continuação)

Opção	Descrição	Valores
-iplf	Número máximo de falhas de login antes que o endereço IP seja bloqueado. **Nota:** Se esse valor não for 0, deverá ser maior ou igual a <Número máximo de falhas de login> que é definido por **<accseccfg-lf>**	Valor numérico entre 0 e 32, 0 = nunca bloquear
-ipbl	Mostrar/configurar a lista de endereços IP que estão sendo bloqueados.	del, clrall, mostrar • **-del**: exclui um endereço IPv4 ou IPv6 da lista de bloqueios • **-clrall**: limpar todos os IP bloqueados • **-show**: mostrar todos os IPs bloqueados

Exemplo:

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

Comando gprofile

Use esse comando para exibir e configurar perfis de grupo para o IMM.

A tabela a seguir mostra os argumentos das opções.

Tabela 30. Comando gprofile

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
-clear	Excluir um grupo	habilitado, desabilitado
-n	O nome do grupo	Sequência de até 63 caracteres para **group_name** O **group_name** deve ser exclusivo.
-a	Nível de autoridade baseada em função	supervisor, operator, rbs <role list>: nsc|am|rca|rcvma|pr|bc|cel|ac Os valores da lista de funções são especificados utilizando uma lista separada por barra vertical de valores.
-h	Exibir o uso e as opções do comando	

Sintaxe:

```
gprofile [1 - 16 group_profile_slot_number] [options]
```

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

Comando hashpw

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.

A tabela a seguir mostra os argumentos das opções.

Tabela 31. Comando hashpw

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
-sw	Status do comutador de senha de terceiros	habilitado, desabilitado
-re	Status de leitura de senha de terceiros **Nota:** 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 -a super
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.

Digite `ifconfig eth0` 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.

Nota: Em um Flex System, as configurações VLAN são gerenciadas pelo CMM do Flex System e não podem ser modificadas no IMM.

A tabela a seguir mostra os argumentos das opções.

Tabela 32. Comando ifconfig

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	Endereço MAC gravado (somente leitura e não configurável)	
-state	Estado da interface	habilitado, desabilitado
-c	Método de configuração	dhcp, static, dthens (dthens corresponde à opção **try dhcp server, if it fails use static config** na interface da Web)
-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.
-r	Taxa de dados	10, 100, auto
-d	Modo duplex	full, half, auto
-m	MTU	Numérico entre 60 e 1500.
-l	LAA	Formato de endereço MAC. Endereços multicast não são permitidos (o primeiro byte deve ser par).
-dn	Nome de domínio	Nome de domínio no formato válido.
-auto	Configuração de negociação automática, que determina se as definições Taxa de dados e Rede duplex são configuráveis	true, false
-ghn	Obter nome do host do DHCP	habilitado, desabilitado
-nic	modo NIC de comutador[1]	shared, dedicated, shared:nixX[2]
-failover[2]	Modo de failover	none, shared, shared:nicX
-nssync[3]	Sincronização da configuração de rede	habilitado, desabilitado
-address_table	Tabela de endereços IPv6 gerados automaticamente e seus comprimentos de prefixo **Nota:** A opção será visível somente se IPv6 e a configuração automática stateless estiverem habilitados.	Esse valor é somente leitura e não é configurável.
-ipv6	Estado do IPv6	disabled, enabled
-lla	Endereço local de link **Nota:** O endereço local de link só aparecerá se o IPv6 estiver habilitado.	O endereço local de link é determinado pelo IMM. Esse valor é somente leitura e não é configurável.
-ipv6static	Estado do IPv6 estático	disabled, enabled
-i6	Endereço IP estático	Endereço IP estático para canal Ethernet 0 no formato IPv6.

Tabela 32. Comando ifconfig (continuação)

Opção	Descrição	Valores
-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	Estado do DHCPv6	habilitado, desabilitado
-sa6	Estado de configuração automática stateless do IPv6	habilitado, desabilitado
-vlan	Ative ou desative a identificação de VLAN	habilitado, desabilitado
-vlanid	Tag de identificação de pacote de rede para o IMM	Valor numérico entre 1 e 4094.

Notas:

1. -nic também mostrará o status da nic. [active] indica que nic 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:nicX 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.

Sintaxe:

```
ifconfig eth0 [options]
options:

  -state interface_state
  -c config_method
  -i static_ipv4_ip_address
  -g ipv4_gateway_address
  -s subnet_mask
  -n hostname
  -r data_rate
  -d duplex_mode
  -m max_transmission_unit
  -l locally_administered_MAC
  -b burned_in_MAC_address
  -dn domain_name
  -auto state
  -nic state
  -failover mode
  -nssync state
  -address_table
  -lla ipv6_link_local_addr
  -dhcp6 state
  -ipv6 state
  -ipv6static state
```

```
  -sa6 state
  -i6 static_ipv6_ip_address
  -g6 ipv6_gateway_address
  -p6 length
  -vlan state
  -vlanid VLAN ID
```

Exemplo:

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

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

Comando keycfg

Use esse comando para exibir, incluir ou excluir chaves de ativação.

Acesso de controle de chaves de ativação para funcionalidade IMM opcional.

Notas:

- 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.
- 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.

A tabela a seguir mostra os argumentos das opções.

Tabela 33. Comando keycfg

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
-add	Incluir chave de ativação	Valores para as opções de comando -ip, -pn, -u, -pw e -f
-ip	Endereço IP do servidor TFTP com a chave de ativação a ser incluída	Endereço IP válido para o servidor TFTP
-pn	Número da porta do servidor TFTP/SFTP com a chave de ativação a ser incluída	Número da porta válido para o servidor TFTP/SFTP (padrão 69/22)
-u	Nome de usuário para o servidor SFTP com chave de ativação a ser incluída	Nome de usuário válido para o servidor SFTP
-pw	Senha para o servidor SFTP com chave de ativação a ser incluída	Senha válida para o servidor SFTP
-f	Nome do arquivo para a chave de ativação a ser incluída	Nome do arquivo válido para o arquivo de chave de ativação
-del	Excluir chave de ativação por número de índice	Número de índice de chave de ativação válido a partir da listagem **keycfg**
-deltype	Excluir chave de ativação por tipo de chave	Valor de tipo de chave válido

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

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.

A tabela a seguir mostra os argumentos das opções.

Tabela 34. Comando ldap

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
-a	Método de autenticação do usuário	Somente local, somente LDAP, local primeiro depois LDAP, LDAP primeiro depois local
-aom	Modo somente autenticação	habilitado, desabilitado
-b	Método de ligação	Anônimo, ligação com ClientDN e senha, ligação com Credencial de Login
-c	Nome distinto do cliente	Sequência de até 127 caracteres para **client_dn**
-d	Domínio de procura	Sequência de até 63 caracteres para **search_domain**
-f	Filtro de grupo	Sequência de até 127 caracteres para **group_filter**
-fn	Nome da floresta	Para ambientes do Active Directory. Sequência de até 127 caracteres.
-g	Atributo de procura de grupo	Sequência de até 63 caracteres para **group_search_attr**
-l	Atributo de permissão de login	Sequência de até 63 caracteres para **string**
-p	Senha do cliente	Sequência de até 15 caracteres para **client_pw**
-pc	Confirmar senha do cliente	Sequência de até 15 caracteres para **confirm_pw** O uso do comando é: ldap -p **client_pw** -pc **confirm_pw** Essa opção é necessária quando você altera a senha do cliente. Ela compara o argumento **confirm_pw** com o argumento **client_pw**. O comando falhará se os argumentos não corresponderem.
-ep	Senha criptografada	Senha de backup/restauração (apenas para uso interno)
-r	Nome distinto (DN) de entrada raiz	Sequência de até 127 caracteres para **root_dn**
-rbs	Segurança Aprimorada Baseada em Função para usuários do Active Directory	habilitado, desabilitado
-s1ip	Nome do host/endereço IP do servidor 1	Sequência de até 127 caracteres ou um endereço IP para **host name/ ip_addr**
-s2ip	Nome do host/endereço IP do servidor 2	Sequência de até 127 caracteres ou um endereço IP para **host name/ ip_addr**
-s3ip	Nome do host/endereço IP do servidor 3	Sequência de até 127 caracteres ou um endereço IP para **host name/ ip_addr**
-s4ip	Nome do host/endereço IP do servidor 4	Sequência de até 127 caracteres ou um endereço IP para **host name/ ip_addr**
-s1pn	Número da porta do servidor 1	Um número de porta com até 5 dígitos para **port_number**
-s2pn	Número da porta do servidor 2	Um número de porta com até 5 dígitos para **port_number**

Tabela 34. Comando ldap (continuação)

Opção	Descrição	Valores
-s3pn	Número da porta do servidor 3	Um número de porta com até 5 dígitos para **port_number**
-s4pn	Número da porta do servidor 4	Um número de porta com até 5 dígitos para **port_number**
-t	Nome de destino do servidor	Quando a opção rbs está habilitada, esse campo especifica um nome de destino que pode ser associado a uma ou mais funções no servidor Active Directory por meio da ferramenta Role-Based Security (RBS) Snap-In.
-u	Atributo de pesquisa de UID	Sequência de até 63 caracteres para **search_attrib**
-v	Obter endereço do servidor LDAP por meio de DNS	off, on
-h	Exibe o uso e as opções do comando	

Sintaxe:

```
ldap [options]
options:
   -a loc|ldap|locId|ldloc
   -aom enable/disabled
   -b anon|client|login
   -c client_dn
   -d search_domain
   -f group_filter
   -fn forest_name
   -g group_search_attr
   -l string
   -p client_pw
   -pc confirm_pw
   -ep encrypted_pw
   -r root_dn
   -rbs enable|disabled
   -s1ip host name/ip_addr
   -s2ip host name/ip_addr
   -s3ip host name/ip_addr
   -s4ip host name/ip_addr
   -s1pn port_number
   -s2pn port_number
   -s3pn port_number
   -s4pn port_number
   -t name
   -u search_attrib
   -v off|on
   -h
```

Comando ntp

Use esse comando para exibir e configurar o Network Time Protocol (NTP).

A tabela a seguir mostra os argumentos das opções.

Tabela 35. Comando ntp

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
-en	Habilita ou desabilita o Network Time Protocol.	habilitado, desabilitado
-i[1]	Nome ou endereço IP do servidor Network Time Protocol. Este é o número de índice do servidor Network Time Protocol.	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.
-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.

1. -i é igual a i1.

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

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

Comando portcfg

Use esse comando para configurar o IMM para o recurso de redirecionamento serial.

O IMM deve ser configurado para corresponder às configurações da porta serial interna do servidor. Para alterar a configuração da porta serial, digite as opções, seguidas pelos valores. Para alterar a configuração da porta serial, você deve ter pelo menos autoridade de Configuração de Rede e Segurança do Adaptador.

Nota: A porta serial externa do servidor só pode ser usada pelo IMM para a funcionalidade IPMI. A CLI não é suportada por meio da porta serial. As opções **serred** e **cliauth** que estavam presentes na CLI do Remote Supervisor Adapter II não são suportadas.

A execução do comando **portcfg** sem opções exibe a configuração da porta serial. A tabela a seguir mostra os argumentos das opções.

Nota: O número de bits de dados (8) é configurado no hardware e não pode ser alterado.

Tabela 36. Comando portcfg

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	Taxa de bauds	9600, 19200, 38400, 57600, 115200
-p	Paridade	none, odd, even
-s	Bits de parada	1, 2
-climode	Modo da CLI	0, 1, 2 Onde: • 0 = none: A CLI é desabilitada • 1 = cliems: A CLI é habilitada com sequências de pressionamento de tecla compatíveis com o EMS • 2 = cliuser: A CLI é habilitada com sequências de pressionamento de tecla definidas pelo usuário

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

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

Comando portcontrol

Use esse comando para ativar ou desativar uma porta de serviço de rede.

Atualmente, esse comando suporta apenas o controle da porta para o protocolo IPMI. Digite **portcontrol** para exibir o estado de porta da IPMI. Para ativar ou desativar a porta de rede da IPMI, digite a opção **-ipmi** seguida pelos valores **on** ou **off**.

Tabela 37. Comando portcontrol

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
-all	Ative ou desative todas as interfaces e protocolos de descoberta	ligar, desligar
-cim	Ative ou desative a descoberta de CIM	ligar, desligar

Tabela 37. Comando portcontrol (continuação)

Opção	Descrição	Valores
-ipmi	Ative ou desative o acesso ao ipmi via LAN	ligar, desligar
-ipmi-kcs	Ative ou desative o acesso ao ipmi do servidor	ligar, desligar
-rest	Ative ou desative a descoberta de REST	ligar, desligar
-slp	Ative ou desative a descoberta de SLP	ligar, desligar
-snmp	Ative ou desative a descoberta de SNMP	ligar, desligar
-ssdp	Ative ou desative a descoberta de SSDP	ligar, desligar
-cli	Ative ou desative a descoberta de CLI	ligar, desligar
-web	Ative ou desative a descoberta de WEB	ligar, desligar

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

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

Comando ports

Use esse comando para exibir e configurar as portas do IMM.

A execução do comando **ports** sem opções exibe informações de todas as portas do IMM. A tabela a seguir mostra os argumentos das opções.

Tabela 38. Comando ports

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
-open	Exibir portas abertas	
-reset	Reconfigurar portas para configurações padrão	

Tabela 38. Comando ports (continuação)

Opção	Descrição	Valores
-httpp	Número da porta HTTP	Número da porta padrão: 80
-httpsp	Número da porta HTTPS	Número da porta padrão: 443
-sshp	Número da porta da CLI legada do SSH	Número da porta padrão: 22
-snmpap	Número da porta do agente SNMP	Número da porta padrão: 161
-snmptp	Número da porta de traps SNMP	Número da porta padrão: 162
-rpp	Número da porta de presença remota	Número da porta padrão: 3900
-cimhp	Número da porta do CIM sobre HTTP	Número da porta padrão: 5988
-cimhsp	Número da porta do CIM sobre HTTPS	Número da porta padrão: 5989

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

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

Comando rdmount

Use esse comando para montar imagens de disco remoto ou compartilhamentos de rede

A tabela a seguir mostra os argumentos das opções.

Tabela 39. Comando rdmount

A tabela a seguir é uma tabela de duas colunas e várias linhas que consiste em opções e descrições de opção.

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

Tabela 39. Comando rdmount (continuação)

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.

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.

A tabela a seguir mostra os argumentos das opções.

Tabela 40. Comando restore

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
-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

Tabela 40. Comando restore (continuação)

Opção	Descrição	Valores
-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

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

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

Comando restoredefaults

Use esse comando para restaurar todas as configurações do IMM para o padrão de fábrica.

- Não há opções para o comando **restoredefaults**.
- Você será solicitado a confirmar o comando antes que ele seja processado.

Sintaxe:
```
restoredefaults
```

Exemplo:
```
system> restoredefaults

This action will cause all IMM settings to be set to factory defaults.

If this is the local system, you will lose your TCP/IP connection as a result.
You will need to reconfigure the IMM network interface to restore connectivity.
After the IMM configuration is cleared, the IMM will be restarted.

Proceed? (y/n)
Y
Restoring defaults
```

comando roles

Use esse comando para exibir ou configurar as funções.

A tabela a seguir mostra os argumentos das opções.

Tabela 41. Comando roles

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
-n	Função para configurar	Limitada a 32 caracteres
-p	Definir privilégios	personalizado :am|rca|rcvma|pr|cel|bc|nsc|ac|us • **am**: acesso de gerenciamento da conta do usuário • **rca**: acesso ao console remoto • **rcvma**: acesso ao console e ao disco remotos (mídia virtual) • **pr**: acesso de energia/reinicialização do servidor remoto • **cel**: capacidade para limpar logs de eventos • **bc**: configuração de adaptador (básica) • **nsc**: configuração de adaptador (rede e segurança) • **ac**: configuração de adaptador (avançada) • **us**: segurança do UEFI **Nota:** Os sinalizadores de permissão personalizada acima podem ser usados em qualquer combinação
d	Excluir uma linha	

Sintaxe

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

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 seccfg

Use esse comando para executar uma reversão de firmware.

A tabela a seguir mostra os argumentos das opções.

Tabela 42. Comando seccfg

A tabela a seguir é uma tabela de duas colunas e várias linhas que consiste em opções e descrições de opção.

Opção	Descrição	Valor
-fwrb	Permite reverter o firmware para a versão anterior	yes, no
-rppen	Presença física remota habilitada (somente leitura)	/
-rppto	Presença física remota com limite de tempo atingido (somente leitura)	/
-rpp	Presença física (se habilitada pelo BIOS)	yes, no
-aubp	habilitar ou desabilitar a função de backup automático para a promoção primária	habilitado, desabilitado

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 43. 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 smtp

Use esse comando para exibir e configurar a interface SMTP.

A execução do comando **smtp** sem opções exibe todas as informações da interface SMTP. A tabela a seguir mostra os argumentos das opções.

Tabela 44. Comando smtp

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
-auth	Suporte de autenticação SMTP	habilitado, desabilitado
-authepw	Senha criptografada de autenticação SMTP	Sequência de senha válida
-authmd	Método de autenticação SMTP	CRAM-MD5, LOGIN
-authn	Nome de usuário da autenticação SMTP	Sequência (limitada a 256 caracteres)
-authpw	Senha de autenticação SMTP	Sequência (limitada a 256 caracteres)
-pn	Número da porta SMTP	Número de porta válido
-s	Endereço IP ou nome do host do servidor SMTP	Endereço IP ou nome do host válido (limite de 63 caracteres)

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

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

Comando snmp

Use esse comando para exibir e configurar informações da interface SNMP.

A execução do comando **snmp** sem opções exibe todas as informações da interface SNMP. A tabela a seguir mostra os argumentos das opções.

Tabela 45. Comando snmp

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.

Tabela 45. Comando snmp (continuação)

Opção	Descrição	Valores
-a3	Agente do SNMPv3	ligar, desligar **Notas:** Para ativar o agente do SNMPv3, os critérios a seguir devem ser atendidos: • Contato do IMM especificado usando a opção de comando -cn. • Local do IMM especificado usando a opção de comando -l.
-t1	Traps SNMPv1	ligar, desligar
-t2	Traps SNMPv2	ligar, desligar
-t	Traps SNMPv3	ligar, desligar
-l	Local do IMM	Sequência (limitada a 47 caracteres). **Notas:** • Argumentos que contêm espaços devem ser colocados entre aspas. Nenhum espaço à esquerda ou direita é permitido nos argumentos. • Limpe o local do IMM sem especificar um argumento ou especificando uma string vazia como o argumento, como "".
-cn	nome do contato do IMM	Sequência (limitada a 47 caracteres). **Notas:** • Argumentos que contêm espaços devem ser colocados entre aspas. Nenhum espaço à esquerda ou direita é permitido nos argumentos. • Limpe o nome do contato do IMM sem especificar um argumento ou especificando uma string vazia como o argumento, como "".
-c	Nome da comunidade SNMP	Sequência (limitada a 15 caracteres). **Notas:** • Argumentos que contêm espaços devem ser colocados entre aspas. Nenhum espaço à esquerda ou direita é permitido nos argumentos. • Limpe o nome da comunidade do SNMP não especificando um argumento ou especificando uma sequência vazia como o argumento, tal como "".
-ct	Nome da comunidade do trap SNMPv2	Sequência (limitada a 15 caracteres). **Notas:** • Argumentos que contêm espaços devem ser colocados entre aspas. Nenhum espaço à esquerda ou direita é permitido nos argumentos. • Limpe o nome do contato do IMM sem especificar um argumento ou especificando uma string vazia como o argumento, como "".
-ci	Endereço IP/nome do host da comunidade SNMP	Endereço IP ou nome do host válido (limitado a 63 caracteres). **Notas:** • 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. • Limpe um endereço IP ou nome do host da comunidade SNMP não especificando um argumento.

Tabela 45. Comando snmp (continuação)

Opção	Descrição	Valores
-cti	Nome do host/endereço IP da comunidade do trap SNMPv2	Endereço IP ou nome do host válido (limitado a 63 caracteres). **Notas:** • 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. • Limpe um endereço IP ou nome do host da comunidade SNMP não especificando um argumento.
-eid	ID do mecanismo SNMP	String (limite de 1 a 27 caracteres)

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

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.

A execução de **snmpalerts** sem opções exibe todas as configurações de alerta de SNMP. A tabela a seguir mostra os argumentos das opções.

Tabela 46. Comando snmpalerts

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.

Tabela 46. Comando snmpalerts (continuação)

Opção	Descrição	Valores
-status	Status de alerta de SNMP	ligar, desligar
-crt	Configura eventos críticos que enviam alertas	all, none, custom:te|vo|po|di|fa|cp|me|in|re|ot Configurações customizadas de alerta crítico são especificadas usando uma lista de valores separados por barra vertical no formato **snmpalerts -crt custom:te|vo**, em que os valores customizados são: • te: limite de temperatura crítico excedido • vo: limite de voltagem crítico excedido • po: falha de energia crítica • di: falha da unidade de disco rígido • fa: falha do ventilador • cp: falha do microprocessador • me: falha de memória • in: incompatibilidade de hardware • re: falha de redundância de energia • ot: todos os outros eventos críticos
-crten	Enviar alertas de evento crítico	habilitado, desabilitado
-wrn	Configura eventos de aviso que enviam alertas	all, none, custom:rp|te|vo|po|fa|cp|me|ot Configurações customizadas de alerta de aviso são especificadas usando uma lista de valores separados por barra vertical no formato **snmpalerts -wrn custom:rp|te**, em que os valores customizados são: • rp: aviso de redundância de energia • te: aviso de limite de temperatura excedido • vo: aviso de limite de voltagem excedido • po: aviso de limite de energia excedido • fa: evento de ventilador não crítico • cp: microprocessador em estado degradado • me: aviso de memória • ot: todos os outros eventos de aviso
-wrnen	Enviar alertas de evento de aviso	habilitado, desabilitado

Tabela 46. Comando snmpalerts (continuação)

Opção	Descrição	Valores
-sys	Configura eventos de rotina que enviam alertas	all, none, custom:lo|tio|ot|po|bf|til|pf|el|ne Configurações customizadas de alerta de rotina são especificadas usando uma lista de valores separados por barra vertical no formato **snmpalerts -sys custom:lo|tio**, em que os valores customizados são: • lo: login remoto bem-sucedido • tio: tempo limite do sistema operacional • ot: todos os outros eventos informativos e do sistema • po: ligar/desligar energia • bf: falha de inicialização do sistema operacional • til: tempo limite de watchdog do carregador do sistema operacional • pf: falha prevista (PFA) • el: log de eventos 75% cheio • ne: mudança de rede
-sysen	Enviar alertas de evento de rotina	habilitado, desabilitado

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

Comando srcfg

Use esse comando para indicar a sequência-chave para entrar na CLI a partir do modo de redirecionamento serial.

Para alterar a configuração de redirecionamento serial, digite as opções, seguidas pelos valores. Para alterar a configuração de redirecionamento serial, você deve ter pelo menos a autoridade de Configuração de Rede e Segurança do Adaptador.

Nota: O hardware do IMM não fornece um recurso de passagem de porta serial para porta serial. Portanto, as opções `-passthru` e `entercliseq` que estão presentes na CLI do Remote Supervisor Adapter II não são suportadas.

A execução do comando **srcfg** sem opções exibe a sequência de pressionamento de tecla de redirecionamento serial atual. A tabela a seguir mostra os argumentos para a opção do comando `srcfg -entercliseq`.

Tabela 47. Comando srcfg

A tabela a seguir é uma tabela de três colunas e uma linha que consiste na opção, na descrição da opção e nas informações de valores da opção.

Tabela 47. Comando srcfg (continuação)

Opção	Descrição	Valores
-entercliseq	Inserir uma sequência de pressionamento de tecla da CLI	Sequência de pressionamento de tecla definida pelo usuário para entrar na CLI. **Nota:** Esta sequência deve ter pelo menos um caractere e no máximo 15 caracteres. O símbolo de acento circunflexo (^) possui um significado especial nesta sequência. Ele denota Ctrl para pressionamentos de tecla que são mapeados para sequências Ctrl (por exemplo, ^[para a tecla de escape e ^M para retorno de linha). Todas as ocorrências de ^ são interpretadas como parte de uma sequência Ctrl. Consulte uma tabela de conversão de ASCII-para-teclas para obter uma lista completa de sequências Ctrl. O valor padrão para esse campo é ^[(que é Esc seguido por (.

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

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

Comando sshcfg

Use esse comando para exibir e configurar os parâmetros do SSH.

A execução do comando **sshcfg** sem opções exibe todos os parâmetros de SSH. A tabela a seguir mostra os argumentos das opções.

Tabela 48. Comando sshcfg

Essa 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
-cstatus	Estado da CLI do SSH	habilitado, desabilitado
-hk gen	Gerar chave privada do servidor SSH	
-hk rsa	Exibir chave pública RSA do servidor	

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

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 ssl

Use esse comando para exibir e configurar os parâmetros do SSL.

Para habilitar um cliente SSL, um certificado de cliente deve ser instalado. A execução do comando **ssl** sem opções exibe os parâmetros de SSL. A tabela a seguir mostra os argumentos das opções.

Tabela 49. Comando ssl

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
-ce	Ativa ou desativa um cliente SSL	ligar, desligar
-se	Ativa ou desativa um servidor SSL	ligar, desligar
-cime	Ativa ou desativa o CIM sobre HTTPS no servidor SSL	ligar, desligar

Sintaxe:

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

Parâmetros: Os parâmetros a seguir são apresentados na exibição de status da opção para o comando **ssl** e são a saída apenas a partir da CLI:

Ativar transporte seguro do Servidor
Esta exibição de status é somente leitura e não pode ser definida diretamente.

Status da chave Web/CMD do servidor
Esta exibição de status é somente leitura e não pode ser definida diretamente. Os possíveis valores de saída da linha de comandos são os seguintes:

Chave Privada e Cert/CSR não disponíveis

Chave Privada e certificado assinado pela CA instalados

Chave Privada e certificado autoassinado autogerado instalados

Chave Privada e certificado autoassinado instalados

Chave Privada armazenada, CSR não disponíveis para download

Status da chave CSR do servidor SSL
Esta exibição de status é somente leitura e não pode ser definida diretamente. Os possíveis valores de saída da linha de comandos são os seguintes:

Chave Privada e Cert/CSR não disponíveis

Chave Privada e certificado assinado pela CA instalados

Chave Privada e certificado autoassinado autogerado instalados

Chave Privada e certificado autoassinado instalados

Chave Privada armazenada, CSR não disponíveis para download

Status da chave LDAP do cliente SSL

Esta exibição de status é somente leitura e não pode ser definida diretamente. Os possíveis valores de saída da linha de comandos são os seguintes:

Chave Privada e Cert/CSR não disponíveis

Chave Privada e certificado assinado pela CA instalados

Chave Privada e certificado autoassinado autogerado instalados

Chave Privada e certificado autoassinado instalados

Chave Privada armazenada, CSR não disponíveis para download

Status da chave CSR do cliente SSL

Esta exibição de status é somente leitura e não pode ser definida diretamente. Os possíveis valores de saída da linha de comandos são os seguintes:

Chave Privada e Cert/CSR não disponíveis

Chave Privada e certificado assinado pela CA instalados

Chave Privada e certificado autoassinado autogerado instalados

Chave Privada e certificado autoassinado instalados

Chave Privada armazenada, CSR não disponíveis para download

Comando sslcfg

Use esse comando para exibir e configurar o SSL para o IMM e gerenciar certificados.

A execução do comando **sslcfg** sem opções exibe todas as informações de configuração do SSL. O comando **sslcfg** é usado para gerar uma nova chave de criptografia e certificado autoassinado ou solicitação de assinatura de certificado (CSR). A tabela a seguir mostra os argumentos das opções.

Tabela 50. Comando sslcfg

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
-server	Status do servidor SSL	habilitado, desabilitado **Nota:** O servidor SSL poderá ser habilitado apenas se houver um certificado válido no local.
-client	Status do cliente SSL	habilitado, desabilitado **Nota:** O cliente SSL poderá ser habilitado apenas se houver um certificado de servidor ou cliente válido no local.
-cim	Status do CIM sobre HTTPS	habilitado, desabilitado **Nota:** O CIM sobre HTTPS poderá ser habilitado apenas se houver um certificado de servidor ou cliente válido no local.
-cert	Gerar certificado autoassinado	server, client, sysdir, storekey **Notas:** • Os valores para as opções de comando **-c**, **-sp**, **-cl**, **-on** e **-hn** são necessários ao gerar um certificado autoassinado. • Os valores para as opções de comando **-cp**, **-ea**, **-ou**, **-s**, **-gn**, **-in** e **-dq** são opcionais ao gerar um certificado autoassinado.

Tabela 50. Comando sslcfg (continuação)

Opção	Descrição	Valores
-csr	Gerar um CSR	server, client, sysdir, storekey **Notas:** • Os valores para as opções de comando **-c**, **-sp**, **-cl**, **-on** e **-hn** são necessários ao gerar um CSR. • Os valores para as opções de comando **-cp**, **-ea**, **-ou**, **-s**, **-gn**, **-in**, **-dq**, **-cpwd** e **-un** são opcionais ao gerar um CSR.
-i	Endereço IP para o servidor TFTP/SFTP	Endereço IP válido **Nota:** 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 **Nota:** 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	Fazer download do arquivo de certificado	Essa opção não usa argumentos; porém, também deve especificar valores para a opção de comando **-cert** ou **-csr** (dependendo do tipo de certificado que está sendo transferido por download). Essa opção não usa argumentos; porém, também deve especificar valores para a opção de comando **-i** e a opção de comando **-l** (opcional).
-upld	Importa o arquivo de certificado	Essa opção não usa argumentos, porém também deve especificar valores para as opções de comando **-cert**, **-i** e **-l**.
-tc**x**	Certificado de confiança **x** para cliente SSL	import, download, remove **Nota:** O número do certificado de confiança, **x**, é especificado como um número inteiro de 1 a 3 na opção de comando.
-c	País	Código do país (2 letras) **Nota:** Necessário ao gerar um certificado autoassinado ou CSR.
-sp	Estado ou município	Sequência delimitada por aspas (máximo 60 caracteres) **Nota:** Necessário ao gerar um certificado autoassinado ou CSR.
-cl	Cidade ou localidade	Sequência delimitada por aspas (máximo 50 caracteres) **Nota:** Necessário ao gerar um certificado autoassinado ou CSR.
-on	Nome da organização	Sequência delimitada por aspas (máximo 60 caracteres) **Nota:** Necessário ao gerar um certificado autoassinado ou CSR.
-hn	Nome do host do IMM	Sequência (máximo 60 caracteres) **Nota:** Necessário ao gerar um certificado autoassinado ou CSR.
-cp	Pessoa de contato	Sequência delimitada por aspas (máximo 60 caracteres) **Nota:** Opcional ao gerar um certificado autoassinado ou CSR.
-ea	Endereço de email da pessoa de contato	Endereço de email válido (máximo 60 caracteres) **Nota:** Opcional ao gerar um certificado autoassinado ou CSR.
-ou	Unidade Organizacional	Sequência delimitada por aspas (máximo 60 caracteres) **Nota:** Opcional ao gerar um certificado autoassinado ou CSR.

Tabela 50. Comando sslcfg (continuação)

Opção	Descrição	Valores
-s	Sobrenome	Sequência delimitada por aspas (máximo 60 caracteres) **Nota:** Opcional ao gerar um certificado autoassinado ou CSR.
-gn	Nome	Sequência delimitada por aspas (máximo 60 caracteres) **Nota:** Opcional ao gerar um certificado autoassinado ou CSR.
-in	Iniciais	Sequência delimitada por aspas (máximo 20 caracteres) **Nota:** Opcional ao gerar um certificado autoassinado ou CSR.
-dq	Qualificador de nome de domínio	Sequência delimitada por aspas (máximo 60 caracteres) **Nota:** Opcional ao gerar um certificado autoassinado ou CSR.
-cpwd	Senha de desafio	Sequência (mínimo 6 caracteres, máximo 30 caracteres) **Nota:** Opcional ao gerar um CSR.
-un	Nome não estruturado	Sequência delimitada por aspas (máximo 60 caracteres) **Nota:** Opcional ao gerar um CSR.

Sintaxe:

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

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 CIM Certificate status:
 A self-signed certificate is installed
SSL Client Trusted Certificate status:
 Trusted Certificate 1: Not available
 Trusted Certificate 2: Not available
 Trusted Certificate 3: Not available
 Trusted Certificate 4: Not available
```

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

O exemplo acima é exibido em várias linhas devido a limitações de espaço.

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

  O exemplo acima é exibido em várias linhas devido a limitações de espaço.

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 storekeycfg

Use esse comando para configurar o nome do host, o endereço IP e a porta de rede para um servidor SKLM.

É possível definir até quatro destinos de servidor SKLM. O comando **storekeycfg** também é usado para instalar e remover os certificados utilizados pelo IMM para autenticação do servidor SKLM.

A tabela a seguir mostra os argumentos das opções.

Tabela 51. Comando storekeycfg

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.

Tabela 51. Comando storekeycfg (continuação)

Opção	Descrição	Valores
-add	Incluir a chave de ativação	Os valores são as opções de comando -ip, -pn, -u, -pw e -f
-ip	Nome do host ou endereço IP do servidor TFTP/SFTP	Nome do host ou endereço IP válido do servidor TFTP/SFTP
-pn	Número da porta do servidor TFTP ou SFTP	Número da porta válido para o servidor TFTP/SFTP (o valor padrão é 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
-f	Nome do arquivo para a chave de ativação	Nome do arquivo válido para o nome do arquivo de chave de ativação
-del	Use esse comando para excluir a chave de ativação por número de índice	Número de índice de chave de ativação válido a partir da listagem keycfg
-dgrp	Inclui o grupo de dispositivos	Nome do grupo de dispositivos
-sxip	Inclui o nome do host ou o endereço IP do servidor SKLM	Nome do host ou endereço IP válido do servidor SKLM. Valor numérico de 1, 2, 3 ou 4.
-sxpn	Inclui o número da porta do servidor SKLM	Número de porta válido para o servidor SKLM. Valor numérico de 1, 2, 3 ou 4.
-testx	Testa a configuração e a conexão com o servidor SKLM	Valor numérico de 1, 2, 3 ou 4
-h	Exibir o uso e as opções do comando	

Sintaxe:

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

Exemplos:

Para importar o certificado do servidor SKLM, insira o seguinte comando:

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

Para configurar o endereço e o número da porta do servidor SKLM, insira o seguinte comando:

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

Para definir o nome de grupo de dispositivos, insira o seguinte comando:

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

Comando syncrep

Use este comando para iniciar a sincronização de firmware do repositório remoto.

A tabela a seguir mostra os argumentos das opções.

Tabela 52. Comando syncrep

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
-t	Protocolo para conectar o repositório	samba, nfs
-l	Local do repositório remoto	No formato URL
-u	Usuário	
-p	Senha	
-o	Opção	-String de opção adicional para montagens samba e nfs
-d	Domínio	Domínio para montagem samba
-q	Status de atualização atual da consulta	
-c	Cancelar o processo de sincronização	

Sintaxe

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

Exemplo

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

Comando thermal

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.

Tabela 53. Comando thermal

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
-mode	Seleção de modo térmico	normal, desempenho, mínimo, eficiência, personalizado
-table	Fornecedor, identificação do dispositivo (ID) e tabela térmica alternativa	

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

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

Comando timeouts

Use esse comando para exibir ou alterar os valores de tempo limite.

- Para exibir os tempos limite, digite `timeouts`.
- Para alterar os valores de tempo limite, digite as opções seguidas pelos valores.
- Para alterar os valores de tempo limite, você deve ter pelo menos autoridade de Configuração de Adaptador.

A tabela a seguir mostra os argumentos para os valores de tempo limite. Estes valores correspondem às opções suspensas de escala graduada para tempos limites do servidor na interface da Web.

Tabela 54. Comando timeouts

A tabela a seguir é uma tabela de quatro colunas e várias linhas que consiste nas opções, descrições das opções e os valores associados das opções.

Opção	Tempo limite	Unidades	Valores
-f	Atraso de desligamento	minutos	desabilitado, 0.5, 1, 2, 3, 4, 5, 7.5, 10, 15, 20, 30, 60, 120
-l	Tempo limite do carregador	minutos	desabilitado, 0.5, 1, 1.5, 2, 2.5, 3, 3.5, 4, 4.5, 5, 7.5, 10, 15, 20, 30, 60, 120

Tabela 54. Comando timeouts (continuação)

Opção	Tempo limite	Unidades	Valores
-o	Tempo limite do sistema operacional	minutos	desabilitado, 2.5, 3, 3.5, 4
-s	Captura de tela de falha do SO com erro de HW	/	habilitado, desabilitado

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

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

Comando tls

Use esse comando para definir o nível mínimo do TLS.

A tabela a seguir mostra os argumentos das opções.

Tabela 55. Comando tls

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
-min	Selecione o nível mínimo de TLS	1.0, 1.1, 1.2[1], 1.3
-h	Liste o uso e as opções	

Notas:

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.

Uso:
```
tls [-options] - configures the minimum TLS level
   -min <1.0 | 1.1 | 1.2 | 1.3> - Selects the minimum TLS level
   -h - Lists usage and options
```

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.

A tabela a seguir mostra os argumentos das opções.

Tabela 56. Comando uefipw

A tabela a seguir é uma tabela de duas colunas e várias linhas que consiste em opções e descrições de opção.

Opção	Descrição
-s	Configurar mensagens de infração
-h	Lista o uso e as opções

Sintaxe:

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

Exemplo:

Nota: A mensagem de infração não contém nenhum espaço.

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

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

Comando uefipw

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.

A tabela a seguir mostra os argumentos das opções.

Tabela 57. Comando uefipw

A tabela a seguir é uma tabela de duas colunas e várias linhas que consiste em opções e descrições de opção.

Opção	Descrição
-cp	Senha atual (limitada a 20 caracteres)
-p	Nova senha (limitada a 20 caracteres)
-cep	Senha atual criptografada
-ep	Nova senha criptografada

Sintaxe:

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

Comando usbeth

Use esse comando para habilitar ou desabilitar a interface LAN sobre USB dentro da banda.

Sintaxe:

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

Exemplo:

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

Comando usbfp

Use este comando para controlar o uso do BMC da porta USB no painel frontal

A tabela a seguir mostra os argumentos das opções.

Tabela 58. Comando usbfp

A tabela a seguir é uma tabela de duas colunas e várias linhas que consiste em opções e descrições de opção.

Opção	Descrição
-mode <bmc | server | shared>	Definir o modo de uso como BMC, servidor ou compartilhado
-it <minutes>	Tempo limite de inatividade em minutos (modo compartilhado
-btn <on | off>	Habilitar usando o botão de ID para alternar o proprietário (modo compartilhado)
-own <bmc | server >	Definir o proprietário como bmc ou servidor (modo compartilhado)

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. A tabela a seguir mostra os argumentos das opções.

Tabela 59. Comando users

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
-**user_index**	Número de índice da conta do usuário	1 a 12, inclusive, ou `all` para todos os usuários.
-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 20 caracteres. Null cria uma conta sem uma senha que o usuário deve configurar durante seu primeiro login.
-a	Nível de autoridade	O nível de autoridade pode ser um dos seguintes: • `super` (supervisor) • `ro` (somente leitura) • Qualquer combinação dos valores a seguir, separados por |: – `am` (acesso ao gerenciamento de conta do usuário) – `rca` (acesso ao console remoto) – `rcvma` (acesso a console remoto e mídia virtual) – `pr` (acesso para ligar/reiniciar servidor remoto) – `cel` (capacidade de limpar logs de eventos) – `bc` (configuração de adaptador [básica]) – `nsc` (configuração de adaptador [rede e segurança]) – `ac` (configuração de adaptador [avançada])
-ep	Senha de criptografia (para backup/restauração)	Senha válida

Tabela 59. Comando users (continuação)

Opção	Descrição	Valores
-clear	Apagar conta do usuário especificada 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.	O número de índice da conta do usuário a ser apagado deve ser especificado, seguindo o formato: `users -clear -`**user_index**
-curr	Exibir usuários atualmente com login efetuado	
-sauth	Protocolo de autenticação SNMPv3	HMAC-SHA, nenhum
-spriv	Protocolo de privacidade do SNMPv3	CBC-DES, AES, none
-spw	Senha de privacidade do SNMPv3	Senha válida
-sepw	Senha de privacidade do SNMPv3 (criptografada)	Senha válida
-sacc	Tipo de acesso do SNMPv3	get, set
-strap	Nome do host do trap SNMPv3	Nome do host válido
-pk	Exibir chave pública SSH para o usuário	Número de índice da conta do usuário. **Notas:** • Cada chave SSH designada ao usuário é exibida, juntamente com um número de índice de chave de identificação. • 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`. • Todas as chaves estão no formato OpenSSH. • Para nós Flex, os comandos do usuário são limitados apenas a contas IPMI e SNMP locais. A opção `-pk` não é suportada para Flex Systems.
-e	Exibir uma chave SSH inteira no formato OpenSSH **(opção de chave pública SSH)**	Essa opção não usa argumentos e deve ser usada exclusiva de todas as outras opções `users -pk`. **Nota:** 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`.

Tabela 59. Comando users (continuação)

Opção	Descrição	Valores
-remove	Remover chave pública SSH do usuário **(opção de chave pública SSH)**	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. **Notas:** • 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`. • Para nós Flex, os comandos do usuário são limitados apenas a contas IPMI e SNMP locais. A opção `-remove` não é suportada para Flex Systems.
-add	Incluir chave pública SSH para o usuário **(opção de chave pública SSH)**	Chave delimitada por aspas no formato OpenSSH **Notas:** • A opção `-add` é de uso exclusivo de todas as outras opções de comando `users -pk`. • 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 "AAAAB3NzC1yc2EAAAABIwAAA QEAvfnTUzRF7pdBuaBy4dO/aIFasa/Gtc+o/wlZnuC4aD HMA1UmnMyLOCiIaNOy4OOICEKCqjKEhrYymtAoVtfKApv Y39GpnSGRC/ qcLGWLM4cmirKL5kxHNOqIcwbT1NPceoKH j46X7E +mqlfWnAhhjDpcVFjagM3Ek2y7w/tBGrwGgN7DP HJU1tzcJy68mEAnIrzjUoR98Q3/B9cJD77ydGKe8rPdI2 hIEpXR5dNUiupA1Yd8PSSMgdukASKEd3eRRZTBl3SAtMu cUsTkYjlXcqex1OQz4+N5OR6MbNcwlsx+mTEAvvcpJhug a7OUNPGhLJMl6k7jeJiQ8Xd2p XbOZQ=="` • Para nós Flex, os comandos do usuário são limitados apenas a contas IPMI e SNMP locais. A opção `-add` não é suportada para Flex Systems.
-upld	Fazer upload de uma chave pública SSH **(opção de chave pública SSH)**	Requer as opções `-i` e `-l` para especificar o local da chave. **Notas:** • A opção `-upld` é usada exclusiva de todas as outras opções de comando `users -pk` (exceto `-i` e `-l`). • 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. • 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`. • Para nós Flex, os comandos do usuário são limitados apenas a contas IPMI e SNMP locais. A opção `-upld` não é suportada para Flex Systems.
-dnld	Fazer o download de uma chave pública SSH especificada **(opção de chave pública SSH)**	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. **Notas:** • A opção `-dnld` é usada exclusiva de todas as outras opções de comando `users -pk` (exceto `-i`, `-l` e -**key_index**). • 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`.

Tabela 59. Comando users (continuação)

Opção	Descrição	Valores
-i	Endereço IP do servidor TFTP/SFTP para fazer upload ou fazer o downloading de um arquivo-chave **(opção de chave pública SSH)**	Endereço IP válido **Nota:** A opção `-i` é exigida pelas opções de comando `users -pk -upld` e `users -pk -dnld`.
-pn	Número da porta do servidor TFTP/SFTP **(opção de chave pública SSH)**	Número da porta válido (padrão 69/22) **Nota:** Um parâmetro opcional para as opções de comando `users -pk -upld` e `users -pk -dnld`.
-u	Nome de usuário para o servidor SFTP **(opção de chave pública SSH)**	Nome de usuário válido **Nota:** Um parâmetro opcional para as opções de comando `users -pk -upld` e `users -pk -dnld`.
-pw	Senha para o servidor SFTP **(opção de chave pública SSH)**	Senha válida **Nota:** 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 **(opção de chave pública SSH)**	Nome do arquivo válido **Nota:** A opção `-l` é exigida pelas opções de comando `users -pk -upld` e `users -pk -dnld`.
-af	Aceitar conexões do host **(opção de chave pública SSH)**	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 **(opção de chave pública SSH)**	Sequência limitada por aspas de até 255 caracteres. **Nota:** 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."`.

Sintaxe:

```
users [-options] - display/configure user accounts
options:
   -[1-12]  - user account number
   -l       - display password expiration days
   -n       - username (limited to 16 characters)
   -p       - password (limited to 32 characters)
   -shp     - set hashpassword (total 64 characters)
   -ssalt   - set salt (limited to 64 characters)
   -ghp     - get hashpassword
   -gsalt   - get salt
   -ep      - encrypted password (used with backup/restore )

   -a       - authority level (super, ro, custom:am|rca|rcvma|pr|cel|bc|nsc|ac)
       -am    - User account management access
       -rca   - Remote console access
       -rcvma - Remote console and remote disk (virtual media) access
       -pr    - Remote server power/restart access
       -cel   - Ability to clear event logs
```

```
      -bc    - Adapter Configuration (basic)
      -nsc   - Adapter Configuration (network and security)
      -ac    - Adapter Configuration (advanced)

   -clear   - clear user account
   -curr    - display current users
   -sauth   (none|HMAC-SHA)           - snmpv3 authentication protocol
   -spriv   (none|CBC-DES|AES)        - snmpv3 privacy protocol
   -spw     password                    - snmpv3 privacy password
   -sepw    encryptedpassword          - snmpv3 privacy password (encrypted)
   -sacc    (Get)                  - snmpv3 Access type
   -strap   hostname                    - snmpv3 trap hostname

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

Nota: -os sinalizadores de permissão personalizada podem ser usados em qualquer combinação.

Exemplo:

```
system> users
 Account      Login ID      Advanced Attribute              Role             Password Expires
 -------      --------       ------------------             ------             ----------------
    1           USERID                   Native                 Administrator                    89 day(s)
system> users -2 -n sptest -p PasswOrd12 -a super
The user is required to change the password when the user logs in to the management server for the first time
ok
system> users
 Account      Login ID      Advanced Attribute             Role               Password Expires
 -------      --------       ------------------            ------              ----------------
    1           USERID                   Native            Administrator                    90 day(s)
2           sptest                  Native                 Administrator            Password expired
system> hashpw -sw enabled -re enabled
system> users -5 -n guest5 -shp 292bcbc41bb078cf5bd258db60b63a4b337c8c954409442cfad7148bc6428fee -ssalt abc -a super
system> users -5 ghp
292bcbc41bb078cf5bd258db60b63a4b337c8c954409442cfad7148bc6428fee
system> users -5 gsalt
abc
system> users -2 -n sptest -p PasswOrd12 -a custom:am|rca
The user is required to change the password when the user logs in to the management server for the first time
ok
```

Comandos de controle IMM

Este tópico fornece uma lista alfabética dos comandos CLI de controle IMM.

Atualmente, há 7 comandos de controle IMM:

Comando alertentries

Use esse comando para gerenciar destinatários do alerta.

- **alertentries** sem opções exibe todas as configurações de entrada de alerta.
- **alertentries -number -test** gera um alerta de teste para o número de índice do destinatário fornecido.
- **alertentries -number** (em que o número é de 0 a 12) exibe configurações de entrada de alerta para o número de índice do destinatário especificado ou permite modificar as configurações de alerta para esse destinatário.

A tabela a seguir mostra os argumentos das opções.

Tabela 60. Comando alertentries

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
-number	Número de índice do destinatário do alerta para exibir, incluir, modificar ou excluir	1 a 12
-status	Status do destinatário do alerta	ligar, desligar
-type	Tipo de alerta	email, syslog
-log	Incluir log de eventos no email de alerta	ligar, desligar
-n	Nome do destinatário do alerta	Sequência
-e	Endereço de email do destinatário do alerta	Endereço de email válido
-ip	Endereço IP ou nome do host do syslog	Endereço IP ou nome do host válido
-pn	Número da porta do syslog	Número de porta válido
-del	Excluir número de índice do destinatário especificado	
-test	Gerar um alerta de teste para o número de índice do destinatário especificado	

Tabela 60. Comando alertentries (continuação)

Opção	Descrição	Valores
-crt	Configura eventos críticos que enviam alertas	all, none, custom:te|vo|po|di|fa|cp|me|in|re|ot Configurações customizadas de alerta crítico são especificadas usando uma lista de valores separados por barra vertical no formato **alertentries -crt custom:te|vo**, em que os valores customizados são: • te: limite de temperatura crítico excedido • vo: limite de voltagem crítico excedido • po: falha de energia crítica • di: falha da unidade de disco rígido • fa: falha do ventilador • cp: falha do microprocessador • me: falha de memória • in: incompatibilidade de hardware • re: falha de redundância de energia • ot: todos os outros eventos críticos
-crten	Enviar alertas de evento crítico	habilitado, desabilitado
-wrn	Configura eventos de aviso que enviam alertas	all, none, custom:rp|te|vo|po|fa|cp|me|ot Configurações customizadas de alerta de aviso são especificadas usando uma lista de valores separados por barra vertical no formato **alertentries -wrn custom:rp|te**, em que os valores customizados são: • rp: aviso de redundância de energia • te: aviso de limite de temperatura excedido • vo: aviso de limite de voltagem excedido • po: aviso de limite de energia excedido • fa: evento de ventilador não crítico • cp: microprocessador em estado degradado • me: aviso de memória • ot: todos os outros eventos de aviso
-wrnen	Enviar alertas de evento de aviso	habilitado, desabilitado

Tabela 60. Comando alertentries (continuação)

Opção	Descrição	Valores
-sys	Configura eventos de rotina que enviam alertas	all, none, custom:lo|tio|ot|po|bf|til|pf|el|ne Configurações customizadas de alerta de rotina são especificadas usando uma lista de valores separados por barra vertical no formato **alertentries -sys custom:lo|tio**, em que os valores customizados são: • lo: login remoto bem-sucedido • tio: tempo limite do sistema operacional • ot: todos os outros eventos informativos e do sistema • po: ligar/desligar energia • bf: falha de inicialização do sistema operacional • til: tempo limite de watchdog do carregador do sistema operacional • pf: falha prevista (PFA) • el: log de eventos 75% cheio • ne: mudança de rede
-sysen	Enviar alertas de evento de rotina	habilitado, desabilitado

Sintaxe:

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

Exemplo:

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

system> alertentries -1
```

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

Comando batch

Use esse comando batch para executar um ou mais comandos CLI que estão contidos em um arquivo.

- 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.

A tabela a seguir mostra os argumentos das opções.

Tabela 61. Comando batch

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
-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

Sintaxe:

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

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 clearcfg

Use esse comando para definir a configuração do IMM para seus padrões de fábrica.

Você deve ter pelo menos autoridade de Configuração de Adaptador Avançada para emitir esse comando. Depois que a configuração do IMM é apagada, o IMM é reiniciado.

Comando clock

Use esse comando para exibir a data e hora atuais. Você pode definir as configurações de deslocamento UTC e horário de verão

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.

Para um deslocamento UTC de +2, -7, -6, -5, -4 e -3, configurações especiais de horário de verão são necessárias.

- 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).
- Para -7, as configurações de horário de verão são as seguintes: off, mtn (Montanhas), maz (Mazatlan).
- Para -6, as configurações de horário de verão são as seguintes: off, mex (México), cna (América do Norte Central).
- Para -5, as configurações de horário de verão são as seguintes: off, cub (Cuba), ena (Zona Oriental da América do Norte).
- Para -4, as configurações de horário de verão são as seguintes: off, asu (Assunção), cui (Cuiabá), san (Santiago), cat (Canadá - Atlântico).
- Para -3, as configurações de horário de verão são as seguintes: off, gtb (Godthab), bre (Brasil - Leste).

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

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

Comando identify

Use esse comando para acender ou apagar, ou fazer piscar, o LED de identificação do chassi.

A opção **-d** poderá ser usada com a opção **-s on** para ligar o LED apenas durante o número de segundos especificado com a opção **-d**. O LED é desligado após ter decorrido o número de segundos.

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

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

```
system>
```

Comando info

Use esse comando para exibir e configurar informações sobre o IMM.

A execução do comando **info** sem opções exibe todas as informações de localização e contato do IMM. A tabela a seguir mostra os argumentos das opções.

Tabela 62. Comando info

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
-name	Nome do IMM	Sequência
-contact	Nome da pessoa de contato do IMM	Sequência
-location	Local do IMM	Sequência
-room[1]	Identificador de sala do IMM	Sequência
-rack[1]	Identificador de rack do IMM	Sequência
-rup[1]	Posição do IMM no rack	Sequência
-ruh	Altura da unidade do rack	Somente Leitura
-bbay	Local do compartimento Blade	Somente Leitura

1. O valor é somente leitura e não poderá ser redefinido se o IMM residir em um Flex System.

Sintaxe:

```
info [options]
option:
  -name xcc_name
  -contact contact_name
  -location xcc_location
  -room room_id
  -rack rack_id
  -rup rack_unit_position
  -ruh rack_unit_height
  -bbay blade_bay
```

Comando spreset

Use esse comando para reiniciar o IMM.

Você deve ter pelo menos autoridade de Configuração de Adaptador Avançada para emitir esse comando.

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.

A tabela a seguir mostra os argumentos das opções.

Tabela 63. Comando storage

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
-list	Lista os destinos de armazenamento gerenciados pelo IMM.	**controllers|pools|volumes|drives** Em que **target** é: • **controllers**: lista os controladores RAID suportados [1] • **pools**: lista os conjuntos de armazenamentos associados ao controlador RAID [1] • **volumes**: lista os volumes de armazenamento associados ao controlador RAID [1] • **drives**: lista as unidades de armazenamento associadas ao controlador RAID [1]
-list -target **target_id**	Lista os **destinos** de armazenamento gerenciados pelo IMM de acordo com o **target_id**.	**pools|volumes|drives ctrl[x]|pool[x]** Em que **target** e **target_id** são: • **pools ctrl[x]**: lista os conjuntos de armazenamentos associados ao controlador RAID, com base no target_id [1] • **volumes ctrl[x]|pool[x]**: lista os volumes de armazenamento associados ao controlador RAID, com base no target_id [1] • **drives ctrl[x]|pool[x]**: lista as unidades de armazenamento associadas ao controlador RAID, com base no target_id [1]
-list flashdimms	Lista os DIMMs Flash gerenciados pelo IMM.	
-list devices	Exibe o status de todos os discos e DIMMs Flash gerenciados pelo IMM.	
-show **target_id**	Exibe informações para o destino selecionado que é gerenciado pelo IMM.	Em que **target_id** é: **ctrl[x]|vol[x]|disk[x]|pool[x]** **|flashdimm[x]** [3]
-show **target_id** info	Exibe informações detalhadas para o destino selecionado que é gerenciado pelo IMM.	Em que **target_id** é: **ctrl[x]|vol[x]|disk[x]|pool[x]** **|flashdimm[x]** [3]
-show **target_id firmware**[3]	Exibe as informações de firmware para o destino selecionado que é gerenciado pelo IMM.	Em que **target_id** é: **ctrl[x]|disk[x]|flashdimm[x]**[2]

Tabela 63. Comando storage (continuação)

Opção	Descrição	Valores
-showlog **target_id<m:n|all>**[3]	Exibe os logs de eventos do destino selecionado que é gerenciado pelo IMM.	Em que **target_id** é: **ctrl[x]**[4] **m:n**|**all** Em que **m:n** é um para o número máximo de logs de eventos Em que **all** são todos os logs de eventos
-config ctrl -scanforgn -target **target_id**[3]	Detecta a configuração externa de RAID.	Em que **target_id** é: **ctrl[x]**[5]
-config ctrl -imptforgn -target **target_id**[3]	Importa a configuração externa de RAID.	Em que **target_id** é: **ctrl[x]**[5]
-config ctrl -clrforgn -target **target_id**[3]	Limpa a configuração externa de RAID.	Em que **target_id** é: **ctrl[x]**[5]
-config ctrl -clrcfg -target **target_id**[3]	Limpa a configuração de RAID.	Em que **target_id** é: **ctrl[x]**[5]
-config drv -mkoffline -target **target_id**[3]	Altera o estado da unidade de online para offline.	Em que **target_id** é: **disk[x]**[5]
-config drv -mkonline -target **target_id**[3]	Altera o estado da unidade de offline para online.	Em que **target_id** é: **disk[x]**[5]
-config drv -mkmissing -target **target_id**[3]	Marca a unidade offline como uma unidade válida não configurada.	Em que **target_id** é: **disk[x]**[5]
-config drv -prprm -target **target_id**[3]	Prepara uma unidade válida não configurada para remoção.	Em que **target_id** é: **disk[x]**[5]
-config drv -undoprprm -target **target_id**[3]	Cancela a preparação de uma unidade válida não configurado para operação de remoção.	Em que **target_id** é: **disk[x]**[5]
-config drv -mkbad -target **target_id**[3]	Altera a unidade válida não configurada para uma unidade inválida não configurada.	Em que **target_id** é: **disk[x]**[5]
-config drv -mkgood -target **target_id**[3]	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 **target_id** é: **disk[x]**[5]
-config drv -addhsp -**[dedicated pools]** -target **target_id**[3]	Designa a unidade selecionada como hot spare a um controlador ou conjuntos de armazenamento existentes.	Em que **target_id** é: **disk[x]**[5]
-config drv -rmhsp -target **target_id**[3]	Remove a host spare.	Em que **target_id** é: **disk[x]**[5]
-config vol -remove -target **target_id**[3]	Remove um volume.	Em que **target_id** é: **vol[x]**[5]

Tabela 63. Comando storage (continuação)

Opção	Descrição	Valores
-config vol -set [-N] [-w] [-r] [-i] [-a] [-d] [-b] -target **target_id**[3]	Modifica as propriedades de um volume.	• [-N **volume_name**] é o nome do volume • [-w **<0|1|2>**] é a política de gravação de cache: – Digite **0** para a política de gravação de cache – Digite **1** para a política de write-back – Digite **2** para a política de gravação com unidade de backup de bateria (BBU) • [-r **<0|1|2>**] é a política de leitura de cache: – Digite **0** para a política Nenhuma leitura antecipada – Digite **1** para a política Leitura antecipada – Digite **2** para a política Leitura antecipada adaptada • [-i **<0|1>**] é a política de E/S de cache: – Digite **0** para a política de E/S direta – Digite **1** para a política de E/S em cache • [-a **<0|2|3>**] é a política de acesso: – Digite **0** para a política Leitura e gravação – Digite **2** para a política Somente leitura – Digite **3** para a política Bloqueada • [-d **<0|1|2>**] é a política de cache de disco: – Digite **0** se a política estiver inalterada – Digite **1** para habilitar a política[6] – Digite **2** para desabilitar a política • [-b **<0|1>**] é a inicialização em segundo plano: – Digite **0** para habilitar a inicialização – Digite **1** para desabilitar a inicialização • **-target_id** é **vol[x]**[5]
-config vol -add<[-R] [-D disk] [-H disk] [-1 hole]> [-N] [-w] [-r][3],[7]	Cria um volume para um novo conjunto de armazenamento quando o destino é um controlador. ou Cria um volume com um conjunto de armazenamento existente quando o destino é um conjunto de armazenamento.	• [-R **<0|1|5|1E|6|10|50|60|00|1ERLQ0|1E0RLQ0>**] Essa opção define o nível de RAID e só é usada com um novo conjunto de armazenamento • [-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 • [-H disk **[id1]:disk[id2]:..**]Essa opção define o grupo de hot spare e é usada apenas com um novo conjunto de armazenamento • [-1 hole] Essa opção define o número de índice do espaço livre para um conjunto de armazenamento existente • [-N **volume_name**] é o nome do volume • [-w **<0|1|2>**] é a política de gravação de cache: – Digite **0** para a política de gravação de cache

Tabela 63. Comando storage (continuação)

Opção	Descrição	Valores
		– Digite **1** para a política de write-back – Digite **2** para a política de gravação com unidade de backup de bateria (BBU) • [-r **<0|1|2>**] é a política de leitura de cache: – Digite **0** para a política Nenhuma leitura antecipada – Digite **1** para a política Leitura antecipada – Digite **2** para a política Leitura antecipada adaptada
-config vol -add[-i] [-a] [-d] [-f] [-S] [-P] -target **target_id**[3]	Cria um volume para um novo conjunto de armazenamento quando o destino é um controlador. ou Cria um volume com um conjunto de armazenamento existente quando o destino é um conjunto de armazenamento.	• [-i **<0|1>**] é a política de E/S de cache: – Digite **0** para a política de E/S direta – Digite **1** para a política de E/S em cache • [-a **<0|2|3>**] é a política de acesso: – Digite **0** para a política Leitura e gravação – Digite **2** para a política Somente leitura – Digite **3** para a política Bloqueada • [-d **<0|1|2>**] é a política de cache de disco: – Digite **0** se a política permanecer inalterada – Digite **1** para habilitar a política[6] – Digite **2** para desabilitar a política • [-f **<0/1/2>**] é o tipo de inicialização: – Digite **0** para nenhuma inicialização – Digite **1** para inicialização rápida – Digite **2** para inicialização completa • [-S **volume_size**] é o tamanho do novo volume em MB • [-P **strip_size**] é o tamanho da faixa de volume, por exemplo, 128K ou 1M • -target **target_id** é: – **ctrl[x]** (novo conjunto de armazenamentos)[5] – **pool[x]** (conjunto de armazenamento existente)[5]

Tabela 63. Comando storage (continuação)

Opção	Descrição	Valores
-config vol -getfreecap [-R] [-D disk] [-H disk] -target **target_id**[3]	Obtém a quantidade livre de capacidade do grupo de unidades.	• [-R **<0|1|5|1E|6|10|50|60|00|1ERLQ0|1E0RLQ0>**] Essa opção define o nível de RAID e só é usada com um novo conjunto de armazenamento • [-D disk **[id11]:[id12]:..[id21]:[id22]:..**] Essa opção define o grupo da unidade (incluindo distribuições) e é usada apenas com um novo conjunto de armazenamento • [-H disk **[id1]:[id2]:..**]Essa opção define o grupo de hot spare e é usada apenas com um novo conjunto de armazenamento • -target **target_id** é: – **ctrl[x]**[5]
-help	Exibir o uso e as opções do comando	

Notas:
1. Esse comando é suportado apenas em servidores nos quais o IMM pode acessar o controlador RAID.
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.
3. As informações são exibidas em várias linhas devido a limitações de espaço.
4. Esse comando é suportado somente em servidores que oferecem suporte a logs RAID.
5. Esse comando é suportado somente em servidores que oferecem suporte a configurações RAID.
6. O valor **Enable** não oferece suporte a configurações de nível RAID 1.
7. Uma lista parcial de opções disponíveis é fornecida aqui. As outras opções para o comando **storage -config vol -add** são listadas na linha a seguir.

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

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 flashdimms
flashdimm[1]    Flash DIMM 1
flashdimm[4]    Flash DIMM 4
flashdimm[9]    Flash DIMM 9
system>
system> storage
-list pools
pool[0-0]    Storage Pool 0
pool[0-1]    Storage Pool 1
system>
system> storage
-list volumes
system>storage -list volumes
vol[0-0]    Volume 0
vol[0-1]    Volume 1
Vol[0-2]    Volume 2
system>
system> storage
-list drives -target ctrl[0]
disk[0-0]    Drive 0
disk[0-1]    Drive 1
disk[0-2]    Drive 2
system>
system> storage
-list drives -target pool[0-0]
disk[0-0]    Drive 0
disk[0-1]    Drive 1
system>
system> storage
-list pools -target ctrl[0]
pool[0-0]    Storage Pool 0
system>
system> storage
-list volumes -target ctrl[0]
vol[0-0]    Volume 0
vol[0-1]    Volume 1
system>
system> storage
-list volumes -target pool[0-0]
vol[0-0]    Volume 0
vol[0-1]    Volume 1
system>
system> storage
-show ctrl[0] firmware
```

```
Total Firmware number: 2
Name: RAID Firmware1
Description: RAID Firmware
Manfacture: IBM
Version: 4.01(3)T
Release Date: 01/05/2013
Name: RAID Firmware2
Description: RAID Firmware
system>
system> storage
-show ctrl[0] info
Product Name: ServerRAID M5110e
Firmware Package Version: 23.7.0.1.2
Battery Backup: Installed
Manufacture: IBM
UUID: 1234567890123456
Model Type / Model: 1234AHH
Serial No.: 1234567890
FRU No.: 5005076049CC4
Part No.: LSI2004
Cache Model Status: Unknown
Cache Model Memory Size: 300MB
Cache Model Serial No.: PBKUD0XTA0P04Y
PCI Slot Number: 0
PCI Bus Number: 2
PCI Device Number: 2
PCI Function Number: 10
PCI Device ID: 0x1000
PCI Subsystem Device ID: 0x1413
Ports: 2
Port 1: 12345678901234
Port 2: 12345678901235
Storage Pools: 2
Storage Pool 0
Storage Pool 1
Drives: 3
disk[0-0]    Drive 0
disk[0-1]    Drive 1
disk[0-2]    Drive 2
system>
system> storage
-show disk[0-0] firmware
Total Firmware number: 1
Name: Drive
Description:
Manufacture:
Version: BE24
Release Date:
system>
system> storage
-show disk[0-0] info
Product Name: ST98394893
State: Online
Slot No.: 0
Disk Type: SATA
Media Type: HHD
Health Status: Normal
Capacity: 100.000GB
Speed: 6.0Gb/s
Current Temperature: 33C
Manufacture: ATA
```

```
Device ID: 5
Enclusure ID: 0x00FC
Machine Type:
Model:
Serial No.: 9XKJKL
FRU No.:
Part No.:
system>
system> storage
-show flashdimm[15]
Name: CPU1 DIMM 15
Health Status: Normal
Operational Status: Online
Capacity(GB): 400GB
Model Type: DDR3
Part Number: 93E40400GGM101PAT
FRU S/N: 44000000
Manuf ID: Diablo Technologies
Temperature: 0C
Warranty Writes: 100%
Write Endurance: 100%
F/W Level: A201.0.0.49152
system>
system> storage
-show pool[0-0]
RAID State: RAID 0
RAID Capacity: 67.000GB (0.000GB free)
Drives: 2
disk[0-0]    Drive 0
disk[0-1]    Drive 1
Volumes: 2
vol[0-0]    Volume 0
vol[0-1]    Volume 1
system>
system> storage
-show pool[0-1] info
RAID State: RAID 1
RAID Capacity: 231.898GB (200.000GB free)
Holes: 2
#1 Free Capacity: 100.000GB
#2 Free Capacity: 100.000GB

Drives: 2
disk[0-1]    Drive 1
disk[0-2]    Drive 2

Volume: 1
vol[0-1]    LD_volume
system>
system> storage
-show vol[0-0]
Name: Volume 0
Stripe Size: 64KB
Status: Offline
Capacity: 100.000GB
system>
system> storage
-show vol[0-0] info
Name: LD_volume
Status: Optimal
Stripe Size: 64KB
```

```
Bootable: Not Bootable
Capacity: 231.898GB
Read Policy: No Read Ahead
Write Policy: Write Through
I/O Policy: Direct I/O
Access Policy: Read Write
Disk Cache Policy: Unchanged
Background Initialization: Enable
system>
```

Comando adapter

Esse comando é usado para exibir informações sobre o inventário do adaptador PCIe.

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.`
Se remover, substituir ou configurar qualquer adaptador, você deverá reiniciar o servidor (pelo menos uma vez) para visualizar as informações atualizadas do adaptador.

A tabela a seguir mostra os argumentos das opções.

Tabela 64. Comando adapter

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
-list	Listar todos os adaptadores PCIe no servidor	
-show **target_id**	Mostrar as informações detalhadas para o adaptador PCIe de destino	**target_id [info|firmware|ports|chips]** Onde: • **info**: exibe as informações de hardware para o adaptador • **firmware**: exibe todas as informações de firmware para o adaptador • **ports**: exibe todas as informações da porta Ethernet para o adaptador • **chips**: exibe todas as informações de chip GPU para o adaptador
-h	Exibir o uso e as opções do comando	

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

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> adapter
show ob-1 info
Product Name: Flex System CN4054 10Gbps Virtual Fabric Adapter
Card Interface: PCIe x 16
Function Count: 2

Function Name: xxx Emulx xx component1
Segment Number: 2348
Bus Number: 23949
Device Number: 1334
Function Number: 21
Vendor Id: 12
Device Id: 33
Revision Id: 1
Class Code: 2
Sub Vendor: 334
Sub Device: 223
Slot Description: a slot
Slot Type: 23
Slot Data Bus Width: 0
Hot Plug: 12
PCI Type: 11
Blade Slot Port: xxx
UUID: 39302938485
Manufacturer: IBM
Serial Number: 998AAGG
Part Number: ADB233
Model: 345
Function Sku: 221
Fod Uid: 2355
Required Daughter: 0
Max Data Width: 0
Connector Layout: pci x

Package Type: dici
Function Name: xxx nVidia xx component2
Segment Number: 2348
Bus Number: 23949
Device Number: 1334
Function Number: 21
Vendor Id: 12
Device Id: 33
Revision Id: 1
Class Code: 2
Sub Vendor: 334
Sub Device: 223
Slot Description: a slot
Slot Type: 23
Slot Data Bus Width: 0
Hot Plug: 12
PCI Type: 11
Blade Slot Port: xxx
UUID: 39302938485
Manufacturer: IBM
Serial Number: 998AAGG
Part Number: ADB233
Model: 345
Function Sku: 221
Fod Uid: 2355
Required Daughter: 0
```

```
Max Data Width: 0
Connector Layout: pci x
Package Type: dici
```

Comando m2raid

Use este comando para obter informações de inventário relacionadas a M.2 e gerenciar os volumes virtuais.

A tabela a seguir mostra os argumentos das opções.

Tabela 65. Comando m2raid

A tabela a seguir é uma tabela de duas colunas e várias linhas que consiste em opções e descrições de opção.

Opção	Descrição
-h/?	Imprimir as informações de ajuda para este comando
-version	Exibir informações de firmware do controlador
-disks	Exibir as informações dos discos de mídia
-volumes	Exibir informações de volumes virtuais
-create	Criar um volume virtual, o VD_Name, o RaidLevel e o StripeSize podem ser especificados
-delete	Excluir um volume virtual
-import	Importe um volume virtual externo. Depois de importar o volume virtual, uma reinicialização do sistema recriará o volume virtual automaticamente.

Uso

```
m2raid [-options] - raid configuration for M.2 adapter with Mirroring Enablem
options:
   -version                    - displays controller firmware version.
   -disks                      - displays information of media disks.
   -volumes                    - displays information of virtual volumes
   -create -VD_Name <nameStr> -RaidLevel <0|1> -StripeSize <32|64>  - create virt
   -delete -VD_ID <0|1>        - delete the virtual volume
   -import -VD_ID <0|1>        - import a foreign virtual volume
```

Exemplo

```
system> m2raid -version
    ThinkSystem M.2 with Mirroring Enablement Kit
 Firmware Version = 2.3.10.1193

system> m2raid -disks
    M.2 Bay0          32GB M.2 SATA SSD     LEN      100%
M.2 Bay1          32GB M.2 SATA SSD     LEN      100%

system> m2raid -volumes
    VD_ID    VD_Name    RaidLevel    StripSize    VD Capacity    Status
     0       M2RAID       1             64k           29 GB           Optimal

system> m2raid -delete -VD_ID 0
VD_ID 0 is deleted

system> m2raid -create -VD_Name M2RAID -RaidLevel 1 -StripeSize 64
New volume is created
```

```
system> m2raid -import -VD_ID 0
VD_ID 0 is imported
```

Comandos de suporte

Este tópico fornece uma lista alfabética de comandos de suporte.

Existe apenas um comando de suporte: o "Comando dbgshimm" na página 181.

Comando dbgshimm

Use esse comando para desbloquear o acesso à rede ao shell de depuração seguro.

Nota: Este comando destina-se apenas para uso pela equipe de suporte.

A tabela a seguir mostra os argumentos das opções.

Tabela 66. Comando dbgshimm

A tabela a seguir é uma tabela de duas colunas e várias linhas que consiste em opções e descrições de opção.

Opção	Descrição
status	Exibir status
ativar	Habilitar acesso de depuração (padrão se nenhuma opção for especificada)
desativar	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 PASSW0RD (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/PASSW0RD 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 183.

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 183.

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.

© Copyright Lenovo 2017, 2022

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	dados 1 [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 Nº1, ID do pacote = 03h (eth2),
- placa opcional Nº2, 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
Parâmetro OEM Esse número de parâmetro é usado pelo XCC para indicar qual das possíveis portas Ethernet (pacotes lógicos) deve ser usada. 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. Os dados de resposta retornarão 3 bytes ou, opcionalmente, 4 bytes se o dispositivo estiver em um pacote NCSI. 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	C0h	data1 00h = eth0 01h = eth1 02h = eth2 etc… FFh = desabilitar todas as portas de rede externas O XCC oferece suporte a um segundo byte de dados opcional para especificar qual canal em um pacote é usado data2 00h = canal 0 01h = canal 1 etc… Se data2 não for especificado na solicitação, o canal 0 será assumido

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
Parâmetro OEM (Esse número de parâmetro é usado pelo XCC para habilitar ou desabilitar a interface Ethernet sobre USB.) 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 (desabilitado) ou 01h (habilitado)	C1h	dados 1 0x00 = desabilitado 0x01 = habilitado

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
Parâmetro OEM (Esse número de parâmetro é usado pelo XCC para habilitar ou desabilitar a interface Ethernet sobre USB.) 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 de parâmetro (como na especificação de IPMI) Byte 3 = tamanho dos seguintes bytes de dados (16 bytes atualmente) Byte 4-n DUID_LLT	C2h	

Parâmetros de configuração Ethernet

Os parâmetros a seguir podem ser usados para definir configurações Ethernet específicas.

Parâmetro	#	Dados de parâmetro
Parâmetro OEM (Esse número de parâmetro é usado pelo XCC para habilitar ou desabilitar a configuração de negociação automática para a interface Ethernet.) Os dados de resposta retornarão 3 bytes: Byte 1 = código de conclusão Byte 2 = revisão Byte 3 = 00h (desabilitado) ou 01h (habilitado)	C3h	dados 1 0x00 = desabilitado 0x01 = habilitado Nota: nos sistemas Flex e ThinkSystem D2 Enclosure (ThinkSystem SD530 Compute Node), a configuração de negociação automática não é alterável porque poderia interromper o caminho de comunicação da rede pelo CMM e SMM.
Parâmetro OEM (Esse número de parâmetro é usado pelo XCC para obter ou definir a taxa de dados da interface Ethernet.) Os dados de resposta retornarão 3 bytes: Byte 1 = código de conclusão Byte 2 = revisão Byte 3 = 00h (10 Mb) ou 01h (100 Mb)	C4h	dados 1 0x00 = 10 Mbit 0x01 = 100 Mbit
Parâmetro OEM (Esse número de parâmetro é usado pelo XCC para obter ou definir a configuração Duplex da interface Ethernet.) Os dados de resposta retornarão 3 bytes: Byte 1 = código de conclusão Byte 2 = revisão Byte 3 = 00h (Half Duplex) ou 01h (Full Duplex)	C5h	dados 1 0x00 = Half Duplex 0x01 = Full Duplex

Parâmetro	#	Dados de parâmetro
Parâmetro OEM (Esse número de parâmetro é usado pelo XCC para obter ou definir a Unidade de Transmissão Máxima (MTU) da interface Ethernet.) Os dados de resposta retornarão 3 bytes: Byte 1 = código de conclusão Byte 2 = revisão Byte 3-4 = tamanho da MTU	C6h	dados 1 Tamanho da MTU
Parâmetro OEM (Esse número de parâmetro é usado pelo XCC para obter ou definir o endereço MAC administrado localmente.) Os dados de resposta retornarão 3 bytes: Byte 1 = código de conclusão Byte 2 = revisão Byte 3 – 8 = Endereço MAC	C7h	dados 1 - 6 Endereço MAC

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
Parâmetro OEM Esse parâmetro é usado para obter o endereço de link local do 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 = Comprimento do prefixo de endereço IPV6 Byte 4-19 Endereço do link local em formato binário	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	dados 1 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
Parâmetro OEM 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. Os dados Obter resposta retornarão o seguinte: Byte 1 = código de conclusão Byte 2 = revisão Byte 3 = reservado (00h) Bytes 4:5 = Número da porta Ethernet sobre USB (LSByte primeiro) Bytes 6:7 = Número da porta Ethernet externa (LSByte primeiro) O número de bytes a seguir pode variar (1, 4 ou 16 bytes) dependendo do modo de endereçamento: • Byte 8 = modos predefinidos: 00h = a passagem está desabilitada 01h = o endereço IP do CMM é usado Bytes 8:11 = endereço IP de rede externa IPv4 em formato binário Bytes 8:23 = endereço IP de rede externa IPv6 em formato binário Códigos de conclusão: 00h – sucesso 80h – parâmetro não suportado C1h – comando não suportado C7h – comprimento dos dados da solicitação inválido	CAh	Definir parâmetros de configuração LAN: dados 1 reservado (= 00h) dados 2:3 Número da porta Ethernet sobre USB, LSByte primeiro dados 4:5 Número da porta Ethernet externa, LSByte primeiro O número de bytes a seguir pode variar (1, 4 ou 16 bytes) dependendo do modo de endereçamento: dados 6 00h = desabilitar a passagem 01h = usar o endereço IP do CMM dados 6:9 Endereço IP de rede externa IPv4 em formato binário dados 6:21 Endereço IP de rede externa IPv6 em formato binário
Parâmetro OEM Esse parâmetro é usado para definir e obter o endereço IP de LAN sobre USB e a máscara de rede do XCC: Os dados de resposta retornarão o seguinte: Byte 1 = código de conclusão	CBh	Dados 1:4 Endereço IP da interface LAN sobre USB do lado do XCC. Dados 5:8 Máscara de rede da interface LAN sobre USB do lado do XCC

Parâmetro	#	Dados de parâmetro
Byte 2 = Revisão de parâmetro (como na especificação de IPMI) Byte 3:10 = Valor do endereço IP e da máscara de rede (MS-byte) primeiro		
Parâmetro OEM Esse parâmetro é usado para definir e obter o endereço IP de LAN sobre USB do SO do host: Os dados de resposta retornarão o seguinte: Byte 1 = código de conclusão Byte 2 = Revisão de parâmetro (como na especificação de IPMI) Byte 3:6 = Endereço IP (MS-byte) primeiro	CCh	Dados 1:4 Endereço IP da interface LAN sobre USB do lado do host.

Consultar inventário do pacote lógico

O parâmetro a seguir é usado para consultar o inventário do pacote NCSI.

Parâmetro	#	Dados de parâmetro
Parâmetro OEM 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. Consultar operação de inventário do pacote 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. Consultar inventário do pacote: --> 0x0C 0x02 0x00 0xD3 0x00 0x00 A resposta do XCC inclui um byte de informações para cada pacote presente: bits 7:4 = número de canais NCSI no pacote bits 3:0 = o número do pacote lógico Resposta --> 0x00 0x00 0x40 0x01 0x32 indica que há 3 pacotes lógicos presentes: o pacote 0 tem 4 canais NCSI o pacote 1 não é um NCSI NIC e, portanto, não é compatível a canais NCSI o pacote 2 tem 3 canais NCSI	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
Parâmetro OEM 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. O comando é compatível com 2 operações: • Ler prioridade do pacote • Definir prioridade do pacote Ler operação de prioridade do pacote 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. Ler prioridade do pacote: --> 0x0C 0x02 0x01 0xD4 0x00 0x00 Resposta --> 0x00 0x00 0x00 0x12 0x23 pacote lógico 0 = prioridade 0 pacote lógico 2 = prioridade 1 pacote lógico 3 = prioridade 2 Definir operação de prioridade do pacote A operação para definir a prioridade do pacote é executada emitindo a solicitação com um ou mais parâmetros além do número do parâmetro D4h. Definir prioridade do pacote: --> 0x0C 0x01 0x01 0xD4 0x00 0x12 0x23 definir pacote lógico 0 = prioridade 0 definir pacote lógico 2 = prioridade 1	D4	Obter/definir parâmetros de configuração LAN: Bit [7-4] = prioridade do pacote lógico (1 = maior, 15 = menor) Bit [3-0] = número do pacote lógico

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	dados 1 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
Parâmetro OEM Esse parâmetro é usado para obter/definir o modo de rede da NIC de gerenciamento do XCC. Os dados de resposta retornarão 4 bytes: Byte 1 = código de conclusão Byte 2 = revisão Byte 3 = aplicado/modo de rede especificado Byte 4 = ID do pacote do modo de rede aplicado Byte 5 = ID do canal do modo de rede aplicado	D6h	Definir parâmetros de configuração LAN: dados 1 Modo de rede a ser definido Obter parâmetros de configuração LAN: dados 1 Para obter o modo de rede, estes são dados opcionais, padrões para consultar o modo de rede atual

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

Código	Comandos Netfn 0x3A	Privilégio
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.

Função líquida = 0x2E			
Código	**Comando**	**Solicitação, Dados de resposta**	**Descrição**
0xCC	Redefinir XCC como padrão	**Solicitação:** Byte 1 – 0x5EByte 2 – 0x2B Byte 3 – 0x00 Byte 4 – 0x0AByte 5 – 0x01 Byte 6 – 0xFF Byte 7 – 0x00Byte 8 – 0x00 Byte 9 – 0x00 **Resposta:** Byte 1 – Conclusão de CodeByte 2 – 0x5EByte 3 – 0x2B Byte 4 – 0x00 Byte 5 – 0x0AByte 6 – 0x01 Byte 7 – Dados de resposta 0 = Sucesso diferente de zero = Falha	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	**Solicitação**: Nenhum dado sobre a solicitação **Resposta**: Byte 1 – Código de conclusão Byte 2 - Versão principal Byte 3 - Versão secundária	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. (Revisão, Principal, Secundária)
0x0D	Consultar informações da placa	**Solicitação**: N/A **Resposta**: Byte 1 – ID do sistema Byte 2 – Revisão da placa	Esse comando retorna a revisão do planar e ID da placa.
0x50	Consultar informações de construção	**Solicitação**: N/A **Resposta**: Byte 1 – Código de conclusão. Bytes 2:10 – Nome da construção ASCIIZ Bytes 11:23 – Data de construção ASCIIZ Bytes 24:31 – Tempo de construção ASCII	Esse comando retorna o nome, a data e o tempo de construção. As sequências de nome e data de construção têm uma finalização zero. O formato da data de construção é AAAA-MM-DD. por exemplo, "ZUBT99A" “2005-03-07” “23:59:59”

Função líquida = 0x3A			
Código	**Comando**	**Solicitação, Dados de resposta**	**Descrição**
0x6B	Consultar nível de revisão de firmware FPGA	**Solicitação**: Byte 1 – Tipo de dispositivo FPGA* Tipo de dispositivo FPGA 0 = Local (nível ativo) 1 = Placa de CPU 1 (nível ativo) 2 = Placa de CPU 2 (nível ativo) 3 = Placa de CPU 3 (nível ativo) 4 = Placa de CPU 4 (nível ativo) 5 = ROM primário local 6 = ROM de recuperação local **Resposta**: Byte 1 – Código de conclusão Byte 2 – Nível de revisão principal Byte 3 – Nível de revisão menor Byte 4 – Nível de revisão subinferior (Byte de teste em plataformas do XCC)	Esse comando retorna o nível de revisão do firmware FPGA. Se o Byte 1 for omitido, o local (nível ativo) será selecionado
0x6C	Consultar nível de revisão de hardware de placa	**Solicitação**: Sem dados. **Resposta**: Byte 1 – Código de conclusão Byte 2 – Nível de revisão	Esse comando retorna o nível de revisão do hardware da placa onde o FPGA reside.
0x6D	Consultar nível de revisão de firmware PSoC	**Solicitação**: Nenhum(a) **Resposta**: Byte 1 – Código de conclusão Byte 2 – bin# Byte 3 – APID Byte 4 – Rev	Esse comando retorna o nível de revisão de todos os dispositivos PSoC detectados. Nota: bin# representa um local físico. Consulte as especificações do sistema para obter detalhes.

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.

<table>
<tr><th colspan="4">Função líquida = 0x2E</th></tr>
<tr><th>Código</th><th>Comando</th><th>Solicitação, Dados de resposta</th><th>Descrição</th></tr>
<tr><td>0x1E</td><td>Opções de atraso de restauração de energia do chassi</td><td>Solicitação:<table><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>Resposta:

Byte 1 – Código de conclusão

Byte 2 – Opções de atraso (somente para solicitação de consulta)</td><td>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.

O comando é aceito pelo XCC apenas em servidores de rack.</td></tr>
<tr><td>0x38</td><td>NMI e redefinição</td><td>Solicitação:

Byte 1 – Número de segundos
0 = Apenas NMI

Byte 2 – Tipo de redefinição
0 = redefinição flexível
1 = ciclo de ativação

Resposta:

Byte 1 – Código de conclusão</td><td>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.

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.

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.</td></tr>
</table>

Comandos diversos

Esta seção destina-se a comandos que não se encaixam em outra seção.

<table>
<tr><th colspan="4">Função líquida = 0x3A</th></tr>
<tr><th>Código</th><th>Comando</th><th>Solicitação, Dados de resposta</th><th>Descrição</th></tr>
<tr><td>0x55</td><td>Obter/definir nome do host</td><td>Tamanho da solicitação = 0:

Dados da solicitação vazios

Resposta:

<table><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 nula.</td></tr></table>
Tamanho da solicitação 1-64:

<table><tr><td>Bytes 1-64</td><td>Nome do host do DHCP

ASCIIZ terminado com 00h</td></tr></table></td><td>Use este comando para Obter/definir nome do host.

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 nulo.</td></tr>
<tr><td>0x98</td><td>Controle de porta USB FP</td><td>Solicitação:

Byte 1

<table><tr><td>01h:</td><td>Obter o proprietário atual da porta USB do painel frontal</td></tr></table>
Resposta:

Byte 1 – Código de conclusão

Byte 2

<table><tr><td>00h:</td><td>Pertencente ao host</td></tr><tr><td>01h:</td><td>Pertencente ao BMC</td></tr></table>
Solicitação:

Byte 1

<table><tr><td>02h:</td><td>Obter a configuração da porta USB</td></tr></table></td><td>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.

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.

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.

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.

Se o servidor tiver o botão de identificação, os usuários poderão</td></tr>
</table>

<table>
<tr><th colspan="4">Função líquida = 0x3A</th></tr>
<tr><th>Código</th><th>Comando</th><th>Solicitação, Dados de resposta</th><th>Descrição</th></tr>
<tr><td></td><td></td><td>
<table>
<tr><td></td><td>do painel frontal</td></tr>
</table>
Resposta:
Byte 1 – Código de conclusão
Byte 2
<table>
<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>
Byte 3:4 – Tempo limite de inatividade em minutos (MSB primeiro)
Byte 5 – Habilitar botão de ID
<table>
<tr><td>00h:</td><td>Desabilitado</td></tr>
<tr><td>01h:</td><td>Habilitado</td></tr>
</table>
Byte 6 – Histerese (opcional) em segundos
Solicitação:
Byte 1
03h: definir a configuração da porta USB do painel frontal
Byte 2
<table>
<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>
Byte 3:4 – Tempo limite de inatividade em minutos (MSB primeiro)
Byte 5 – Habilitar botão de ID
<table>
<tr><td>00h:</td><td>Desabilitado</td></tr>
</table>
</td><td>
habilitar/desabilitar o botão de ID para alternar o proprietário da porta USB FP segurando o botão de ID por mais de três segundos.
Histerese em segundos serão configuradas quando a porta for alternada automaticamente durante o ciclo de ativação. Este é um parâmetro opcional.
Servidores SD530
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.

Quando o comando é emitido com byte 1 = 1, o XCC sempre responderá que a porta pertence ao BMC.
Quando o comando é emitido com byte 1 = 2, o XCC sempre responderá que a porta é dedicada ao BMC.
Quando o comando é emitido com byte 1 = 3 ou byte 1 = 4, o XCC responderá com o código de conclusão D6h.

Servidores não SD530
Na plataforma não SD530, o uso do XCC da porta USB do painel frontal pode ser desabilitado alternando para o modo "Apenas host".
Quando o comando é emitido com byte 1 = 5 ou byte 1 = 6, o XCC responderá com o código de conclusão D6h.
</td></tr>
</table>

<table>
<tr><th colspan="4">Função líquida = 0x3A</th></tr>
<tr><th>Código</th><th>Comando</th><th>Solicitação, Dados de resposta</th><th>Descrição</th></tr>
<tr><td></td><td></td><td>
<table>
<tr><td>01h:</td><td>Habilitado</td></tr>
</table>
Byte 6 – Histerese (opcional) em segundos
Resposta:
Byte 1 - Código de conclusão de Byte 2
<table>
<tr><td>00h:</td><td>Alternar para host</td></tr>
<tr><td>01h:</td><td>Alternar para BMC</td></tr>
</table>
Resposta:
Byte 1 – Código de conclusão
Byte 1
<table>
<tr><td>05h:</td><td>Habilitar/ desabilitar a porta USB do painel frontal</td></tr>
</table>
Byte 2
<table>
<tr><td>00h:</td><td>Desabilitar</td></tr>
<tr><td>01h:</td><td>Habilitar</td></tr>
</table>
Resposta:
Byte 1 – Código de conclusão
Solicitação:
Byte 1
<table>
<tr><td>06h:</td><td>Ler o estado de ativação/ desativação da porta USB do painel frontal</td></tr>
</table>
Resposta:
Byte 1 - Código de conclusão
Byte 2
</td><td></td></tr>
</table>

<table>
<tr><th colspan="4">Função líquida = 0x3A</th></tr>
<tr><th>Código</th><th>Comando</th><th>Solicitação, Dados de resposta</th><th>Descrição</th></tr>
<tr><td>0xC7</td><td>Comutador de IPMI NM nativo</td><td>Tamanho da solicitação = 0:

Dados da solicitação vazios

Resposta:

<table><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>
Tamanho da solicitação= 1:

<table><tr><td>Byte 1</td><td>Atributo de ativação/ desativação da interface NM IPMI nativa

00h – Desabilitar

01h – Habilitar</td></tr></table>
Resposta:

<table><tr><td>Byte 1</td><td>Código de conclusão</td></tr></table></td><td>Esse comando é usado para habilitar/desabilitar a função de ponte do XCC para os comandos IPMI Intel nativos.</td></tr>
</table>

Capítulo 12. Servidores Edge

Este tópico descreve funções específicas dos servidores Edge.

Notas:

1. O sistema requer que você altere a senha XCC ao efetuar login pela primeira vez.
2. O IPMI sobre LAN está desabilitado por padrão.
3. O IPMI sobre KCS está desabilitado por padrão.

Modo de bloqueio do sistema

Quando o **Modo de bloqueio do sistema** está no estado ativo, significa que o sistema está no modo de bloqueio. Você deve ativar o sistema e desbloqueá-lo, caso contrário, o sistema do host não poderá ser inicializado.

Nota: O Modo de bloqueio do sistema está disponível apenas para SE350 com pacote de segurança, mas não o padrão SE350. A versão pode ser verificada na guia **Início** em **Informações e configurações do sistema**.

Clique em **Segurança** em **Configuração do BMC** e role até **Modo de bloqueio do sistema**.

Modo de bloqueio do sistema

Para ativar o sistema e sair do **Modo de bloqueio do sistema**, conclua as etapas a seguir.

1. Clique no botão **Inativo** e a janela **Ativação do Key Vault** será exibida para mostrar o **Texto do desafio**.
2. Entre em contato com o administrador de TI e forneça o **Texto do desafio**.
3. Obtenha a **Resposta do desafio** do seu administrador de TI e a insira na janela **Ativação do Key Vault**..
4. Clique no botão **OK** e depois clique em **Aplicar**.
5. Se todas as configurações funcionarem corretamente, você verá o **Modo de bloqueio do sistema** ser alterado para **Inativo**.

Nota: Quando o Modo de bloqueio do sistema está no estado ativo, qualquer acesso aos segredos do sistema é **negado** como chaves SED.

Para forçar o sistema a entrar no Modo de bloqueio do sistema, conclua as etapas a seguir.

1. Clique no botão **Ativo**.
2. Clique no botão **OK** e depois clique em **Aplicar**.

Detecção de movimento

É possível habilitar essa função para proteger o servidor, detectando qualquer movimentação física do servidor.

Se a Detecção de movimento estiver habilitada, você poderá configurar os itens a seguir dependendo da sua preferência e configuração.

- **Nível de sensibilidade**: selecione o nível de sensibilidade entre **Baixo**, **Médio** e **Alto**, de acordo com sua preferência
- **Orientação**: selecione a configuração entre **Desktop de base**, **Montagem na parede (horizontal)**, **Montagem na parede (vertical)**, **Prateleira** e **Montagem de teto**.

© Copyright Lenovo 2017, 2022

Nota: A Detecção de movimento será desativada automaticamente quando o sistema entrar no modo de bloqueio.

Detecção de intrusão no chassi
É possível habilitar essa função para proteger o servidor, detectando qualquer movimentação física da tampa superior.

Configurações adicionais
Se o Pacote LOM habilitado para sem fio estiver instalado, há três configurações que podem ser escolhidas para um evento de violação detectado.
Sob algumas circunstâncias anormais, o **Texto do desafio** pode falhar na verificação pelo ThinkShield Key Vault Portal, pode ser necessário redefinir o contador interno do dispositivo antes de ativar o dispositivo sob a solicitação do administrador de TI.

Gerenciador da SED AK

Para o sistema instalado com SED (unidade autocriptografada), esse recurso controla o BMC para implantar a chave SED. É possível usar a chave SED para criptografar unidades de inicialização e de dados e inicializar o sistema sem intervenção manual

Nota: Esta operação não é permitida quando o sistema não está ativado (o Modo de bloqueio do sistema está declarado) ou o usuário atual não tem autoridade para gerenciar a chave SED.

Nota: O Modo de bloqueio do sistema está disponível apenas para SE350 com pacote de segurança, mas não o padrão SE350. A versão pode ser verificada na guia **Início** em **Informações e configurações do sistema**.

Nota: O SE350 também oferece suporte a um recurso de backup automático, desde que o Kit de ativação ThinkSystem M.2 ou o Kit de ativação de espelhamento ThinkSystem M.2 esteja íntegro. Se o hardware estiver danificado, mas os Kits SED e M.2 estiverem íntegros, eles poderão ser instalados em outro SE350, e o SED AK poderá ser restaurado. No entanto, para estar preparado para uma falha de hardware completa, a Lenovo recomenda fazer um backup do SED AK.

Clique em **Segurança** em **Configuração do BMC** e role para **Gerenciador da SED AK**.

Alterar a SED AK
Gerar SED AK a partir da senha: defina a senha e a insira novamente para confirmação. Clique em **Gerar novamente** para obter a nova SED AK.
Gerar uma SED AK aleatória: clique em **Gerar novamente** para obter uma SED AK aleatória.
Backup da SED AK: defina a senha e a insira novamente para confirmação. Clique em **Iniciar backup** para fazer backup da SED AK; em seguida, baixe o arquivo da SED AK e guarde-o em segurança para uso futuro.

Nota: Se você usar o arquivo de backup da SED AK para restaurar uma configuração, o sistema solicitará a senha definida aqui.

Recuperar a SED AK: você só pode executar essa tarefa enquanto a SED não estiver funcionando corretamente. Há duas maneiras de recuperar a SED AK:

- **Recuperar a SED AK usando senha**: use a senha definida no modo **Gerar SED AK a partir da senha** para recuperar a SED AK.
- **Recuperar a SED AK a partir do arquivo de backup**: atualize o arquivo de backup gerado no modo **Backup da SED AK** e insira a senha do arquivo de backup correspondente para recuperar a SED AK.

Rede Edge

Essa página de função oferece suporte apenas enquanto o Pacote LOM habilitado para sem fio estiver instalado.

Para obter as tabelas predefinidas da topologia de rede, consulte https://thinksystem.lenovofiles.com/help/topic/SE350/pdf_files.html para obter mais detalhes.

Conectividade Wi-Fi
Clique em **Habilitado** e será possível definir as configurações de acordo com a configuração de Wi-Fi.

Conectividade LTE
Isso permite controlar a conectividade LTE para a placa Edgenetwork.

Endereço da placa de rede Edge

Status **IPv4 ou IPv6**	Status do **Servidor DHCP**	**Método**
Desabilitado	**Desabilitado**	**Obter IP de DHCP**
Habilitado	**Habilitado**	**Usar endereço IP estático**
Habilitado	**Desabilitado**	**Obter IP de DHCP** ou **Usar endereço IP estático** dependendo do uso.

Ponte de rede BMC
É possível acessar o BMC por **Portas de downlink**, **Portas Wi-Fi**, **Portas de uplink** ou **Nenhum**.

Nota: Selecionar **Nenhum** refere-se de que essa função está desabilitada.

Solução de problemas da placa de rede Edge
Reiniciar imediatamente: você pode reiniciar a placa de rede por esse botão.
Redefinir para os padrões de fábrica: você pode redefinir a placa de rede para a configuração padrão por esse botão.

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 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

© Copyright Lenovo 2017, 2022

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/xcc/NN1ia_c_servicesandsupport.html.
  - Para obter mais informações sobre como usar a CLI para coletar dados de serviço, consulte https://pubs.lenovo.com/xcc/nn1ia_r_ffdccommand.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.

- **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.

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/supportphonelist 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

© Copyright Lenovo 2017, 2022

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 67. Limites para substâncias particuladas e gases

Contaminação	Limites
Particulada	• 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[1]. • 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. • A umidade relativa deliquescente da contaminação por substância particulada deve ser superior a 60%[2]. • O ambiente deve estar livre de contaminação condutora, como espanadores de zinco.
Gasosa	• Cobre: Classe G1 conforme ANSI/ISA 71.04-1985[3] • Prata: Taxa de corrosão de menos de 300 Å em 30 dias

[1] ASHRAE 52.2-2008 - **Método de Teste de Dispositivos Gerais de Limpeza de Renovação de Ar para Eficiência de Remoção por Tamanho de Partícula**. Atlanta: American Society of Heating, Refrigerating and Air-Conditioning Engineers, Inc.

[2] 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.

[3] ANSI/ISA-71.04-1985. **Environmental conditions for process measurement and control systems: Airborne contaminants**. Instrument Society of America, Research Triangle Park, Carolina do Norte, EUA.

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^{+6})	多溴聯苯 Polybrominated biphenyls (PBB)	多溴二苯醚 Polybrominated diphenyl ethers (PBDE)
機架	○	○	○	○	○	○
外部蓋板	○	○	○	○	○	○
機械組合件	–	○	○	○	○	○
空氣傳動設備	–	○	○	○	○	○
冷卻組合件	–	○	○	○	○	○
內存模塊	–	○	○	○	○	○
處理器模塊	–	○	○	○	○	○
鍵盤	–	○	○	○	○	○
調製解調器	–	○	○	○	○	○
監視器	–	○	○	○	○	○
滑鼠	–	○	○	○	○	○
電纜組合件	–	○	○	○	○	○
電源	–	○	○	○	○	○
儲備設備	–	○	○	○	○	○
電池匣組合件	–	○	○	○	○	○
有mech的電路卡	–	○	○	○	○	○
無mech的電路卡	–	○	○	○	○	○
雷射器	–	○	○	○	○	○

備考1. 〝超出0.1 wt %〞及〝超出0.01 wt %〞係指限用物質之百分比含量超出百分比含量基準值。

Note1 : “exceeding 0.1wt%” and “exceeding 0.01 wt%” indicate that the percentage content of the restricted substance exceeds the reference percentage value of presence condition.

備考2. 〝○〞係指該項限用物質之百分比含量未超出百分比含量基準值。

Note2 : “○”indicates that the percentage content of the restricted substance does not exceed the percentage of reference value of presence.

備考3. 〝-〞係指該項限用物質為排除項目。

Note3 : The “-“ indicates that the restricted substance corresponds to the exemption.

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 82
a utilização do sistema
  visualizando 52
Acesso a unidades
  gerenciamento de certificado 151
  segurança 151
acesso remoto 2
ajuda 211
armazenamento
  opções de configuração 85
as informações do sistema
  visualizando 50
Assinado por CA
  certificado 42
atributo de permissão de login
  LDAP 130
Atributo de pesquisa de UID
  Servidor LDAP 130
atributo de procura do grupo
  LDAP 130
autenticação de tentativa de login 17
autoassinado
  certificado 42
avisos 215
avisos e instruções 8
avisos importantes 216

B

Baseboard Management Controller (BMC) 1
BIOS (sistema BIOS) 1
BMC
  solicitação de assinatura de certificado 42

C

captura de tela azul 67
captura de tela do sistema operacional 67
certificado do servidor
  gerenciamento 45
Certificado SKLM
  gerenciamento 42
chave de ativação
  exportação 92
  gerenciar 129
  instalar 91, 129
  remover 92, 129
chaves de criptografia
  gerenciamento centralizado 40
Chaves SSH
  usuário 158
CIM sobre HTTPS
  gerenciamento de certificado 147–148
  segurança 147–148
classificações de certificado
  Assinado por CA 42
  autoassinado 42
cliente
  gerenciamento de certificado 42
coletando dados de serviço 80, 212
Comando accseccfg 113
Comando adapter 178
Comando alertcfg 115
Comando alertentries 163
Comando asu 116
Comando backup 119
Comando batch 166
Comando clearcfg 166
Comando clearlog 100
Comando clock 167
Comando console 113
Comando dbgshimm 181
Comando dhcpinfo 120
Comando dns 121
Comando encaps 123
Comando ethtousb 123
Comando exit 99
Comando fans 101
Comando ffdc 101
Comando firewall 124
Comando fuelg 111
Comando gprofile 125
Comando hashpw 126
Comando help 99
Comando history 99
Comando hreport 102
Comando identify 167
Comando ifconfig 126
Comando info 168
Comando keycfg 129
Comando ldap 130
Comando led 104
Comando m2raid 180
Comando mhlog 103
Comando ntp 132
Comando portcfg 133
Comando portcontrol 134
Comando ports 135
Comando power 109
Comando pxeboot 112
Comando rdmount 136
Comando readlog 105
Comando reset 111
Comando restore 137
Comando restoredefaults 138
Comando roles 138
Comando seccfg 140
Comando serial redirect 113
Comando set 140
Comando smtp 140
Comando snmp 141
Comando snmpalerts 143
Comando spreset 168
Comando srcfg 145
Comando sshcfg 146
Comando ssl 147
Comando sslcfg 148
Comando storage 169
  dispositivos de armazenamento 169
Comando storekeycfg 151
Comando syncrep 153
Comando syshealth 106
Comando temps 107
Comando thermal 154
Comando timeouts 154
Comando TLS 155
Comando trespass 156
Comando uefipw 157
Comando usbeth 157
Comando usbfp 157
Comando users 158
Comando volts 107

© Copyright Lenovo 2017, 2022

Comando vpd 108
Comandos da ipmi
consumo de energia 63
comandos de configuração 113
Comandos de controle IMM 162
Comandos de suporte 181
comandos de utilitário 99
Comandos do
accseccfg 113
adaptador 178
ajuda 99
alertcfg 115
alertentries 163
armazenamento 169
asu 116
backup 119
clearcfg 166
clearlog 100
clock 167
configurar 140
console 113
dbgshimm 181
dhcpinfo 120
dns 121
encaps 123
energia 109
ethtousb 123
ffdc 101
firewall 124
fuelg 111
funções 138
gprofile 125
hashpw 126
histórico 99
hreport 102
identificar 167
ifconfig 126
informativo 168
keycfg 129
ldap 130
led 104
Lote 166
m2raid 180
mhlog 103
ntp 132
portas 135
portcfg 133
portcontrol 134
pxeboot 112
rdmount 136
readlog 105
redefinição 111
restore 137
restoredefaults 138
sair 99
seccfg 140
smtp 140
snmp 141
snmpalerts 143
spreset 168
srcfg 145
sshcfg 146
ssl 147
sslcfg 148
storekeycfg 151
syncrep 153
syshealth 106
temps 107
térmica 154
timeouts 154
TLS 155
trespass 156
uefipw 157
usbeth 157
usbfp 157
usuários 158
ventiladores 101
volts 107
vpd 108
comandos do monitor 100
Comandos OEM IPMI 196
Comandos sem agente 168
comandos, lista alfabética 97
comandos, tipos de
configuração 113
Controle IMM 162
energia e reinicialização do servidor 109
monitor 100
Sem agente 168
serial redirect 113
Suporte 181
utilitário 99
Comunidades de SNMPv1
gerenciar 141
conexão de rede 10
endereço IP estático padrão 10
endereço IP estático, padrão 10
Endereço IP, estático padrão 10
Configuração de criptografia
Configuração de criptografia 45
configuração do servidor
propriedade de servidor 80
Configuração do Servidor
Configurar RAID 85
Detalhe de RAID 85
informações do adaptador 59
configuração padrão
IMM 138
configurações
Alerta SNMP 34
avançado 30, 184
DDNS 32
designações de porta 35
DNS 32
Ethernet 30, 184
Ethernet sobre USB 33
LDAP 25
lista de bloqueios e restrição de tempo 36
login global 23
configurações de política de segurança da conta 23
segurança 38
Servidor SSH 39
configurações de rede
Comandos IPMI 34
Configurações de SNMPv3
usuário 158
configurações globais de login
configurações de política de segurança da conta 23
configurando
a data e a hora do XClarity Controller 82
configurações globais de login 23
porta USB do painel frontal para gerenciamento 37
redirecionamento serial para SSH 95
configurando o armazenamento
opções para configurar
o armazenamento 85
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 81
configurar
Configurações de alerta SNMPv3 34
Configurações de Ethernet sobre USB 33
Configurações de LDAP 25
configurações de segurança 38
Configurações do DDNS 32
Configurações do DNS 32

Configurações Ethernet 30, 184
Contas de usuário de SNMPv3 158
Contato de SNMPv1 141
Contato de SNMPv3 141
data 167
DDNS 121
designações de porta 35
DNS 121
Ethernet 126
Ethernet sobre USB 123
evitar o rebaixamento do firmware do sistema 40
Grupo de dispositivos SKLM 41
horário 167
IPMI 34
IPMI sobre acesso via KCS 40
IPv4 126
IPv6 126
LDAP 130
lista de bloqueios e restrição de tempo 36
Método de autenticação do usuário 113
MTU 126
negociação automática 126
níveis de segurança da conta do usuário 113
nome do host do 126
Porta da CLI SSH 135
porta de console remoto 135
porta de serviço de rede 134
Porta de Traps SNMP 135
Porta do agente do SNMP 135
Porta do CIM sobre HTTP 135
Porta do CIM sobre HTTPS 135
Porta do Servidor LDAP 130
Porta HTTP 135
Porta HTTPS 135
porta serial 133
portas 135
protocolos de rede 30
Sequência-chave da CLI 133
Servidor LDAP 130
Servidor SSH 39
Servidores de repositório de chaves do SKLM 41
SMTP 140
SNMPv1 141
tempo limite de inatividade da Web 113
Traps SNMPv1 141
unidade de transmissão máxima 126
USB 123
configurar números de porta 135
Configurar RAID
Configuração do Servidor 85
console remoto
captura de tela 67
comandos de energia e reinicialização 67
controle de mouse absoluto 68
controle de mouse relativo 68
controle de mouse relativo para Linux (aceleração padrão Linux) 68
sessão de mídia virtual 65
suporte de mouse 68
suporte de teclado 68
visualizador de vídeo 65
consumo de energia
Comandos da ipmi 63
conta do usuário
criar 158
excluindo 20
contaminação gasosa 217
contaminação particulada 217
contaminação, particulada e gasosa 217
Contas de usuário de SNMPv3
configurar 158
Contato de SNMPv1
configurar 141
Contato de SNMPv3
configurar 141
controle de mouse
absoluto 68
relativo 68
relativo com aceleração padrão Linux 68
controle de mouse absoluto 68
controle de mouse relativo 68
controle de mouse relativo para Linux (aceleração padrão Linux) 68
controle remoto de energia 67
criando uma página da web de suporte personalizada 211
criar
conta do usuário 158

D

Dados da tela de falha do S.O.
capturar 56
dados de serviço 212
coletando 80
fazendo download 80
data
configurar 167
dcmi
funções e comandos 64
gerenciamento de energia 64
DDNS
configurar 121
gerenciar 121
nome de domínio customizado 121
Nome de domínio especificado pelo servidor DHCP 121
origem de nome de domínio 121
declaração regulamentar de telecomunicação 217
Declaração RoHS BSMI de Taiwan 218
definindo o local e o contato 80
delete
usuário 158
designações de porta
configurações 35
configurar 35
Destinatários de SNMP TRAP 54
Detalhe de RAID
Configuração do Servidor 85
dispositivos de armazenamento
Comando storage 169
DNS
configurar 121
endereçamento do servidor 121
Endereçamento IPv4 121
Endereçamento IPv6 121
Servidor LDAP 130
domínio de procura
Servidor LDAP 130

E

encaminhamento de porta
Ethernet sobre USB 123
endereçamento do servidor
DNS 121
Endereçamento IPv4
DNS 121
Endereçamento IPv6
DNS 121
Endereço IP
configurando 9
IPv4 9
IPv6 9
Servidor LDAP 130
Servidor SMTP 140
endereço IP estático padrão 10
endereço IP estático, padrão 10
Endereço IP, estático padrão 10

© Copyright Lenovo 2017, 2022

Endereço MAC
  gerenciar 126
energia
  gerenciando com comandos da IPMI 63
  monitorando com comandos da IPMI 63
energia e reinicialização do servidor
  Comandos do 109
Ethernet
  configurar 126
Ethernet avançada
  configurações 30, 184
Ethernet sobre USB
  configurar 123
  encaminhamento de porta 123
eventos ativos de sistema
  visão geral 49
evitar o rebaixamento do firmware do sistema
  configurar 40
excluir grupo
  ativar, desativar 125
exibir e configurar as unidades virtuais 85
exportação
  chave de ativação 92

F

Fazendo login no XClarity Controller 12
Features on Demand
  gerenciar 129
  instalar recurso 129
  remover recurso 129
ferramentas
  IPMItool 183
filtro de grupo
  LDAP 130
firmware
  servidor de visualização 108
firmware do servidor
  atualizando 89
firmware, servidor
  atualizando 89
Flex System 1
FoD
  gerenciar 129
  instalar recurso 129
  remover recurso 129
funcionamento do hardware 49
Funções do XClarity Controller
  na interface da Web 13
funções e comandos
  dcmi 64
  node manager 63

G

gerenciamento
  certificado do servidor 45
  Certificado SKLM 42
gerenciamento centralizado
  chaves de criptografia 40
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
  Acesso a unidades 151
  CIM sobre HTTPS 147–148
  cliente 42
  LDAP 147–148
  Servidor 45
  Servidor HTTPS 147–148
  Servidor SSH 146
Gerenciamento de certificado SKLM
  página de acesso a unidades 42
gerenciamento de certificados de cliente
  Assinado por CA 42
  autoassinado 42
gerenciamento de energia
  dcmi 64
  ipmi bridging 63
Gerenciamento de licenças 91
gerenciamento do servidor
  Dados da tela de falha do S.O. 56
  firmware do servidor 89
  gravação/reprodução de tela de vídeo 69
  modo de inicialização do sistema 59
  sequência de inicialização do sistema 59
  tempos limites do servidor, configurando 81
  única 60
Gerenciamento do XClarity Controller
  configurações de segurança 38
  configurando contas de usuário 17
  configurando o LDAP 17
  criando um novo usuário local 18
  exclusão de uma conta do usuário 20
  Propriedades do XClarity Controller
    data e hora 82
gerenciando energia
  usando comandos da IPMI 63
gerenciar
  chave de ativação 129
  Comunidades de SNMPv1 141
  DDNS 121
  Endereço MAC 126
  Features on Demand 129
  FoD 129
  usuário 158
gravação/reprodução de tela de vídeo
  gerenciamento do servidor 69
grupo de dispositivos
  página de acesso a unidades 41
Grupo de dispositivos SKLM
  configuração 41
Guia Acesso a unidades
  opção de segurança 40–42
Guia Gerenciamento do Servidor
  opção de gerenciamento de energia 61

H

histórico de manutenção 54
horário
  configurar 167

I

IMM
  configuração padrão 138
  redefinição 168
  redefinir configuração 138
  restauração de configuração 137
  restaurar configuração 137
  spreset 168
Informações de contato de Taiwan para importação e exportação 218
informações do adaptador
  Configuração do Servidor 59
informações do sistema 50
instalar
  chave de ativação 91, 129
instalar recurso
  Features on Demand 129

FoD 129
interface da linha de comandos (CLI)
acessando 95
descrição 95
efetuando login 95
recursos e limitações 96
sintaxe do comando 96
interface da Web
fazendo login na interface da Web 12
interface da Web, abrindo e usando 9
Interface IPMI
descrição 183
Introdução a MIBs 7
inventário de armazenamento 86
IPMI
configurar 34
gerenciamento de servidor remoto 183
ipmi bridging
gerenciamento de energia 63
por meio do XClarity Controller 63
IPMI sobre acesso via KCS
configurar 40
IPMItool 183
IPv4
configurar 126
IPv6 9
configurar 126

J

janela de evento
log 53–54

L

LDAP
atributo de permissão de login 130
atributo de procura do grupo 130
configurando 17
configurar 130
filtro de grupo 130
gerenciamento de certificado 147–148
nome de destino do servidor 130
segurança 147–148
segurança aprimorada baseada em função 158
segurança baseada em função, aprimorada 158
Usuários do Active Directory 158
lista alfabética de comandos 97
lista de bloqueios e restrição de tempo
configurações 36
log de auditoria 54
Log de auditoria estendida
log de auditoria estendida 45
Log de eventos do 53
login global
configurações 23

M

marcas registradas 216
Método de autenticação do usuário 17
configurar 113
método de ligação
Servidor LDAP 130
métodos de montagem de mídia 70
mínimos, níveis
TLS 155
modos de tela de console remoto 69
módulo de gerenciamento avançado 1
monitorando a energia
usando comandos da IPMI 63
monitorando o status de servidor 49
MTU
configurar 126

N

negociação automática
configurar 126
níveis baseados em função
operador 125
rbs 125
supervisor 125
níveis de segurança da conta do usuário
configurar 113
node manager
funções e comandos 63
nome de destino do servidor
LDAP 130
nome de destino, servidor
LDAP 130
nome de domínio, customizado
DDNS 121
nome de domínio, especificado pelo servidor DHCP
DDNS 121
nome distinto do cliente
Servidor LDAP 130
nome distinto raiz
Servidor LDAP 130
nome distinto, cliente
Servidor LDAP 130
nome distinto, raiz
Servidor LDAP 130
nome do host do
configurar 126
Servidor LDAP 130
Servidor SMTP 140
notas, importantes 216
notificações por email e syslog 54
nova conta local
criando 18
número de porta
Servidor LDAP 130
Servidor SMTP 140
números de portas
configurar 135
números de telefone 213
números de telefone de serviço e suporte para hardware 213
números de telefone de serviço e suporte para software 213

O

Obtendo ajuda 211
OneCLI 1
opção
SKM 40
opção de gerenciamento de energia
ações de energia 62
Guia Gerenciamento do Servidor 61
política de limitação de energia 61
política de restauração de energia 62
redundância de energia 61
opção de mensagem de infração 82
opção de segurança
Guia Acesso a unidades 40–41
Opção de segurança
Guia Acesso a unidades 41–42
origem de nome de domínio
DDNS 121

© Copyright Lenovo 2017, 2022

P

página da web de suporte personalizada 211
página da web de suporte, personalizar 211
página de acesso a unidades
  configurar 41
  Gerenciamento de certificado SKLM 42
  grupo de dispositivos 41
  servidores gerenciamento de chaves 41
Porta da CLI SSH
  configurar 135
porta de console remoto
  configurar 135
porta de serviço de rede
  configurar 134
Porta de Traps SNMP
  configurar 135
Porta do agente do SNMP
  configurar 135
Porta do CIM sobre HTTP
  configurar 135
Porta do CIM sobre HTTPS
  configurar 135
Porta do Servidor LDAP
  configurar 130
Porta HTTP
  configurar 135
Porta HTTPS
  configurar 135
porta serial
  configurar 133
portas
  configurar 135
  configurar números 135
  visualizar abertas 135
pré-configurado
  Servidor LDAP 130
problemas de erro de montagem de mídia 78
propriedade de servidor
  configuração do servidor 80
  definindo o local e o contato 80
propriedades do protocolo de rede
  Configurações de alerta SNMP 34
  Configurações Ethernet 30, 184
  DDNS 32
  declarar Presença Física 40
  designações de porta 35
  DNS 32
  Ethernet sobre USB 33
  evitar o rebaixamento do firmware do sistema 40
  IPMI 34
  IPMI sobre acesso via KCS 40
  lista de bloqueios e restrição de tempo 36
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 65
  ativando 66
recursos de nível corporativo 5
recursos de nível padrão 2
recursos do XClarity Controller 2
Recursos do XClarity Controller
  nível corporativo 5
  nível padrão 2
Recursos do XClarity Controller recursos de nível avançado
  nível avançado 5
redefinição
  IMM 168
redefinir configuração
  IMM 138
redirecionamento serial para SSH 95
reiniciar o XClarity Controller 48
remover
  chave de ativação 92, 129
remover recurso
  Features on Demand 129
  FoD 129
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 137
restaurar configuração
  IMM 137

S

saindo da sessão de console remoto 80
segurança
  Acesso a unidades 151
  CIM sobre HTTPS 147–148
  Gerenciamento de certificado SSL 39
  LDAP 147–148
  manipulação de certificado ssl 38
  Servidor HTTPS 147–148
  Servidor SSH 39, 146
  visão geral do ssl 38
segurança aprimorada baseada em função
  LDAP 158
segurança baseada em função, aprimorada
  LDAP 158
senha
  Servidor LDAP 130
  usuário 158
senha com hash 20
Sequência-chave da CLI
  configurar 133
Serial over LAN 183
serviço e suporte
  antes de fazer uma chamada 211
  hardware 213
  software 213
Servidor
  gerenciamento de certificado 45
  opções de configuração 59
Servidor HTTPS
  gerenciamento de certificado 147–148
  segurança 147–148
Servidor LDAP
  Atributo de pesquisa de UID 130
  configurar 130
  DNS 130
  domínio de procura 130
  Endereço IP 130
  método de ligação 130
  nome distinto do cliente 130
  nome distinto raiz 130
  nome do host do 130
  número de porta 130
  pré-configurado 130
  senha 130
Servidor SSH
  gerenciamento de certificado 146
  segurança 146
Servidores Flex 1
servidores gerenciamento de chaves
  configurar 41
  página de acesso a unidades 41
SKLM
  servidores gerenciamento de chaves 41

SKM
  opção 40
SMTP
  configurar 140
  endereço IP do servidor 140
  nome do host do servidor 140
  número da porta do servidor 140
SNMPv1
  configurar 141
solicitação de assinatura de certificado
  BMC 42
SSL
  gerenciamento de certificado 39
  manipulação de certificado 38
status de servidor
  monitorar 49
suporte a mouse de console remoto 68
suporte a teclado no console remoto 68
suporte a vários idiomas 7
suporte de mouse no console remoto 68

T

tempo limite de inatividade da sessão da Web 23
tempo limite de inatividade da Web
  configurar 113
tempo limite do servidor
  seleções 81
ThinkSystem Server Firmware
  descrição 1
TLS
  nível mínimo 155
trabalhando com
  eventos no log de auditoria 54
  eventos no log de eventos 53
Traps SNMPv1
  configurar 141

U

única
  configuração 60
unidade de transmissão máxima
  configurar 126
usando
  função do console remoto 65
  recurso de console remoto 65
USB
  configurar 123
usuário
  Chaves SSH 158
  Configurações de SNMPv3 158
  delete 158
  gerenciar 158
  senha 158
usuários
  visualizar atuais 158
Usuários do Active Directory
  LDAP 158
utilização do sistema 52

V

visão geral 49
  ssl 38
Visualizador de Vídeo
  captura de tela 67
  comandos de energia e reinicialização 67
  controle de mouse absoluto 68
  controle de mouse relativo 68
  controle de mouse relativo para Linux (aceleração padrão Linux) 68
  modo de cor de vídeo 68
  suporte de mouse 68
visualizar atuais
  usuários 158
visualizar informações do firmware
  Servidor 108
visualizar portas abertas 135

X

XClarity Controller
  conexão de rede 10
  configurar o protocolo de rede 30
  descrição 1
  interface da Web 9
  ipmi bridging 63
  Nível avançado do XClarity Controller 2
  Nível corporativo do XClarity Controller 2
  Nível padrão do XClarity Controller 2
  novas funções 1
  opções de configuração 17
  recursos 2
  redirecionamento serial 95
XClarity Provisioning Manager
  Utilitário de configuração 10

© Copyright Lenovo 2017, 2022

Lenovo

Número de Peça: SP47A30085

Printed in China

(1P) P/N: SP47A30085