



Integrated Management Module II
Guia do Usuário





Integrated Management Module II
Guia do Usuário

Terceira Edição (Maio de 2013)

© Copyright IBM Corporation 2013.

Índice

Tabelas	vii
--------------------------	------------

Capítulo 1. Introdução. **1**

Recursos de Nível Básico, Padrão e Avançado do IMM2.	2
Recursos de Nível Básico do IMM2.	2
Recursos de Nível Padrão do IMM2	3
Recursos de Nível Avançado do IMM2	3
Melhorias de Recursos do IMM2.	3
Atualizando o IMM2	3
Usando o IMM2 com o Módulo de Gerenciamento Avançado BladeCenter	4
Requisitos de navegador da web e sistema operacional.	4
Avisos usados neste manual	5

Capítulo 2. Abrindo e Usando a Interface da Web do IMM2 **7**

Acessando a Interface da Web do IMM2	7
Configurando a Conexão de Rede do IMM2 por meio do Utilitário de Configuração do IBM System x Server Firmware	8
Efetuando Login no IMM2	10
Descrições das Ações do IMM2.	11

Capítulo 3. Visão Geral da Interface com o Usuário da Web do IMM2. **17**

Configurações de Sessão da Web	17
Atualização Automática de Página.	17
Mensagem de Infração.	19
Efetuar logout	20
Guia Status do Sistema	21
Guia Eventos	27
Log de Eventos	28
Destinatários de Eventos	30
Guia Serviço e Suporte	33
Fazer o Download de Dados de Serviço	33
Guia Gerenciamento do Servidor	34
Firmware do Servidor	35
Controle remoto	40
Propriedades do Servidor.	45
Ações de Energia do Servidor	49
Discos	49
Memória	50
Processadores.	51
Tempos Limites do Servidor.	52
inicialização da rede PXE.	52
Tela de Falha mais Recente do S.O.	52
Guia Gerenciamento do IMM	53

Capítulo 4. Configurando o IMM2 **55**

Configurando tempos limites do servidor	58
Configurando a Data e Hora do IMM2	59
Configurando as Definições de Porta Serial.	61

Configurando Contas de Usuário	62
Contas de Usuário	63
Perfis de Grupo	66
Definindo as Configurações de Login Global	67
Configurações Gerais	67
Configurações de Política de Segurança de Conta	69
Configurando protocolos de rede	71
Configurando as Definições de Ethernet.	72
Configurando definições de alerta SNMP	74
Configurando o DNS	75
Configurando o DDNS	76
Configurando o SMTP.	76
Configurando o LDAP.	77
Configurando Telnet	82
Configurando USB	83
Configurando designações de porta	84
Definindo a Configuração de Segurança	85
Configurando o Protocolo HTTPS	85
Configurando o Protocolo CIM sobre HTTPS	86
Configurando o Protocolo do Cliente LDAP	87
Configurando o servidor Shell Seguro	89
Visão Geral do SSL	90
Manipulação de Certificado SSL	90
Gerenciamento de Certificado SSL.	90
Restaurando e modificando a configuração do IMM	92
Reiniciando o IMM2	92
Reconfigurando o IMM2 para os Padrões de Factory	93
Chave de Gerenciamento de Ativação	94

Capítulo 5. Monitorando o Status de Servidor **95**

Visualizando o Status do Sistema	95
Visualizando as Informações do Sistema.	97
Visualizando o Funcionamento do Servidor.	98
Visualizando o Funcionamento do Hardware	99

Capítulo 6. Executando Tarefas do IMM2 **103**

Controlando o Status de Energia do Servidor.	104
Funções de Presença Remota e Controle Remoto	105
Atualizando o Firmware do IMM2 e o Applet Java ou ActiveX	106
Ativando a função de presença remota	106
Captura de tela de controle remoto	106
Modos de Visualização do Visualizador de Vídeo de Controle Remoto	107
Modo de cor de vídeo do controle remoto.	108
Suporte a teclado de controle remoto	108
Suporte a mouse de controle remoto.	110
Controle de energia remota.	112
Visualizando Estatísticas de Desempenho	112
Iniciando o Remote Desktop Protocol	112
Descrição do Recurso Knock-knock	112
Disco Remoto	115
Configurando a inicialização da rede PXE	117

Atualizando o Firmware do Servidor	118
Gerenciando eventos do sistema	123
Gerenciando o Log de Eventos	123
Notificação de Eventos do Sistema	125
Coletando Informações de Serviço e Suporte	130
Capturando os Dados da Tela de Falha mais Recente do S.O.	132
Gerenciando a Energia do Servidor	133
Controlando a Fonte de Alimentação e a Energia Total do Sistema	134
Exibindo as Fontes de Alimentação Instaladas Atualmente	136
Exibindo a Capacidade da Fonte de Alimentação	137
Exibindo o Histórico de Energia	137

Capítulo 7. Features on Demand 139

Instalando uma Chave de Ativação	139
Removendo uma Chave de Ativação	141
Exportando uma Chave de Ativação.	143

Capítulo 8. Interface da linha de comandos. 145

Gerenciando a IMM2 com o IPMI	145
Usando o IPMItool	145
Acessando a Interface da Linha de Comandos	145
Efetuando login na sessão de linha de comandos	146
Configurando o redirecionamento serial para Telnet ou SSH	146
Sintaxe de Comandos	146
Recursos e limitações	147
Listagem Alfabética de Comandos	148
Comandos Utilitários	149
comando exit	149
comando help	149
Comando history	149
Comandos de Monitor	150
Comando clearlog	150
Comando fans	150
Comando ffdc	150
Comando led	152
Comando readlog	153
Comando show	154
Comando syshealth	155
Comando temps	155
Comando volts	155
Comando vpd	156
Comandos de controle de energia e reinicialização do servidor	157
Comando power	157
Comando pxeboot	157
Comando reset	158
Comando de redirecionamento serial	158
comando do console	158
Comandos de configuração.	158
Comando accsecfg	159
Comando alertcfg	160
Comando asu	161
Comando backup	165
Comando dhcpcinfo	166

Comando dns	167
comando ethtousb	168
Comando gprofile	169
Comando ifconfig	170
Comando keycfg	172
Comando ldap	173
Comando ntp	175
Comando passwordcfg	176
Comando ports	176
Comando portcfg	177
comando restaurar	178
Comando restoredefaults	179
Comando set	179
Comando smtp	180
Comando Snmp	181
Comando snmpalerts	183
Comando srcfg	184
Comando sshcfg	185
Comando ssl	186
Comando sslcfg	187
Comando telnetcfg	190
Comando thermal	191
Comando timeouts	191
Comando usbeth	192
Comando users	192
Comandos de Controle do IMM2.	197
Comando alertentries	197
Comando batch	200
Comando clearcfg	200
Comando clock	201
Comando identify	201
Comando info	202
Comando resetsp	202
Comando spreset	202

Apêndice A. Obtendo ajuda e assistência técnica 203

Antes de ligar	203
Usando a documentação.	204
Obtendo ajuda e informações na World Wide Web	204
Como enviar dados do DSA para a IBM	204
Criando uma página da web de suporte personalizada	205
Serviço e Suporte de Software	205
Serviço e suporte de hardware	205
Serviço do Produto da IBM Taiwan	205

Apêndice B. Avisos 207

Marcas registradas.	208
Notas importantes.	208
Contaminação por partículas	209
Formato da documentação	210
Declaração Regulamentar de Telecomunicação	210
Avisos de emissão eletrônica	211
Declaração da Federal Communications Commission (FCC)	211
Declaração de conformidade de emissão de Classe A do segmento de mercado do Canadá	211
Avis de conformité à la réglementation d'Industrie Canada	211

Declaração de Classe A da Austrália e Nova Zelândia	211
Declaração de conformidade com a Diretiva EMC da União Europeia.	211
Declaração de Classe A da Alemanha	212
Declaração de Classe A VCCI do Japão.	213
Instrução da Korea Communications Commission (KCC)	213
Declaração de Classe A de Interferência Eletromagnética (EMI) da Rússia	213

Declaração de emissão eletrônica de Classe A da República Popular da China	214
Declaração de conformidade de Classe A de Taiwan	214

Índice Remissivo 215

Tabelas

1. Ações do IMM2	11	5. Descrições de Estados do Sistema	96
2. Estados de Energia e de Operação do Servidor	24	6. Ações de Energia e Descrições	104
3. Valores de Política de Configuração de		7. Comandos ASU.	161
Segurança	69	8. Comandos de Transação	164
4. Bits de permissão	81	9. Limites para partículas e gases.	210

Capítulo 1. Introdução

O processador de serviços Integrated Management Module II (IMM2) é a segunda geração do processador de serviços Integrated Management Module (IMM) que consolida a funcionalidade do processador de serviços, Super E/S, controladora de vídeo e recursos de presença remota em um único chip na placa-mãe do servidor. Como no caso do IMM, o IMM2 oferece várias melhorias sobre a funcionalidade combinada do Baseboard Management Controller (BMC) e do Remote Supervisor Adapter II incluindo estes recursos:

- Opção de uma conexão Ethernet dedicada ou compartilhada para gerenciamento de sistemas.
- Um endereço IP para a Intelligent Platform Management Interface (IPMI) e a interface do processador de serviço. O recurso não se aplica aos servidores blade IBM® BladeCenter.
- Dynamic System Analysis (DSA) Integrada.
- Configuração remota com o Advanced Settings Utility (ASU). O recurso não se aplica a servidores blade IBM BladeCenter.
- Capacidade para aplicativos e ferramentas acessarem o IMM2, dentro da banda ou fora da banda. Somente a conexão do IMM2 dentro da banda é suportada em servidores blade IBM BladeCenter.
- Recursos aprimorados de presença remota. O recurso não se aplica a servidores blade IBM BladeCenter.

Notas:

- Uma porta de rede de gerenciamento de sistemas dedicada não está disponível nos servidores blade IBM BladeCenter e alguns servidores System x; para esses servidores, apenas a configuração *compartilhada* está disponível.
- Para servidores blade IBM BladeCenter, o módulo de gerenciamento avançado IBM BladeCenter é o módulo de gerenciamento primário para funções de gerenciamento de sistemas e multiplexação de teclado/vídeo/mouse (KVM).

O IBM System x® Server Firmware é a implementação da IBM do Unified Extensible Firmware Interface (UEFI). Ele substitui o sistema BIOS nos servidores IBM System x e servidores blade IBM BladeCenter. O BIOS era o código de firmware padrão que controlava operações básicas de hardware, como interações com unidades de disquete, unidades de disco rígido e o teclado. O IBM System x Server Firmware oferece vários recursos que o BIOS não oferece, incluindo conformidade com UEFI 2.3, compatibilidade iSCSI, tecnologia Active Energy Manager e recursos aprimorados de confiabilidade e serviço. O utilitário Setup fornece informações do servidor, configuração do servidor, compatibilidade de customização e estabelece a ordem dos dispositivos de inicialização.

Notas:

- O IBM System x Server Firmware geralmente é chamado de firmware do servidor e ocasionalmente chamado de UEFI, neste documento.
- O IBM System x Server Firmware é totalmente compatível com sistemas operacionais não UEFI.
- Para obter mais informações sobre como usar o IBM System x Server Firmware, consulte a documentação fornecida com seu servidor IBM.

Este documento explica como usar as funções do IMM2 em um servidor IBM. O IMM2 trabalha com o IBM System x Server Firmware para fornecer a capacidade de gerenciamento de sistemas para os servidores System x, BladeCenter e IBM Flex System.

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

Nota: Na primeira vez que acessar o IBM Support Portal, você deverá escolher a categoria do produto, a família de produtos e os números dos modelos para seus subsistemas de armazenamento. A próxima vez que acessar o IBM 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 mudanças periodicamente no website da IBM. Os procedimentos para localização de firmware e documentação podem variar um pouco em relação ao que está descrito neste documento.

1. Acesse <http://www.ibm.com/support/entry/portal>.
2. Em **Escolher os produtos**, selecione **Procurar um produto** e expanda **Hardware**.
3. Dependendo do tipo de servidor, clique em **Sistemas > System x** ou **Sistemas > BladeCenter** e marque a caixa para seu servidor ou servidores.
4. Em **Escolher a tarefa**, clique em **Downloads**.
5. Em **Ver os resultados**, clique em **Visualizar sua página**.
6. Na caixa **Flashes & alertas**, clique no link para o download aplicável ou clique em **Mais resultados** para ver links adicionais.

Recursos de Nível Básico, Padrão e Avançado do IMM2

Com o IMM2, os níveis Básico, Padrão e Avançado da funcionalidade do IMM2 são oferecidos. Consulte a documentação para seu servidor para obter informações adicionais sobre o nível do IMM2 instalado em seu servidor IBM. 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

Além disso, os níveis Padrão e Avançado suportam gerenciamento baseado na web com navegadores da web padrão.

Nota: Alguns recursos podem não se aplicar a servidores blade IBM BladeCenter.

A seguir está uma lista dos recursos de nível básico do IMM2:

Recursos de Nível Básico do IMM2

A seguir está uma lista de recursos de Nível Básico do IMM2:

- Interface IPMI 2.0
- Monitoramento Térmico
- Controle de Ventilador
- Gerenciamento de LED
- Controle de Energia/Reconfiguração do Servidor
- Monitoramento de Sensor

- Alertas de Traps de Eventos da Plataforma IPMI
- Serial over LAN do IPMI

Recursos de Nível Padrão do IMM2

A seguir está uma lista dos recursos de Nível Padrão do IMM2:

- Todos os recursos de nível Básico do IMM2
- Gerenciamento Baseado na Web com Navegadores da Web Padrão
- Interfaces SNMPv1 e SNMPv3
- CLI do Telnet e SSH
- Controle de Energia/Reconfiguração do Servidor Planejado
- Criação de Log de Evento e Auditoria Legível
- Indicação de Funcionamento do Sistema
- Carregador do Sistema Operacional e Watchdogs do Sistema Operacional
- Autenticação e Autorização LDAP
- Trap SNMP, Email, Syslog e Alertas de Indicação do CIM
- Sincronização do Clock NTP
- Redirecionamento do Console Serial sobre Telnet/SSH

Recursos de Nível Avançado do IMM2

A seguir está uma lista dos recursos de Nível Avançado do IMM2:

- Todos os recursos de nível Básico e Padrão do IMM2
- Clientes Java e ActivX de Presença Remota:
 - Suporte a Teclado, Vídeo e Mouse Remotos
 - Mídia Remota
 - Disco Remoto na Placa
- Captura de Tela de Falha para Quedas do Sistema Operacional

Melhorias de Recursos do IMM2

A seguir está uma lista de melhorias de recursos do IMM2 sobre o IMM:

- Segurança (processador de serviços de confiança):
 - Inicialização segura
 - Atualizações assinadas
 - IMM2 Core Root for Trust Measurement
 - Trusted Platform Module
- Novo design da GUI da web consistente no IBM System x
- Aumento de resolução de vídeo e intensidade de cor da presença remota
- Cliente de presença remota ActiveX
- Interface Ethernet-sobre-USB atualizada para USB 2.0
- Alertas do syslog
- Nenhuma reconfiguração do IMM2 é necessária após mudanças na configuração

Atualizando o IMM2

Se o seu servidor IBM foi fornecido com a funcionalidade de firmware do IMM2 de nível Básico ou Padrão, é provável que você consiga atualizar a funcionalidade

do IMM2 em seu servidor. Para obter informações adicionais, sobre níveis de upgrade disponíveis e como pedi-los, consulte Capítulo 7, "Features on Demand", na página 139.

Usando o IMM2 com o Módulo de Gerenciamento Avançado BladeCenter

O módulo de gerenciamento avançado BladeCenter é a interface de gerenciamento de sistemas padrão para produtos IBM BladeCenter. Embora o IMM2 esteja agora incluso em alguns servidores blade IBM BladeCenter, o módulo de gerenciamento avançado continua sendo o módulo de gerenciamento para funções de gerenciamento de sistemas e multiplexação de KVM para produtos IBM BladeCenter, incluindo servidores blade IBM.

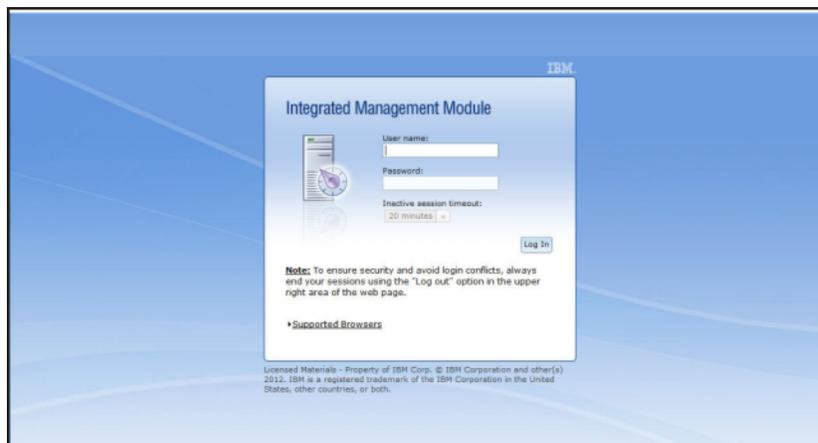
Não há nenhum acesso de rede externa ao IMM2 em servidores blade IBM BladeCenter e o módulo de gerenciamento avançado deve ser usado para gerenciamento remoto de servidores blade IBM BladeCenter. O IMM2 substitui a funcionalidade do BMC e a placa da opção Teclado, Vídeo e Mouse Simultâneos (cKVM) disponíveis em produtos de servidor blade IBM anteriores.

Requisitos de navegador da web e sistema operacional

A interface da web do IMM2 requer o Java™ Plug-in 1.5 ou mais recente (para o recurso de presença remota) e um dos navegadores da web a seguir:

- Microsoft Internet Explorer versão 7 ou 8
- Mozilla Firefox versão 3.5 ou mais recente

Se você estiver usando versões mais recentes do Microsoft Internet Explorer, é recomendável usar a Visualização de Compatibilidade no Internet Explorer para exibir as páginas da web do IMM2. Os navegadores listados acima correspondem àqueles suportados atualmente pelo firmware do IMM2. O firmware do IMM2 pode ser aprimorado periodicamente para incluir suporte para outros navegadores. Consulte a lista "Navegadores Suportados" na página de login do IMM2 para obter a lista de navegadores que são suportados pela versão do firmware do IMM2 que está em execução atualmente no sistema. A ilustração a seguir exibe a tela de login do IMM2.



Os seguintes sistemas operacionais de servidor têm suporte USB, que é necessário para o recurso de presença remota:

- Microsoft Windows Server 2008
- Microsoft Windows Server 2003
- Red Hat Enterprise Linux versões 4.0 e 5.0
- SUSE Linux versão 10.0
- Novell NetWare 6.5

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 IMM2, seu navegador pode continuar a usar as informações de seu cache em vez de recuperá-las do IMM2. Depois de atualizar o firmware do IMM2, é recomendável limpar o cache do navegador para assegurar que as páginas da web entregues pelo IMM2 sejam exibidas corretamente.

Avisos usados neste manual

Os seguintes avisos são utilizados na documentação:

- **Nota:** Esses avisos fornecem dicas, orientações ou recomendações importantes.
- **Importante:** Esses avisos fornecem informações ou conselhos que podem ajudar a evitar situações inconvenientes ou problemáticas.
- **Atenção:** Esses avisos indicam potenciais danos a programas, dispositivos ou dados. Um aviso de atenção é colocado logo antes da instrução ou situação na qual poderia ocorrer dano.

Capítulo 2. Abrindo e Usando a Interface da Web do IMM2

Importante: Esta seção não se aplica ao IBM BladeCenter e a servidores blade IBM. Embora o IMM2 seja padrão em alguns produtos IBM BladeCenter e servidores blade IBM, o módulo de gerenciamento avançado IBM BladeCenter é o módulo de gerenciamento primário para funções de gerenciamento de sistemas e multiplexação de KVM para produtos IBM BladeCenter, incluindo servidores blade IBM. Os usuários que desejam configurar as definições do IMM2 em servidores blade devem usar o Advanced Settings Utility (ASU) no servidor blade para executar essas ações.

O IMM2 combina funções do processador de serviços, uma controladora de vídeo e a função de presença remota (quando uma chave de mídia virtual opcional está instalada) em um único chip. Para acessar o IMM2 remotamente usando a interface da web do IMM2, você deve primeiro efetuar login. Este capítulo descreve os procedimentos de login e as ações que podem ser executadas a partir da interface da web do IMM2.

Acessando a Interface da Web do IMM2

O IMM2 suporta endereçamento IPv4 estático e Protocolo de Configuração de Host Dinâmico (DHCP). O endereço IPv4 estático padrão designado ao IMM2 é 192.168.70.125. O IMM2 é configurado inicialmente para tentar obter um endereço de um servidor DHCP e, se não conseguir, ele usará o endereço IPv4 estático.

O IMM2 também suporta IPv6, mas não tem um endereço IP IPv6 estático fixo por padrão. Para acesso inicial ao IMM2 em um ambiente IPv6, é possível usar o endereço IP IPv4 ou o endereço local de link IPv6. O IMM2 gera um endereço IPv6 local de link exclusivo, que é mostrado na interface da web do IMM2 na página Interfaces de Rede. O endereço IPv6 local de link tem o mesmo formato do exemplo a seguir.

```
fe80::21a:64ff:fee6:4d5
```

Ao acessar o IMM2, as condições de IPv6 a seguir são configuradas como padrão:

- A configuração de endereço IPv6 automática é ativada.
- A configuração de endereço IP estático IPv6 é desativada.
- O DHCPv6 é ativado.
- A configuração automática stateless é ativada.

O IMM2 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.

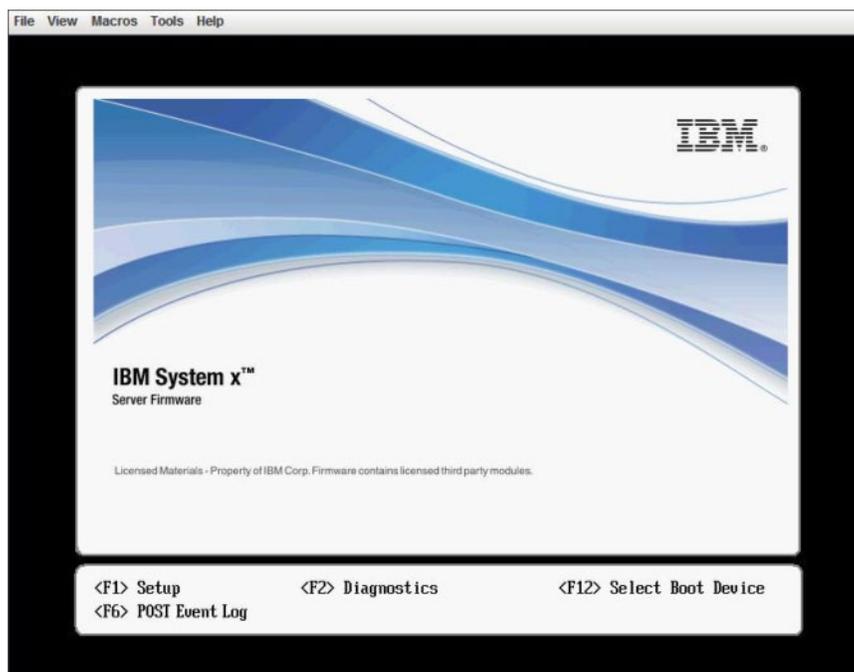
Nota: Uma porta de rede de gerenciamento de sistemas dedicada pode não estar disponível em seu servidor. Se o hardware não tiver uma porta de rede dedicada, a configuração *compartilhada* será a única configuração do IMM2 disponível.

Configurando a Conexão de Rede do IMM2 por meio do Utilitário de Configuração do IBM System x Server Firmware

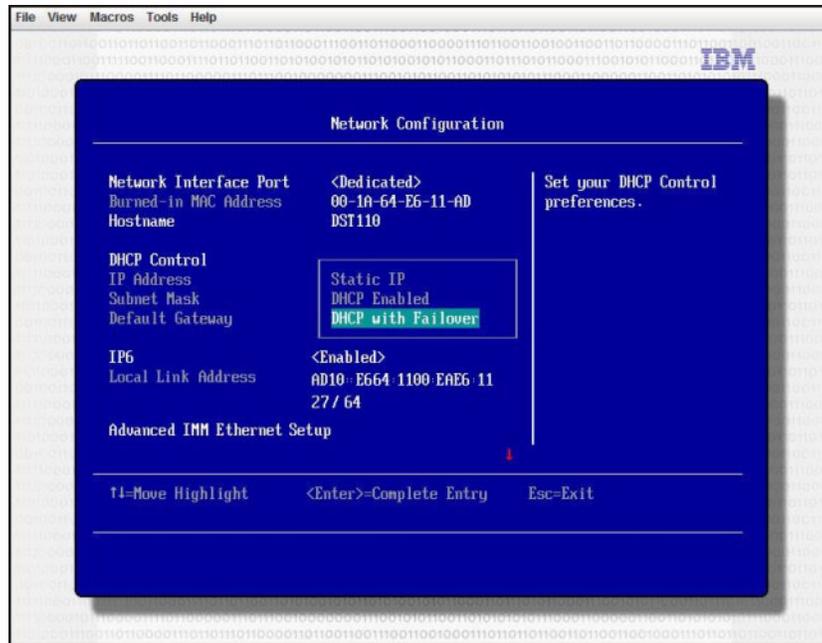
Depois de iniciar o servidor, é possível usar o utilitário de Configuração para selecionar uma conexão de rede do IMM2. O servidor com o hardware IMM2 deve estar conectado a um servidor DHCP, ou a rede do servidor deve estar configurada para usar o endereço IP estático do IMM2. Para configurar a conexão de rede do IMM2 por meio do utilitário de Configuração, conclua as etapas a seguir:

1. Ligue o servidor. A tela de boas-vindas do IBM System x Server Firmware é exibida.

Nota: Aproximadamente 90 segundos após o servidor ser conectado à energia de corrente alternada, o botão de controle de energia torna-se ativo.



2. Quando o prompt <F1> Configurar for exibido, pressione F1. Se você tiver definido uma senha de inicialização e uma de administrador, digite a de administrador para acessar o menu completo do utilitário de configuração.
3. No menu principal do utilitário de Configuração, selecione **Configurações do Sistema**.
4. Na próxima tela, selecione **Módulo de Gerenciamento Integrado**.
5. Na próxima tela, selecione **Configuração de Rede**.
6. Destaque **Controle DHCP**. Há três opções de conexão de rede do IMM2 no campo **Controle DHCP**:
 - IP Estático
 - DHCP Ativado
 - DHCP com Failover (padrão)



7. Selecione uma das opções de conexão de rede.
8. Se você optar por usar um endereço IP estático, especifique o endereço IP, a máscara de sub-rede e o gateway padrão.
9. É possível também usar o utilitário de Configuração para selecionar uma conexão de rede dedicada (se o seu servidor tiver uma porta de rede dedicada) ou uma conexão de rede do IMM2 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 IMM2 disponível. Na tela **Configuração de Rede**, selecione **Dedicada** (se aplicável) ou **Compartilhada** no campo **Porta da Interface de Rede**.
 - Para localizar os locais dos conectores Ethernet em seu servidor que são usados pelo IMM2, consulte a documentação fornecida com seu servidor.
10. Role para baixo e selecione **Salvar Configurações de Rede**.
 11. Saia do utilitário de Configuração.

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 IMM2 por meio da interface da web do IMM2 ou da interface da linha de comandos (CLI). Na interface da web do IMM2, as conexões de rede são configuradas na página **Propriedades do Protocolo de Rede** (selecione **Rede** no menu **Gerenciamento do IMM**). Na CLI do IMM2, as conexões de rede são configuradas usando vários comandos que dependem da configuração de sua instalação.

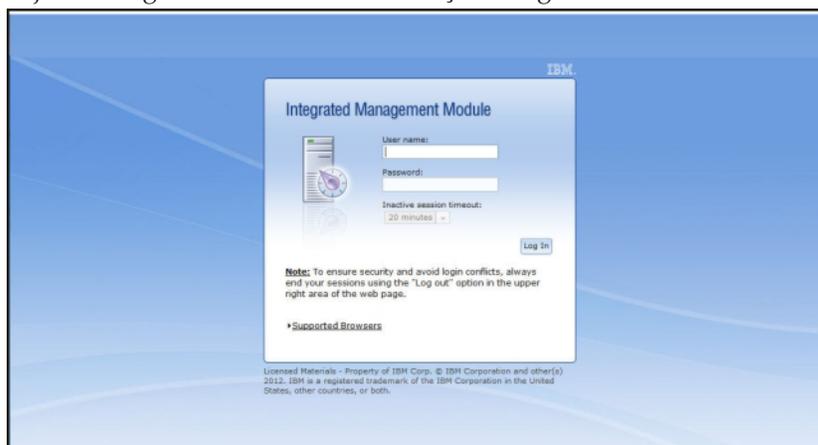
Efetuando Login no IMM2

Importante: O IMM2 é configurado inicialmente com um nome de usuário USERID e uma senha PASSW0RD (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.

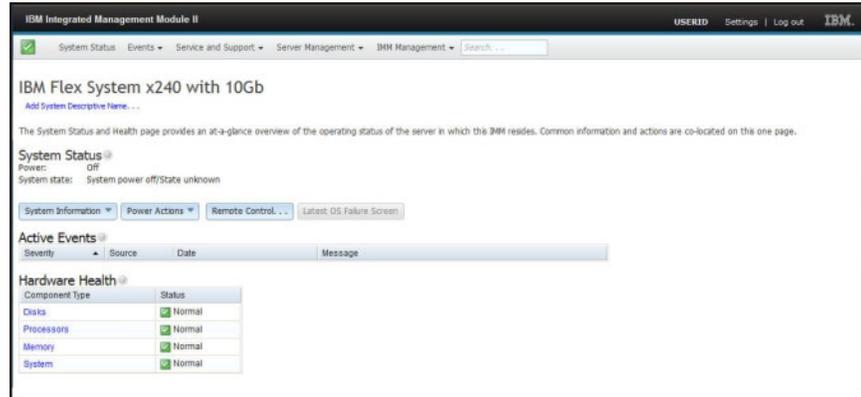
Para acessar o IMM2 por meio da interface da web do IMM2, conclua as etapas a seguir:

1. Abra um navegador da web. No campo de endereço ou URL, digite o endereço IP ou nome do host do IMM2 ao qual você deseja se conectar.
2. Digite seu nome de usuário e senha na janela Login do IMM2. Se você estiver usando o IMM2 pela primeira vez, poderá obter seu nome de usuário e a senha com o 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.

A janela Login é mostrada na ilustração a seguir.



3. Clique em **Efetuar Login** para iniciar a sessão. O navegador abre a página Status do Sistema, conforme mostrado na ilustração a seguir. Essa página fornece uma visualização rápida do status do servidor e do resumo do funcionamento do servidor.



Para descrições das ações que podem ser executadas a partir das guias na parte superior da interface da web do IMM2, consulte “Descrições das Ações do IMM2”.

Descrições das Ações do IMM2

Navegue para a parte superior da janela do IMM2 para executar atividades com o IMM2. A barra de título identifica o nome de usuário que efetuou login. A barra de título permite configurar **Configurações** para a taxa de atualização da tela de status e uma mensagem de infração customizada e **Efetuar Logout** da interface da web do IMM2. Abaixo da barra de título estão guias que permitem acessar várias funções do IMM2, conforme listado na Tabela 1.



Tabela 1. Ações do IMM2

Guia	Seleção	Descrição
Status do Sistema		A página Status do Sistema permite visualizar o status do sistema, eventos do sistema ativo e informações de funcionamento de hardware. Ela fornece links rápidos para as Informações do Sistema, Ações de Energia do Servidor e Funções de Controle Remoto da guia Gerenciamento do Servidor e permite visualizar uma imagem da última captura de tela de falha do sistema operacional. Consulte “Guia Status do Sistema” na página 21 e “Visualizando o Status do Sistema” na página 95 para obter informações adicionais.

Tabela 1. Ações do IMM2 (continuação)

Guia	Seleção	Descrição
Eventos	Log de Eventos	A página Log de Eventos exibe entradas que estão atualmente armazenadas no log de eventos do IMM2. O log inclui uma descrição de texto de eventos do sistema que são relatados, incluindo informações sobre todas as tentativas de acesso remoto e as mudanças na configuração. Todos os eventos no log são registrados com data e hora usando as configurações de data e hora do IMM2. Alguns eventos também gerarão alertas, se estiverem configurados para isso. É possível classificar e filtrar eventos no log de eventos e exportá-los para um arquivo de texto. Consulte "Guia Eventos" na página 27 e "Gerenciando o Log de Eventos" na página 123 para obter informações adicionais.
	Destinatários de Eventos	A página Destinatários de Eventos permite gerenciar 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 a operação do recurso de notificação. Consulte "Destinatários de Eventos" na página 30 e "Notificação de Eventos do Sistema" na página 125 para obter informações adicionais.
Serviço e Suporte	Fazer o Download de Dados de Serviço	A página Fazer o Download de Dados de Serviço cria um arquivo compactado de informações que pode ser usado pelo Suporte IBM para ajudá-lo. Consulte "Fazer o Download de Dados de Serviço" na página 33 e "Coletando Informações de Serviço e Suporte" na página 130 para obter informações adicionais.

Tabela 1. Ações do IMM2 (continuação)

Guia	Seleção	Descrição
Gerenciamento de Servidores	Firmware do Servidor	A página Firmware do Servidor exibe os níveis de firmware e permite a atualização do firmware do IMM2, do firmware do servidor e do firmware do DSA. Consulte “Firmware do Servidor” na página 35 e “Atualizando o Firmware do Servidor” na página 118 para obter informações adicionais.
	Controle Remoto	A página Controle Remoto permite controlar o servidor no nível do sistema operacional. Ela fornece acesso a ambas as funcionalidades, Disco Remoto e e Console Remoto. É possível visualizar e operar o console do servidor a partir do computador e montar uma das unidades de disco do computador, como a unidade de CD-ROM ou a unidade de disquete, no servidor. Após a montagem de um disco, será possível usá-lo para reiniciar o servidor e atualizar o firmware no servidor. O disco montado aparece como uma unidade de disco USB conectada ao servidor. Consulte “Controle remoto” na página 40 e “Funções de Presença Remota e Controle Remoto” na página 105 para obter informações adicionais.
	Propriedades do Servidor	A página Propriedades do Servidor fornece acesso a várias propriedades, condições de status e configurações para seu servidor. As opções a seguir estão disponíveis na página Propriedades do Servidor: <ul style="list-style-type: none"> • A guia Configurações Gerais exibe informações que identificam o sistema para a equipe de operações e de suporte. • A guia LEDs exibe o status de todos os LEDs do sistema. Ela também permite alterar o estado do LED de localização. • A guia Informações de Hardware exibe dados vitais do produto (VPD) do servidor. O IMM2 coleta informações do servidor, informações do componente do servidor e informações de hardware da rede. • A guia Ambientes exibe informações de voltagem e de temperatura do servidor e de seus componentes. • A guia Atividade de Hardware exibe um histórico de componentes de Unidade Substituível em Campo (FRU) que foram incluídos ou removidos do sistema. Consulte “Propriedades do Servidor” na página 45 para obter informações adicionais.
	Ações de Energia do Servidor	A página Ações de Energia do Servidor fornece controle de energia remota integral sobre o servidor com as ações ligar, desligar e reiniciar. Consulte “Ações de Energia do Servidor” na página 49 e “Controlando o Status de Energia do Servidor” na página 104 para obter informações adicionais.
	Discos	A página Discos Rígidos exibe o status de unidades de disco rígido no servidor. É possível clicar em um nome de unidade para exibir eventos ativos da unidade de disco rígido. Consulte “Discos” na página 49 para obter informações adicionais.
	Memória	A página Memória exibe os módulos de memória disponíveis no sistema, juntamente com seu status, tipo e capacidade. É possível clicar em um nome de módulo para exibir um evento e informações de hardware adicionais para o módulo de memória. Se você remover ou substituir um dual inline memory module (DIMM), o servidor precisará ser ligado pelo menos uma vez após a remoção ou substituição para exibir as informações de memória corretas. Consulte “Memória” na página 50 para obter informações adicionais.

Tabela 1. Ações do IMM2 (continuação)

Guia	Seleção	Descrição
Gerenciamento de Servidores <i>(continuação)</i>	Processadores	A página CPUs exibe os microprocessadores no sistema, juntamente com seu status e velocidade do clock. É possível clicar em um nome de microprocessador para exibir eventos e informações de hardware adicionais do microprocessador. Consulte “Processadores” na página 51 para obter informações adicionais.
	Tempos Limites do Servidor	A página Tempos Limites do Servidor permite gerenciar tempos limites de início do servidor para detectar ocorrências de interrupção do servidor e recuperar-se delas. Consulte “Tempos Limites do Servidor” na página 52 e “Configurando tempos limites do servidor” na página 58 para obter informações adicionais.
	Inicialização da Rede PXE	A página Inicialização de Rede PXE permite alterar a sequência de inicialização do servidor host para a próxima reinicialização tentar uma inicialização da rede do Ambiente de Execução de Pré-inicialização (PXE)/Protocolo de Configuração de Host Dinâmico (DHCP). A sequência de inicialização do host será alterada apenas se o host não estiver sob Proteção de Acesso Privilegiado (PAP). Consulte “inicialização da rede PXE” na página 52 e “Configurando a inicialização da rede PXE” na página 117 para obter informações adicionais.
	Tela de Falha mais Recente do S.O.	A página Tela de Falha mais Recente do S.O. exibe uma imagem de tela (quando disponível) da falha de sistema operacional mais recente no servidor. Para que o IMM2 capture telas de falha do sistema operacional, o watchdog do sistema operacional deve estar ativado. Consulte “Tela de Falha mais Recente do S.O.” na página 52 e “Capturando os Dados da Tela de Falha mais Recente do S.O.” na página 132 para obter informações adicionais.
	Gerenciamento de Energia	A página Gerenciamento de Energia do Servidor permite gerenciar políticas relacionadas à energia e o hardware e contém o histórico da quantidade de energia usada pelo servidor. Consulte “Gerenciando a Energia do Servidor” na página 133 para obter informações adicionais.
Gerenciamento do IMM <i>(continuação na próxima página)</i>	Propriedades do IMM	<p>A página Propriedades do IMM fornece acesso a várias propriedades e configurações para seu IMM2. As opções a seguir estão disponíveis na página Propriedades do IMM:</p> <ul style="list-style-type: none"> • A guia Firmware fornece um link para a seção Firmware do Servidor de Gerenciamento do Servidor. • A guia Configurações de Data e Hora do IMM permite visualizar e configurar as definições de data e hora do IMM2. • A guia Porta Serial configura as definições de porta serial do IMM2. Essas configurações incluem a taxa de bauds da porta serial usada pela função de redirecionamento de porta serial e a sequência-chave para alternar entre os modos CLI e redirecionamento serial. <p>Consulte Capítulo 4, “Configurando o IMM2”, na página 55 para obter informações adicionais.</p>
	Usuários	A página Usuários configura os perfis de login do IMM2 e as configurações de login global. Também é possível visualizar as contas do usuário que estão atualmente com login efetuado no IMM2. As configurações de login global incluem a ativação da autenticação do servidor Lightweight Directory Access Protocol (LDAP), a configuração do tempo limite de inatividade da web e a customização das configurações de segurança da conta. Consulte “Configurando Contas de Usuário” na página 62 para obter informações adicionais.

Tabela 1. Ações do IMM2 (continuação)

Guia	Seleção	Descrição
Gerenciamento do IMM <i>(continuação)</i>	Rede	<p>A página Propriedades do Protocolo de Rede fornece acesso a propriedades de rede, status e configurações do IMM2:</p> <ul style="list-style-type: none"> • A guia Ethernet gerencia o modo de comunicação do IMM2 usando Ethernet. • A guia SNMP configura os agentes SNMPv1 e SNMPv3. • A guia DNS configura os servidores DNS com os quais o IMM2 interage. • A guia DDNS ativa ou desativa e configura o DNS Dinâmico para o IMM2. • A guia SMTP configura informações do servidor SMTP usadas para alertas enviados por email. • A guia LDAP configura a autenticação do usuário para uso com um ou mais servidores LDAP. • A guia Telnet gerencia o acesso Telnet ao IMM2. • A guia USB controla a interface USB usada para comunicação dentro da banda entre o servidor e o IMM2. Essas configurações não afetam as funções de controle remoto USB (teclado, mouse e armazenamento em massa). • A guia Designações de Portas permite alterar os números de portas usados por alguns serviços no IMM2. <p>Consulte “Configurando protocolos de rede” na página 71 para obter informações adicionais.</p>
	Segurança	<p>A página Segurança do IMM fornece acesso a propriedades de segurança, status e configurações do IMM2:</p> <ul style="list-style-type: none"> • A guia Servidor HTTPS permite ativar ou desativar o servidor HTTPS e gerenciar seus certificados. • A guia CIM sobre HTTPS permite ativar ou desativar o CIM sobre HTTPS e gerenciar seus certificados. • A guia Cliente LDAP permite ativar ou desativar a segurança LDAP e gerenciar seus certificados. • A guia Servidor SSH permite ativar ou desativar o servidor SSH e gerenciar seus certificados. <p>Consulte “Definindo a Configuração de Segurança” na página 85 para obter informações adicionais.</p>
	Configuração do IMM	<p>A página Configuração do IMM exibe um resumo das definições de configuração atuais do IMM2. Consulte “Restaurando e modificando a configuração do IMM” na página 92 para obter informações adicionais.</p>
	Reiniciar IMM	<p>A página Reiniciar o IMM permite reconfigurar o IMM2. Consulte “Reiniciando o IMM2” na página 92 para obter informações adicionais.</p>
	Reconfigurar o IMM com padrões de factory...	<p>A página Reconfigurar o IMM para Padrões de Factory... permite redefinir a configuração do IMM2 com os padrões de factory. Consulte “Reconfigurando o IMM2 para os Padrões de Factory” na página 93 para obter informações adicionais.</p> <p>Atenção: Quando você clica em Reconfigurar o IMM para Padrões de Factory..., todas as modificações feitas no IMM2 são perdidas.</p>
	Gerenciamento de Chaves de Ativação	<p>A página Gerenciamento de Chaves de Ativação permite gerenciar chaves de ativação de recursos Features on Demand (FoD) opcionais do IMM2 ou do servidor. Consulte “Chave de Gerenciamento de Ativação” na página 94 para obter informações adicionais.</p>

Capítulo 3. Visão Geral da Interface com o Usuário da Web do IMM2

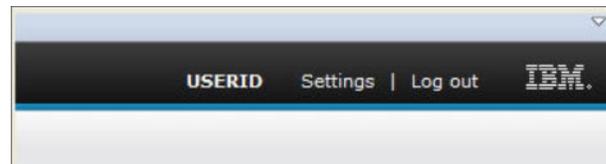
Este capítulo fornece uma visão geral de como usar os recursos da interface com o usuário da web do IMM2.

Importante: Esta seção não se aplica ao IBM BladeCenter e a servidores blade IBM. Embora o IMM2 seja padrão em alguns produtos IBM BladeCenter e servidores blade IBM, o módulo de gerenciamento avançado IBM BladeCenter é o módulo de gerenciamento primário para funções de gerenciamento de sistemas. Os usuários que desejam configurar as definições do IMM2 em servidores blade devem usar o Advanced Settings Utility (ASU) no servidor blade para executar essas ações.

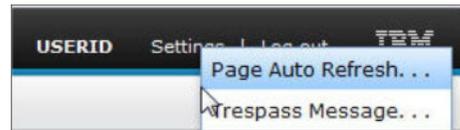
Configurações de Sessão da Web

Esta seção fornece informações sobre as configurações para a página principal de sessão da interface da web.

A página principal do IMM2 exibe as seleções de menu na área superior direita da página da web. Esses itens de menu permitem configurar o comportamento de atualização da página da web e a mensagem que é exibida a um usuário quando ele insere suas credenciais para efetuar login. A ilustração a seguir mostra as seleções de menu na área superior direita da página da web.

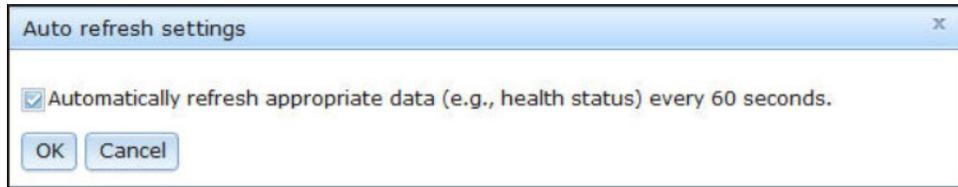


Clique no item **Configurações** e as seleções de menu a seguir são exibidas:



Atualização Automática de Página

Use a opção **Atualização Automática de Página** sob o item de menu Configurações na área superior direita da página de sessão da web para configurar o conteúdo da página para atualizar automaticamente a cada 60 segundos. Para configurar o conteúdo da página para atualizar a cada 60 segundos, marque a caixa de seleção **Atualizar automaticamente os dados apropriados...** e pressione **OK**. Para desativar a atualização automática de página, cancele a seleção da caixa de seleção e pressione **OK**. A ilustração a seguir mostra a janela Configurações de Atualização Automática.



Algumas páginas da web do IMM2 são atualizadas automaticamente, mesmo se a caixa de seleção de atualização automática não estiver selecionada. As páginas da web do IMM2 atualizadas automaticamente são as seguintes:

- **Status do Sistema:**

O status do sistema e de energia é atualizado automaticamente a cada três segundos.

- **Ações de Energia do Servidor:** (sob a guia Gerenciamento do Servidor):

O status de energia é atualizado automaticamente a cada três segundos.

- **Controle Remoto:** (sob a guia Gerenciamento do Servidor):

Os botões Iniciar Controle Remoto... são atualizados automaticamente a cada segundo. A tabela Lista de Sessões é atualizada uma vez a cada 60 segundos.

Notas:

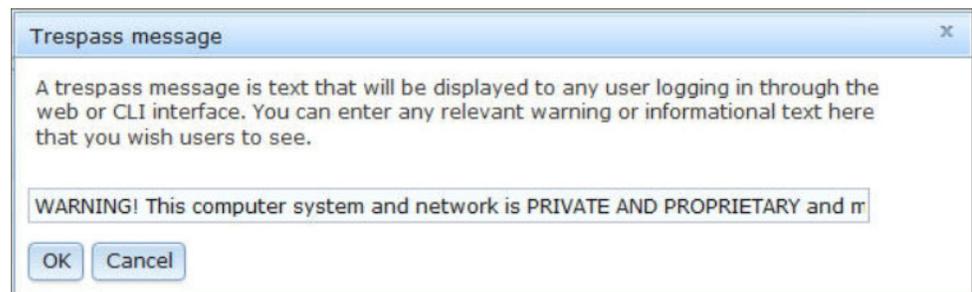
- Se você navegar de seu navegador da web para uma página da web que é atualizada automaticamente, o tempo limite de inatividade não terminará automaticamente a sessão da web.
- Se você enviar uma solicitação a um usuário do Controle Remoto usando a página Opção de Controle Remoto sob Gerenciamento do Servidor, sua sessão da web não atingirá o tempo limite independentemente para qual página da web você navegar até que uma resposta seja recebida do usuário do Controle Remoto ou até que o usuário do Controle Remoto atinja o tempo limite. Quando a solicitação do usuário do Controle Remoto concluir o processamento, a função de tempo limite de inatividade continuará.

Nota: A nota anterior se aplica a todas as páginas da web.

- O firmware do IMM2 suporta até seis sessões da web simultâneas. Para liberar sessões para outros usuários, efetue logout da sessão da web quando tiver concluído, em vez de aguardar o tempo limite de inatividade para fechar automaticamente sua sessão. Se você sair do navegador enquanto em uma página da web do IMM2 que é atualizada automaticamente, sua sessão da web não fechará automaticamente devido à inatividade.

Mensagem de Infração

Use a opção **Mensagem de Infração** sob o item de menu Configurações na área superior direita da página de sessão da web para configurar a mensagem que você deseja que seja exibida quando um usuário efetuar login no servidor IMM2. A tela a seguir é exibida quando você seleciona a opção Mensagem de Infração. Insira o texto da mensagem que você deseja que seja exibido para o usuário no campo fornecido e pressione **OK**.



O texto da mensagem será exibido na área Mensagem da página de login do IMM2 quando um usuário efetua login, conforme mostrado na ilustração a seguir.

Integrated Management Module

User name:

Password:

Inactive session timeout:

Message:
WARNING! This computer system and network is PRIVATE AND PROPRIETARY and may only be accessed by authorized users.

[Log In](#)

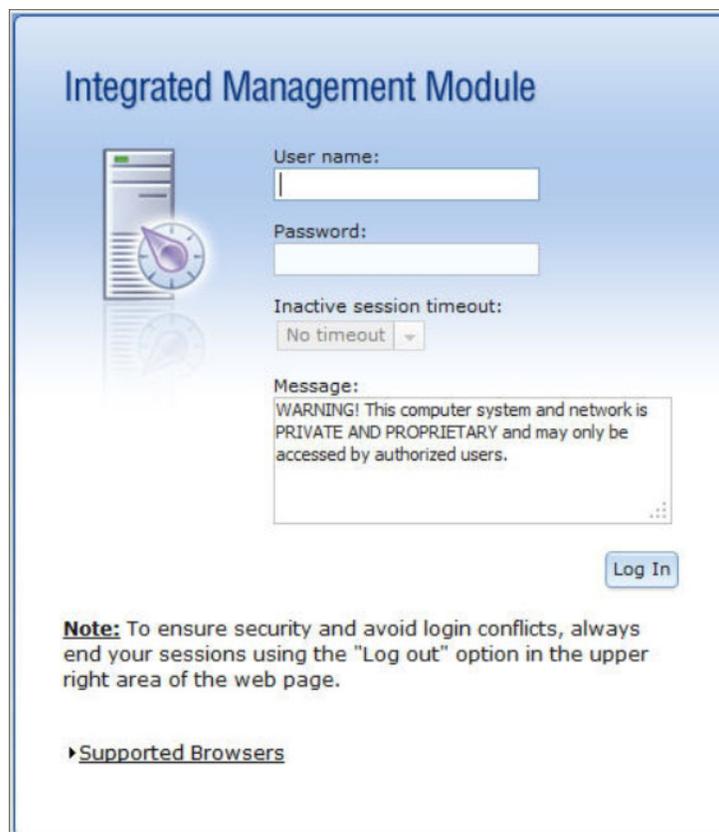
Note: To ensure security and avoid login conflicts, always end your sessions using the "Log out" option in the upper right area of the web page.

[Supported Browsers](#)

Efetuar logout

Para assegurar a segurança, efetua logout da sessão da web do IMM2 quando você tiver concluído e feche manualmente quaisquer outras janelas do navegador da web do IMM2 que possam ter sido abertas.

Para efetuar logout da sessão da web, clique em **Efetuar Logout** na área superior direita da página da web. A janela Login será mostrada.

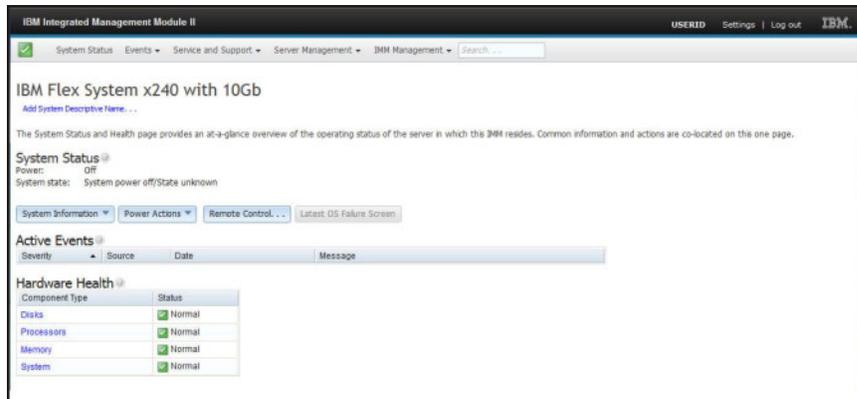


Nota: O firmware do IMM2 suporta até seis sessões da web simultâneas. Para liberar sessões para outros usuários, efetue logout da sessão da web quando tiver concluído, em vez de aguardar o tempo limite de inatividade para fechar automaticamente sua sessão. Se você sair do navegador enquanto em uma página da web do IMM2 que é atualizada automaticamente, sua sessão da web não fechará automaticamente devido à inatividade.

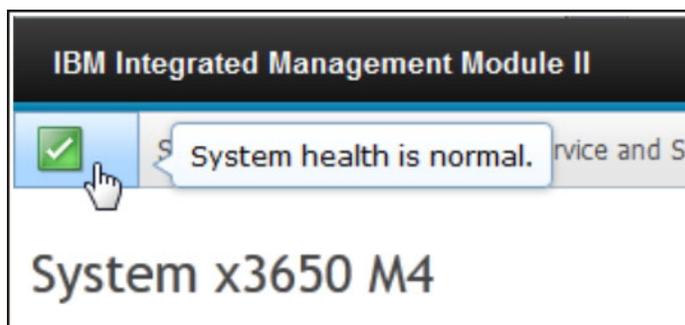
Guia Status do Sistema

Esta seção fornece informações para usar as opções sob a guia Status do Evento na interface com o usuário da web do IMM2.

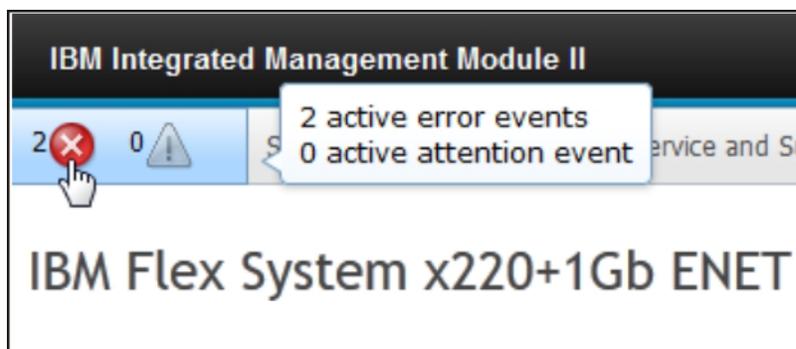
A página Status do Sistema é exibida depois que você efetua login na interface com o usuário da web do IMM2 ou quando clica na guia Status do Sistema. Na página Status do Sistema, é possível visualizar o status do sistema, eventos do sistema ativo e informações de funcionamento de hardware. A exibição a seguir é mostrada quando você clica na guia Status do Sistema ou efetua login na interface da web do IMM2.



É possível clicar no ícone verde (com a marca de seleção) no canto superior esquerdo da página para obter um resumo rápido do funcionamento do servidor. Uma marca de seleção indica que o servidor está operando normalmente.



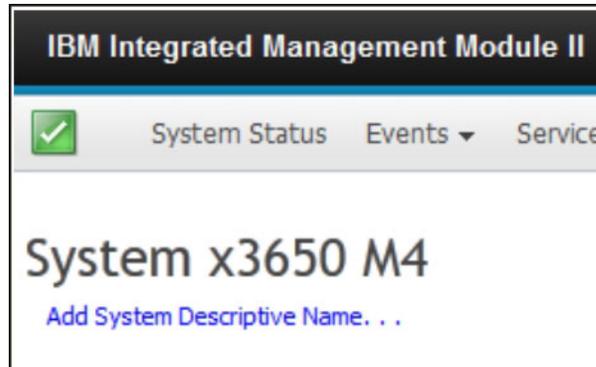
Se um ícone de círculo vermelho ou triângulo amarelo for exibido, isso indica que existe uma condição de erro ou aviso, conforme mostrado na ilustração a seguir.



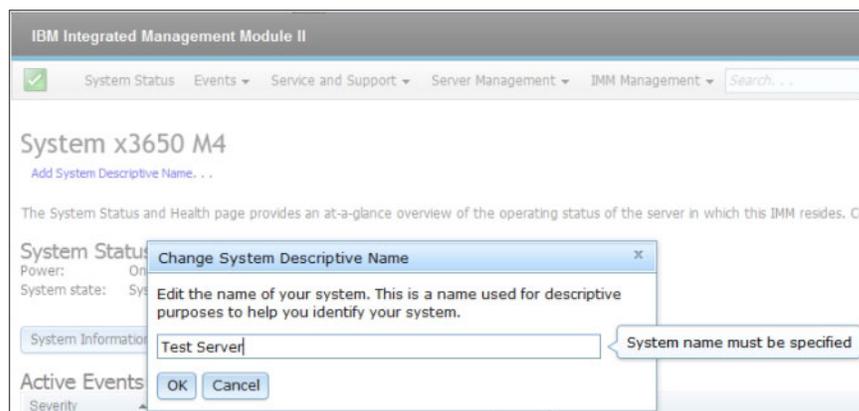
O ícone de círculo vermelho indica que existe uma condição de erro no servidor. Um ícone de triângulo amarelo indica que existe uma condição de aviso. Quando um ícone de círculo vermelho ou um triângulo amarelo é exibido, os eventos associados a essa condição são listados sob a seção Eventos Ativos na página Status do Sistema, conforme mostrado na ilustração a seguir.

Severity	Source	Date	Message
Error	System	16 Jul 2012 01:00:28.000 PM	Sensor Mezz Exp 2 Fault has transitioned to critical from a less severe state.
Error	System	16 Jul 2012 01:00:29.000 PM	Sensor Mezz Exp 2 Fault has transitioned to critical from a less severe state.

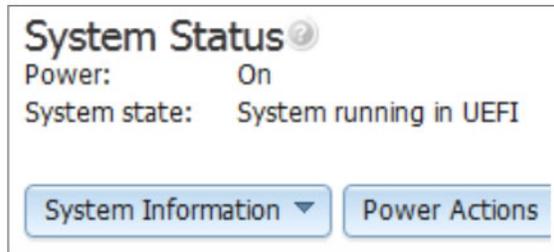
É possível incluir um nome descritivo para o servidor IMM2 para ajudar você a identificar entre um servidor IMM2 e outro. Para designar um nome descritivo ao servidor IMM2, clique no link **Incluir Nome Descritivo do Sistema...** localizado abaixo do nome do produto do servidor.



Ao clicar no link **Incluir Nome Descritivo do Sistema...**, a janela a seguir é exibida para você especificar um nome para associar ao servidor IMM2. É possível alterar o Nome Descritivo do Sistema a qualquer momento.



A seção **Status do Sistema** na página Status do Sistema fornece o estado da energia e o estado da operação do servidor. O status que é exibido é o estado do servidor no momento em que a página Status do Sistema é aberta, (conforme mostrado na ilustração a seguir).



O servidor pode estar em um dos estados a seguir:

Tabela 2. Estados de Energia e de Operação do Servidor

Estado do servidor	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 S.O. ou em S.O. não suportado	O servidor pode estar nesse estado por um dos motivos a seguir: <ul style="list-style-type: none"> • O carregador do sistema operacional foi iniciado mas o sistema operacional não está sendo executado ainda. • A interface Ethernet sobre USB do IMM2 está desativada. • O sistema operacional não possui os drivers carregados que suportam a interface Ethernet sobre USB.
S.O. inicializado	O sistema operacional do servidor está em execução.
Suspender para RAM	O servidor foi colocado no estado de espera ou de suspensão.

A página Status do Sistema também fornece guias para **Informações do Sistema**, **Ações de Energia**, **Controle Remoto** e **Tela de Falha mais Recente do S.O.**



Clique na guia **Informações do Sistema** para visualizar informações sobre o servidor.

Name	Value
Machine Name	System x3650 M4
Machine Type	7915
Model	35Z
Serial Number	06CNZ40
UUID	E596B684B75E11E0A0B0E41F13EB0F72
Server Power	On
Server State	System running in UEFI
Total hours powered-on	117
Restart count	6
Ambient Temperature	80.60 F / 27.00 C
Enclosure Identify LED	Off Change...
Check Log LED	Off

Close

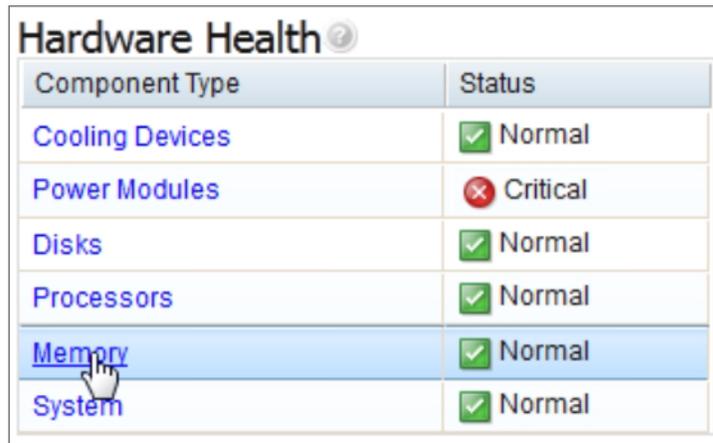
Clique na guia **Ações de Energia** para visualizar as ações que podem ser executadas para controle integral de energia remota sobre o servidor com as ações ligar, desligar e reiniciar. Consulte “Controlando o Status de Energia do Servidor” na página 104 para obter detalhes sobre como controlar remotamente a energia do servidor.

Clique na guia **Controle Remoto** para obter informações sobre como controlar o servidor no nível do sistema operacional. Consulte “Funções de Presença Remota e Controle Remoto” na página 105 para obter detalhes sobre a função Controle Remoto.

Clique na guia **Tela de Falha mais Recente do S.O.** para obter informações sobre como capturar os dados da Tela de Falha mais Recente do S.O. Consulte “Capturando os Dados da Tela de Falha mais Recente do S.O.” na página 132 para obter detalhes sobre a Tela de Falha mais Recente do S.O.

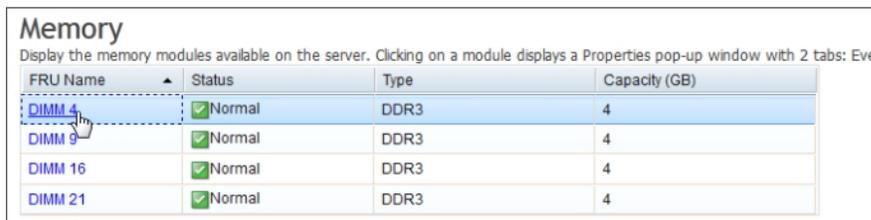
Na seção **Funcionamento do Hardware** da página Status do Sistema, há uma tabela com uma lista dos componentes de hardware que estão sendo monitorados e seu status de funcionamento. O funcionamento que é exibido para um componente pode refletir o estado mais crítico do componente na coluna Tipo de Componente na tabela. Por exemplo, um servidor pode ter vários módulos de energia instalados e todos os módulos de energia estão operando normalmente,

exceto um. O status dos componentes de Módulo de Energia na tabela terão um status de crítico por causa daquele módulo de energia (conforme mostrado na tela a seguir).



Component Type	Status
Cooling Devices	✓ Normal
Power Modules	✗ Critical
Disks	✓ Normal
Processors	✓ Normal
Memory	✓ Normal
System	✓ Normal

Cada tipo de componente é um link que você pode clicar para obter informações mais detalhadas. Quando você clica no tipo de componente, uma tabela listando o status de cada um dos componentes individuais é exibida (conforme mostrado na tela a seguir).



Memory

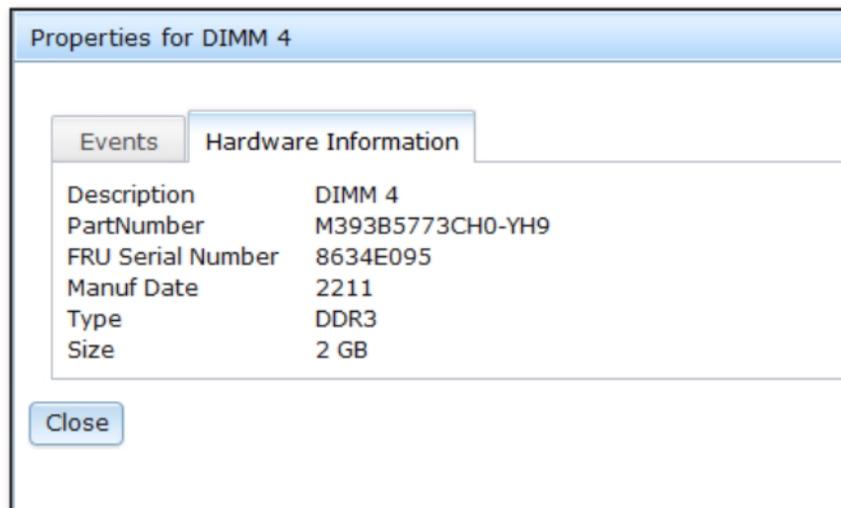
Display the memory modules available on the server. Clicking on a module displays a Properties pop-up window with 2 tabs: Eve

FRU Name	Status	Type	Capacity (GB)
DIMM 4	✓ Normal	DDR3	4
DIMM 9	✓ Normal	DDR3	4
DIMM 16	✓ Normal	DDR3	4
DIMM 21	✓ Normal	DDR3	4

É possível clicar em um componente na coluna Nome da FRU da tabela para obter informações adicionais desse componente. Todos os eventos ativos para o componente serão exibidos.



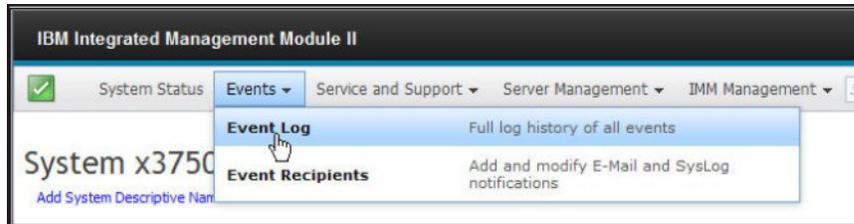
Clique na guia **Informações de Hardware** para obter informações detalhadas sobre o componente.



Guia Eventos

Esta seção fornece informações para usar as opções sob a guia Eventos na interface com o usuário da web do IMM2.

As opções sob a guia **Eventos** permitem gerenciar o histórico de Log de Eventos e gerenciar Destinatários de Eventos para notificações por email e syslog. A ilustração a seguir mostra as opções sob a guia Eventos na página da web do IMM2.



Log de Eventos

Selecione **Log de Eventos** sob a guia Eventos para exibir a página Log de Eventos. A página Log de Eventos mostra a severidade dos eventos que são relatados pelo IMM2, além de informações sobre todas as tentativas de acesso remoto e mudanças na configuração. Todos os eventos no log são registrados com data e hora usando as configurações de data e hora do IMM2. Alguns eventos também gerarão alertas, se estiverem configurados para isso na página Destinatários de Eventos. É possível classificar e filtrar eventos no log de eventos. A seguir está uma ilustração da página Log de Eventos.

Severity	Source	Date	Event ID	Message
Informational	System	31 1 2013 09:02:42.771 AM	0x400000e000000000	Remote Login Successful. Login ID: USERID from webgpus at IP address 9.111.29.57.
Informational	System	31 1 2013 09:01:00.297 AM	0x4000001600000000	ENET[CR] ep1 DHCP-HTTP[882-5cae8b4e83c5, Dhcp.on.ibm.com, IP@=9.186.166.78, Dhcp=255.255.255.126, Gw@=9.186.166.1, Dhc1@=9.0.148.50.
Informational	System	31 1 2013 09:00:58.957 AM	0x4000001900000000	LAN: Ethernet[BI ep2] interface is now active.
Informational	System	31 1 2013 09:00:55.004 AM	0x4000001700000000	ENET[CR] ep2 IP-Cg=169.254.95.118, NetMtu=255.255.0.0, Gw@=0.0.0.0.
Informational	System	31 1 2013 09:00:53.403 AM	0x4000003700000000	ENET[CR] ep1 IP-F-LinkLocal-HostName=882-5cae8b4e83c5, IP@=169.0.5ae8b0ff6ae83c5, Pref=64.
Informational	System	31 1 2013 09:00:51.592 AM	0x4000001900000000	LAN: Ethernet[BI ep1] interface is now active.
Informational	System	31 1 2013 09:00:47.069 AM	0x4000001000000000	Management Controller SNR 09K3N1.9 Network Installation Complete.
Informational	System	31 1 2013 09:00:02.874 AM	0x0080128210111111	Device Low Security Jmp has been added.
Informational	Power	31 1 2013 09:00:02.304 AM	0x0900000913011111	Host Power has been turned off.
Informational	System	31 1 2013 08:55:11.252 AM	0x4000001500000000	Management Controller SNR 09K3N1.9 reset was initiated by user USERID.
Informational	System	31 1 2013 08:47:59.118 AM	0x4000002300000000	Flash of SNR 09K3N1.9 from (9.186.166.119) succeeded for user USERID.
Informational	System	31 1 2013 08:43:15.666 AM	0x400000e000000000	Remote Login Successful. Login ID: USERID from webgpus at IP address 9.186.166.119.
Informational	System	31 1 2013 08:42:42.771 AM	0x400000e000000000	Remote Login Successful. Login ID: USERID from webgpus at IP address 9.111.29.57.

Para classificar e filtrar eventos no log de eventos, selecione o título da coluna (conforme mostrado na ilustração a seguir).

Severity	Source	Date	Event ID	Message
Informational	System	31 Jan 2013 09:11:04:024 AM	0x400000e000000000	Remote Login Successful. Login ID: USERID from webgpus at IP address 9.186.166.119.
Informational	System	31 Jan 2013 09:02:42.771 AM	0x400000e000000000	Remote Login Successful. Login ID: USERID from webgpus at IP address 9.111.29.57.

É possível salvar todos os eventos, ou os eventos selecionados, do log de eventos em um arquivo usando o botão **Exportar**. Para selecionar eventos específicos, escolha um ou mais eventos na página Log de Eventos principal e clique com o botão esquerdo no botão **Exportar** (conforme mostrado na ilustração a seguir).

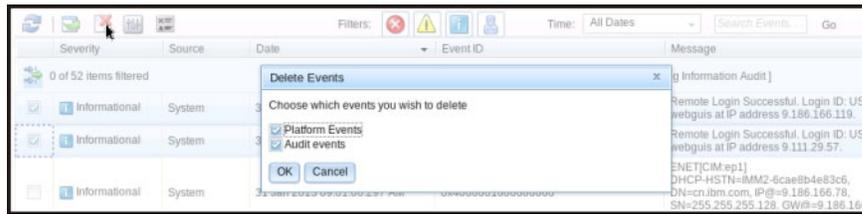
Event Log

This page displays the contents of the IMM event log, and allows you to export the log entries (sorted by severity, then by date, with the most recent entry first). For each log entry, the severity of the event is displayed

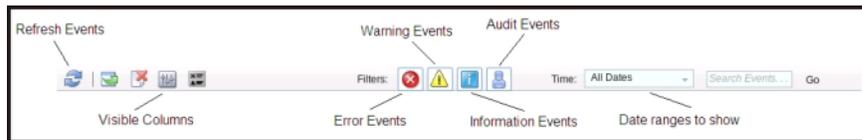
 

	Severity	Source	Date
 0 of 52 items filtered		2 items selected	
<input checked="" type="checkbox"/>	 Informational	System	31 Jan 2013 09:1
<input checked="" type="checkbox"/>	 Informational	System	31 Jan 2013 09:0

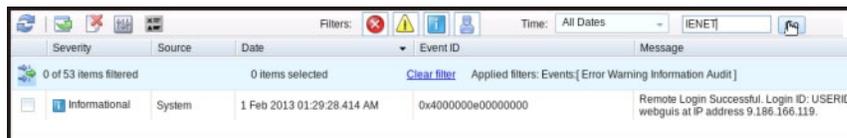
Use o botão **Excluir Eventos** para escolher o tipo de evento que você deseja excluir (conforme mostrado na ilustração a seguir).



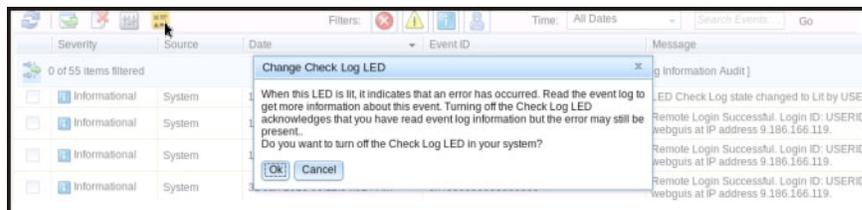
Para selecionar o tipo de entrada de log de eventos que você deseja que seja exibido, clique no botão apropriado (conforme mostrado na ilustração a seguir).



Para procurar tipos específicos de eventos ou palavras-chave, digite o tipo de evento ou palavra-chave na caixa **Procurar Eventos**; em seguida, clique em **Ir** (conforme mostrado na ilustração a seguir).



Para desligar o LED Verificar Log quando ele estiver ligado e os Logs de Eventos relacionados tiverem sido selecionados, clique no botão **Status do LED Verificar Log** (conforme mostrado na ilustração a seguir).

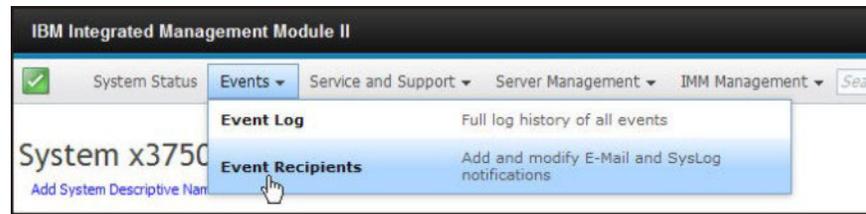


Na barra de ferramentas do Log de Eventos, é possível clicar em qualquer um dos botões **Eventos de Filtro** para selecionar os eventos a serem exibidos. Para limpar o filtro e mostrar todos os tipos de eventos, clique no link **Limpar Filtro** mostrado na ilustração a seguir.



Destinatários de Eventos

Use a opção **Destinatários de Eventos** sob a guia **Eventos** para incluir e modificar notificações por email e syslog.

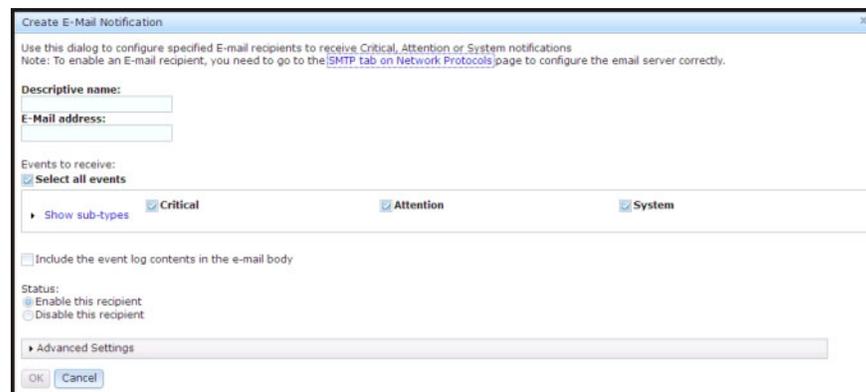


A opção Destinatários de Eventos permite gerenciar quem será notificado sobre eventos do sistema. É possível configurar cada destinatário e gerenciar as configurações que se aplicam a todos os destinatários de eventos. Também é possível gerar um evento de teste para verificar o recurso de notificação.

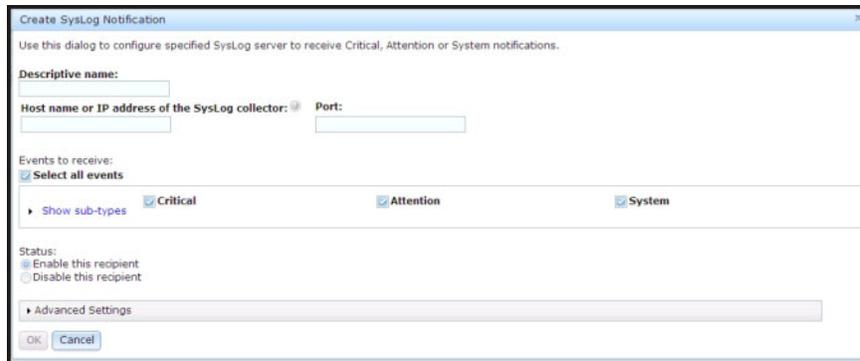
Clique no botão **Criar** para criar notificações por email e syslog.



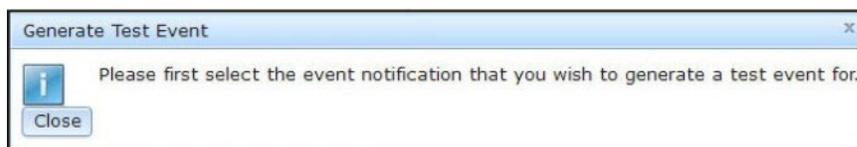
Selecione a opção **Criar Notificação por Email** para configurar um endereço de email de destino e escolha o tipo de evento sobre o qual você deseja ser notificado. Além disso, é possível clicar em **Configurações Avançadas** para selecionar o número de índice inicial. Para incluir o log de eventos no email, marque a caixa de seleção **Incluir o conteúdo do log de eventos no corpo do email**. A seguir está uma ilustração da janela Criar Notificação por Email:



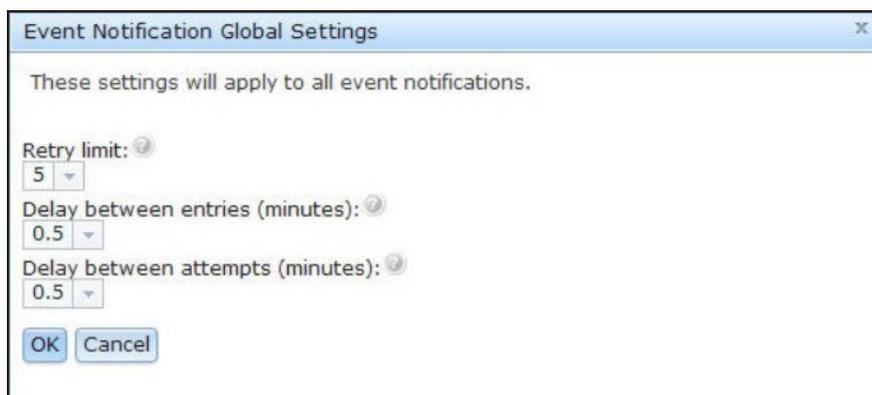
Selecione a opção **Criar Notificação por SysLog** para configurar o Nome do Host ou Endereço IP para o coletor do SysLog e escolha o tipo de evento sobre o qual você deseja ser notificado. Além disso, é possível clicar em **Configurações Avançadas** para selecionar o número de índice inicial. Também é possível especificar a porta que você deseja usar para este tipo de notificação. A seguir está uma ilustração da janela Criar Notificação por SysLog:



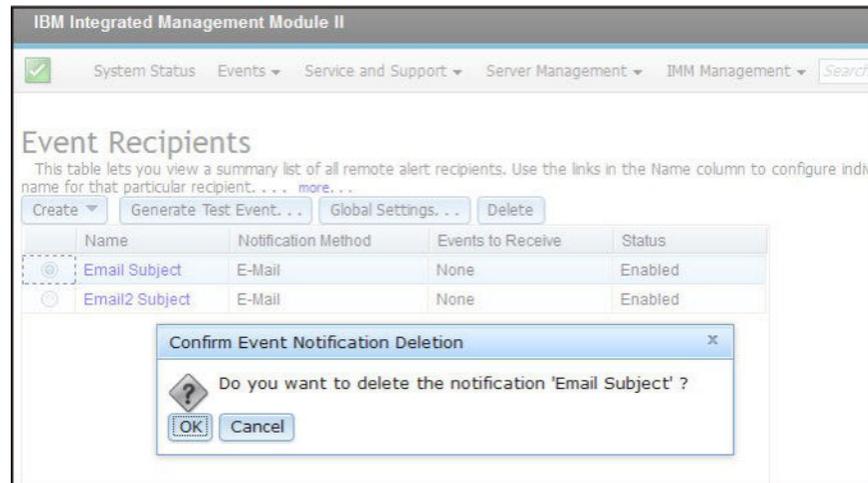
Selecione o botão **Gerar Evento de Teste** para enviar um email de teste para um destino de email selecionado (conforme mostrado na ilustração a seguir).



Selecione o botão **Configurações Globais** para configurar um limite para tentar novamente a notificação de eventos, o atraso (em minutos) entre as entradas de notificação de eventos e o atraso (em minutos) entre as tentativas (conforme mostrado na ilustração a seguir).



Se você deseja remover um destino de notificação por email ou syslog, selecione o botão **Excluir**. A janela a seguir é aberta:

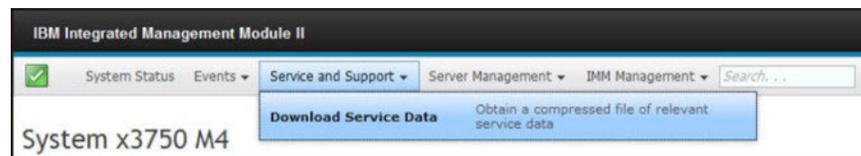


Guia Serviço e Suporte

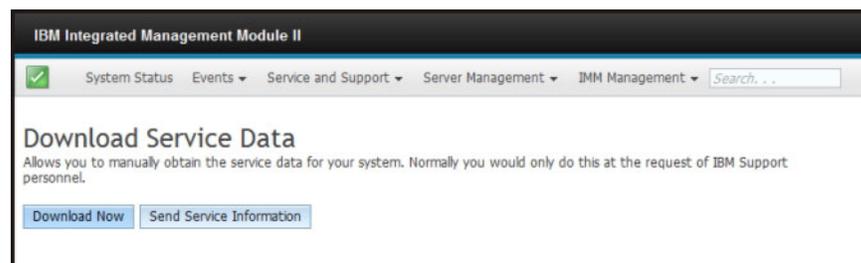
Esta seção fornece informações para usar as opções sob a Serviço e Suporte na página da interface com o usuário da web do IMM2.

Fazer o Download de Dados de Serviço

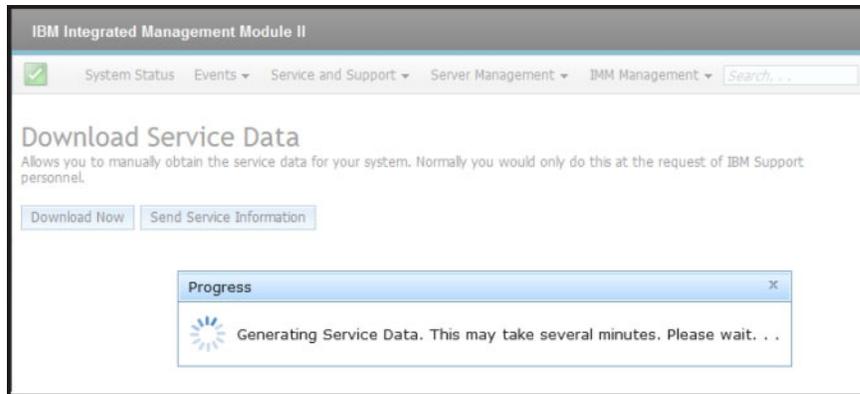
Use a opção **Fazer o Download de Dados de Serviço** sob a guia Serviço e Suporte para coletar informações e criar um arquivo compactado sobre o servidor que pode ser enviado ao Suporte IBM para ajudar na determinação de problemas.



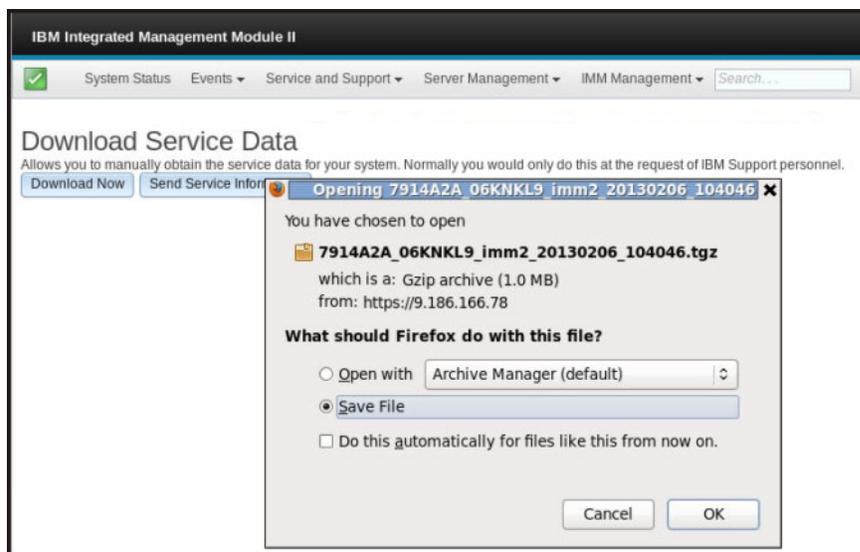
Clique no botão **Fazer o Download Agora** para fazer o download de dados de serviço e suporte (conforme mostrado na ilustração a seguir).



O processo para coletar os dados é iniciado. O processo demora alguns minutos para gerar os dados de serviço que, então, podem ser salvos em um arquivo. Uma janela de progresso é exibida indicando que os dados estão sendo gerados.



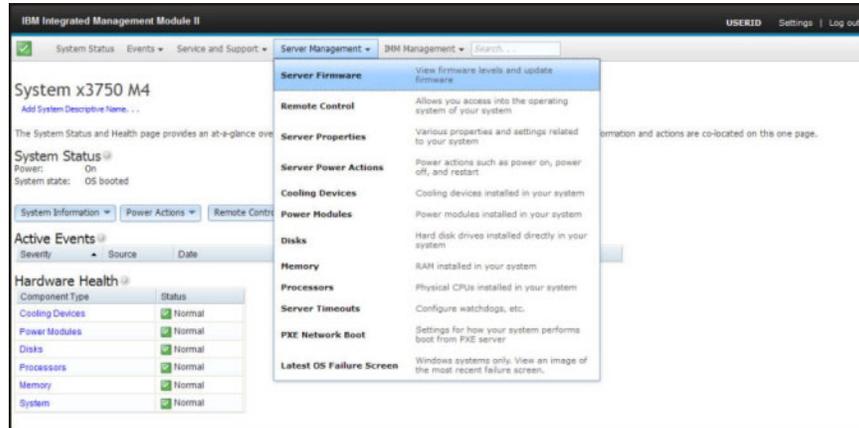
Quando o processo for concluído, a janela a seguir será exibida solicitando a você o local para salvar o arquivo gerado.



Guia Gerenciamento do Servidor

Esta seção fornece informações sobre as opções na guia Gerenciamento do Servidor na página inicial da interface com o usuário da web do IMM2.

As opções na guia Gerenciamento do Servidor permitem visualizar informações sobre o status e controle do firmware do servidor, acesso ao controle remoto, status e controle de propriedades do servidor, ações de energia do servidor, dispositivos de resfriamento, módulos de energia, discos, memória, processadores, tempos limites do servidor, inicialização da rede PXE e tela de falha mais recente do S.O. (conforme mostrado na ilustração a seguir).



Firmware do Servidor

Selecione a opção **Firmware do Servidor** na guia Gerenciamento do Servidor para visualizar os níveis de firmware que estão instalados no servidor e para aplicar as atualizações de firmware. A ilustração a seguir exibe os níveis de firmware do servidor e permite atualizar o firmware do DSA, IMM2 e UEFI.

Firmware Type	Status	Version	Build	Release Date
DSA	Active	9.24	DSYT44B	2012-08-10
IMM2				
IMM2 (Primary)	Active	2.15	140039Q	2013-01-28
IMM2 (Backup)	Inactive	3.00	140038T	2013-01-30
UEFI				
UEFI (Primary)	Active	1.20	O7E120CUS	2012-08-23
UEFI (Backup)	Inactive	1.20	O7E120CUS	2012-08-23

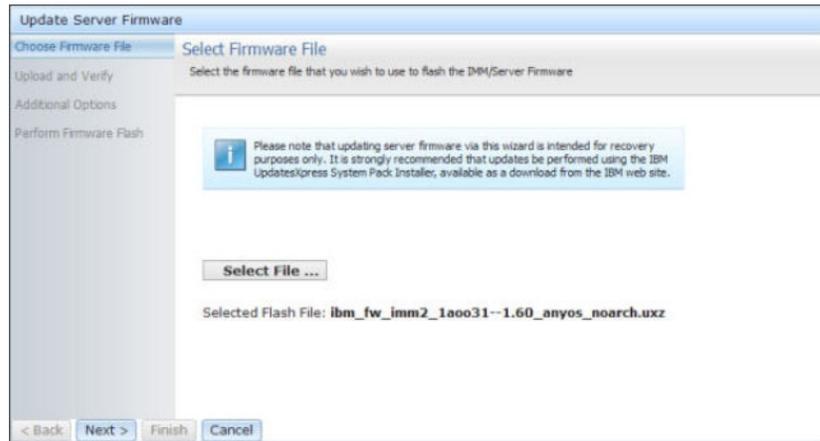
O status e as versões atuais de firmware para o IMM2, UEFI e DSA são exibidos, incluindo as versões primária e de backup. Há três categorias para o status de firmware:

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

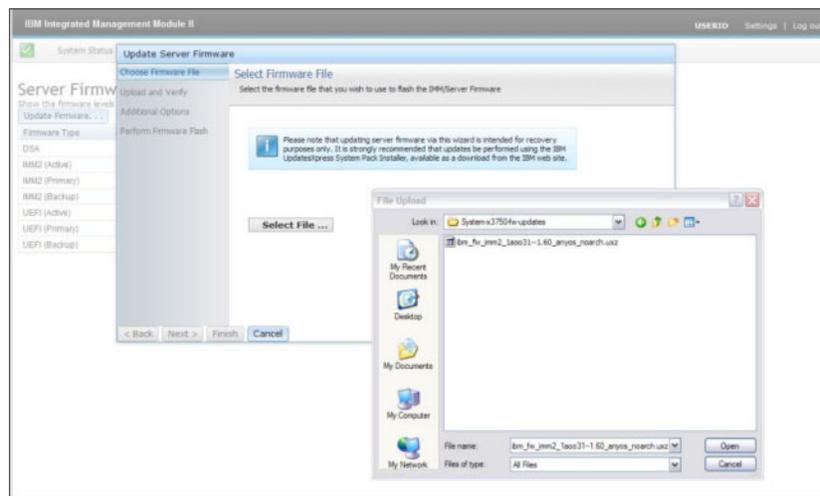
Atenção: A instalação da atualização de firmware errada pode causar mau funcionamento do servidor. Antes de instalar uma atualização de firmware ou de driver de dispositivo, leia quaisquer arquivos leia-me e de histórico de mudanças que são fornecidos com a atualização transferida por download. Esses arquivos contêm informações importantes sobre a atualização e o procedimento para instalar a atualização, incluindo qualquer procedimento especial para atualizar a partir de uma versão de firmware ou de driver de dispositivo anterior para a versão mais recente.

Para atualizar o firmware, selecione o botão **Atualizar Firmware...** A janela Atualizar Firmware do Servidor é exibida. É possível clicar em **Cancelar** e retornar à janela Firmware do Servidor anterior ou clicar no botão **Selecionar Arquivo...** para selecionar o arquivo de firmware que você deseja usar para atualizar o firmware do servidor.

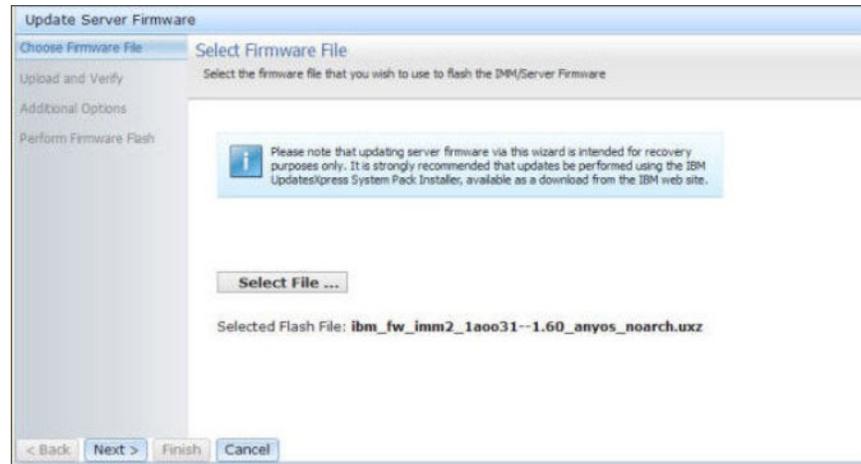
Nota: Antes de clicar no botão **Selecionar Arquivo...**, leia o aviso exibido no prompt da janela antes de continuar.



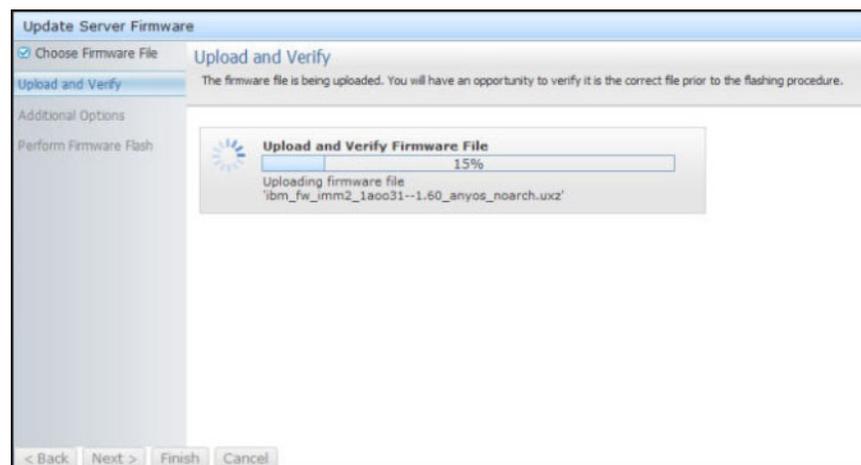
Quando você clica no botão **Selecionar Arquivo...**, a janela Upload de Arquivo é exibida, que permite procurar o arquivo desejado.



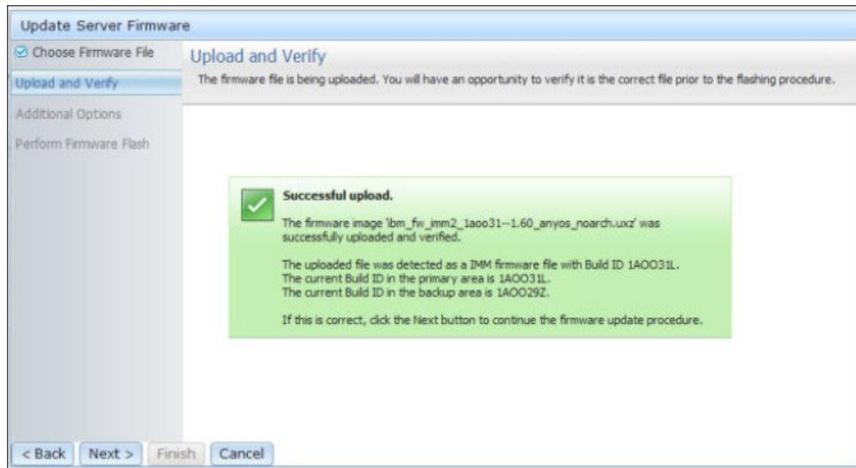
Depois de navegar para o arquivo que você deseja selecionar, clique no botão **Abrir**, você é retornado para a janela Atualizar Firmware do Servidor com o arquivo selecionado exibido (conforme mostrado na ilustração a seguir).



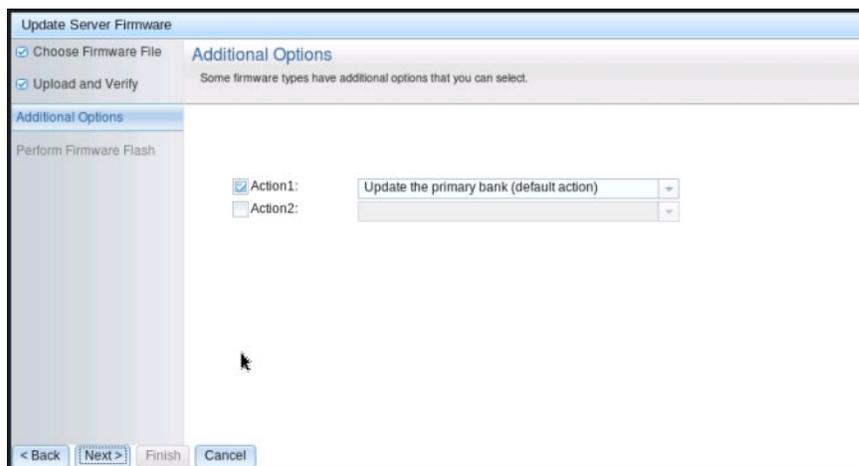
Clique no botão **Avançar >** para iniciar o upload e verificar o processo no arquivo selecionado (conforme mostrado na ilustração a seguir). Um medidor de progresso será exibido enquanto o arquivo estiver sendo transferido por upload e verificado.



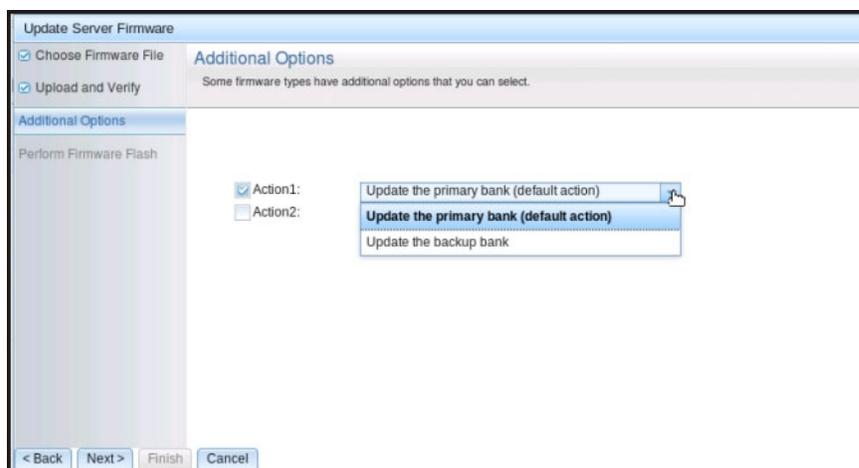
Uma janela de status aparece (conforme mostrado na ilustração a seguir) para que seja possível verificar se o arquivo selecionado para atualização é o arquivo correto. A janela terá informações sobre o tipo de arquivo de firmware que deve ser atualizado, como DSA, IMM2 ou UEFI. Se as informações estiverem corretas, clique no botão **Avançar >**. Se você desejar refazer qualquer uma das seleções, clique no botão **< Voltar**.



Quando você clica no botão Avançar >, um conjunto de opções adicionais é exibido conforme mostrado na ilustração a seguir.



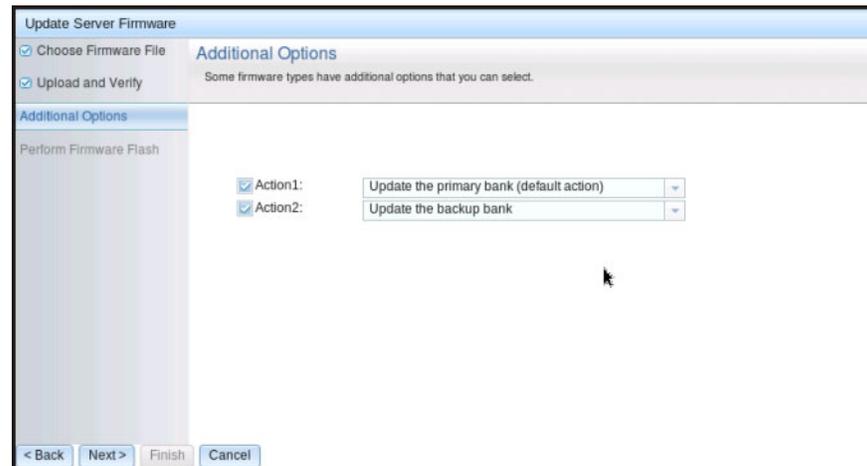
O menu suspenso ao lado de **Ação 1** (mostrado na ilustração a seguir) fornece a opção para **Atualizar o Banco Primário (ação padrão)** ou **Atualizar o Banco de Backup**.



Depois de selecionar uma ação, você é retornado à janela anterior para permitir ações adicionais clicando na caixa de seleção **Ação 2**.

Quando a ação é carregada, a ação selecionada e um novo menu suspenso **Ação 2** são exibidos (conforme mostrado na ilustração a seguir).

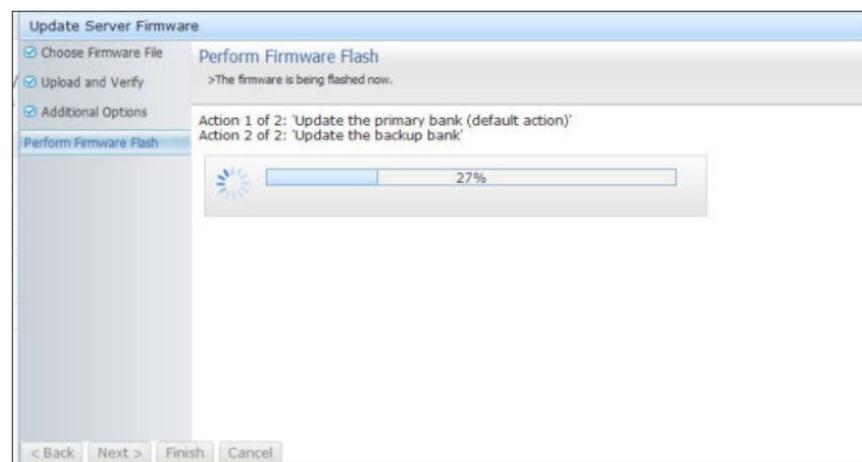
Nota: Para desativar uma ação, clique na caixa de seleção ao lado da ação relacionada.



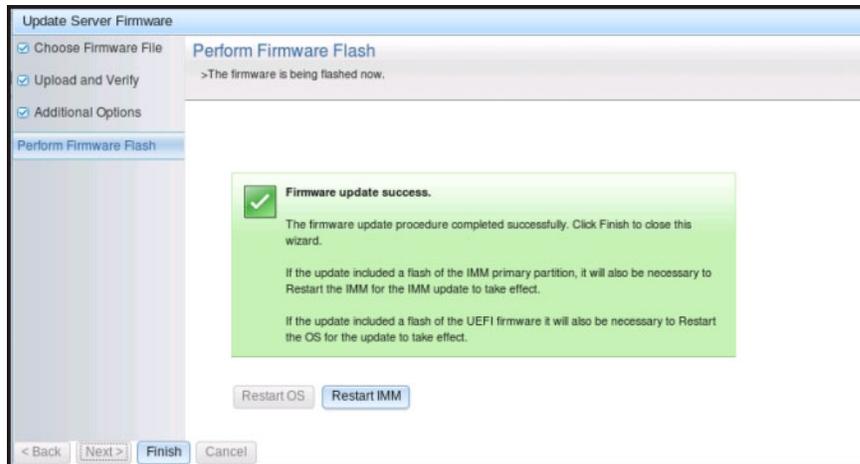
A tela anterior mostra que para a Ação 1, o banco primário é selecionado para ser atualizado. Também é possível selecionar atualizar o banco de backup sob Ação 2 (conforme mostrado na janela anterior). Tanto o banco primário como o banco de backup serão atualizados ao mesmo tempo quando você clicar em **Avançar >**.

Nota: A Ação 1 deve ser diferente da Ação 2.

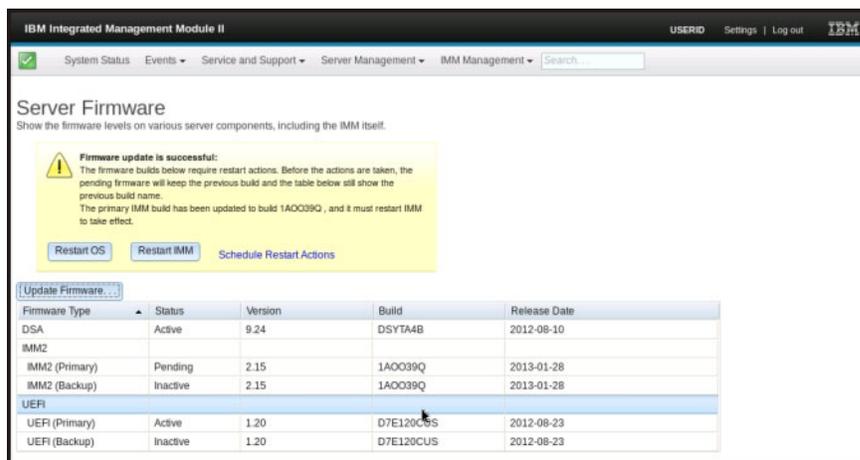
É exibido um medidor de progresso que mostra o progresso da atualização de firmware (conforme mostrado na ilustração a seguir).



Quando a atualização de firmware é concluída com êxito, a janela a seguir é aberta. Selecione a operação relacionada de acordo com o conteúdo exibido para concluir o processo de atualização.



Se a atualização de firmware primária não foi concluída, a janela a seguir será aberta.



Controle remoto

Esta seção fornece informações sobre o recurso de controle remoto.

O cliente ActiveX e o cliente Java são consoles remotos gráficos que permitem visualizar remotamente a exibição de vídeo do servidor e interagir com ela usando o teclado e o mouse do cliente.

Notas:

- O cliente ActiveX está disponível apenas com o navegador Internet Explorer.
- Para usar o cliente Java, o Java Plug-in 1.5 ou liberação mais recente é necessário.
- O cliente Java é compatível com o IBM Java 6 SR9 FP2 ou liberação mais recente.

O recurso de controle remoto consiste em duas janelas separadas:

- **Visualizador de Vídeo**

A janela Visualizador de Vídeo usa um console remoto para gerenciamento de sistemas remotos. Um console remoto é uma exibição interativa da interface gráfica com o usuário (GUI) do servidor visualizada em seu computador. Seu monitor exibe exatamente o que está no console do servidor e você tem o controle do teclado e mouse do console.

- **Sessão de Mídia Virtual**

A janela Sessão de Mídia Virtual lista todas as unidades no cliente que podem ser mapeadas como unidades remotas e permite mapear arquivos de imagem de disquete e ISO como unidades virtuais. Cada unidade mapeada pode ser marcada como somente leitura. As unidades de CD, DVD e as imagens ISO são sempre somente leitura. A janela Sessão de Mídia Virtual é acessada a partir da barra de menus Ferramentas da janela Visualizador de Vídeo.

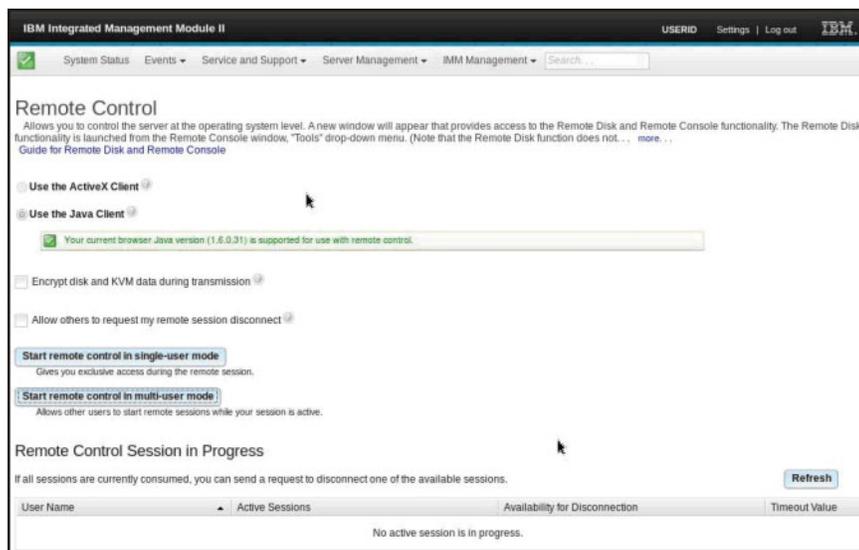
Notas:

- A Sessão de Mídia Virtual só pode ser usada por um cliente de sessão de controle remoto por vez.
- Se o cliente ActiveX for usado, uma janela-pai será aberta e essa janela deverá permanecer aberta até que a sessão remota esteja concluída.

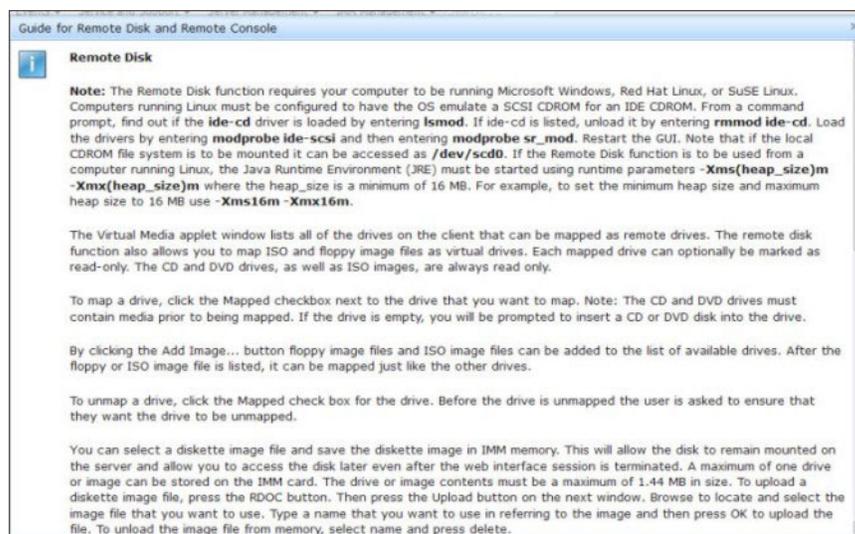
Para acessar remotamente um console do servidor, conclua as etapas a seguir:

1. Efetue login no IMM2, (consulte “Efetuando Login no IMM2” na página 10 para obter informações adicionais).
2. Acesse a página Controle Remoto selecionando uma das opções de menu a seguir:
 - Clique em **Controle Remoto** na guia Gerenciamento do Servidor.
 - Clique em **Controle Remoto...** na página Status do Sistema.

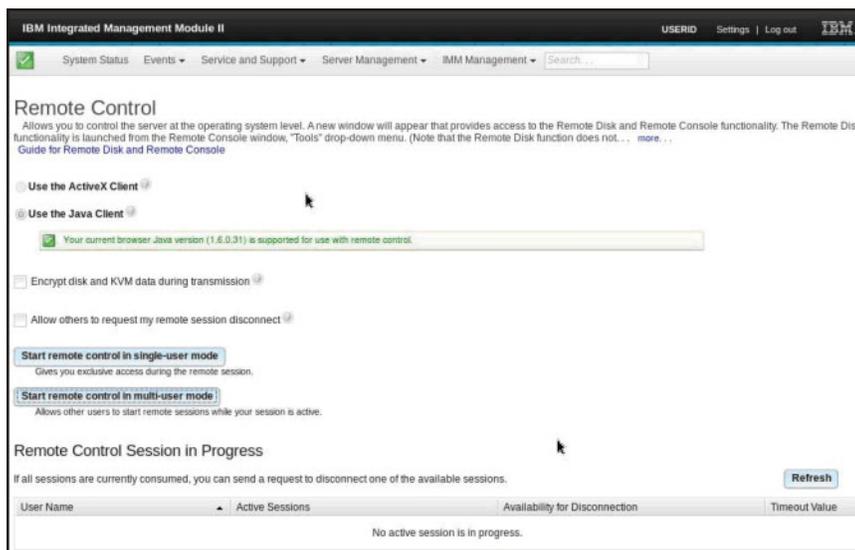
A página Controle Remoto é aberta conforme mostrado na ilustração a seguir.



3. É possível clicar no link **Guia para Disco Remoto e Console Remoto** para acessar informações adicionais. A ilustração a seguir mostra a janela Guia para Disco Remoto e Console Remoto.



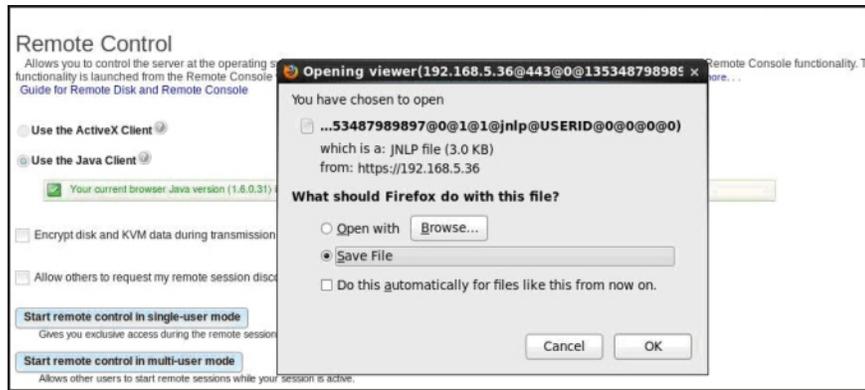
- a. Clique em **Fechar** para sair da janela Guia para Disco Remoto e Console Remoto.
4. Selecione uma das opções gráficas do console remoto a seguir:
 - Para usar o Internet Explorer como seu navegador, selecione **Usar o Cliente ActiveX**.
 - Para usar o cliente Java, selecione **Usar o Cliente Java** conforme mostrado na ilustração a seguir.



Notas:

- Se você não estiver usando o navegador Internet Explorer, apenas o cliente Java pode ser selecionado.
- Os clientes ActiveX e Java possuem funcionalidade idêntica.
- Uma linha de status será exibida indicando se o cliente é suportado.

A seguinte janela é aberta. Ela mostra as informações que o navegador (por exemplo, o navegador Firefox) usará para abrir o arquivo do Visualizador.



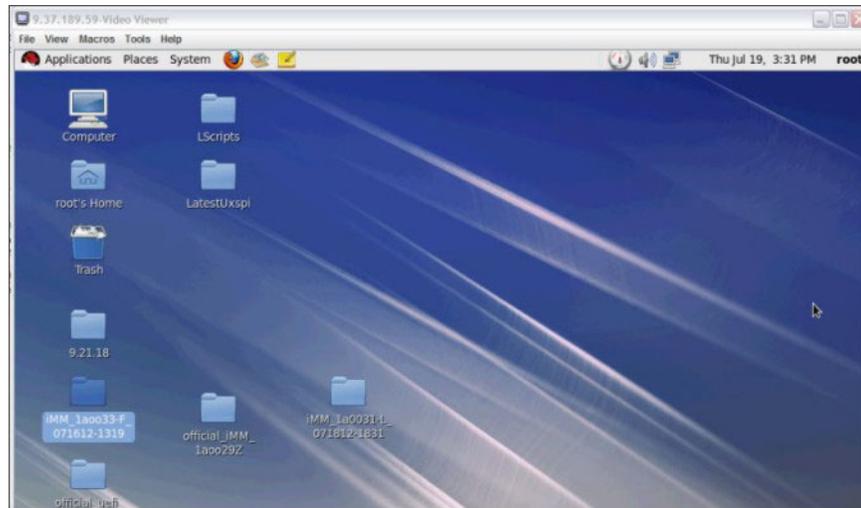
5. Depois que o navegador faz o download e abre o arquivo do Visualizador, uma janela de confirmação é aberta com um aviso sobre a verificação do certificado do website (conforme mostrado na ilustração a seguir). Clique em **Sim** para aceitar o certificado.



6. Para controlar o servidor remotamente, selecione uma das opções de menu a seguir:
 - Para ter acesso remoto exclusivo durante sua sessão, clique em **Iniciar Controle Remoto no Modo de Usuário Único**.
 - Para permitir que outros tenham acesso ao console remoto durante sua sessão, clique em **Iniciar Controle Remoto no Modo de Multiusuário**.

Nota: Se a caixa de seleção **Criptografar dados do disco e do KVM durante a transmissão** for marcada antes que a janela Visualizador de Vídeo seja aberta, os dados do disco serão criptografados com a criptografia ADES durante a sessão.

A janela Visualizador de Vídeo é aberta (conforme mostrado na ilustração a seguir). Essa janela fornece acesso à funcionalidade do Console Remoto.



7. Feche as janelas Visualizador de Vídeo e Sessão de Mídia Virtual quando você tiver concluído o uso do recurso Controle Remoto.

Notas:

- O Visualizador de Vídeo fechará automaticamente a janela Sessão de Mídia Virtual.
- *Não* feche a janela Sessão de Mídia Virtual se um disco remoto estiver atualmente mapeado. Consulte “Disco Remoto” na página 115 para obter instruções sobre como fechar e remover o mapeamento de um disco remoto.
- Se você tiver problemas com mouse ou teclado ao usar a funcionalidade de controle remoto, consulte a ajuda que está disponível na página Controle Remoto na interface da web.
- Se você usar o console remoto para alterar configurações do IMM2 no programa utilitário de Configuração, o servidor poderá reiniciar o IMM2. Você perderá o console remoto e a sessão de login. Depois de um curto atraso, é possível efetuar login no IMM2 novamente com uma nova sessão, iniciar o console remoto novamente e sair do programa utilitário de Configuração.

Importante: O IMM2 usa um applet Java ou ActiveX para executar a função de presença remota. Quando o IMM2 é atualizado para o nível de firmware mais recente, os applets Java e ActiveX também são atualizados para o nível mais recente. Por padrão, o Java armazena em cache (armazena localmente) os applets que foram usados anteriormente. Após uma atualização flash do firmware do IMM2, o applet Java que o servidor usa pode não estar no nível mais recente.

Para corrigir esse problema, desative o armazenamento em cache. O método usado varia com base na plataforma e na versão Java. As etapas a seguir são para Oracle Java 1.5 no Windows:

1. Clique em **Iniciar** → **Configurações** → **Painel de Controle**.
2. Clique duas vezes em **Java Plug-in 1.5**. A janela Painel de Controle do Plug-in Java é aberta.
3. Clique na guia **Cache**.
4. Escolha uma das opções a seguir:
 - Desmarque a caixa de seleção **Ativar Armazenamento em Cache** para que o armazenamento em cache Java esteja sempre desativado.

- Clique em **Limpar Armazenamento em Cache**. Se você escolher essa opção, deverá clicar em **Limpar Armazenamento em Cache** após cada atualização de firmware do IMM2.

Para obter informações adicionais sobre como atualizar o firmware do IMM2, consulte “Atualizando o Firmware do Servidor” na página 118.

Para obter informações adicionais sobre o recurso de controle remoto, consulte “Funções de Presença Remota e Controle Remoto” na página 105.

Propriedades do Servidor

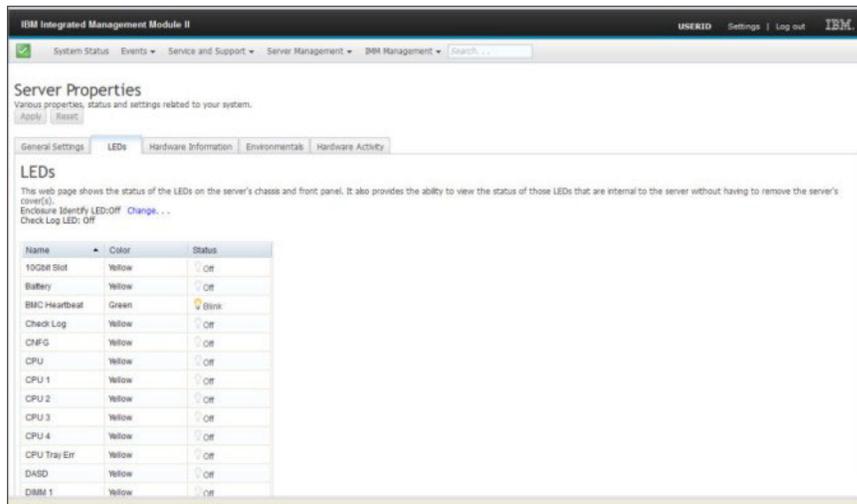
Selecione a opção **Propriedades do Servidor** sob a guia Gerenciamento do Servidor e a janela a seguir aparecerá. Essa opção permite configurar vários parâmetros para ajudar a identificar o sistema. Isso inclui um nome descritivo, pessoa de contato, local e assim por diante. As informações inseridas nesses campos entrarão em vigor quando você clicar em **Aplicar**. Para limpar as informações que foram digitadas nos campos de a última vez que você aplicou mudanças, clique em **Reconfigurar**.

The screenshot shows the 'Server Properties' page in the IBM IMM2 interface. The 'General Settings' tab is active. The page contains several input fields for system identification: 'System descriptive name', 'Contact person', 'Location (site, geographical coordinates, etc.)', 'Room ID', 'Rack ID', and 'Lowest unit of system'. The 'Lowest unit of system' field is currently set to 'N/A'. There are 'Apply' and 'Reset' buttons at the top of the form area.

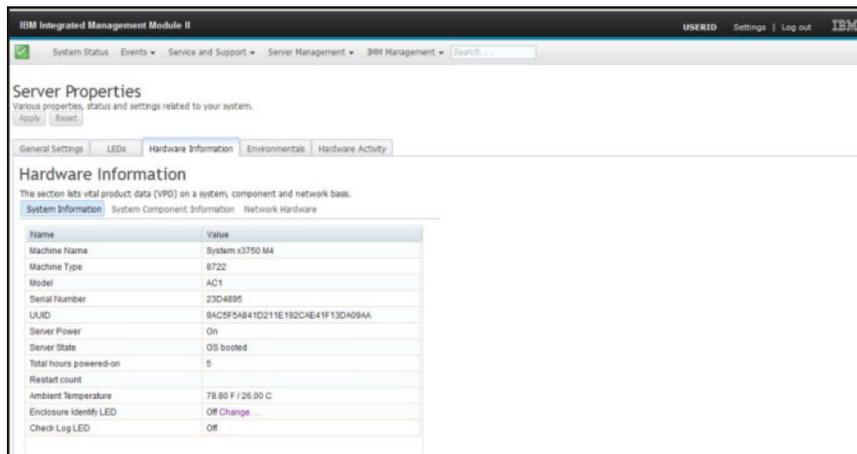
Na ilustração a seguir, é possível especificar a **Menor Unidade do Sistema**. O campo **Menor unidade do sistema** requer uma conexão com o módulo de gerenciamento (por exemplo, o Advanced Management Module ou CMM).

This screenshot is similar to the previous one but shows the 'Lowest unit of system' dropdown menu expanded. The menu lists options from 1 to 7, with 'N/A' selected at the top. The 'Apply' and 'Reset' buttons are still visible at the top of the form.

Para visualizar os LEDs no sistema, clique na guia **LED**. A seguinte janela é aberta.

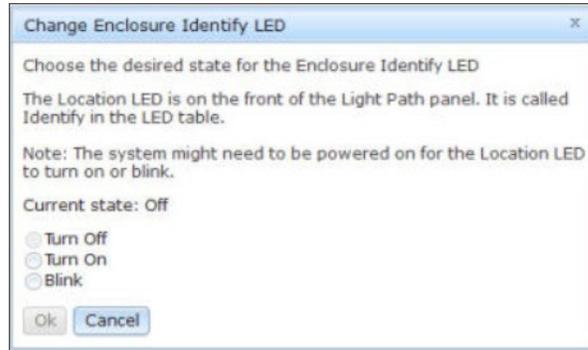


Para visualizar informações do sistema, informações de componentes do sistema e informações do hardware de rede, clique na guia **Informações do Hardware**. Selecione a guia apropriada na guia Informações do Hardware para visualizar várias informações de VPD. A guia **Informações do Sistema** fornece informações como o nome da máquina, número de série e modelo. A ilustração a seguir mostra a janela Informações do Sistema.

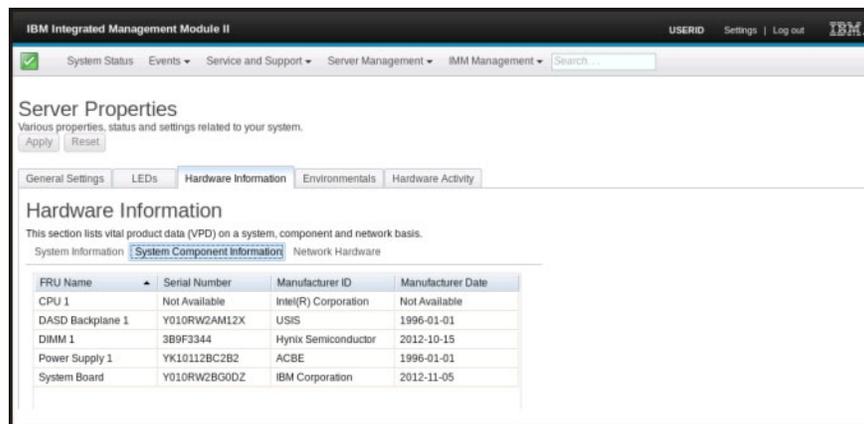


O status do **LED de Identificação de Gabinete** pode ser visualizado e alterado na janela Informações do Sistema. Para alterar o **LED de Identificação de Gabinete**, clique no link **Alterar....** A seguinte janela é aberta.

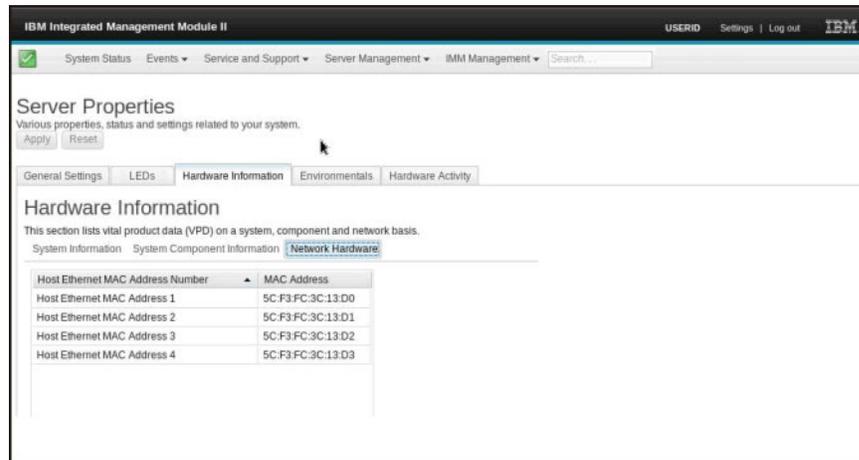
Nota: O LED de Identidade do Gabinete está na parte frontal do painel de Indicadores Luminosos.



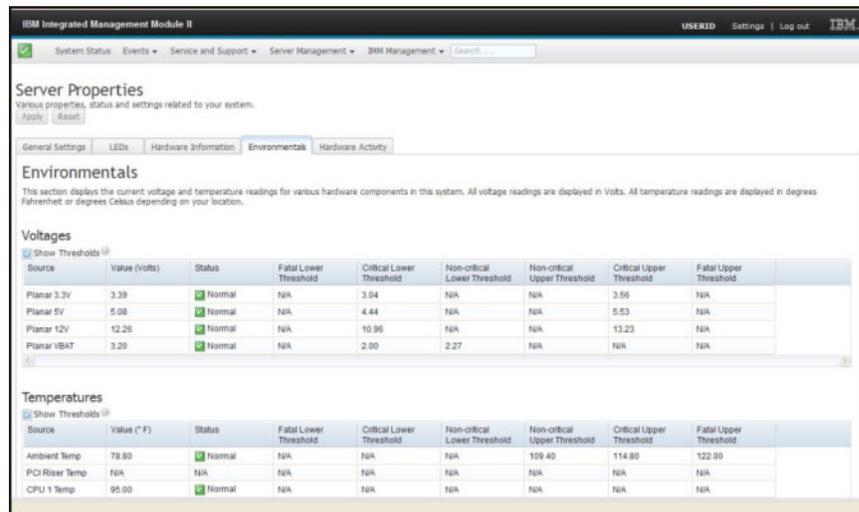
Selecione a guia **Informações de Componentes do Sistema** para visualizar informações de componentes. As informações de componentes incluem o Nome de FRU, Número de Série, ID de Fabricante e Data do Fabricante. A ilustração a seguir mostra as informações que você verá quando clicar na guia **Informações de Componentes do Sistema**.



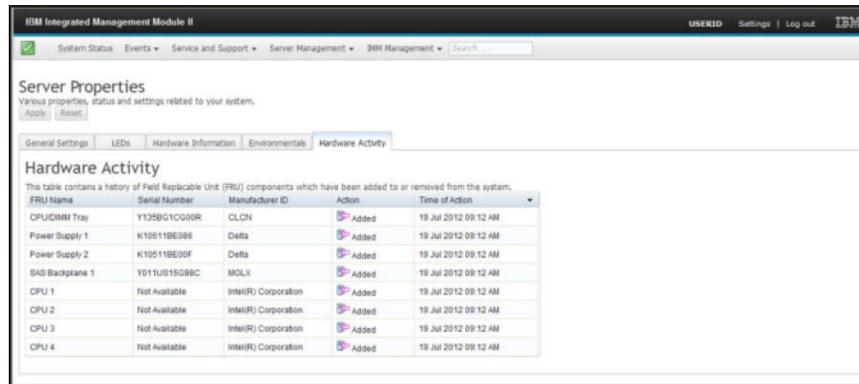
Selecione a guia **Hardware de Rede** para visualizar as informações de hardware de rede. As informações de hardware de rede incluem o Número do Endereço MAC Ethernet do Host e o Endereço MAC. A ilustração a seguir mostra as informações que você verá quando clicar na guia Hardware de Rede.



Selecione a guia **Ambientes** na página Propriedades do Servidor para visualizar as voltagens e temperaturas dos componentes de hardware no sistema. A seguinte janela é aberta. A coluna **Status** na tabela mostra as áreas de atividade normal ou de problema no servidor.



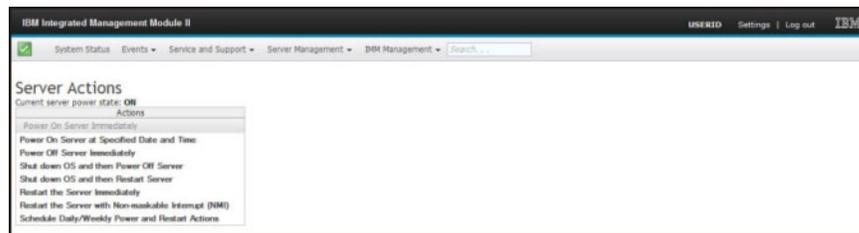
A guia **Atividade de Hardware** na página Propriedades do Servidor fornece um histórico do hardware que foi incluído ou removido do sistema. A ilustração a seguir mostra as informações que você verá quando clicar na guia Atividade de Hardware.



Ações de Energia do Servidor

Esta seção fornece informações sobre a opção Ações de Energia do Servidor sob a guia Gerenciamento do Servidor na página inicial da interface da web do IMM2.

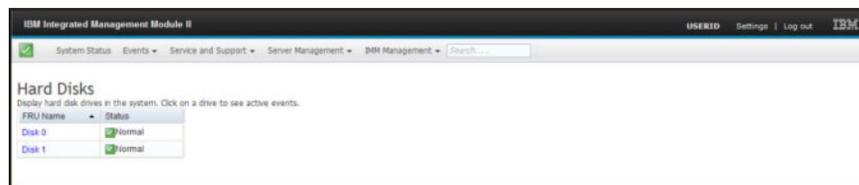
Selecione a opção **Ações de Energia do Servidor** sob a guia Gerenciamento do Servidor para visualizar uma lista de ações que podem ser usadas para controlar a energia do sistema. A ilustração a seguir é um exemplo da janela Ações de Energia do Servidor.



É possível escolher ligar o servidor imediatamente ou em um horário planejado. Também é possível escolher encerrar e reiniciar o sistema operacional. Para obter informações adicionais sobre como controlar a energia do sistema, consulte “Controlando o Status de Energia do Servidor” na página 104.

Discos

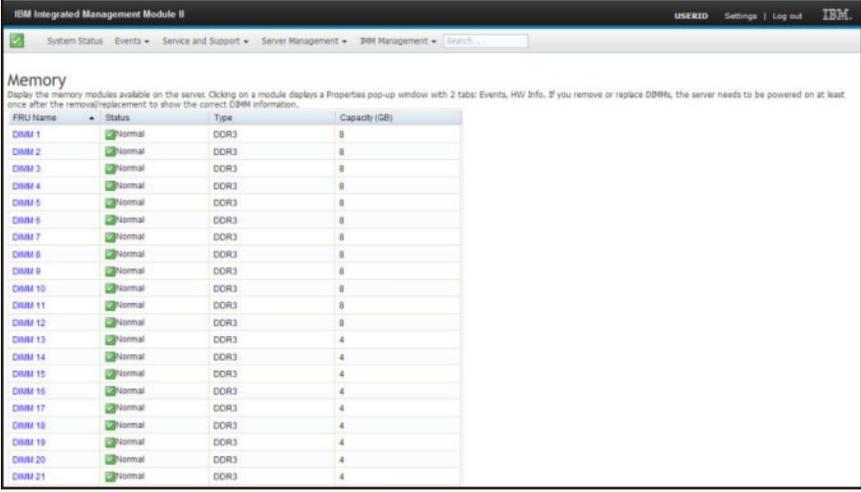
Selecione a opção **Discos** na guia Gerenciamento do Servidor para visualizar as unidades de disco rígido no sistema. A tela a seguir é exibida. Clique em uma unidade de disco rígido para visualizar os eventos associados à unidade de disco rígido.



Memória

Selecione a opção **Memória** na guia Gerenciamento do Servidor para visualizar informações sobre os módulos de memória instalados no sistema. A seguinte janela é aberta. Cada módulo de memória é exibido na tabela como um link que você pode clicar para obter informações mais detalhadas sobre o módulo de memória. A tabela também exibe o status do DIMM, tipo de DIMM e capacidade do DIMM.

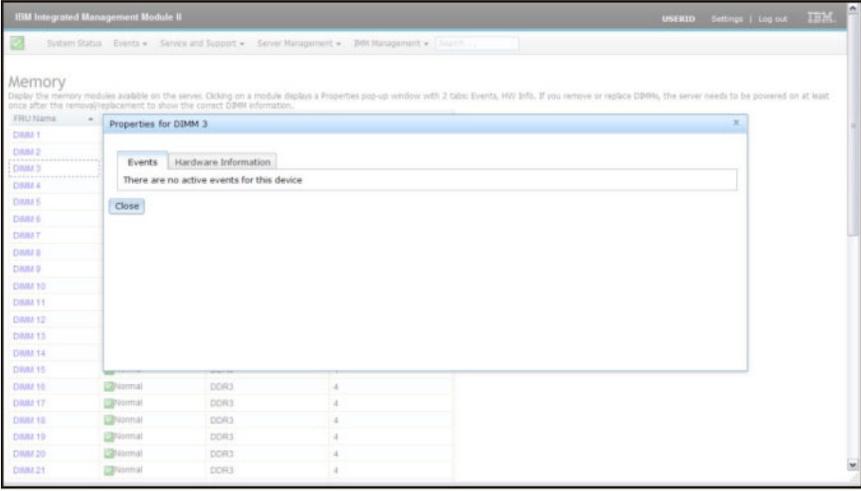
Nota: Se você remover ou substituir um DIMM, deverá reiniciar o sistema para visualizar as informações atualizadas do DIMM para as mudanças feitas nos DIMMs do sistema.



The screenshot shows the 'Memory' section of the IBM Integrated Management Module II interface. It displays a table with the following columns: FRU Name, Status, Type, and Capacity (GB). The table lists 21 DIMM modules, all with a status of 'Normal' and a type of 'DDR3'. The capacity varies between 8 GB and 4 GB.

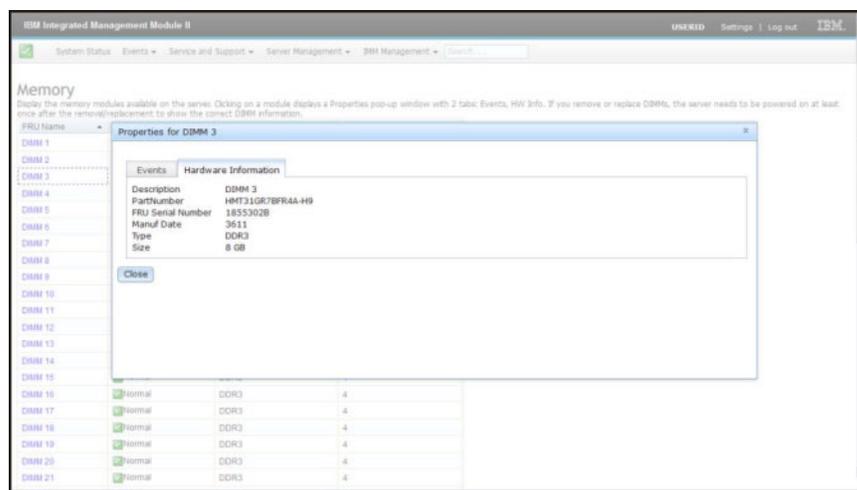
FRU Name	Status	Type	Capacity (GB)
DIMM 1	Normal	DDR3	8
DIMM 2	Normal	DDR3	8
DIMM 3	Normal	DDR3	8
DIMM 4	Normal	DDR3	8
DIMM 5	Normal	DDR3	8
DIMM 6	Normal	DDR3	8
DIMM 7	Normal	DDR3	8
DIMM 8	Normal	DDR3	8
DIMM 9	Normal	DDR3	8
DIMM 10	Normal	DDR3	8
DIMM 11	Normal	DDR3	8
DIMM 12	Normal	DDR3	8
DIMM 13	Normal	DDR3	4
DIMM 14	Normal	DDR3	4
DIMM 15	Normal	DDR3	4
DIMM 16	Normal	DDR3	4
DIMM 17	Normal	DDR3	4
DIMM 18	Normal	DDR3	4
DIMM 19	Normal	DDR3	4
DIMM 20	Normal	DDR3	4
DIMM 21	Normal	DDR3	4

Clique em um link **DIMM** na tabela para visualizar quaisquer eventos ativos e informações adicionais sobre o componente (conforme mostrado na tela a seguir).



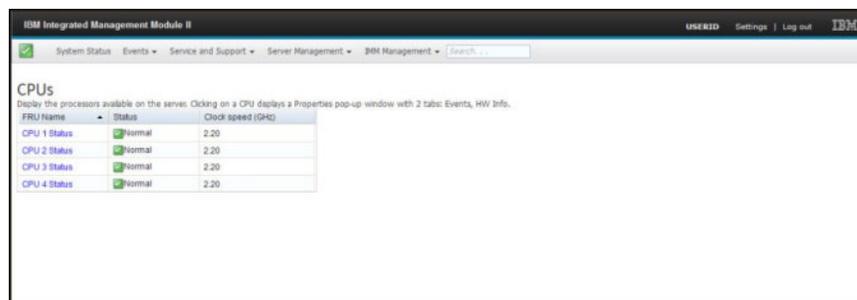
The screenshot shows the same 'Memory' page as above, but with a 'Properties for DIMM 3' dialog box open. The dialog box has two tabs: 'Events' and 'Hardware Information'. The 'Events' tab is selected, and it displays the message 'There are no active events for this device'. A 'Close' button is visible at the bottom of the dialog box.

Clique na guia **Informações de Hardware** para visualizar detalhes sobre o componente, como descrição, número de peça, número de série de FRU, data de manufatura (semana/ano), tipo (por exemplo, DDR3) e tamanho em gigabytes (conforme mostrado na ilustração a seguir).

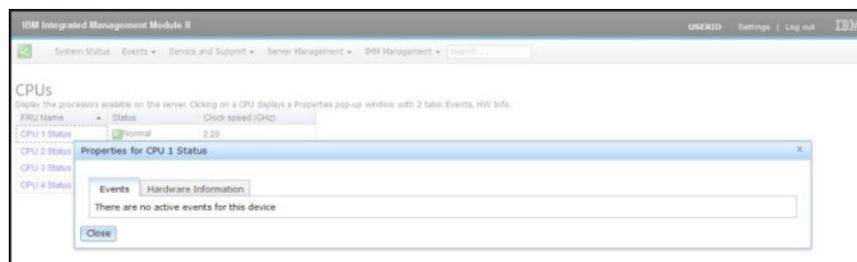


Processadores

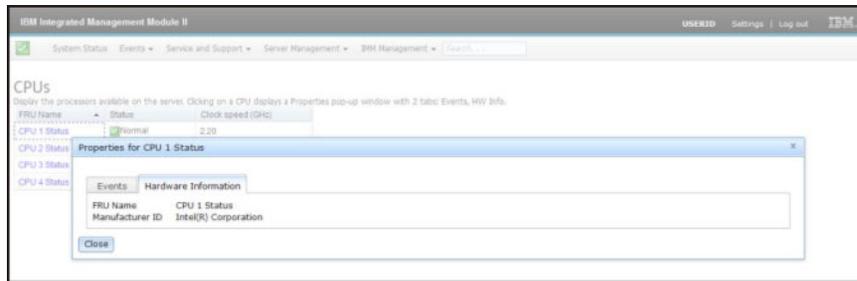
Selecione a opção **Processadores** na guia Gerenciamento do Servidor para visualizar informações sobre os microprocessadores instalados no sistema. A seguinte janela é aberta.



Clique em um link **CPU** na tabela para visualizar quaisquer eventos ativos e informações adicionais sobre o componente (conforme mostrado na ilustração a seguir).



Clique na guia **Informações de Hardware** para visualizar detalhes sobre o componente, como o nome da FRU e o ID do fabricante (conforme mostrado na ilustração a seguir).

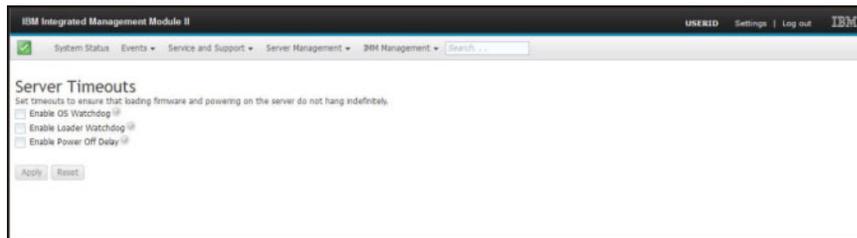


Tempos Limites do Servidor

Selecione a opção **Tempos Limites do Servidor** sob a guia Gerenciamento do Servidor para configurar tempos limites para assegurar que, durante uma atualização de firmware e ligação do sistema, o sistema não seja interrompido indefinidamente. É possível ativar essa função configurando os valores para as opções.

Nota: Os tempos limites do servidor requerem que a interface USB dentro da banda (ou LAN sobre USB) seja ativada para usar comandos. Para obter informações adicionais sobre como configurar a interface USB, consulte “Configurando USB” na página 83.

A ilustração a seguir mostra a janela Tempos Limites do Servidor.



Para obter informações adicionais sobre tempos limites do servidor, consulte “Configurando tempos limites do servidor” na página 58.

inicialização da rede PXE

Selecione a opção **Inicialização da Rede PXE** sob a guia Gerenciamento do Servidor para configurar seu servidor para tentar uma inicialização da rede PXE na próxima reinicialização do servidor. Para obter informações adicionais sobre como configurar uma inicialização da rede PXE, consulte “Configurando a inicialização da rede PXE” na página 117.

Tela de Falha mais Recente do S.O.

Selecione a opção **Tela de Falha mais Recente do S.O.** sob a guia Gerenciamento do Servidor para visualizar ou limpar os dados da tela de falha mais recente do sistema operacional que foram salvos pelo IMM2. O IMM2 armazena apenas as informações de eventos de erro mais recentes, sobrescrevendo os dados da tela de falha do S.O. mais antigos quando ocorre um novo evento de erro.

A ilustração a seguir é um exemplo da Tela de Falha do S.O.

```
A problem has been detected and windows has been shut down to prevent damage
to your computer.

The end-user manually generated the crashdump.

If this is the first time you've seen this stop error screen,
restart your computer. If this screen appears again, follow
these steps:

Check to make sure any new hardware or software is properly installed.
If this is a new installation, ask your hardware or software manufacturer
for any windows updates you might need.

If problems continue, disable or remove any newly installed hardware
or software. Disable BIOS memory options such as caching or shadowing.
If you need to use Safe Mode to remove or disable components, restart
your computer, press F8 to select Advanced Startup options, and then
select Safe Mode.

Technical information:

*** STOP: 0x000000E2 (0x0000000000000000,0x0000000000000000,0x0000000000000000,0
x0000000000000000)

Collecting data for crash dump ...
Initializing disk for crash dump ...
Beginning dump of physical memory.
Dumping physical memory to disk: 100
Physical memory dump complete.
Contact your system admin or technical support group for further assistance.
```

Para obter informações adicionais sobre a opção Tela de Falha mais Recente do S.O., consulte “Capturando os Dados da Tela de Falha mais Recente do S.O.” na página 132.

Guia Gerenciamento do IMM

Esta seção fornece informações sobre as opções na guia Gerenciamento do IMM2 na página inicial da interface com o usuário da web do IMM2.

As opções sob a guia Gerenciamento do IMM permitem visualizar e modificar a configuração do IMM2. Para obter a lista das opções e detalhes sobre como usar as opções para configurar o IMM2, consulte Capítulo 4, “Configurando o IMM2”, na página 55.

Capítulo 4. Configurando o IMM2

A guia Gerenciamento do IMM contém opções para configurar o IMM2. Use a guia Gerenciamento do IMM para visualizar e alterar configurações do IMM2. As opções a seguir são listadas sob a guia Gerenciamento do IMM (conforme mostrado na ilustração a seguir).

- Propriedades do IMM
- Usuários
- Rede
- Segurança
- Configuração do IMM
- Reiniciar IMM
- Reconfigurar o IMM para os padrões de factory
- Gerenciamento da Chave de Ativação



Na página Propriedades do Integrated Management Module (IMM), é possível executar as funções a seguir:

- Acessar as informações do firmware do servidor
- Configurar a data e hora:
 - Escolher o método de configuração de horário do IMM2: manual ou NTP
 - Configurar a data e hora do IMM2 para o método de configuração manual
 - Configurar as informações de NTP para o método de configuração NTP
 - Configurar informações de fuso horário do IMM2
- Acessar as informações da porta serial do IMM2:
 - Configurar a porta serial do IMM2
 - Configurar as seqüências-chave de CLI do IMM2

Na página Contas do Usuário, é possível executar as funções a seguir:

- Gerenciar contas do usuário do IMM2:
 - Criar uma conta do usuário
 - Clicar em um nome de usuário para editar propriedades para esse usuário:

- Editar o nome de usuário
- Configurar senha de usuário
- Configurar definições de SNMPv3 para o usuário
- Gerenciar chaves de autenticação pública de Shell Seguro (SSH) para o usuário
- Excluir uma conta de usuário
- Configurar definições de login de usuário global:
 - Configurar método de autenticação do usuário
 - Configurar tempo limite de inatividade da web
 - Configurar níveis de segurança da conta do usuário disponíveis para o IMM2
- Visualizar usuários que estão atualmente conectados ao IMM2

Na página Propriedades do Protocolo de Rede, é possível executar as funções a seguir:

- Configurar definições de Ethernet:
 - Configurações de Ethernet:
 - Nome do host
 - Configurações de ativação e endereço IPv4 e IPv6
 - Configurações avançadas de Ethernet:
 - Ativação de negociação automática
 - Gerenciamento de endereço MAC
 - Configurar unidade máxima de transmissão
- Configurar definições de SNMP:
 - Ativação e configuração de SNMPv1:
 - Configurar informações de contato
 - Ativação e configuração de traps SNMP
 - Gerenciamento de comunidade
 - Ativação e configuração de SNMPv3:
 - Configurar informações de contato
 - Configuração de conta do usuário
- Configurar definições de DNS:
 - Configurar preferência de endereçamento de DNS (IPv4 ou IPv6)
 - Ativação e configuração de endereçamento do servidor do Sistema de Nomes de Domínio adicional
- Configurar definições de DDNS:
 - Ativação de DDNS
 - Selecionar origem de nome de domínio (customizada ou servidor DHCP)
 - Configurar nome de domínio customizado para origem customizada especificada manualmente
 - Visualizar nome de domínio especificado pelo servidor DHCP
- Configurar definições de SMTP:
 - Configurar endereço IP ou nome do host do servidor SMTP
 - Configurar número da porta do servidor SMTP
 - Testar a conexão de SMTP
- Configurar definições de LDAP:
 - Definir a configuração do servidor LDAP (DNS ou pré-configurado):

- Se configuração do servidor LDAP especificada pelo DNS, configurar o domínio de procura:
 - Extrair domínio de procura do ID de login
 - Domínio de procura e nome do serviço especificados manualmente
 - Tentar extrair o domínio de procura do ID de login, em seguida, usar manualmente o domínio de procura e o nome do serviço especificados
- Se estiver usando um servidor LDAP pré-configurado:
 - Configurar o nome do host ou endereço IP do servidor LDAP
 - Configurar número da porta do servidor LDAP
- Configurar o nome distinto raiz do servidor LDAP
- Configurar o atributo de procura UID
- Selecionar o método de ligação (anônimo, com credenciais configuradas, com credenciais de login):
 - Para credenciais configuradas, configurar nome distinto e senha
- Segurança aprimorada baseada em função para ativação de Usuários do Active Directory:
 - Se desativado:
 - Configurar filtro de grupo
 - Configurar atributo de procura do grupo
 - Configurar atributo de permissão de login
 - Se ativado, configurar o nome de destino do servidor
- Configurar definições de Telnet:
 - Ativação de acesso ao Telnet
 - Configurar número máximo de sessões Telnet
- Configurar definições de USB:
 - Ativação de Ethernet sobre USB
 - Ativação e gerenciamento de encaminhamento de porta de Ethernet externa para Ethernet sobre USB
- Configurar Designações de Porta:
 - Visualizar números de porta abertas
 - Configurar números de porta usados por serviços do IMM2:
 - HTTP
 - HTTPS
 - CLI Telnet
 - CLI SSH
 - Agente do SNMP
 - Traps SNMP
 - Controle Remoto
 - CIM sobre HTTPS
 - CIM sobre HTTP

Na página Segurança, é possível executar as funções a seguir:

- Ativação do servidor HTTPS e gerenciamento de certificado
- Ativação do CIM sobre HTTPS e gerenciamento de certificado
- Seleção de segurança de LDAP e gerenciamento de certificado
- Ativação do servidor SSH e gerenciamento de certificado

Na página Configuração do IMM, é possível executar as funções a seguir:

- Visualizar um resumo de configuração do IMM2
- Fazer backup ou restaurar a configuração do IMM2
- Visualizar o status de backup ou restauração
- Redefinir a configuração do IMM2 para suas configurações padrão de factory
- Acessar o assistente de configuração inicial do IMM2

Na página Reiniciar o IMM, é possível reconfigurar o IMM2.

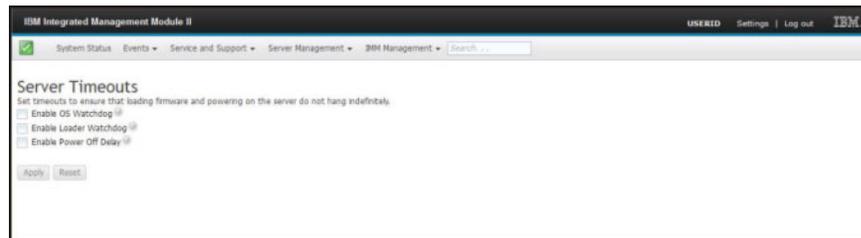
Na página Reconfigurar o IMM2 para Padrões de Factory... , é possível redefinir a configuração do IMM2 para suas configurações padrão de factory.

Na página Gerenciamento de Chaves de Ativação, é possível gerenciar chaves de ativação para Features on Demand (FoD) opcionais do IMM2 e do servidor. Consulte Capítulo 7, “Features on Demand”, na página 139 para obter informações sobre como gerenciar chaves de ativação de FoD.

Configurando tempos limites do servidor

Use a opção Tempos Limites do Servidor para configurar tempos limites para assegurar que o servidor não seja interrompido indefinidamente durante uma atualização de firmware ou ligação do servidor. É possível ativar esta função configurando o valor para essa opção, mostrado na ilustração a seguir.

Nota: Os tempos limites do servidor requerem que a interface USB dentro da banda (ou LAN sobre USB) seja ativada para usar comandos. Para obter informações adicionais sobre como ativar e desativar a interface USB, consulte “Configurando USB” na página 83.



Para configurar os valores de tempo limite do servidor, conclua as etapas a seguir:

1. Efetue login no IMM2 no qual você deseja configurar os tempos limites do servidor. (Consulte “Efetuando Login no IMM2” na página 10).
2. Clique em **Gerenciamento do Servidor**; em seguida, selecione **Tempos Limites do Servidor**.

É possível configurar o IMM2 para responder automaticamente aos eventos a seguir:

- Sistema operacional parado
 - Falha ao carregar sistema operacional
3. Ative os tempos limites do servidor que correspondam aos eventos que você deseja que o IMM2 responda automaticamente. Consulte “Seleções de Tempo Limite do Servidor” para obter uma descrição de cada opção.
 4. Clique em **Aplicar**.

Nota: Há um botão **Reconfigurar** que pode ser usado para limpar todos os tempos limites simultaneamente.

Seleções de Tempo Limite do Servidor

Ativar Watchdog do S.O.

Use o campo **Ativar Watchdog do S.O.** para especificar o número de minutos entre as verificações do sistema operacional pelo IMM2. Se o sistema operacional falhar em responder a uma dessas verificações, o IMM2 gerará um alerta de tempo limite do S.O. e reiniciará o servidor. Após o servidor ser reiniciado, o watchdog do S.O. fica desativado até que o sistema operacional seja encerrado e o servidor passe pelo ciclo de ativação. Para configurar o valor de watchdog do S.O., selecione **Ativar Watchdog do S.O.** e selecione um intervalo de tempo no menu. Para desligar esse watchdog, cancele a seleção de **Ativar Watchdog do S.O.**. Para capturar telas de falha do sistema operacional, você deve ativar o campo **Ativar Watchdog do S.O.**.

Ativar Watchdog do Carregador

Use o campo **Ativar Watchdog do Carregador** para especificar o número de minutos que o IMM2 aguarda entre a conclusão do POST e o início do sistema operacional. Se esse intervalo for excedido, o IMM2 gerará um alerta de tempo limite do carregador e reiniciará o servidor automaticamente. Após a reinicialização do servidor, o tempo limite do carregador é automaticamente desativado até que o sistema operacional seja encerrado e o ciclo de ativação do servidor ocorra (ou até que o sistema operacional seja iniciado e o software seja carregado com êxito). Para configurar o valor de tempo limite do carregador, selecione o limite de tempo que o IMM2 aguarda para que a inicialização do sistema operacional seja concluída. Para desligar esse watchdog, cancele a seleção de **Ativar Watchdog do Carregador** no menu.

Ativar Atraso de Desligamento

Use o campo **Ativar Atraso de Desligamento** para especificar o número de minutos que o subsistema IMM2 aguardará para que o sistema operacional seja encerrado antes de desligar o sistema. Para configurar o valor de tempo limite de atraso de desligamento, selecione o limite de tempo que o IMM2 aguarda após o desligamento do sistema operacional. Para desligar esse watchdog, cancele a seleção de **Ativar Watchdog do Carregador** no menu.

Configurando a Data e Hora do IMM2

Nota: As configurações de Data e Hora do IMM2 não podem ser modificadas em um IBM Flex System.

Selecione a guia **Data e Hora** para visualizar ou alterar a data e hora do IMM2. O IMM2 usa seu próprio clock em tempo real para registrar a data e hora de todos os eventos registrados no log de eventos. Os alertas que são enviados por email e pelo Simple Network Management Protocol (SNMP) usam a configuração de clock em tempo real para registrar a data e hora dos alertas. As configurações do clock suportam deslocamentos da Hora de Greenwich (GMT) e horário de verão para maior facilidade de uso pelos administradores que estão gerenciando sistemas remotamente em fusos horários diferentes. É possível acessar remotamente o log de eventos mesmo que o servidor esteja desligado ou desativado.

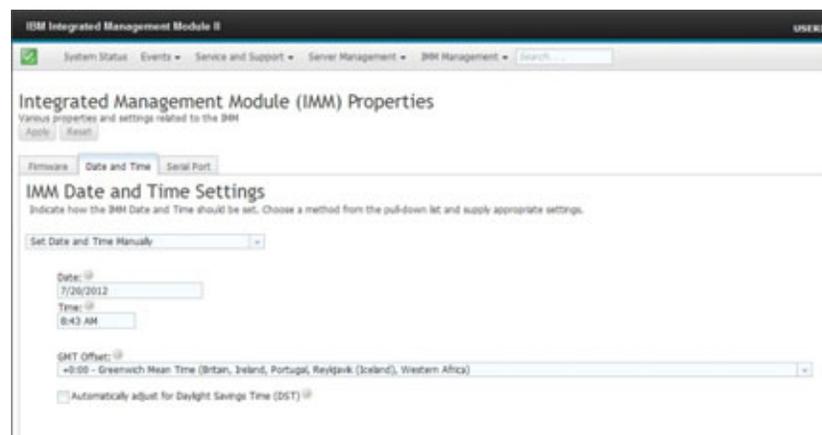
A configuração de data e hora do IMM2 afeta apenas o clock do IMM2 e não o clock do servidor. O clock em tempo real do IMM e o clock do servidor são separados, independentes e podem ser configurados para horários diferentes.

Alterando a Configuração de Hora e Data (Modo Manual)

Conclua as etapas a seguir para alterar manualmente a configuração de horário e data:

1. Na lista de menu **Indicar como a data e hora do IMM devem ser configuradas**, clique em **Configurar data e hora manualmente**.
2. No campo **Data**, digite o mês, dia e ano atuais.
3. No campo **Horário**, digite os números que correspondem à hora e os minutos atuais.
 - A hora deve ser um número de 1 a 12 conforme representado em um clock de 12 horas.
 - Os minutos devem ser números de 00 a 59.
 - Selecione **AM** ou **PM**.
4. No campo **Deslocamento GMT**, selecione o número que especifica o deslocamento, em horas, do GMT. Esse número deve corresponder ao fuso horário no qual o servidor está localizado.
5. Selecione ou limpe a caixa de seleção **Ajustar automaticamente para Horário de Verão (DST)** para especificar se o clock do IMM2 é ajustado automaticamente quando o horário local é alterado entre horário padrão e horário de verão.

A ilustração a seguir mostra a guia Data e Hora do IMM ao configurar a data e hora manualmente.



Alterando as Configurações de Horário e Data (Modo do Servidor NTP)

Conclua as etapas a seguir para sincronizar o clock do IMM2 com o clock do servidor:

1. Na lista de menu **Indicar como a data e hora do IMM devem ser configuradas**, clique em **Sincronizar com um servidor NTP**.
2. No campo **Nome do Host ou Endereço IP do Servidor NTP**, especifique o nome do servidor NTP a ser usado para sincronização de clock.

3. No campo **Frequência de Sincronização (em minutos)**, especifique o intervalo aproximado entre as solicitações de sincronização. Insira um valor entre 3 e 1440 minutos.
4. Marque a caixa de seleção **Sincronizar quando estas configurações forem salvas** para solicitar uma sincronização imediata (ao clicar em **Aplicar**), em vez de aguardar a decorrência do intervalo de tempo.
5. No campo **Deslocamento GMT**, selecione o número que especifica o deslocamento, em horas, de GMT, correspondente ao fuso horário no qual o servidor está localizado.
6. Selecione ou limpe a caixa de seleção **Ajustar automaticamente para Horário de Verão (DST)** para especificar se o clock do IMM2 é ajustado automaticamente quando o horário local é alterado entre horário padrão e horário de verão.

A ilustração a seguir mostra a guia Data e Hora do IMM ao sincronizar com o clock do servidor.

Configurando as Definições de Porta Serial

Selecione a opção **Porta Serial** para especificar o redirecionamento de porta serial do host. O IMM2 fornece duas portas seriais que são usadas para redirecionamento serial:

Porta serial 1 (COM1)

A porta serial 1 (COM1) nos servidores System x é usada para IPMI Serial sobre LAN (SOL). A COM1 é configurável apenas por meio da interface IPMI.

Porta serial 2 (COM2)

Em servidores blade, a porta serial 2 (COM2) é usada SOL. Em servidores de rack System x e no IBM Flex System, a COM2 é usada para redirecionamento serial por meio de Telnet ou SSH. A COM2 não é configurável apenas por meio da interface IPMI. Em servidores montados em rack e torre, a porta COM2 é uma porta COM interna sem acesso externo.

Conclua os campos a seguir para redirecionamento de porta serial:

Taxa de Transmissão de dados

Especifique a taxa de transferência de dados de sua conexão de porta serial neste campo. Para configurar a taxa de bauds, selecione a taxa de transferência de dados, entre 9600 e 115200, que corresponda à sua conexão de porta serial.

Paridade

Especifique os bits de paridade de sua conexão de porta serial nesse campo. As opções disponíveis são Nenhum, Ímpar ou Par.

Bits de Parada

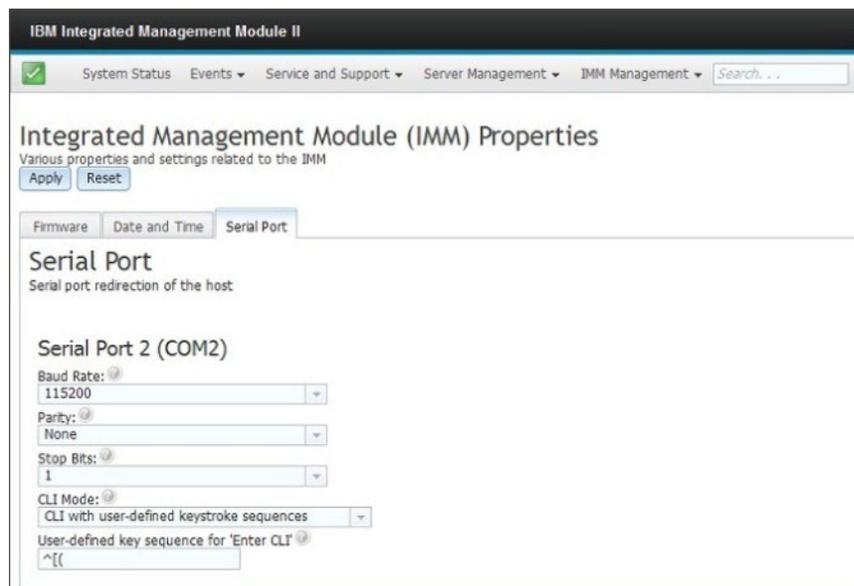
Especifique o número de bits de parada de sua conexão de porta serial nesse campo. As opções disponíveis são 1 ou 2.

Modo de CLI

Nesse campo, selecione **CLI com sequências de pressionamento de tecla compatíveis com o IMM2** ou selecione **CLI com sequências de pressionamento de tecla definidas pelo usuário** se desejar usar sua própria sequência-chave. Se você selecionar **CLI com sequências de pressionamento de tecla definidas pelo usuário**, deverá definir a sequência-chave no campo **Sequência-chave definida pelo usuário para 'Entrar na CLI'**.

Após o início do redirecionamento serial, ele continua até que você digite a sequência-chave de saída. Quando a sequência-chave de saída é digitada, o redirecionamento serial é parado e você é retornado para o modo de comando na sessão Telnet ou SSH. Use o campo **Sequência-chave definida pelo usuário para 'Entrar na CLI'** para especificar a sequência-chave de saída.

A ilustração a seguir mostra a guia Porta Serial.



Configurando Contas de Usuário

Selecione a opção **Usuários** sob a guia Gerenciamento do IMM para criar e modificar contas de usuário para o IMM2 e visualizar perfis de grupo. Você verá a mensagem informativa a seguir.

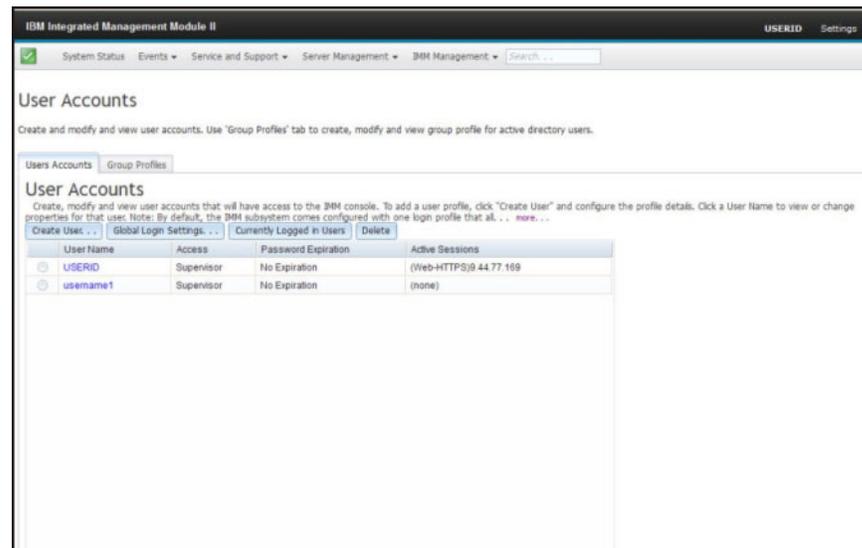
Nota: Em um IBM Flex System, as contas do usuário do IMM2 são gerenciadas pelo CMM.



Contas de Usuário

Selecione a guia **Contas de Usuário** para criar, modificar e visualizar contas de usuário conforme mostrado na ilustração a seguir.

Nota: O subsistema IMM2 é fornecido com um perfil de login.



Criar Usuário

Clique na guia **Criar Usuário...** para criar uma nova conta do usuário. Conclua os campos a seguir: **Nome de Usuário**, **Senha** e **Confirmar Senha** (conforme mostrado na ilustração a seguir).

Create New User

User Credentials

Authority
SNMPv3

User Credentials
Enter a user name and password.

User name:
username1

Password:

Confirm password:

User name rules:

- Must be 1-16 characters
- Cannot contain white space characters
- Can only contain the characters A-Z, a-z, 0-9, '.' (underscore) and '.' (period)
- Must be different for each user

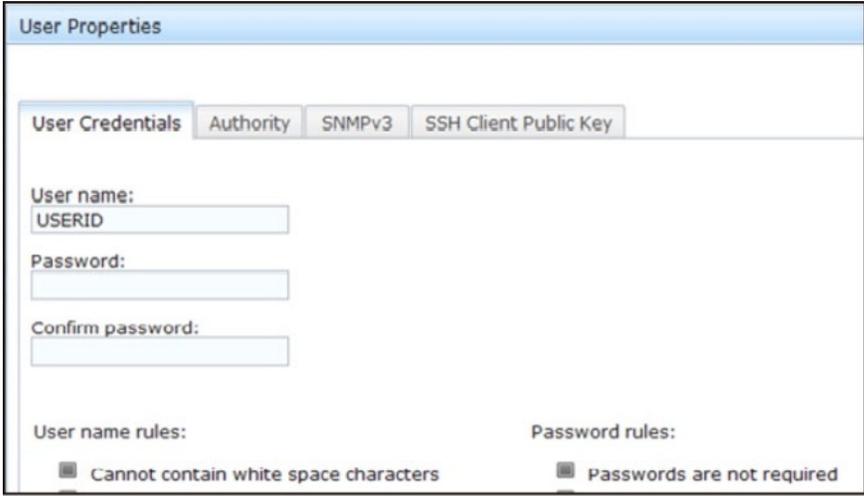
Password rules:

- Passwords are not required
- Must be 0-20 characters
- Cannot contain white space characters
- Password and password confirm values must match
- Can only contain the characters A-Z, a-z, 0-9, ~ ` ! @ # \$ % ^ & * () + = { } | ; : " ' < > , ? /

< Back Next > Finish Cancel

Propriedades de Usuário

Clique na guia **Propriedades do Usuário** para modificar contas de usuário existentes (conforme mostrado na ilustração a seguir).



The screenshot shows a window titled "User Properties" with four tabs: "User Credentials", "Authority", "SNMPv3", and "SSH Client Public Key". The "User Credentials" tab is active. It contains the following fields and options:

- User name:** A text box containing "USERID".
- Password:** An empty text box.
- Confirm password:** An empty text box.
- User name rules:** A checkbox that is checked, with the label "Cannot contain white space characters".
- Password rules:** A checkbox that is unchecked, with the label "Passwords are not required".

Autoridade do usuário

Clique na guia **Autoridade** para configurar a autoridade de usuário. Os níveis de autoridade do usuário a seguir estão disponíveis:

Supervisor

O usuário não tem restrições.

Somente Leitura

O usuário tem apenas acesso somente leitura e não pode executar ações como transferências de arquivo, ações de energia e reinicialização ou funções de presença remota.

Customizado

Permite um perfil mais customizado para autoridade de usuário com configurações para as ações que o usuário é permitido executar.

Direitos de Acesso de SNMP

Clique na guia **SNMPv3** para configurar o acesso SNMP para a conta. As opções de acesso de usuário a seguir estão disponíveis:

Protocolo de Autenticação

Especifique **HMAC-MD5** ou **HMAC-SHA** como o protocolo de autenticação. Existem os algoritmos usados pelo modelo de segurança do SNMPv3 para autenticação. Se o **Protocolo de Autenticação** não for ativado, nenhum protocolo de autenticação será usado.

Protocolo de privacidade

A transferência de dados entre o cliente SNMP e o agente pode ser protegida usando criptografia. Os métodos suportados são **DES** e **AES**. O protocolo de privacidade será válido somente se o protocolo de autenticação estiver configurado como **HMAC-MD5** ou **HMAC-SHA**.

Senha de privacidade

Especifique a senha de criptografia neste campo.

Confirmar senha de privacidade

Especifique a senha de criptografia novamente para confirmação.

Tipo de acesso

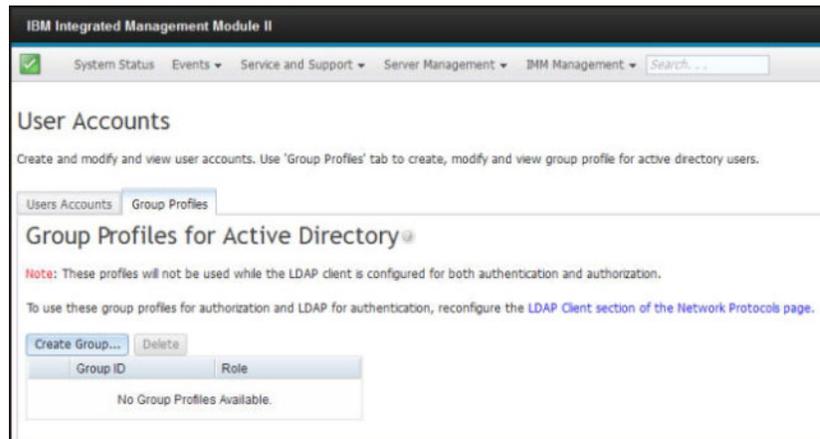
Especifique **Get** ou **Set** como o tipo de acesso. Os usuários do SNMPv3 com **Get** como o tipo de acesso podem executar somente operações de consulta. Os usuários do SNMPv3 com **Set** como o tipo de acesso, podem executar operações de consulta e modificar configurações (por exemplo, configurando a senha para um usuário).

Nome do host/endereço IP para traps

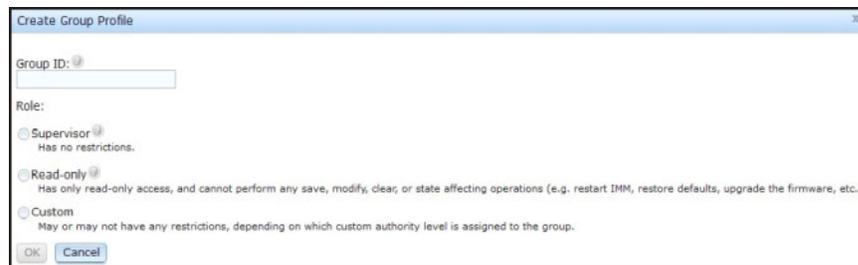
Especifique o destino do trap para o usuário. Esse pode ser um endereço IP ou nome de host. Usando traps, o agente do SNMP notifica a estação de gerenciamento sobre eventos (por exemplo, quando a temperatura de um processador excede o limite).

Perfis de Grupo

Selecione a guia **Perfis de Grupo** para criar, modificar e visualizar perfis de grupo (conforme mostrado na ilustração a seguir).

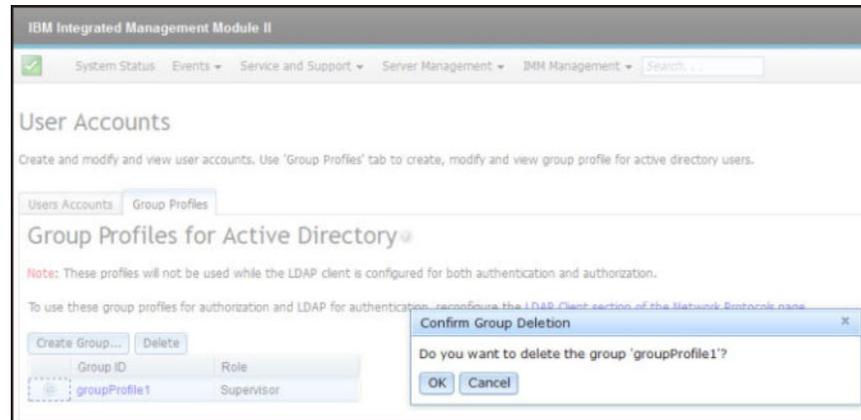


Clique em **Criar Grupo** para criar um novo grupo de usuários. A ilustração a seguir mostra a janela Criar Perfil do Grupo.



Insira um **ID do Grupo** e selecione a **Função**, (consulte "Autoridade do usuário" na página 65 para obter informações sobre os níveis de autoridade do usuário).

Se for necessário excluir um grupo, clique em **Excluir**. A ilustração a seguir mostra a janela Confirmar Exclusão de Grupo.



Definindo as Configurações de Login Global

Use a guia Configurações de Login Global para configurar as definições de login que se aplicam a todos os usuários.

Configurações Gerais

Clique na guia **Geral** para selecionar como as tentativas de login de usuário são autenticadas e especificar quanto tempo, em minutos, o IMM2 aguarda antes de desconectar uma sessão da web inativa. No campo **Método de Autenticação do Usuário**, é possível especificar como os usuários que estão tentando efetuar login devem ser autenticados. É possível selecionar um dos métodos de autenticação a seguir:

- **Somente local:** Os usuários são autenticados por uma procura da conta de uso local configurada no IMM2. Se não houver correspondência do ID do usuário e senha, o acesso será negado.
- **Somente LDAP:** O IMM2 tenta autenticar o usuário usando um servidor LDAP. As contas de usuário locais no IMM2 *não* são procuradas 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 Local:** A autenticação LDAP é tentada primeiro. Se a autenticação LDAP falhar, então, será tentada a autenticação local.

Notas:

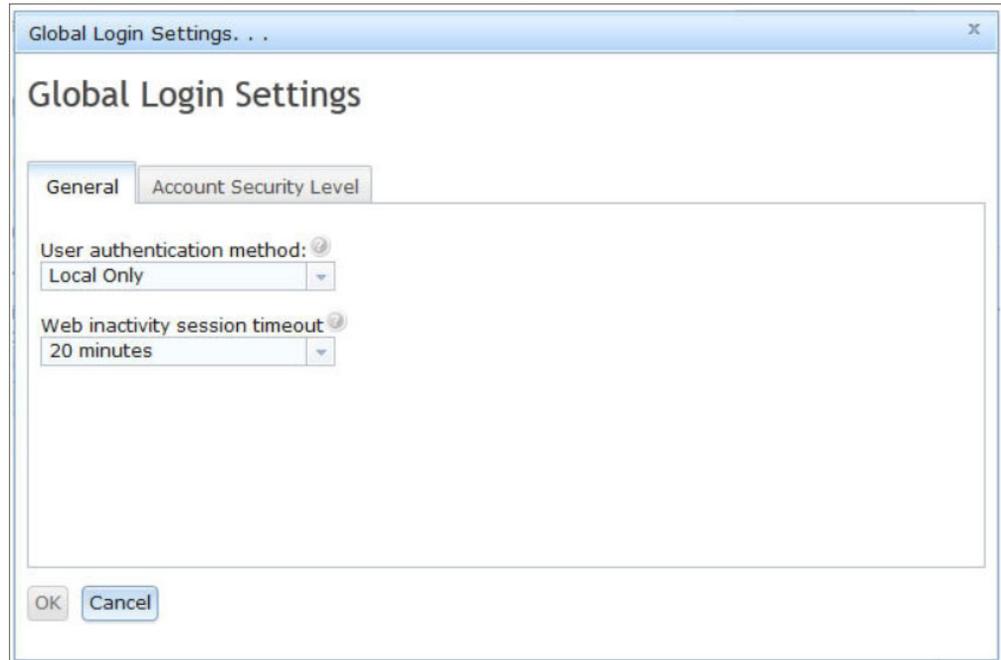
- Somente as contas localmente administradas são compartilhadas com as interfaces IPMI e SNMP. Essas interfaces não suportam autenticação LDAP.
- Os usuários do IPMI e do SNMP podem efetuar login usando as contas localmente administradas quando o campo **Método de Autenticação do Usuário** for configurado como **Somente LDAP**.

No campo **Tempo Limite da Sessão de Inatividade da Web**, é possível especificar por quanto tempo, em minutos, o IMM aguarda antes de desconectar uma sessão da web inativa. Selecione **Sem tempo limite** para desativar esse recurso. Selecione **Usuário seleciona o tempo limite** para selecionar o período de tempo limite durante o processo de login.

O tempo limite de inatividade se aplica somente a páginas da web que *não* são atualizadas automaticamente. Se um navegador da web solicitar continuamente

atualizações da página da web quando um usuário navegar para uma página da web que é atualizada automaticamente, o tempo limite de inatividade não terminará automaticamente a sessão do usuário. Os usuários podem escolher se desejam, ou não, que o conteúdo da página da web seja atualizado automaticamente a cada 60 segundos. Consulte “Atualização Automática de Página” na página 17 para obter informações adicionais que descrevem a configuração de atualização automática.

A guia Geral é mostrada na ilustração a seguir.



Existem algumas páginas da web do IMM2 que são atualizadas automaticamente mesmo se a configuração de atualização automática não for selecionada. As páginas da web do IMM2 atualizadas automaticamente são as seguintes:

- **Status do Sistema:** O status do sistema e de energia será atualizado automaticamente a cada três segundos.
- **Ações de Energia do Servidor:** O status de energia será atualizado automaticamente a cada três segundos.
- **Controle Remoto:** Os botões Iniciar Controle Remoto serão atualizados automaticamente a cada segundo. A tabela Lista de Sessões será atualizada automaticamente uma vez a cada minuto.

O firmware do IMM2 suporta 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.

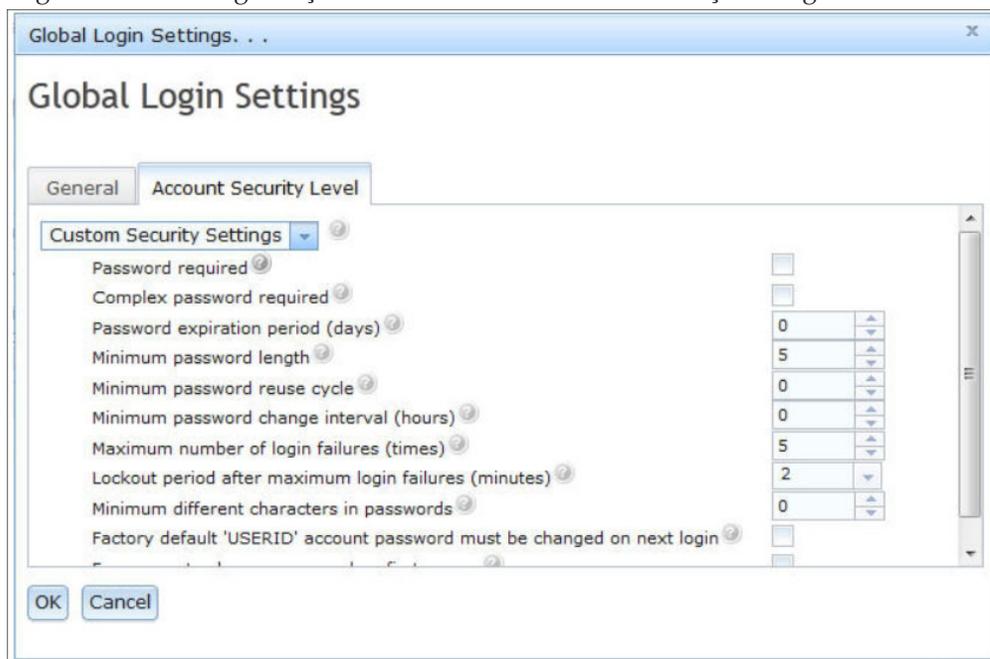
Nota: Se você deixar o navegador aberto em uma página da web do IMM2 que é atualizada automaticamente, sua sessão da web não fechará automaticamente devido à inatividade.

Configurações de Política de Segurança de Conta

Clique na guia **Nível de Segurança de Conta** para selecionar a configuração de política de segurança de conta. Existem três níveis de configurações de política de segurança de conta:

- Configurações de Segurança Legada
- Configurações de Segurança Alta
- Configurações de Segurança Customizada

A guia **Nível de Segurança de Conta** é mostrada na ilustração a seguir.



Selecione o nível desejado na lista de itens. As Configurações de Segurança Legada e as Configurações de Segurança Alta predefinem os valores de configuração de política e não podem ser alteradas. As Configurações de Segurança Customizada permitem que os usuários customizem as políticas de segurança conforme necessário.

A tabela a seguir mostra os valores para cada nível das configurações de segurança.

Tabela 3. Valores de Política de Configuração de Segurança

Configuração de Política/Campo	Configurações de Segurança Legada	Configurações de Segurança Alta	Configurações de Segurança Customizada
Senha Necessária	Não	Sim	Sim ou Não
Senha Complexa Necessária	Não	Sim	Sim ou Não
Período de Expiração da Senha (Dias)	Nenhuma	90	0 – 365
Comprimento Mínimo de Senha	Nenhuma	8	5 – 20
Ciclo Mínimo de Reutilização de Senha	Nenhuma	5	0 – 5

Tabela 3. Valores de Política de Configuração de Segurança (continuação)

Configuração de Política/Campo	Configurações de Segurança Legada	Configurações de Segurança Alta	Configurações de Segurança Customizada
Intervalo Mínimo de Mudança de Senha (Horas)	Nenhuma	24	0 – 240
Número Máximo de Falhas de Login (Veze)	5	5	0 – 10
Período de Bloqueio Após Máximo de Falhas de Login (Minutos)	2	60	0 – 240
Mínimo de Caracteres Diferentes em Senhas	Nenhuma	2	0 – 19
A senha de conta 'USERID' padrão de factory deve ser alterada no próximo login	Não	Sim	Sim ou Não
Forçar o usuário a alterar a senha no primeiro acesso	Não	Sim	Sim ou Não

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

Senha Necessária

Esse campo indica se os IDs de login sem senha são permitidos ser criados. Se a caixa de seleção **Senha Necessária** for marcada, quaisquer IDs de login existentes sem senha serão necessários para definir uma senha na próxima vez que o usuário efetuar login.

Senha Complexa Necessária

Se senhas complexas forem necessárias, a senha deverá aderir às regras a seguir:

- As senhas devem ter no mínimo oito caracteres.
- As senhas devem conter pelo menos três das quatro categorias a seguir:
 - Pelo menos um caractere alfabético minúsculo.
 - Pelo menos um caractere alfabético maiúsculo.
 - Pelo menos um caractere numérico.
 - Pelo menos um caractere especial.
- Espaços ou caracteres de espaço em branco não são permitidos.
- As senhas não podem ter mais que três dos mesmos caracteres usados consecutivamente (por exemplo, aaa).
- As senhas não devem ser uma repetição ou reverso do ID do usuário associado.

Se senhas complexas não forem necessárias, a senha:

- Deverá ter no mínimo cinco (ou o número especificado no campo **Comprimento Mínimo de Senha**) caracteres.

- Não poderá conter quaisquer espaços ou caracteres de espaço em branco.
- Deverá conter pelo menos um caractere numérico.
- Poderá ser em branco (apenas se a caixa de seleção **Senha Necessária** estiver desativada).

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 365 dias é suportado. O valor padrão para esse campo é 0 (desativado).

Comprimento Mínimo de Senha

Esse campo contém o comprimento mínimo da senha. 5 a 20 caracteres são suportados para esse campo. Se a caixa de seleção **Senha Complexa Necessária** estiver marcada; o comprimento mínimo de senha deverá ser pelo menos oito caracteres.

Ciclo Mínimo de Reutilização de Senha

Esse campo contém o número de senhas anteriores que não podem ser reutilizadas. Até cinco senhas anteriores podem ser comparadas. Selecione 0 para permitir a reutilização de todas as senhas anteriores. O valor padrão para esse campo é 0 (desativado).

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 0 (desativado).

Número Máximo de Falhas de Login (Veze)

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 0 (desativado).

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

Esse campo especifica quanto tempo (em minutos), o subsistema IMM2 desativará as tentativas de login remoto de todos os usuários depois de detectar mais de cinco falhas de login sequenciais de qualquer servidor.

Mínimo de Caracteres Diferentes em Senhas

Esse campo especifica o número de caracteres que devem ser diferentes entre a nova senha e a senha anterior. Um valor de 0 a 19 é suportado.

A senha de conta 'USERID' padrão de factory deve ser 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 ativada, a senha padrão deve ser alterada para que a conta possa ser usada. A nova senha está sujeita a todas as regras de comprimento de senha ativas.

Forçar o usuário a alterar a senha no primeiro acesso

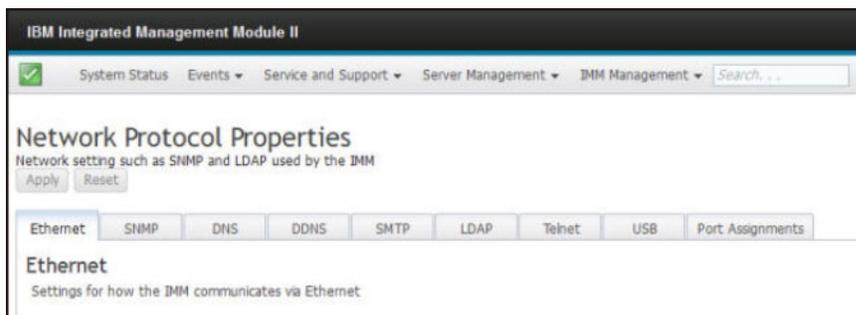
Depois de configurar um novo usuário com uma senha padrão, a seleção dessa caixa de seleção forçará esse usuário a alterar sua senha na primeira vez que ele efetuar login.

Configurando protocolos de rede

Clique na opção **Rede** na guia Gerenciamento do IMM para visualizar e configurar definições de rede.

Configurando as Definições de Ethernet

Clique na guia **Ethernet** para visualizar ou modificar as configurações de Ethernet do IMM2 (conforme mostrado na ilustração a seguir).



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

1. Selecione a opção **IPv4**; em seguida, marque a caixa de seleção correspondente.

Nota: A desativação da interface Ethernet evita o acesso ao IMM2 a partir da rede externa.

2. Na lista **Configurar Definições de Endereço IP**, selecione uma das opções a seguir:
 - Obter um endereço IP de um servidor DHCP
 - Usar endereço IP estático
3. Se você desejar que o IMM2 assuma por padrão um endereço IP estático, caso não seja possível entrar em contato com um servidor DHCP, marque a caixa de seleção correspondente.
4. No campo **Endereço Estático**, digite o endereço IP do IMM2.

Nota: O endereço IP deve conter quatro números inteiros de 0 a 255 sem espaços e separados por pontos.

5. No campo **Máscara de Sub-rede**, digite a máscara de sub-rede que é usada pelo IMM2.

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.

6. 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.

A ilustração a seguir mostra a guia Ethernet.

Ethernet Advanced Ethernet

Host name: IMM2-e41f13d90631

IPv4 IPv6

Enable IPv4

Currently assigned IPv4 address information

	Address
Host name	IMM2-e41f13d90631
IP address	9.37.189.59
Subnet mask	255.255.240.0
Gateway address	9.37.176.1
Domain name	raleigh.ibm.com
Primary DNS Server	9.0.128.50
Second DNS Server	9.0.130.50
Tertiary DNS Server	0.0.0.0

Configure IP address settings

Obtain IP address from DHCP server

Use static IP address

Obtain IP address from DHCP server

Static address: 192.168.70.125

Subnet mask: 255.255.255.0

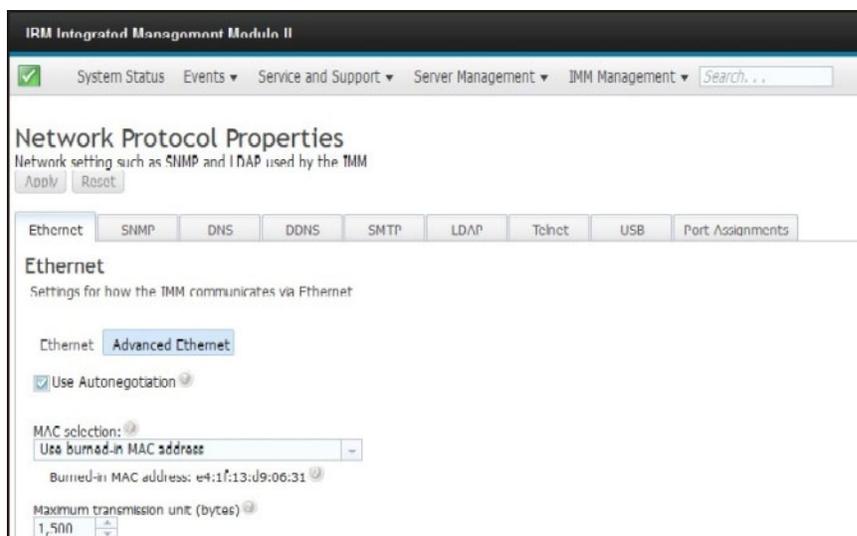
Default gateway: 0.0.0.0

Configurando as Definições de Ethernet Avançada

Clique na guia **Ethernet Avançada** para configurar definições de Ethernet adicionais. Na lista **Seleção de MAC**, escolha uma das seleções a seguir:

- Endereço MAC gravado usado
 - A opção Endereço MAC Gravado é um endereço físico exclusivo designado a este IMM2 pelo fabricante. O endereço é um campo somente leitura.
- Endereço MAC localmente administrado usado
 - 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 a FFFFFFFF. Esse valor deve estar no formato *xx:xx:xx:xx:xx:xx* em que *x* é um número de 0 a 9. O IMM2 não suporta o 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.

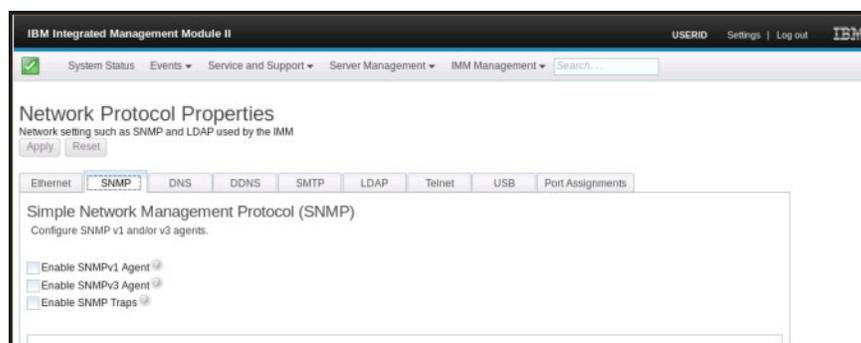
No campo **Unidade Máxima de Transmissão**, especifique a unidade máxima de transmissão de um pacote (em bytes) para sua interface de rede. O intervalo de unidade máxima de transmissão é de 60 a 1500. O valor padrão para esse campo é 1500. A ilustração a seguir mostra a guia Ethernet Avançada e os campos associados.



Configurando definições de alerta SNMP

Conclua as etapas a seguir para configurar a definição SNMP do IMM2.

1. Clique na guia **SNMP** (conforme mostrado na ilustração a seguir).



2. Marque a caixa de seleção correspondente para ativar o agente do SNMPv1, o agente do SNMPv3 ou Traps SNMP.
3. Se ativar o agente do SNMPv1, continue com a etapa 4. Se ativar o agente do SNMPv3, continue com a etapa 5 na página 75. Se ativar os Traps SNMP, continue com a etapa 6 na página 75
4. Se ativar agente do SNMPv1, conclua os campos a seguir:
 - a. Clique na guia **Contato**. No campo **Pessoa de Contato**, insira o nome da pessoa de contato. No campo **Local**, insira o site (coordenadas geográficas).
 - b. Clique na guia **Comunidades** para configurar uma comunidade para definir o relacionamento administrativo entre agentes do SNMP e gerenciadores de SNMP. Você deve definir pelo menos uma comunidade.

Notas:

- Se aparecer uma janela de mensagem de erro, faça os ajustes necessários nos campos que são listados na janela de erro; em seguida, role para a parte superior da página e clique em **Aplicar** para salvar suas informações corrigidas.
- Você deve configurar pelo menos uma comunidade para ativar esse agente do SNMP.

Preencha os campos a seguir:

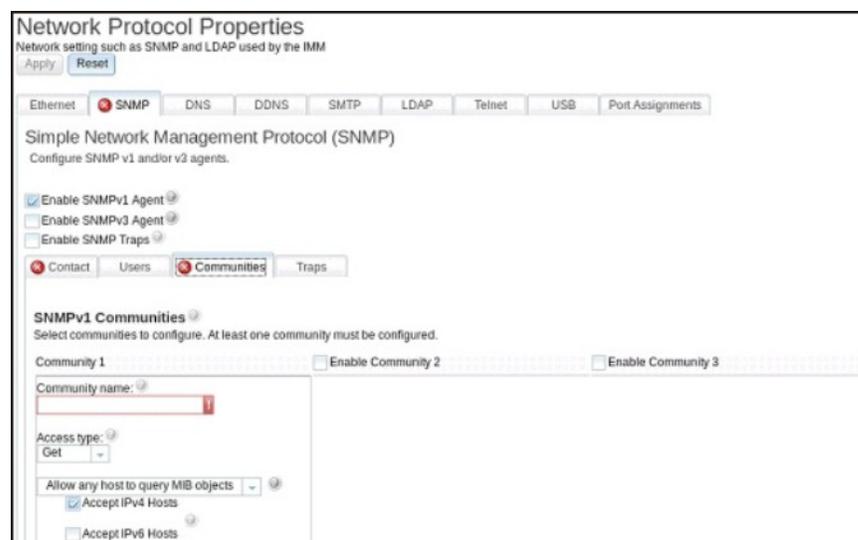
- 1) No campo **Nome da Comunidade**, insira um nome ou sequência de autenticação para especificar a comunidade.
- 2) No campo **Tipo de Acesso**, selecione um tipo de acesso.
 - Selecione **Trap** para permitir que todos os hosts na comunidade recebam traps.
 - Selecione **Obter** para permitir que todos os hosts na comunidade recebam traps e objetos Management Information Base (MIB) de consulta.
 - Selecione **Configurar** para permitir que todos os hosts na comunidade recebam traps, consultem e configurem objetos MIB.
- c. No campo **Nome do Host** ou **Endereço IP**, insira o nome do host ou endereço IP de cada gerenciador de comunidade.
- d. Clique em **Aplicar** para aplicar as mudanças feitas.
5. Se ativar o agente do SNMPv3, conclua os campos a seguir:
 - a. Clique na guia **Contato**. No campo **Pessoa de Contato**, insira o nome da pessoa de contato. No campo **Local**, insira o site (coordenadas geográficas).
 - b. Clique na guia **Usuários** para mostrar a lista de contas de usuário locais para o console.

Nota: Esta é a mesma lista que está na opção Usuários. Você deve configurar o SNMPv3 para cada conta do usuário que precisará de acesso ao SNMPv3.

- c. Clique em **Aplicar** para aplicar as mudanças feitas.
6. Se ativar os Traps SNMP, configure os eventos alertados na guia **Traps**.

Nota: Ao configurar o SNMP, os campos obrigatórios que não estão concluídos ou possuem valores incorretos são destacados com um X vermelho que pode ser usado para orientá-lo na conclusão dos campos obrigatórios.

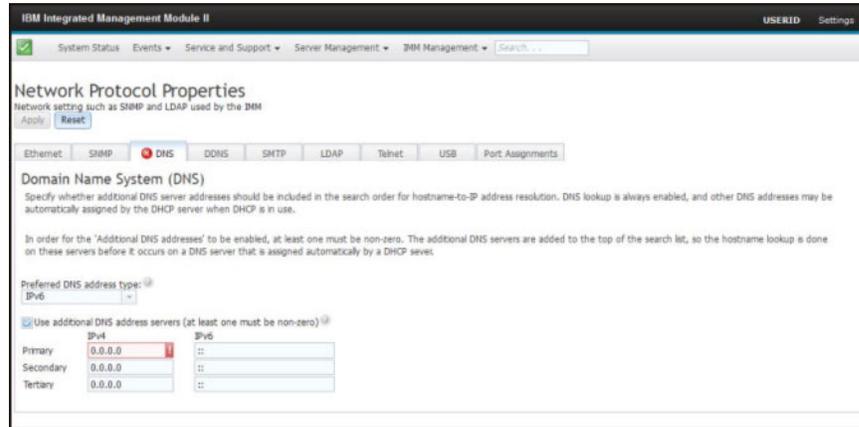
A ilustração a seguir mostra a guia SNMP ao configurar o agente do SNMPv1.



Configurando o DNS

Clique na guia **DNS** para visualizar ou modificar configurações do Sistema de Nomes de Domínio do IMM2. Se você clicar na caixa de seleção **Usar servidores**

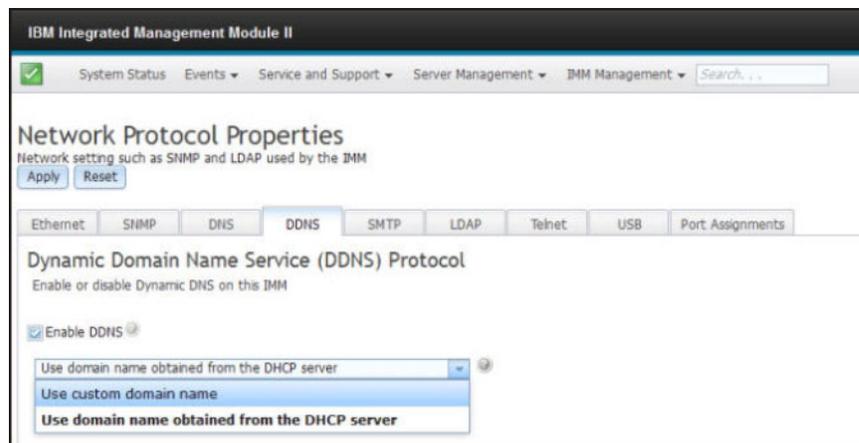
de endereço DNS adicionais, especifique os endereços IP de até três servidores do Sistema de Nomes de Domínio em sua rede. Cada endereço IP deve conter números inteiros de 0 a 255, separados por pontos (conforme mostrado na ilustração a seguir).



Configurando o DDNS

Clique na guia **DDNS** para visualizar ou modificar configurações do Sistema Dinâmico de Nomes de Domínio do IMM2. Clique na caixa de seleção **Ativar DDNS** para ativar o DDNS. Quando o DDNS é ativado, o IMM2 notifica um servidor de nomes de domínio para alterar, em tempo real, a configuração do servidor de nomes de domínio ativo de seus nomes de host, endereços ou outras informações configuradas, armazenadas no servidor de nomes de domínio.

Escolha uma opção a partir da lista de itens para selecionar como você deseja que o nome de domínio do IMM2 seja selecionado (conforme mostrado na ilustração a seguir).



Configurando o SMTP

Clique na guia **SMTP** para visualizar ou modificar configurações de SMTP do IMM2. Conclua os campos a seguir para visualizar ou modificar configurações de SMTP:

Endereço IP ou nome do host

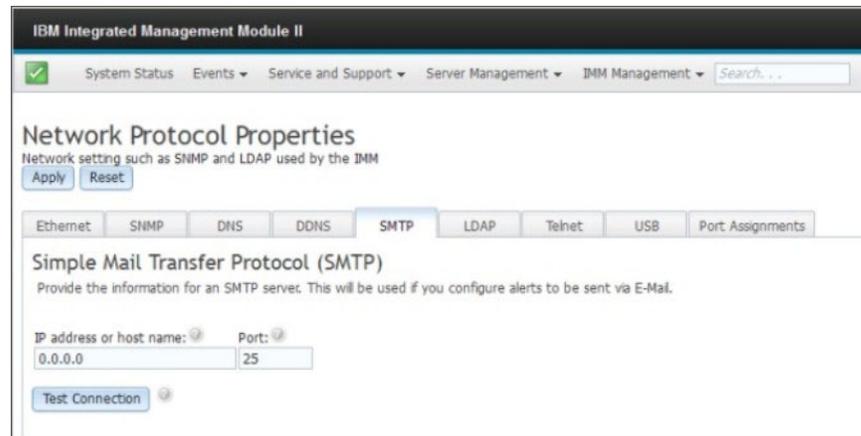
Digite o nome do host do servidor SMTP. Use esse campo para especificar o endereço IP ou, se o DNS estiver ativado e configurado, o nome do host do servidor SMTP.

Porta Especifique o número da porta para o servidor SMTP. O valor padrão é 25.

Conexão de Teste

Clique em **Conexão de Teste**, um email de teste é enviado para verificar se suas configurações de SMTP estão corretas.

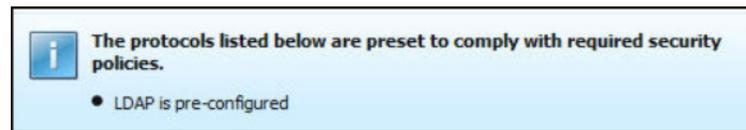
A ilustração a seguir mostra a guia SMTP.



Configurando o LDAP

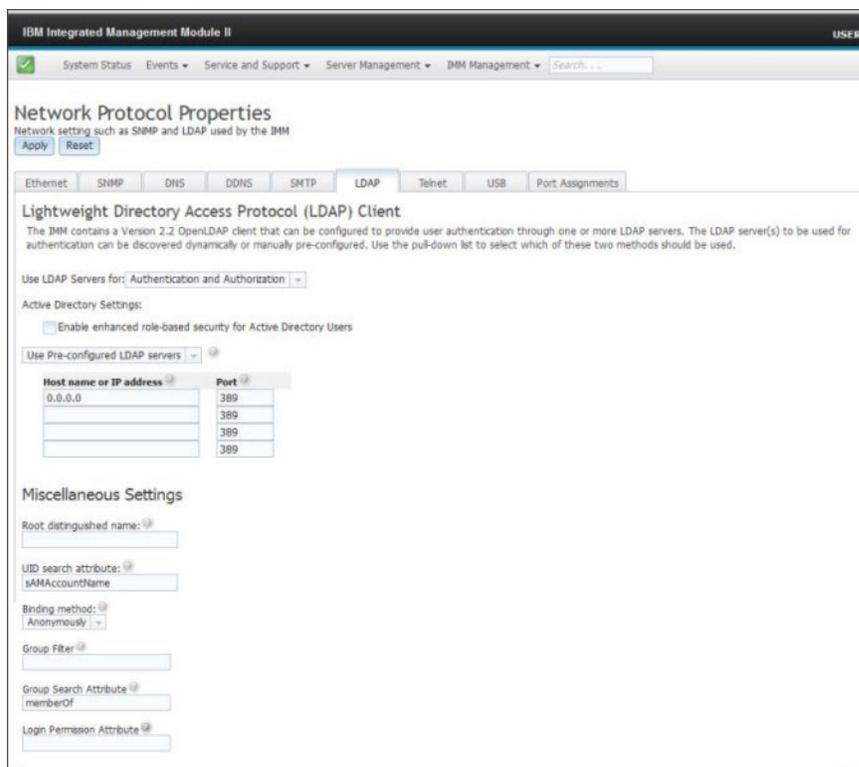
Clique na guia **LDAP** para visualizar ou modificar as configurações do Cliente LDAP do IMM2.

Nota: Em um IBM Flex System, o IMM2 é configurado para usar o servidor LDAP em execução no CMM. Você verá uma mensagem informativa que o lembrará de que as configurações LDAP não podem ser alteradas (conforme mostrado na ilustração a seguir).



Usando um servidor LDAP, o IMM2 pode autenticar um usuário, consultando ou procurando um diretório LDAP em um servidor LDAP, em vez de passar por seu banco de dados do usuário local. O IMM pode autenticar remotamente qualquer acesso de usuário por meio de um servidor LDAP central. É possível designar níveis de autoridade de acordo com as informações localizadas no servidor LDAP. É possível também usar o LDAP para designar usuários e IMM2s a grupos e executar a autenticação do grupo, além da autenticação normal do usuário (verificação de senha). Por exemplo, um IMM2 pode ser associado a um ou mais grupos; o usuário só passaria pela autenticação de grupo se o usuário pertencesse a pelo menos um grupo associado ao IMM2.

A ilustração a seguir mostra a guia LDAP.



Para usar um servidor LDAP pré-configurado, conclua os campos a seguir:

Lista de itens de configuração do servidor LDAP

Selecione **Usar Servidor LDAP Pré-configurado** na lista de itens. 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 asseguradas, o valor padrão é 636. Você deve configurar pelo menos um servidor LDAP.

Nome Distinto Raiz

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

Atributo de Procura de UID

Quando o método de ligação é configurado para **Anonimamente** ou **Com Credenciais Configuradas**, a ligação inicial para o servidor LDAP é seguida por uma solicitação de procura que recupera informações específicas sobre o usuário, incluindo o DN do usuário, as permissões de login e a associação ao grupo. Essa solicitação de procura 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**.

Método de ligação

Antes de 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:

- Anonimamente

- Use esse método para ligação sem um 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.
- Com Credenciais Configuradas
 - Use esse método para ligação com DN e senha do cliente configurados.
- Com 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 por meio de um DN, um nome completo de domínio ou um ID do usuário que corresponda ao **Atributo de Procura de UID** que é configurado no IMM2. 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 isso falhar, o usuário terá o acesso negado. A segunda ligação será executada apenas quando os métodos de ligação **Anônimo** ou **Com Credenciais Configuradas** forem usados.

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 processador de serviços pertence. Isso significa que o usuário deve pertencer a pelo menos um dos grupos configurados para que a autenticação de grupo seja bem-sucedida. 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. Uma seleção para permitir, ou não, o uso de curingas no nome do grupo é fornecida. O filtro pode ser um nome de grupo específico (por exemplo, IMMWest), um asterisco (*) usado como um curinga que corresponde a tudo ou um curinga com um prefixo (por exemplo, IMM*). O filtro padrão é IMM*. Se as políticas de segurança em sua instalação proibirem o uso de curingas, será possível escolher não permitir o uso de curingas. O caractere curinga (*) é, então, tratado como um caractere normal em vez do curinga. 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 de *cn=adminGroup,dc=mycompany,dc=com* pode ser especificado usando o DN real ou com *adminGroup*.

Somente em ambientes Active Directory, a associação ao grupo aninhado é suportada. 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 é o da posição 0 e o bit mais à direita é o da posição 11. Um valor de 1 em uma posição de bit ativa 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 4. Bits de permissão

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 Conta 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 Disco Remoto	Um usuário pode acessar o console do servidor remoto e as funções de disco remoto para o servidor remoto.
7	Acesso a Energia/Reinicialização do 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 para Limpar Logs de Eventos	Um usuário pode limpar os logs de eventos. Nota: Todos os usuários podem visualizar os logs de eventos; mas, o usuário precisa ter esse nível de permissão para limpar os logs.

Tabela 4. Bits de permissão (continuação)

Posição do Bit	Função	Explicação
10	Configuração de Adaptador Avançada	Um usuário não tem restrições ao configurar o IMM2. Além disso, o usuário tem acesso administrativo ao IMM2. O usuário pode executar as funções avançadas a seguir: upgrades de firmware, inicialização da rede rede PXE, restaurar os padrões de factory do IMM2, modificar e restaurar a configuração de adaptador a partir de um arquivo de configuração e reiniciar/reconfigurar o IMM2.
11	Reservado	<p>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.</p> <p>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.</p> <p>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.</p>

Configurando Telnet

Selecione a guia **Telnet** para visualizar ou modificar as configurações de Telnet do IMM2. Conclua os campos a seguir para visualizar ou modificar configurações de Telnet:

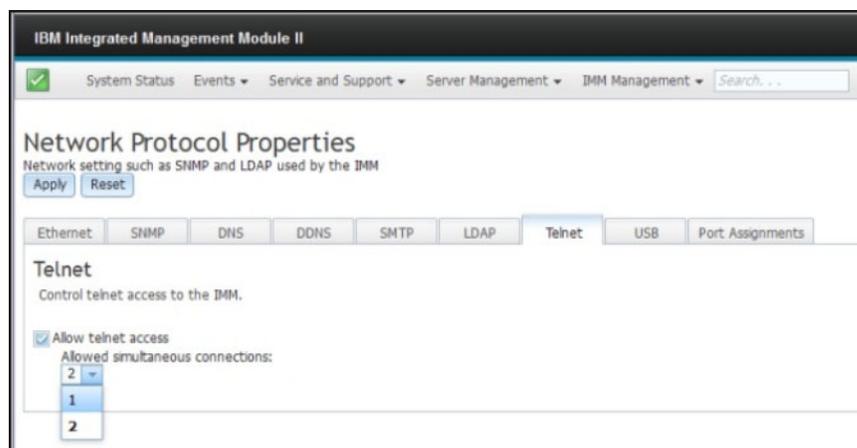
Permitir Acesso Telnet

Coloque uma marca de seleção na caixa de seleção para escolher se deseja, ou não, que o IMM2 permita acesso Telnet.

Conexões Simultâneas Permitidas

Use a lista **Conexões Simultâneas Permitidas** para escolher o número de conexões Telnet a serem permitidas ao mesmo tempo.

A ilustração a seguir mostra a guia Telnet.

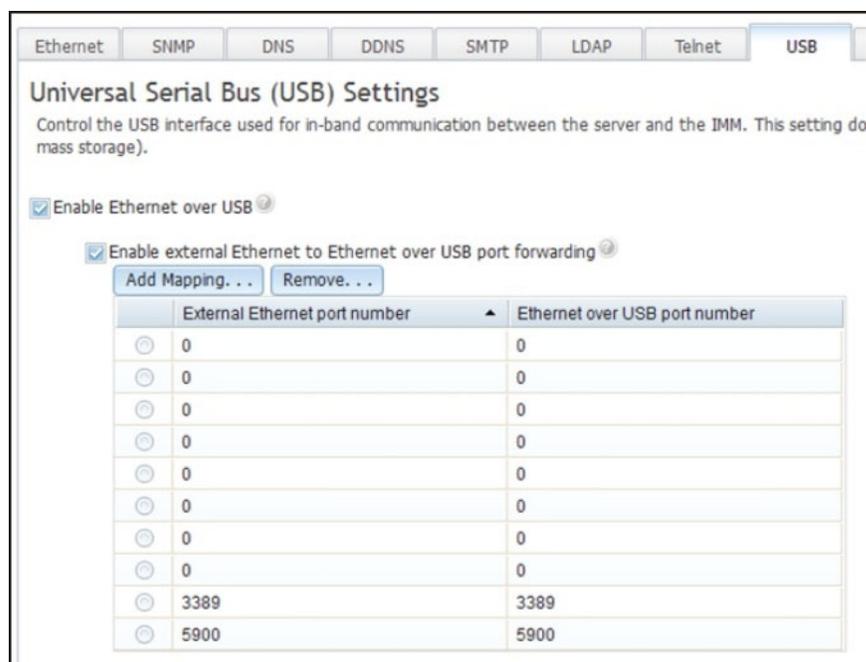


Configurando USB

Selecione a guia **USB** para visualizar ou modificar as configurações de USB do IMM2. A interface USB dentro da banda, ou LAN sobre USB, é usada para comunicação dentro da banda com o IMM2. Clique na caixa de seleção **Ativar Ethernet sobre USB** para ativar ou desativar a interface LAN sobre USB do IMM2.

Importante: Se você desativar a interface USB dentro da banda, não será possível executar uma atualização dentro da banda do firmware do IMM2, do firmware do servidor e do firmware do DSA usando os utilitários de atualização do Linux ou Windows. Se a interface USB dentro da banda estiver desativada, use a opção Servidor do Firmware na guia Gerenciamento do Servidor para atualizar o firmware. Se você desativar a interface USB dentro da banda, desative também os tempos limites de watchdog para evitar que o servidor seja reiniciado inesperadamente.

A ilustração a seguir mostra a guia USB.



O mapeamento de números de portas Ethernet externas para números de portas Ethernet sobre USB é controlado clicando na caixa de seleção **Ativar encaminhamento de portas Ethernet externas para Ethernet sobre USB** e concluindo as informações de mapeamento das portas que você deseja que sejam encaminhadas.

Configurando designações de porta

Selecione a guia **Designações de Porta** para visualizar ou modificar designações de porta do IMM2. Conclua os campos a seguir para visualizar ou modificar designações de porta:

HTTP Nesse campo, especifique o número da porta para o servidor HTTP do IMM2. O valor padrão é 80. Os valores de números de porta válidos são de 1 a 65535.

HTTPS

Nesse campo, especifique o número da porta que é usado para o tráfego HTTPS Secure Sockets Layer (SSL) da interface da web. O valor padrão é 443. Os valores de números de porta válidos são de 1 a 65535.

CLI Telnet

Nesse campo, especifique o número da porta da CLI Legada para efetuar login usando o serviço Telnet. O valor padrão é 23. Os valores de números de porta válidos são de 1 a 65535.

CLI Legada SSH

Nesse campo, especifique o número da porta que é configurado para a CLI Legada para efetuar login 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 IMM2. 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.

Controle Remoto

Nesse campo, especifique o número da porta que o recurso de controle remoto usa para visualizar e interagir com o console do servidor. O valor padrão é 3900 para servidores torre e montados em rack.

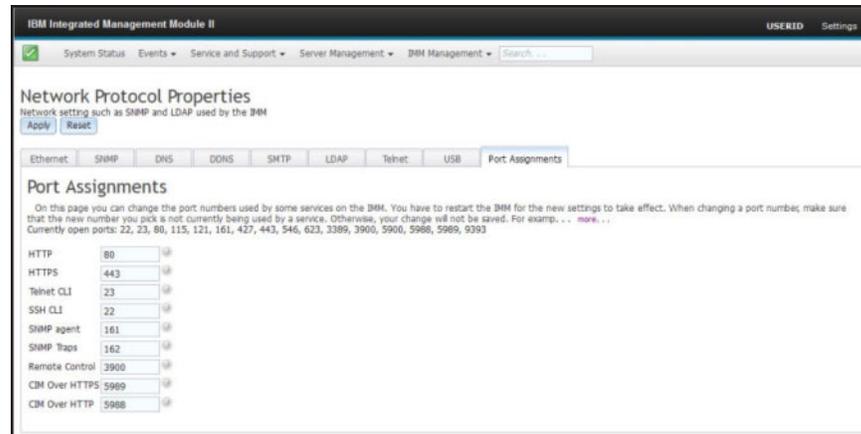
CIM sobre HTTP

Nesse campo, especifique o número da porta para o CIM sobre HTTP. O valor padrão é 5988.

CIM sobre HTTPS

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

A ilustração a seguir mostra a guia Designações de Porta.



Definindo a Configuração de Segurança

Clique na opção **Segurança** na guia Gerenciamento do IMM (conforme mostrado na ilustração a seguir) para acessar e configurar as propriedades de segurança, o status e as configurações para seu IMM2.

Para aplicar quaisquer mudanças feitas, você deve clicar no botão **Aplicar** na parte superior esquerda da janela Segurança do IMM. Para reconfigurar quaisquer mudanças feitas, você deve clicar no botão **Reconfigurar Valores**.



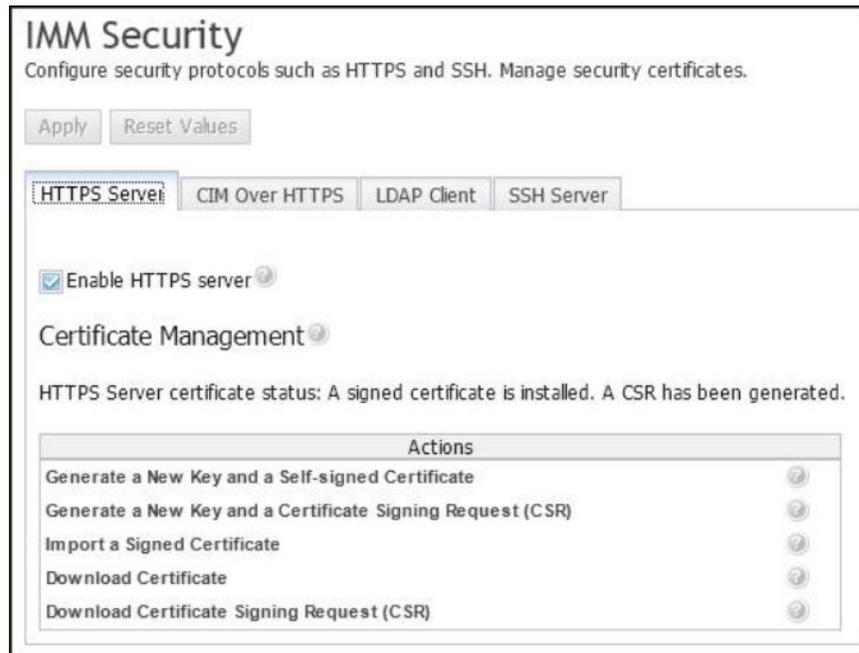
Configurando o Protocolo HTTPS

Clique na guia **Servidor HTTPS** para configurar a interface da web do IMM2 para usar o protocolo HTTPS mais seguro, em vez do protocolo HTTP padrão.

Notas:

- Apenas um protocolo pode ser ativado por vez.
- A ativação dessa opção requer configuração adicional dos certificados SSL.
- Ao alterar os protocolos, você deve reiniciar o servidor da web do IMM2.

Para obter informações adicionais sobre SSL, consulte “Visão Geral do SSL” na página 90. A ilustração a seguir mostra a guia Servidor HTTPS.



Nota: Em alguns servidores, os níveis de segurança do IMM2 podem ser controlados por outro sistema de gerenciamento. Em tais ambientes, é possível desativar as ações acima na interface da web do IMM2.

Manipulação de Certificado HTTPS

Use as opções no menu Ações para manipulação de certificado HTTPS. Se uma opção for desativada, poderá ser necessário executar uma outra ação primeiro para ativá-la. Ao trabalhar com certificados HTTPS, você deve desativar o servidor HTTPS. Para obter informações adicionais sobre manipulação de certificado, consulte “Manipulação de Certificado SSL” na página 90.

Nota: Depois de configurar a manipulação de certificado, você deve reiniciar o IMM2 para que as mudanças entrem em vigor.

Configurando o Protocolo CIM sobre HTTPS

Clique na guia **CIM sobre HTTPS** para configurar a interface da web do IMM2 para usar o protocolo CIM sobre HTTPS mais seguro, em vez do protocolo CIM sobre HTTP padrão.

Notas:

- Apenas um protocolo pode ser ativado por vez.
- A ativação dessa opção requer configuração adicional dos certificados SSL.

- Ao alterar os protocolos, você deve reiniciar o servidor da web do IMM2.

Para obter informações adicionais sobre SSL, consulte “Visão Geral do SSL” na página 90. A ilustração a seguir mostra a guia CIM sobre HTTPS.



Manipulação de Certificado CIM sobre HTTPS

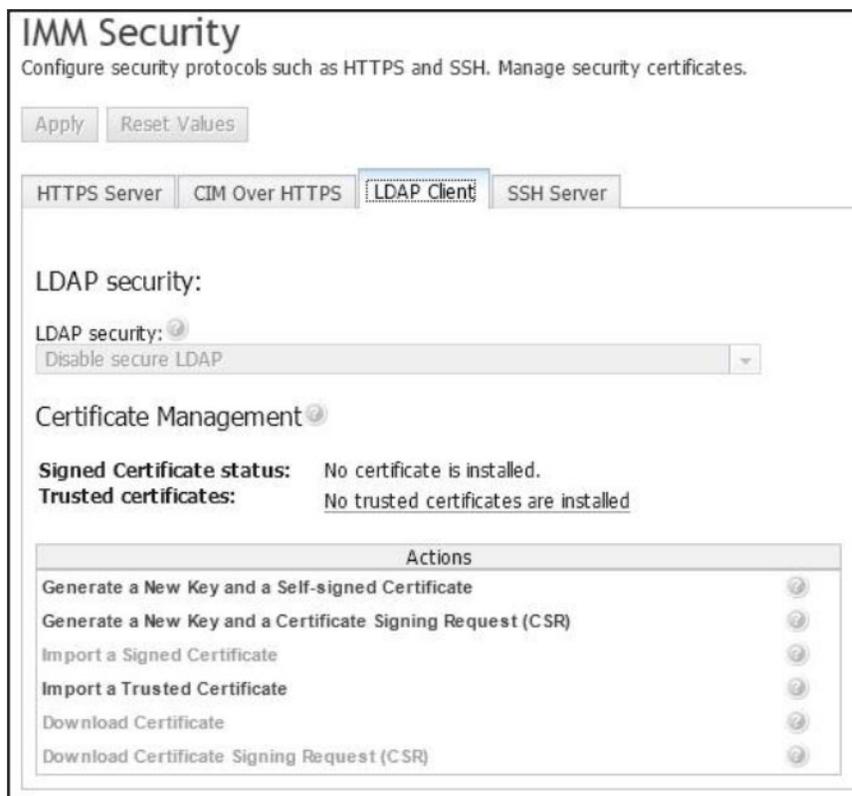
Use as opções sob o menu Ações para manipulação de certificado CIM sobre HTTPS. Se uma opção for desativada, poderá ser necessário executar uma outra ação primeiro para ativá-la. Para obter informações adicionais sobre manipulação de certificado, consulte “Manipulação de Certificado SSL” na página 90.

Nota: Depois de configurar a manipulação de certificado, você deve reiniciar o IMM2 para que as mudanças entrem em vigor.

Configurando o Protocolo do Cliente LDAP

Clique na opção **Cliente LDAP** para usar o protocolo LDAP sobre SSL mais seguro em vez do protocolo LDAP padrão.

Nota: A ativação dessa opção requer configuração adicional dos certificados SSL. Para obter informações adicionais sobre SSL, consulte “Visão Geral do SSL” na página 90. A ilustração a seguir mostra a guia Cliente LDAP.

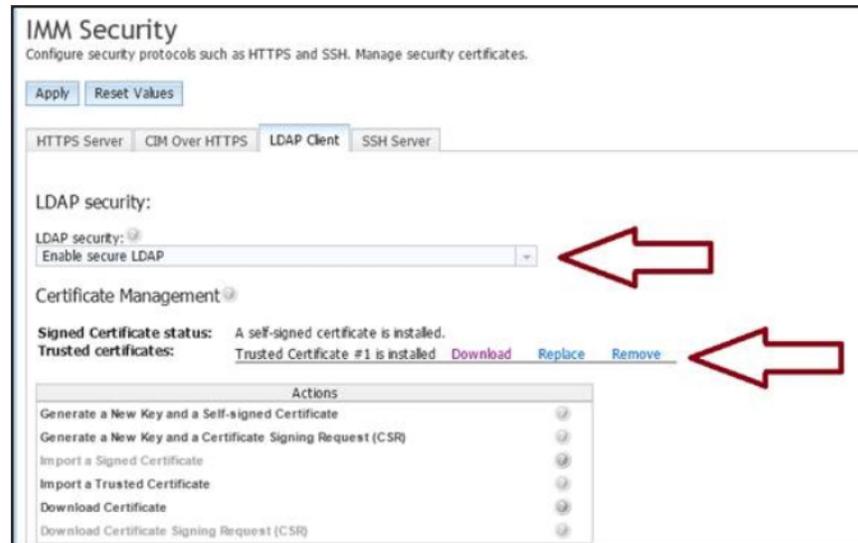


Manipulação de Certificado de Cliente LDAP Seguro

Use as opções sob o menu Ações para manipulação de certificado LDAP sobre SSL. Se uma opção for desativada, poderá ser necessário executar uma outra ação primeiro para ativá-la. Ao manipular certificados HTTPS, você deve desativar o servidor HTTPS. Para obter informações adicionais sobre manipulação de certificado, consulte “Manipulação de Certificado SSL” na página 90. Após a instalação do Certificado de Confiança, é possível ativar o LDAP sobre SSL conforme mostrado na ilustração a seguir.

Notas:

- As mudanças em seu IMM2 entrarão em vigor imediatamente.
- Seu servidor LDAP deve suportar o Secure Socket Layer 3 (SSL3) ou a Segurança da Camada de Transporte (TLS) para ser compatível com o cliente LDAP seguro do IMM2.



Configurando o servidor Shell Seguro

Clique na guia **Servidor SSH** para configurar a interface da web do IMM2 para usar o protocolo SSH mais seguro, em vez do protocolo Telnet padrão.

Nota:

- Nenhum gerenciamento de certificado é necessário para usar essa opção.
- O IMM2 criará inicialmente uma chave do Servidor SSH. Se você deseja gerar uma nova chave do Servidor SSH, clique em **Gerar Chave do Host Privado do Servidor SSH** no menu Ações.
- Depois de concluir a ação, você deve reiniciar o IMM2 para que suas mudanças entrem em vigor.

A guia Servidor SSH é mostrada na ilustração a seguir.



Visão Geral do 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 foi designada para evitar intrusões, violações e falsificação de mensagens. É possível configurar o IMM2 para usar suporte SSL para diferentes tipos de conexões, como servidor da web seguro (HTTPS), conexão LDAP segura (LDAPS), CIM sobre HTTPS e servidor SSH. É possível visualizar ou alterar as configurações de SSL a partir da opção Segurança na guia Gerenciamento do IMM. Também é possível ativar ou desativar o SSL e gerenciar os certificados requeridos para SSL.

Manipulação de Certificado 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 IMM2 e interceptar os dados que fluem entre o servidor da web do IMM2 real e o navegador da web do usuário. Se, no momento da conexão inicial entre o navegador e o IMM2, 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, clique em **Gerar uma Nova Chave e uma Certificate Signing Request (CSR)** no menu Ações. Em seguida, você deve enviar a Certificate Signing Request (CSR) para uma CA e fazer acordos para obter um certificado final. Quando o certificado final é recebido, ele é importado para o IMM2 clicando em **Importar um Certificado Assinado** no menu Ações.

A função da CA é verificar a identidade do IMM2. Um certificado contém assinaturas digitais para a CA e o IMM2. 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 IMM2.

O IMM2 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

Ao gerenciar certificados do IMM2, é apresentada uma lista de ações ou um subconjunto delas (conforme mostrado na ilustração a seguir).



Se um certificado estiver atualmente instalado, será possível usar a ação **Fazer o Download do Certificado** no menu Ações para fazer o download do CSR ou certificado atualmente instalado. Os certificados que aparecem esmaecidos *não* estão atualmente instalados. O cliente LDAP seguro requer que o usuário importe um certificado de confiança. Clique em **Importar um Certificado de Confiança** no menu Ações. Após a geração de um CSR, clique em **Importar um Certificado Assinado** no menu Ações.

Ao executar uma das ações "Gerar", uma janela Gerar Nova Chave e Certificado Autoassinado é aberta (conforme mostrado na ilustração a seguir).

The image shows a dialog box titled "Generate New Key and Self-signed Certificate". It contains two sections: "Required SSL Certificate Data" and "Optional SSL Certificate Data".

Required SSL Certificate Data:

- Country: US United States
- State or Province: NY
- City or Locality: New York
- Organization Name: My Company
- IMM Host Name: imm1234

Optional SSL Certificate Data:

- Contact Person: Chris Manager
- E-Mail address: cmanager@mycomp.com
- Organizational Unit: Sales
- Surname: (empty)
- Given Name: (empty)
- Initials: (empty)
- DN Qualifier: (empty)

At the bottom of the dialog are "Ok" and "Cancel" buttons.

A janela Gerar Nova Chave e Certificado Autoassinado solicitará a você para concluir os campos obrigatórios e opcionais. Você *deve* concluir os campos obrigatórios. Depois de inserir suas informações, clique em **Ok** para concluir a tarefa. Uma janela Certificado Gerado é aberta (conforme mostrado na ilustração a seguir).



Restaurando e modificando a configuração do IMM

Selecione a opção **Configuração do IMM** na guia Gerenciamento do IMM para obter as opções para executar as ações a seguir:

- Visualizar um resumo de configuração do IMM2
- Fazer backup ou restaurar a configuração do IMM2
- Visualizar o status de backup ou restauração
- Redefinir a configuração do IMM2 para suas configurações padrão de factory
- Acessar o assistente de configuração inicial do IMM2

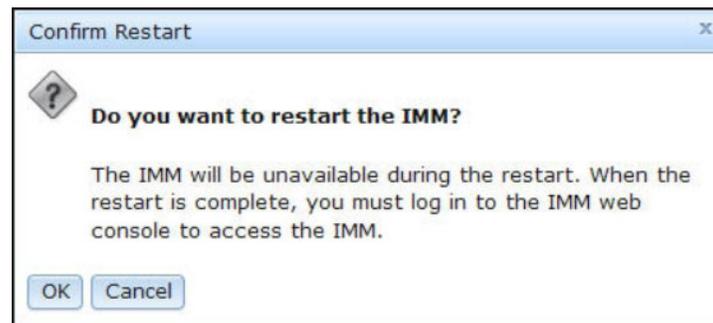
Reiniciando o IMM2

Selecione a opção **Reiniciar o IMM** na guia Gerenciamento do IMM para reiniciar o IMM2. Apenas pessoas com autoridade de supervisor podem executar esta função. Quando conexões Ethernet são temporariamente eliminadas, você deve efetuar login no IMM2 para acessar a interface da web do IMM2.

Para reiniciar o IMM2, conclua as etapas a seguir:

1. Efetue login no IMM2. Para obter mais informações, consulte “Efetuando Login no IMM2” na página 10.
2. Clique na guia **Gerenciamento do IMM**; em seguida, clique em **Reiniciar o IMM**.
3. Clique no botão **OK** na janela Confirmar Reinicialização. O IMM2 será reiniciado.

A ilustração a seguir mostra a janela Confirmar Reinicialização.



Quando você reinicia o IMM2, suas conexões TCP/IP ou de modem são interrompidas.

A ilustração a seguir mostra a janela de notificação que você verá quando o IMM2 estiver sendo reiniciado.



4. Efetue login novamente para usar a interface da web do IMM2 (consulte "Efetuando Login no IMM2" na página 10 para obter instruções.

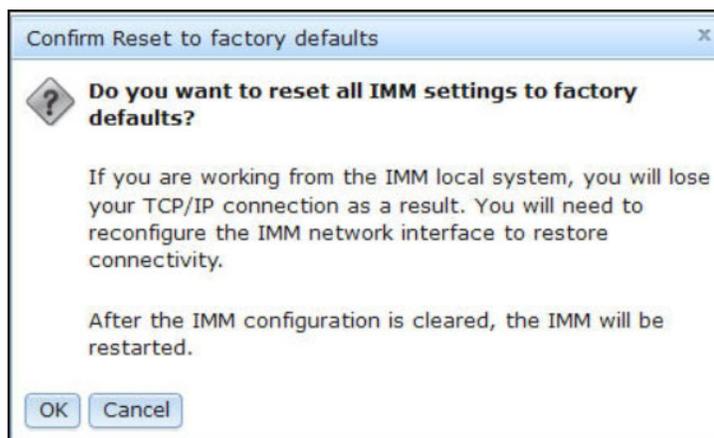
Reconfigurando o IMM2 para os Padrões de Factory

Selecione a opção **Reconfigurar o IMM para Padrões de Factory...** na guia Gerenciamento do IMM para restaurar o IMM2 para as configurações padrão de factory. Apenas pessoas com autoridade de supervisor podem executar esta função. Quando conexões Ethernet são temporariamente eliminadas, você deve efetuar login no IMM2 para acessar a interface da web do IMM2.

Atenção: Quando você usar a opção Reconfigurar o IMM para Padrões de Factory, todas as modificações feitas no IMM2 serão perdidas.

Para restaurar os padrões de factory do IMM2, conclua as etapas a seguir:

1. Efetue login no IMM2. Para obter mais informações, consulte "Efetuando Login no IMM2" na página 10.
2. Clique na guia **Gerenciamento do IMM**; em seguida, clique em **Reconfiguração do IMM para Padrões de Factory...**
3. Clique no botão **OK** na janela Confirmar Reconfiguração para Padrões de Factory (conforme mostrado na ilustração a seguir).



Nota: Depois que a configuração do IMM2 for concluída, o IMM2 será reiniciado. Se este for um servidor local, a conexão TCP/IP será interrompida e você deverá reconfigurar a interface de rede para restaurar a conectividade.

4. Efetue login novamente no IMM2 para usar a interface da web do IMM2, (consulte "Efetuando Login no IMM2" na página 10 para obter instruções).
5. Reconfigure a interface de rede para restaurar a conectividade.

Chave de Gerenciamento de Ativação

Clique na opção **Gerenciamento de Chave de Ativação** na guia Gerenciamento do IMM para gerenciar chaves de ativação para recursos Features on Demand (FoD) opcionais do IMM2 e do servidor. Consulte Capítulo 7, "Features on Demand", na página 139 para obter informações sobre como gerenciar chaves de ativação de FoD.

Capítulo 5. Monitorando o Status de Servidor

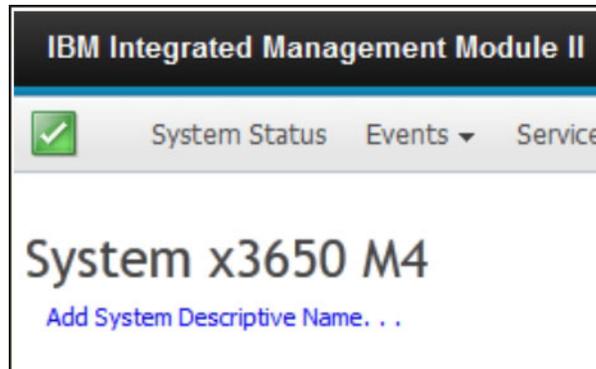
Este capítulo fornece informações sobre como visualizar e monitorar as informações para o servidor que você está acessando.

Visualizando o Status do Sistema

A página Status do Sistema fornece uma visão geral do status de operação do servidor IMM2. Essa página também exibe o funcionamento do hardware do servidor e quaisquer eventos ativos que ocorrerem no servidor.

Nota: Se você acessar outra página a partir da página Status do Sistema, será possível retornar à página Status do Sistema clicando em **Status do Sistema** nos itens de menus na parte superior da página.

É possível incluir um nome descritivo para o IMM2 para ajudar você a identificar entre um IMM2 e outro. Clique no link **Incluir Nome Descritivo do Sistema...** localizado abaixo do nome do produto do servidor para designar um nome para associar ao IMM2 (conforme mostrado na ilustração a seguir).



Na janela Alterar Nome Descritivo do Sistema, especifique um nome para associar ao IMM2 (conforme mostrado na ilustração a seguir).



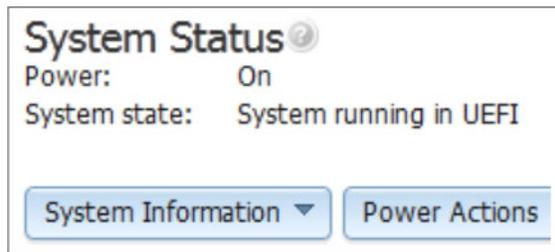
É possível renomear o Nome Descritivo do Sistema clicando no link **Renomear...** que está localizado próximo ao Nome Descritivo do Sistema.

A ilustração a seguir mostra o link Renomear.



A página Status do Sistema exibe o estado da energia e o estado de operação do servidor. O status exibido é o estado do servidor no momento em que a página Status do Sistema é aberta.

A ilustração a seguir mostra os campos **Energia** e **Estado do Sistema**.



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

Tabela 5. Descrições de Estados do Sistema

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.

Tabela 5. Descrições de Estados do Sistema (continuação)

Estado	Descrição
Inicializando S.O. ou em S.O. não suportado	O servidor pode estar nesse estado por um dos motivos a seguir: <ul style="list-style-type: none"> • O carregador do sistema operacional (OS) foi iniciado; mas o S.O. não está em execução • A interface Ethernet sobre USB do IMM2 está desativada. • O S.O. não possui os drivers carregados que suportam a interface Ethernet sobre USB.
S.O. inicializado	O S.O. do servidor está em execução.
Suspender para RAM	O servidor foi colocado no estado de espera ou de suspensão.

As opções de menu a seguir na página Status do Sistema fornecem informações adicionais do servidor e ações que podem ser executadas no servidor.

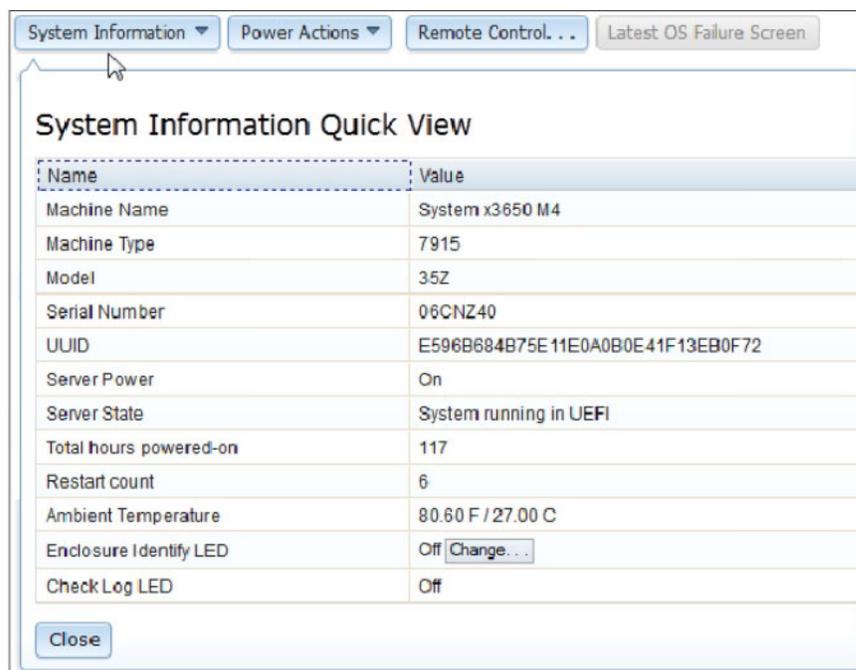
- Informações do Sistema
- Ações de Energia
- Controle Remoto, (consulte “Funções de Presença Remota e Controle Remoto” na página 105 para obter informações adicionais).
- Tela de Falha mais Recente do S.O., (consulte “Capturando os Dados da Tela de Falha mais Recente do S.O.” na página 132 para obter informações adicionais).

Visualizando as Informações do Sistema

O menu Informações do Sistema fornece um resumo das informações comuns do servidor. Clique na guia **Informações do Sistema** na página Status do Sistema para visualizar as informações a seguir:

- Nome da máquina
- Tipo de máquina
- Modelo
- Número de série
- Identificador Exclusivo Universal (UUID)
- Energia do servidor
- Estado do servidor
- Total de horas ligado
- Contagem de reinicializações
- Temperatura ambiente
- LED de identidade do gabinete
- LED do log de verificação

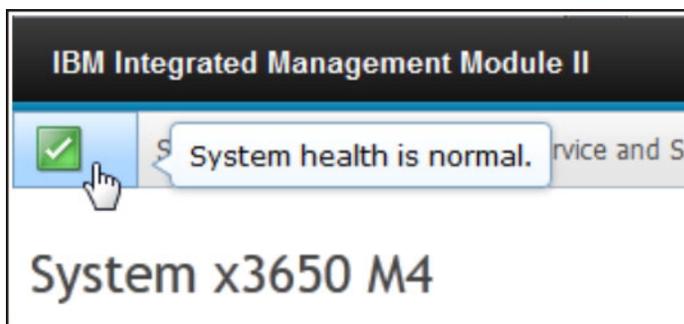
A ilustração a seguir mostra a janela Informações do Sistema.



Visualizando o Funcionamento do Servidor

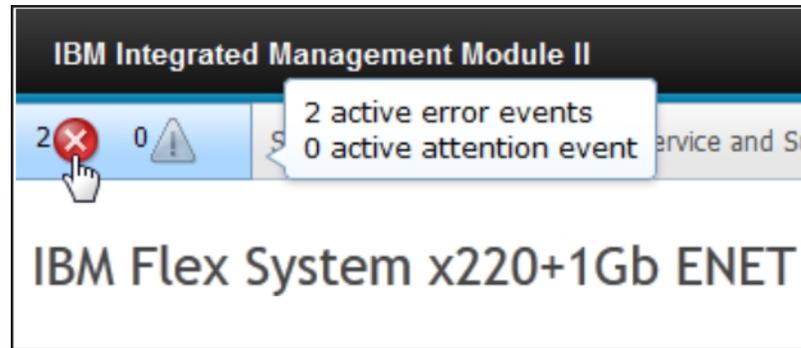
O funcionamento do servidor é exibido sob a barra de título no canto superior esquerdo da página Status do Sistema e é designado por um ícone. Uma marca de seleção verde indica que o hardware do servidor está operando normalmente. Mova o cursor sobre o visto verde para obter uma indicação rápida do funcionamento do servidor.

A ilustração a seguir é um exemplo de um servidor em um modo de operação normal.



Um ícone de triângulo amarelo indica que existe uma condição de aviso. Um ícone de círculo vermelho indica que existe uma condição de erro.

A ilustração a seguir é um exemplo de um servidor com eventos de erro ativos.



Se um ícone de aviso (triângulo amarelo) ou ícone de erro (círculo vermelho) for exibido, clique no ícone para exibir os eventos correspondentes na seção Eventos Ativos da página Status do Sistema.

A ilustração a seguir é um exemplo da seção Eventos Ativos com condições de erro.

Active Events			
Severity	Source	Date	Message
Error	System	16 Jul 2012 01:00:28.000 PM	Sensor Mezz Exp 2 Fault has transitioned to critical from a less severe state.
Error	System	16 Jul 2012 01:00:29.000 PM	Sensor Mezz Exp 2 Fault has transitioned to critical from a less severe state.

Visualizando o Funcionamento do Hardware

A seção Funcionamento do Hardware da página Status do Sistema lista os componentes de hardware do servidor e exibe o status de funcionamento de cada componente monitorado pelo IMM2. O status de funcionamento exibido para um componente pode refletir o estado mais crítico de todos os componentes individuais para um tipo de componente. Por exemplo, um servidor pode ter vários módulos de energia instalados e todos os módulos de energia estão operando normalmente, exceto um. O status do componente Módulos de Energia indicará crítico por causa do módulo de energia que não está operando normalmente.

A ilustração a seguir mostra a seção Funcionamento do Hardware da página Status do Sistema.

Hardware Health ⓘ	
Component Type	Status
Cooling Devices	✓ Normal
Power Modules	✗ Critical
Disks	✓ Normal
Processors	✓ Normal
Memory	✓ Normal
System	✓ Normal

Cada tipo de componente é exibido como um link que pode ser clicado para obter informações mais detalhadas. Quando você seleciona um Tipo de Componente para visualização, uma tabela listando o status de todos os componentes para esse Tipo de Componente é exibida.

A ilustração a seguir mostra os componentes para o Tipo de Componente de Memória.

Memory			
Display the memory modules available on the server. Clicking on a module displays a Properties pop-up window with 2 tabs: Eve			
FRU Name	Status	Type	Capacity (GB)
DIMM 4	✓ Normal	DDR3	4
DIMM 9	✓ Normal	DDR3	4
DIMM 16	✓ Normal	DDR3	4
DIMM 21	✓ Normal	DDR3	4

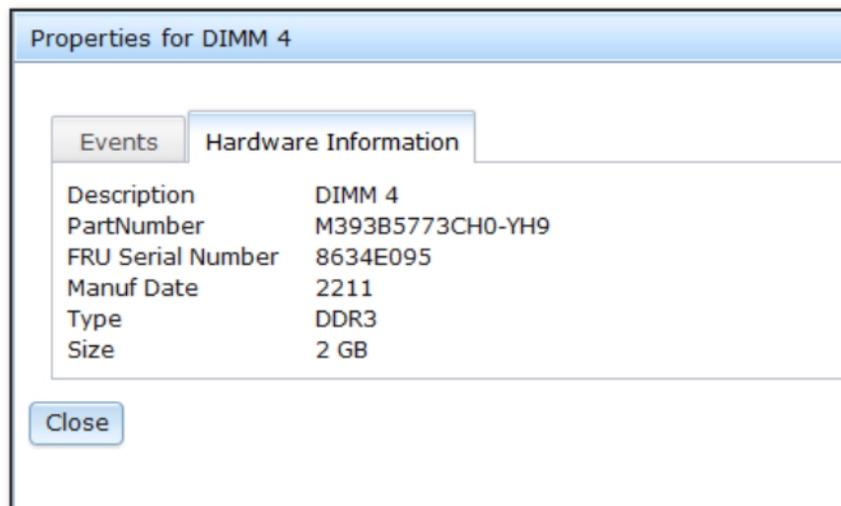
É possível clicar em um link de Unidade Substituível em Campo (FRU) individual na tabela para obter informações adicionais para esse componente. Todos os eventos ativos para o componente são, então, exibidos na guia Eventos.

A ilustração a seguir mostra a guia Eventos para o DIMM 4.



Se aplicável, informações adicionais para o componente podem ser fornecidas na guia Informações do Hardware.

A ilustração a seguir mostra a guia Informações do Hardware para o DIMM 4.



Capítulo 6. Executando Tarefas do IMM2

É possível usar as informações nesta seção e no Capítulo 3, “Visão Geral da Interface com o Usuário da Web do IMM2”, na página 17 para executar as tarefas a seguir para controlar o IMM2.

Na guia Status do Sistema, é possível executar as tarefas a seguir:

- Visualizar o funcionamento do servidor
- Visualizar as informações do servidor, por exemplo, o nome e o tipo da máquina e o número de série
- Visualizar a atividade de energia e reinicialização do servidor
- Controlar remotamente o status de energia do servidor
- Acessar remotamente o console do servidor
- Conectar remotamente um disco ou imagem de disco ao servidor
- Visualizar eventos ativos
- Visualizar o funcionamento do hardware dos componentes do servidor

Nota: A página Status do Sistema é exibida depois de efetuar login no IMM2. Informações e ações comuns são colocadas nessa página.

Na guia Eventos, é possível executar as tarefas a seguir:

- Gerenciar histórico de log de eventos
- Gerenciar destinatários de eventos para notificações por email
- Gerenciar destinatários de eventos para notificações por syslog

Na guia Serviços e Suporte, é possível executar a tarefa a seguir:

- Obter manualmente os dados de serviço para seu servidor

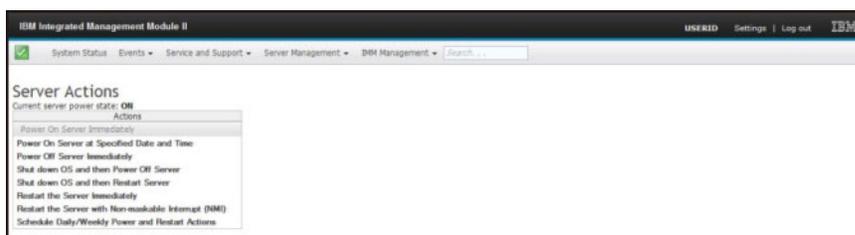
Na guia Gerenciamento do Servidor, é possível selecionar opções para executar as tarefas a seguir:

- Na opção Firmware do Servidor, visualizar e atualizar os níveis de firmware de componentes do servidor.
- Na opção Controle Remoto, visualizar e interagir com o console do servidor remotamente:
 - Controlar remotamente o status de energia do servidor
 - Acessar remotamente o console do servidor
 - Conectar remotamente uma unidade de CD, unidade de DVD, unidade de disquete, unidade flash USB ou imagem de disco ao servidor
- Na opção Propriedades do Servidor, é possível configurar parâmetros para ajudar a identificar o servidor.
- Na opção Ações de Energia do Servidor, é possível executar ações como, por exemplo, ligar, desligar e reiniciar.
- Na opção Discos, é possível visualizar unidades de disco rígido e eventos associados à unidades de disco rígido instaladas no servidor.
- Na opção Memória, é possível visualizar informações sobre os módulos de memória instalados no servidor.

- Na opção **Processador**, é possível visualizar informações sobre os microprocessadores instalados no servidor.
- Na opção **Tempos Limites do Servidor**, é possível configurar tempos limites para assegurar que o servidor não seja interrompido indefinidamente durante uma atualização de firmware ou ligação do servidor.
- Na opção **Inicialização da Rede PXE**, é possível configurar tentativas de pré-inicializar o Ambiente de Execução do Servidor.
- Na opção **Tela de Falha mais Recente do S.O.**, é possível capturar os dados da tela de falha do S.O. e armazená-los.
- Na opção **Gerenciamento de Energia**, é possível visualizar o uso de energia do sistema e a capacidade da fonte de alimentação e configurar parâmetros para uso de energia do sistema.

Controlando o Status de Energia do Servidor

A opção **Ações de Energia** contém uma lista de ações que podem ser executadas para controlar a energia do servidor (conforme mostrado na ilustração a seguir). É possível escolher ligar o servidor imediatamente ou em um horário planejado. Também é possível escolher encerrar e reiniciar o sistema operacional.



Conclua as etapas a seguir para executar ações de energia e reinicialização do servidor:

1. Acesse o menu **Ações de Energia** executando uma das etapas a seguir:
 - Clique na guia **Ações de Energia** na página Status do Sistema.
 - Clique em **Ações de Energia do Servidor** na guia Gerenciamento do Servidor.
2. Selecione a ação do servidor na lista do menu **Ações**.

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

Ação de Energia	Descrição
Ligar o servidor imediatamente	Selecione esse item de ação para ligar o servidor e inicializar o sistema operacional.
Ligar o servidor em uma data e hora especificadas	Selecione esse item de ação para planejar o servidor para ligar automaticamente em uma data e hora específicas.
Desligar o servidor imediatamente	Selecione esse item de ação para desligar o servidor sem encerrar o sistema operacional.
Encerrar o sistema operacional e, em seguida, desligar o servidor ¹	Selecione esse item de ação para encerrar o sistema operacional e desligar o servidor.

Tabela 6. Ações de Energia e Descrições (continuação)

Ação de Energia	Descrição
Encerrar o sistema operacional e, em seguida, reiniciar o servidor ¹	Selecione esse item de ação para reinicializar o sistema operacional.
Reiniciar o servidor imediatamente	Selecione esse item de ação para o efetuar o ciclo de ativação do servidor imediatamente sem encerrar o sistema operacional.
Reiniciar o servidor com non-maskable interrupt (NMI)	Selecione esse item de ação para forçar uma NMI em um sistema "interrompido". 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. O firmware do IMM2 usa a reinicialização automática na configuração NMI a partir da UEFI F1 no menu Configuração para determinar se uma reinicialização após a NMI é necessária.
Planejar ações diárias/semanais de energia e reinicialização	Selecione esse item de ação para planejar ações de energia e reinicialização diárias e semanais para o servidor.
<p>1. Se o sistema operacional estiver no modo de proteção de tela ou bloqueado quando uma solicitação "Encerrar" for tentada, o IMM2 pode não ser capaz de iniciar um encerramento normal. O IMM2 executará uma reconfiguração brusca ou encerramento após o intervalo de atraso de desligamento expirar, enquanto o sistema operacional ainda pode estar em execução.</p>	

Funções de Presença Remota e Controle Remoto

É possível usar o recurso Controle Remoto do IMM2 ou a função de presença remota na interface da web do IMM2 para visualizar e interagir com o console do servidor. É possível designar ao servidor uma unidade de CD ou DVD, unidade de disquete, unidade flash USB ou uma imagem de disco que esteja em seu computador. A funcionalidade de presença remota está disponível com os recursos IMM2 Premium e está disponível apenas por meio da interface da web do IMM2. Você deve efetuar login no IMM2 com um ID de usuário que tenha acesso de Supervisor para usar qualquer um dos recursos de controle remoto. Para obter informações adicionais sobre upgrade do IMM2 Basic ou IMM2 Standard para IMM2 Premium, consulte "Atualizando o IMM2" na página 3. Consulte a documentação fornecida com seu servidor para obter informações sobre o nível do IMM2 que está instalado em seu servidor.

Use os recursos de controle remoto para fazer o seguinte:

- Visualiza remotamente o vídeo com resolução gráfica de até 1600 x 1200 em 75 Hz, independentemente do estado do servidor.
- Acessar remotamente o servidor usando o teclado e mouse a partir de um cliente remoto.
- Mapear a unidade de CD ou DVD, unidade de disquete e unidade flash USB em um cliente remoto e mapear arquivos de imagem de disquete e ISO como unidades virtuais disponíveis para uso do servidor.
- Fazer upload de uma imagem de disquete na memória IMM2 e mapeá-la para o servidor como uma unidade virtual.

Atualizando o Firmware do IMM2 e o Applet Java ou ActiveX

Esta seção fornece informações sobre como atualizar o firmware e o applet Java e ActiveX.

Importante: O IMM2 usa um applet Java ou ActiveX para executar a função de presença remota. Quando o IMM2 é atualizado para o nível de firmware mais recente, os applets Java e ActiveX também são atualizados para o nível mais recente. Por padrão, o Java armazena em cache (armazena localmente) os applets que foram usados anteriormente. Após uma atualização flash do firmware do IMM2, o applet Java que o servidor usa pode não estar no nível mais recente.

Para corrigir esse problema, desative o armazenamento em cache. O método usado varia com base na plataforma e na versão Java. As etapas a seguir são para Oracle Java 1.5 no Windows:

1. Clique em **Iniciar** → **Configurações** → **Painel de Controle**.
2. Clique duas vezes em **Java Plug-in 1.5**. A janela Painel de Controle do Plug-in Java é aberta.
3. Clique na guia **Cache**.
4. Escolha uma das opções a seguir:
 - Desmarque a caixa de seleção **Ativar Armazenamento em Cache** para que o armazenamento em cache Java esteja sempre desativado.
 - Clique em **Limpar Armazenamento em Cache**. Se você escolher essa opção, deverá clicar em **Limpar Armazenamento em Cache** após cada atualização de firmware do IMM2.

Para obter informações adicionais sobre como atualizar o firmware do IMM2, consulte “Atualizando o Firmware do Servidor” na página 118.

Ativando a função de presença remota

A função de presença remota do IMM2 está disponível apenas no IMM2 Premium. Para obter mais informações sobre o upgrade do IMM Standard para o IMM Premium, consulte “Atualizando o IMM2” na página 3.

Depois de ter comprado e obtido a chave de ativação para o upgrade do IMM Premium instale-a, consulte “Instalando uma Chave de Ativação” na página 139.

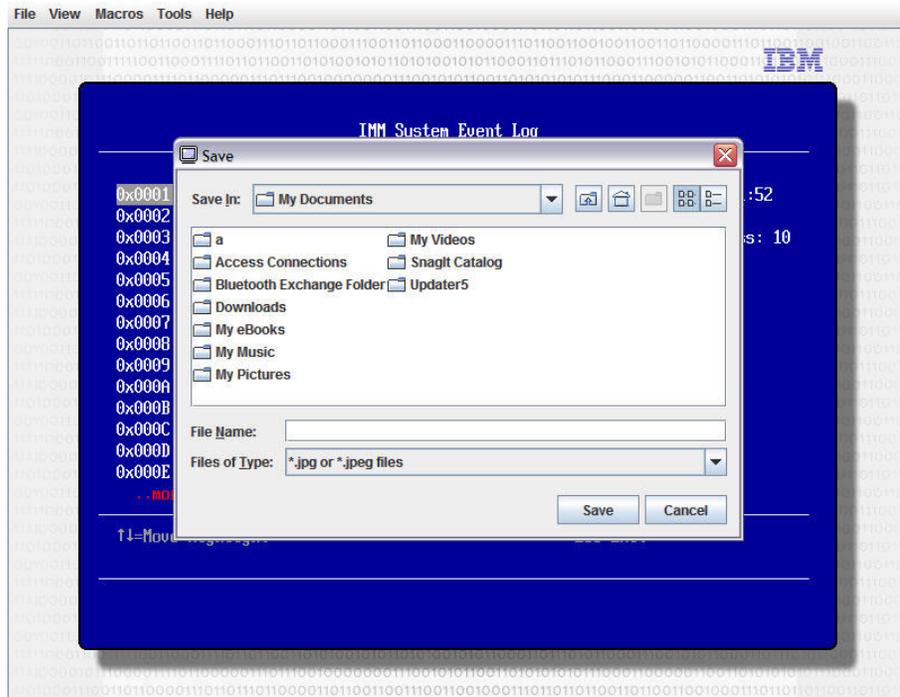
Captura de tela de controle remoto

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

1. Na janela Visualizador de Vídeo, clique em **Arquivo**.
2. Selecione **Capturar para Arquivo** no menu.
3. Quando solicitado, insira um nome para o arquivo de imagem e salve-o no local que você escolher no cliente local.

Nota: O cliente Java salva a imagem de captura de tela como um tipo de arquivo JPG. O cliente ActiveX salva a imagem de captura de tela como um tipo de arquivo BMP.

A ilustração a seguir mostra a janela na qual você especifica o local para o arquivo de imagem e insere o nome do arquivo de imagem.



Modos de Visualização do Visualizador de Vídeo de Controle Remoto

Para alterar a visualização da janela Visualizador de Vídeo, clique em **Visualizar**. As seguintes opções de menu estão disponíveis:

Ocultar Barra de Status

Oculte a barra de status que mostra o estado das teclas caps lock, num lock e scroll lock. Essa opção está disponível apenas quando a barra de status é mostrada.

Mostrar Barra de Status

Mostre a barra de status que exibe o estado das teclas caps lock, num lock e scroll lock. Essa opção está disponível apenas quando a barra de status está oculta.

Atualizar

O Visualizador de Vídeo redesenha a exibição do vídeo com os dados de vídeo do servidor.

Tela Cheia

O Visualizador de Vídeo preenche a área de trabalho do cliente com a exibição do vídeo. Essa opção está disponível somente quando o Visualizador de Vídeo não está no modo de tela cheia.

Em Janela

O Visualizador de Vídeo alterna do modo de tela cheia para o modo de janela. Essa opção está disponível somente enquanto o Visualizador de Vídeo está no modo de tela cheia.

Ajustar

O Visualizador de Vídeo é redimensionado para exibir completamente a área de trabalho de destino sem uma borda extra ou barras de rolagem. Isso requer que a área de trabalho do cliente seja grande o suficiente para exibir a janela redimensionada.

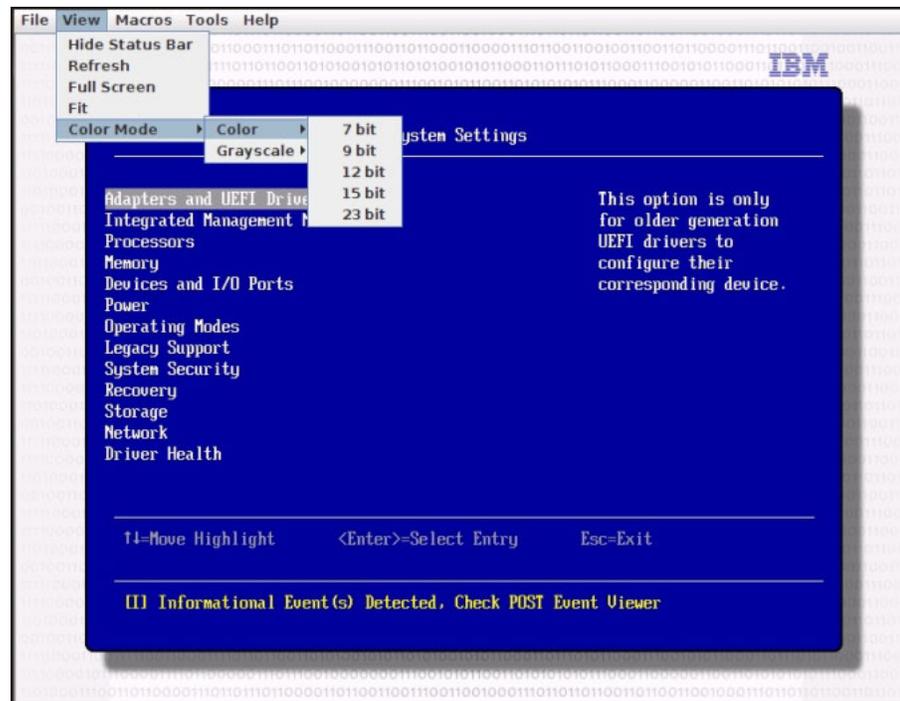
Modo de cor de vídeo do controle remoto

Se sua conexão com o servidor remoto tiver largura de banda limitada, será possível reduzir a demanda de largura de banda do Visualizador de Vídeo ajustando as configurações de cor na janela Visualizador de Vídeo.

Nota: O IMM2 tem um item de menu que permite o ajuste de intensidade de cor para reduzir os dados transmitidos em situações de largura de banda estreita. Esse item de menu substitui a régua de controle da largura da banda usada na interface do Remote Supervisor Adapter II.

Para alterar o modo de cor de vídeo, conclua as etapas a seguir:

1. Na janela Visualizador de Vídeo, clique em **Visualizar**.
2. Clique em **Modo de Cor**. Duas opções de modo de cor estão disponíveis (conforme mostrado na ilustração a seguir):
 - Cor: 7, 9, 12, 15 e 23 bits
 - Escala de tons: 16, 32, 64 e 128 sombras



3. Selecione a configuração Cor ou Escala de Tons.

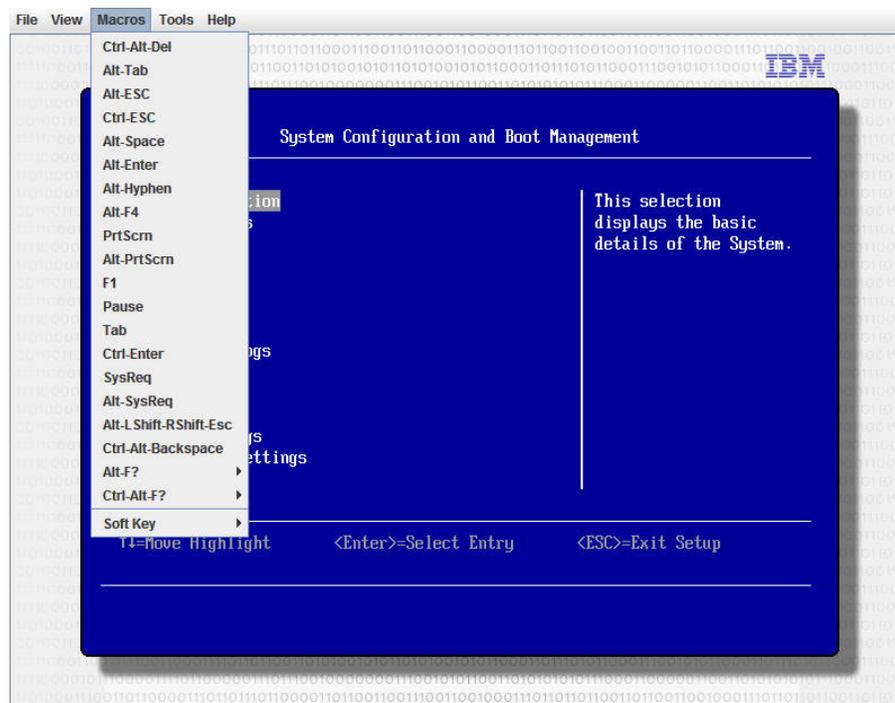
Suporte a teclado de controle remoto

O sistema operacional no servidor cliente que você está usando intercepta determinadas combinações de teclas, como Ctrl+Alt+Del no Microsoft Windows, em vez de transmiti-las para o servidor. Outras teclas, como F1, podem causar uma ação em seu computador e também no servidor.

Para usar combinações de teclas que afetam o servidor remoto, e não o cliente local, conclua as etapas a seguir:

1. Na janela Visualizador de Vídeo, clique em **Macros**.
2. Selecione uma das combinações de teclas predefinidas no menu ou selecione **Tecla Configurada** para escolher ou incluir uma combinação de teclas definida

pele usuário (conforme mostrado na ilustração a seguir).



Use o item de menu **Macros** do Visualizador de Vídeo para criar e editar botões customizados que podem ser usados para enviar pressionamentos de teclas para o servidor.

Para criar e editar botões customizados, conclua as etapas a seguir:

1. Na janela Visualizador de Vídeo, clique em **Macros**.
2. Selecione **Tecla Configurada** e, em seguida, selecione **Incluir**. Uma nova janela é aberta.
3. Clique em **Novo** para incluir uma nova combinação de teclas, ou selecione uma combinação e clique em **Excluir** para remover uma combinação de teclas existente.
4. Se você estiver incluindo uma nova combinação, digite a combinação de teclas que deseja definir na janela que é aberta depois de selecionar **Novo**; em seguida, clique em **OK**.
5. Quando concluir a definição ou remoção de combinações de teclas, clique em **OK**.

Suporte de teclado internacional

O Visualizador de Vídeo usa o código nativo específico da plataforma para interceptar eventos de teclas para acessar informações de teclas físicas diretamente. O cliente detecta os eventos de teclas físicas e os transmite junto com o servidor. O servidor detecta os mesmos pressionamentos de teclas físicas que o cliente experimentou e suporta todos os layouts de teclado padrão com a única limitação de que o destino e o cliente usam o mesmo layout de teclado. Se um usuário remoto tiver um layout de teclado diferente do servidor, o usuário poderá alternar o layout do servidor enquanto estiver sendo acessado remotamente e, em seguida, alternar novamente.

Modo de passagem do teclado

O modo de passagem do teclado desativa a manipulação da maioria das combinações de teclas especiais no cliente para que elas possam ser passadas diretamente ao servidor. Isso fornece uma alternativa ao uso das macros.

Alguns sistemas operacionais definem certos pressionamentos de teclas como fora do controle de um aplicativo, de modo que o comportamento do mecanismo de passagem opera independentemente do servidor. Por exemplo, em uma sessão do Linux X, a combinação de pressionamento de tecla Ctrl+Alt+F2 alterna para o Console Virtual 2. Não há nenhum mecanismo para interceptar essa sequência de pressionamentos de teclas e, portanto, não há uma maneira de o cliente passar esses pressionamentos de teclas diretamente para o destino. A única opção nesse caso é usar as macros de teclado definidas para esse propósito.

Para ativar ou desativar o modo de passagem de teclado, conclua as etapas a seguir:

1. Na janela Visualizador de Vídeo, clique em **Ferramentas**.
2. Selecione **Opções da Sessão** no menu.
3. Quando a janela Opções da Sessão for aberta, clique na guia **Geral**.
4. Marque a caixa de seleção **Passar todos os pressionamentos de teclas para o destino** para ativar ou desativar o modo de passagem do teclado.
5. Clique em **OK** para salvar a opção.

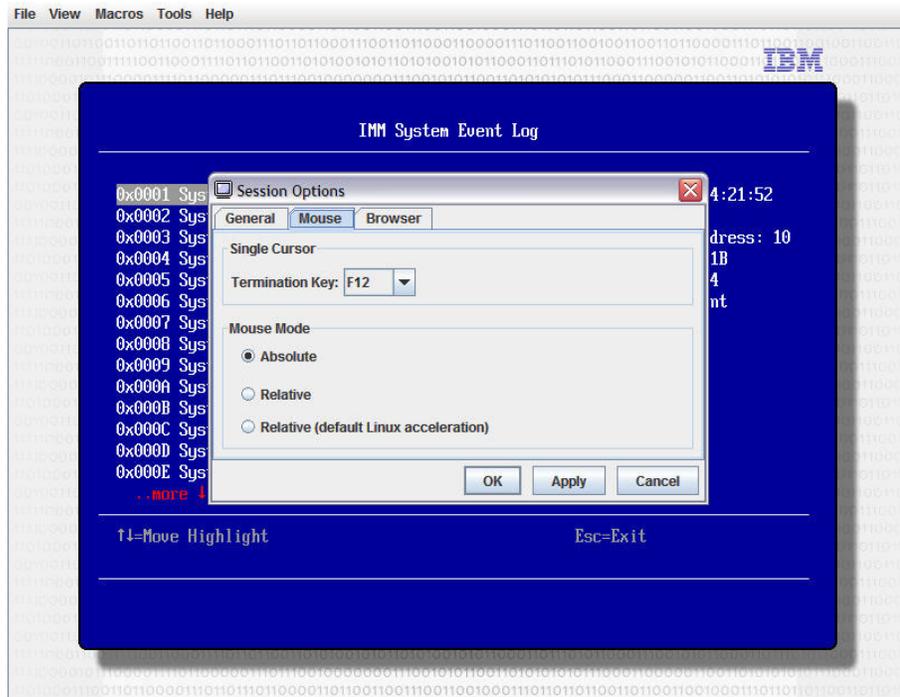
Suporte a mouse de controle remoto

A janela Visualizador de Vídeo oferece diversas opções para controle de mouse, incluindo controle de mouse absoluto, controle de mouse relativo e modo de cursor único.

Controle de mouse absoluto e relativo

Para acessar as opções absoluto e relativo para controlar o mouse, conclua as etapas a seguir:

1. Na janela Controle Remoto, clique em **Ferramentas**.
2. Selecione **Opções da Sessão** no menu.
3. Quando a janela Opções da Sessão for aberta, clique na guia **Mouse** (conforme mostrado na ilustração a seguir).



4. Selecione um dos **Modos de Mouse** a seguir:

- **Absoluto:**
O cliente envia mensagens do local do mouse para o servidor que são sempre relativas à origem (área superior esquerda) da área de visualização.
- **Relativo:**
O cliente envia o local do mouse como um deslocamento da localização anterior.
- **Relativo (aceleração padrão Linux):**
O cliente aplica um fator de aceleração para alinhar o mouse melhor nos destinos Linux. As configurações de aceleração foram selecionados para maximizar a compatibilidade com as distribuições do Linux.

Modo de cursor único

Alguns sistemas operacionais não alinham os cursores local e remoto, o que resulta em deslocamentos entre os cursores do mouse local e remoto. O modo de cursor único oculta o cursor do cliente local enquanto o mouse está dentro da janela Visualizador de Vídeo. Quando o modo de cursor único é ativado, você vê apenas o cursor remoto. Para ativar o modo de cursor único, clique em **Ferramentas > Cursor Único** na janela Visualizador de Vídeo.

Nota: Quando o Visualizador de Vídeo está no modo de cursor único, não é possível usar o mouse para alternar para outra janela ou clicar fora da janela do cliente KVM, porque não há cursor local.

Para desativar o modo de cursor único, clique na tecla **Terminação Definida**. Para visualizar a tecla de terminação definida, ou alterá-la, clique em **Ferramentas > Opções da Sessão > Mouse**.

Controle de energia remota

É possível enviar comandos de energia e reinicialização do servidor na janela Visualizador de Vídeo sem retornar ao navegador da web. Para controlar a energia do servidor com o Visualizador de Vídeo, conclua as etapas a seguir:

1. Na janela Visualizador de Vídeo, clique em **Ferramentas**.
2. Clique em **Energia**. Selecione um dos comandos a seguir:

Ligado

Liga o servidor.

Desligado

Desliga o servidor.

Reinicializar

Reinicia o servidor.

Ciclo Desliga o servidor e depois torna a ligá-lo.

Visualizando Estatísticas de Desempenho

Para visualizar as estatísticas de desempenho do Visualizador de Vídeo na janela Visualizador de Vídeo, clique em **Ferramentas**; em seguida, clique em **Estatísticas**. As informações a seguir são exibidas:

Taxa de Quadros

Uma média de execução do número de quadros, decodificados por segundo pelo cliente.

Largura de banda

Uma média de execução do número total de kilobytes por segundo recebido pelo cliente.

Compactação

Uma média de execução da redução da largura de banda devido à compactação de vídeo. Esse valor é geralmente exibido como 100.0%. Ele é arredondado para o décimo de um percentual.

Taxa de Pacotes

Uma média de execução do número de pacotes de vídeo recebidos por segundo.

Iniciando o Remote Desktop Protocol

Se o cliente Remote Desktop Protocol (RDP) baseado no Windows estiver instalado, será possível usar um cliente RDP em vez do cliente KVM. O servidor remoto deve estar configurado para receber conexões RDP.

Descrição do Recurso Knock-knock

Quando todas as sessões de controle remoto possíveis estão ocupadas (uma opção de modo de usuário único ou quatro opções de modo de multiusuário), um outro usuário da web pode ser capaz de enviar uma solicitação de desconexão para o usuário do controle remoto que ativou o recurso Knock-knock e se esse usuário não estiver manipulando uma solicitação de desconexão de outro usuário da web.

Se o usuário do controle remoto que ativou o recurso Knock-knock aceitar a solicitação ou não responder à solicitação dentro do valor de tempo limite, a sessão de controle remoto será terminada e será reservada para o usuário da web que está enviando a solicitação. Se o usuário da web que está enviando a solicitação de desconexão não ativar uma sessão de controle remoto Java ou ActiveX com a

sessão de controle remoto reservada dentro de cinco minutos, a sessão de controle remoto não será mais reservada para o usuário da web.

Para ativar o recurso Knock-knock, conclua as etapas a seguir:

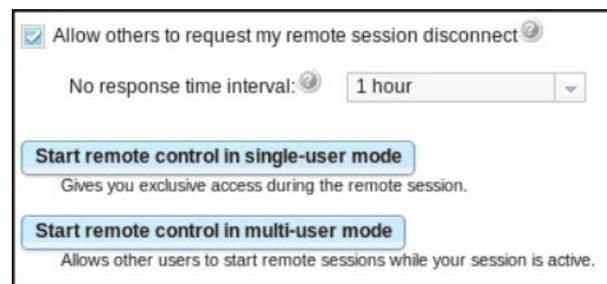
1. Acesse a página Controle Remoto selecionando uma das opções de menu a seguir:
 - Clique em **Controle Remoto** na guia Gerenciamento do Servidor.
 - Clique em **Controle Remoto...** na página Status do Sistema.
2. Clique na caixa de seleção **Permitir que outros solicitem minha desconexão de sessão remota**.

Nota: Devem existir um ou mais usuários adicionais marcando a caixa de seleção **Permitir que outros solicitem minha desconexão de sessão remota** ao usar o recurso de controle remoto.

3. Selecione um intervalo de tempo no campo **Nenhum Intervalo de Tempo de Resposta**.
4. Inicie a sessão de controle remoto selecionando o modo de usuário. Selecione um dos modos a seguir:
 - Iniciar o controle remoto no modo de usuário único
 - Iniciar o controle remoto no modo de multiusuário

Nota: O recurso Knock-knock é ativado automaticamente.

A ilustração a seguir mostra os campos descritos nas etapas de 2 a 4.



Para solicitar uma sessão remota, conclua as etapas a seguir:

1. Clique em **Atualizar** para exibir a sessão de Controle Remoto que está em andamento.

A ilustração a seguir mostra a janela Sessão de Controle Remoto em Andamento.

User Name	Active Sessions	Availability for Disconnection	Timeout Value
USERID	192.168.5.11	Request to connect	1 hour

Você verá uma das respostas a seguir no campo **Disponibilidade para Desconexão**:

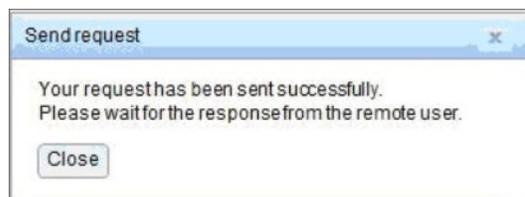
- **Solicitação para conectar:** Este texto é exibido quando o usuário do controle remoto ativa o recurso Knock-knock e não está manipulando uma solicitação de desconexão de outro usuário da web. O usuário da web atual não enviou uma solicitação de desconexão para o usuário do controle remoto.
- **Aguardando resposta:** Este texto é exibido quando o usuário do controle remoto está manipulando a solicitação de desconexão do usuário da web

atual. O usuário da web atual pode enviar uma solicitação de cancelamento para o usuário do controle remoto clicando no botão **Cancelar**.

- **Outra solicitação está pendente:** Este texto é exibido para uma das condições a seguir:
 - O usuário do controle remoto está manipulando a solicitação de desconexão de outro usuário da web.
 - O usuário do controle remoto ativou o recurso Knock-knock e o usuário da web atual está aguardando a resposta da solicitação de desconexão de outro usuário do controle remoto.
- **Não disponível:** Este texto é exibido sob uma das condições a seguir:
 - Nenhuma das sessões de controle remoto está ocupada. Se o usuário do controle remoto ativou, ou não, o recurso Knock-knock, isso não tem efeito nesta condição.
 - Todas as sessões de controle remoto estão ocupadas e o usuário do controle remoto não ativou o recurso Knock-knock.
 - Esta conexão de controle remoto está reservada para outro usuário por cinco minutos.

2. Clique em **Solicitação para conectar** para enviar uma solicitação de desconexão para o usuário do controle remoto.

A ilustração a seguir mostra a janela que é exibida quando a solicitação é enviada com êxito.



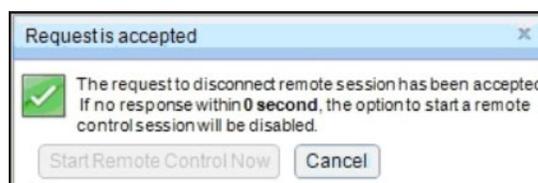
Se o usuário do controle remoto aceitar a solicitação de desconexão, o usuário da web deverá iniciar a sessão de controle remoto dentro de cinco minutos. Se o usuário da web não iniciar a sessão dentro de cinco minutos, a sessão não será reservada.

As ilustrações a seguir mostram as informações que são exibidas quando a solicitação de desconexão é aceita.

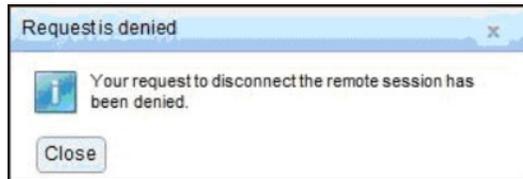
A ilustração a seguir mostra a solicitação de desconexão em um estado reservado.



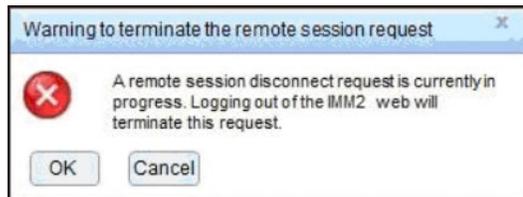
A ilustração a seguir mostra a solicitação de desconexão em um estado não reservado.



Se o usuário do controle remoto negar a solicitação de desconexão, o usuário que estiver enviando a solicitação de desconexão receberá informações indicando que a solicitação foi negada (conforme mostrado na ilustração a seguir).

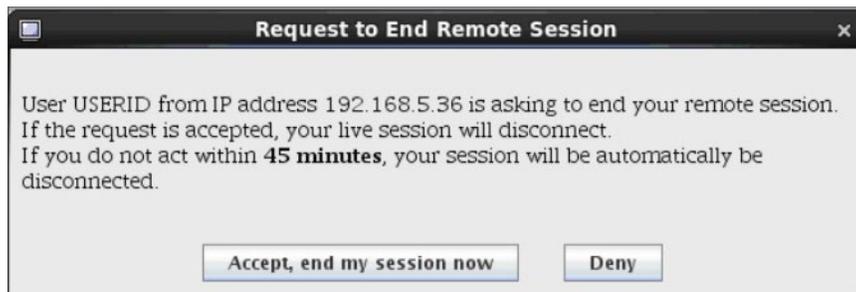


Se o usuário da web tentar efetuar logout do IMM2 antes de receber uma mensagem sobre sua solicitação, o usuário da web receberá uma mensagem (conforme mostrado na ilustração a seguir).



Depois que o usuário do controle remoto recebe a solicitação, o usuário deve determinar se deseja liberar a sessão remota no intervalo de tempo selecionado antes de iniciar a sessão de controle remoto. Uma janela Solicitação para Terminar a Sessão Remota é exibida para lembrar o usuário do controle remoto de qualquer tempo restante.

A janela Solicitação para Terminar a Sessão Remota é mostrada na ilustração a seguir.



Se o usuário do controle remoto selecionar **Aceitar, terminar minha sessão agora**, o visualizador remoto fechará automaticamente. Se o usuário do controle remoto selecionar **Negar**, o usuário do controle remoto continuará a manter a sessão remota. Depois que a Solicitação para Terminar a Sessão Remota for terminada, a sessão remota será liberada automaticamente e a janela a seguir será aberta.



Disco Remoto

Na janela Sessão de Mídia Virtual, é possível 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:

- Os sistemas operacionais de servidor a seguir têm suporte USB. O suporte USB é necessário para a funcionalidade do disco remoto.
 - Microsoft Windows Server 2003: Web, Std, Ent, DC (SP2, R2, SBS)
 - Microsoft Windows Server 2008 SP2: Std, SBS, EBS
 - Microsoft Windows Server 2008 R2
 - SUSE Linux Enterprise Server V10 SP3: x86_64
 - SUSE Linux Enterprise Server V11: x86_64
 - Red Hat Enterprise Linux Enterprise Servers V3.7: x86, x86_64
 - Red Hat Enterprise Linux Enterprise Servers V4.8: x86, x86_64
 - Red Hat Enterprise Linux Enterprise Servers V5.5: x86, x86_64
 - Red Hat Enterprise Linux Enterprise Servers V6.0: x86, x86_64
 - ESX 4.5: 4.0 U1
- O servidor do cliente requer o Plug-in Java 1.5 ou posterior.
- O servidor do cliente deve ter um microprocessador Intel Pentium III ou superior, operando a 700 MHz ou mais rápido, ou equivalente.

Acessando o Controle Remoto

Para iniciar uma sessão de controle remoto e acessar o disco remoto, conclua as etapas a seguir:

1. Na janela Visualizador de Vídeo, clique em **Ferramentas**.
2. Clique em **Ativar Mídia Virtual**. A janela do Visualizador de Vídeo é aberta.

Nota: Se a caixa de seleção **Criptografar dados do disco e KVM durante a transmissão** foi marcada antes que a janela Visualizador de Vídeo fosse aberta, os dados do disco serão criptografados com a criptografia ADES.

A janela Sessão de Mídia Virtual é separada da janela Visualizador de Vídeo. A janela Sessão de Mídia Virtual lista todas as unidades no cliente que podem ser mapeadas como unidades remotas. A janela Sessão de Mídia Virtual também permite que você mapeie arquivos de imagem de disquete e ISO como unidades virtuais. Cada unidade mapeada pode ser marcada como somente leitura. As unidades de CD e DVD e imagens ISO sempre são somente leitura.

Mapeando e Removendo o Mapeamento de Unidades

Para mapear uma unidade, marque a caixa de seleção **Selecionar** ao lado da unidade que você deseja mapear.

Nota: Uma unidade de CD ou DVD deve conter a mídia para que possa ser mapeada. Se a unidade estiver vazia, você será solicitado a inserir um CD ou DVD na unidade.

Clique no botão **Montagem Selecionada** para montar e mapear a(s) unidade(s) selecionada(s). Se você clicar em **Incluir Imagem**, arquivos de imagem de disquete e arquivos de imagem ISO poderão ser incluídos na lista de unidades disponíveis. Depois que o arquivo de imagem de disquete ou ISO for listado na janela Sessão

de Mídia Virtual, ele poderá ser mapeado exatamente como as outras unidades. Para remover o mapeamento das unidades, clique no botão **Desmontar Todos**. Antes de remover o mapeamento das unidades, você deve confirmar se deseja removê-lo.

Nota: Depois de confirmar seu desejo de remover o mapeamento das unidades, todas as unidades serão desmontadas. Não é possível desmontar as unidades individualmente.

Assim que uma imagem for incluída na lista e a caixa de seleção **Mapear** for marcada (se a imagem for adequada para carregamento na memória IMM2 para o recurso RDOC), uma janela será aberta, fornecendo a opção para transferir a imagem para o servidor. Se você selecionar **Sim**, insira um nome para a imagem.

Nota: Não insira caracteres especiais, como o comercial (símbolo &) ou espaços no nome.

Fazer upload de uma imagem na memória IMM2 permite que o disco permaneça montado no servidor para que seja possível acessar o disco mais tarde, mesmo depois que a sessão da interface da web do IMM2 tiver terminado. Várias imagens podem ser armazenadas no IMM2; mas o espaço total usado não pode exceder 50 Mb. Para descarregar o arquivo de imagem da memória, selecione o nome na janela Configuração do RDOC e clique em **Excluir**.

Saindo do Controle Remoto

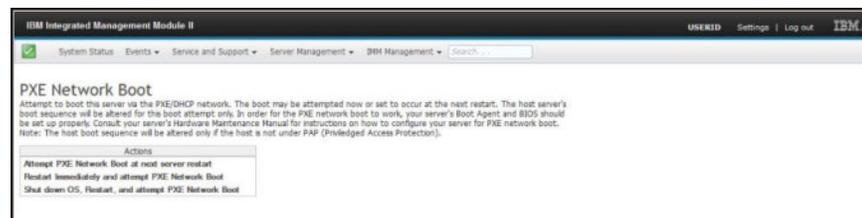
Feche as janelas Visualizador de Vídeo e Sessão de Mídia Virtual quando você tiver concluído o uso do recurso Controle Remoto.

Configurando a inicialização da rede PXE

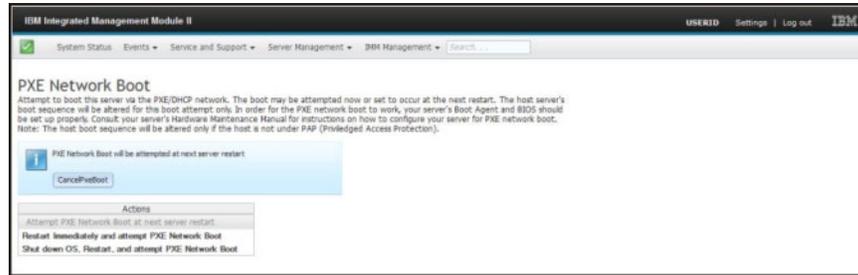
Use a opção Inicialização da Rede PXE para configurar tentativas de pré-inicializar o Ambiente de Execução do Servidor. Execute as etapas a seguir para configurar seu servidor para tentar uma inicialização da rede do Ambiente de Execução de Pré-inicialização na próxima reinicialização de servidor.

1. Efetue login no IMM2. Para obter informações adicionais, consulte “Efetuando Login no IMM2” na página 10.
2. Clique em **Gerenciamento do Servidor**; em seguida, selecione **Inicialização da Rede PXE**.

A seguinte janela é aberta.



3. Selecione **Tentar Inicialização da Rede PXE na próxima reinicialização do servidor** a partir das opções de Ação. A seguinte janela é aberta.



Se você desejar cancelar a seleção, clique em **CancelPxeBoot**. A janela Confirmar Cancelamento a seguir é aberta.



Atualizando o Firmware do Servidor

A opção Firmware do Servidor exibe níveis de firmware e permite atualizar o firmware do DSA, IMM2 e UEFI. As versões atuais do firmware do IMM2, UEFI e DSA são exibidas. Isso inclui as versões Ativa, Primária e Backup.

A ilustração a seguir mostra a página Firmware do Servidor.

Firmware Type	Status	Version	Build	Release Date
DSA	Active	9.24	DSV144B	2012-08-10
IMM2				
IMM2 (Primary)	Active	2.15	140039Q	2013-01-28
IMM2 (Backup)	Inactive	3.00	140039T	2013-01-30
UEFI				
UEFI (Primary)	Active	1.20	D7E120CJ5	2012-08-23
UEFI (Backup)	Inactive	1.20	D7E120CJ5	2012-08-23

O status e as versões atuais de firmware para o IMM2, UEFI e DSA são exibidos, incluindo as versões primária e de backup. Há três categorias para o status de firmware:

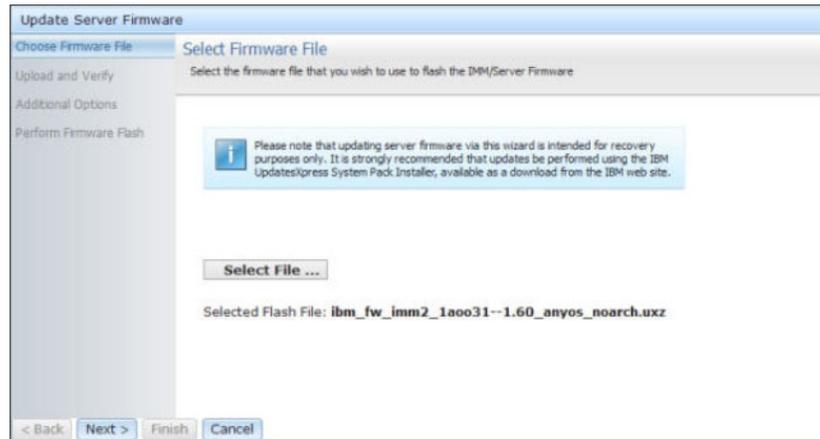
- **Ativo:** O firmware está ativo.
- **Inativo:** O firmware não está ativo.
- **Pendente:** O firmware está aguardando para tornar-se ativo.

Atenção: A instalação da atualização de firmware errada pode causar mau funcionamento do servidor. Antes de instalar uma atualização de firmware ou de driver de dispositivo, leia quaisquer arquivos leia-me e de histórico de mudanças 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 atualizar a partir de uma versão de firmware ou de driver de dispositivo anterior para a versão mais recente.

Para atualizar o firmware do servidor, conclua as etapas a seguir:

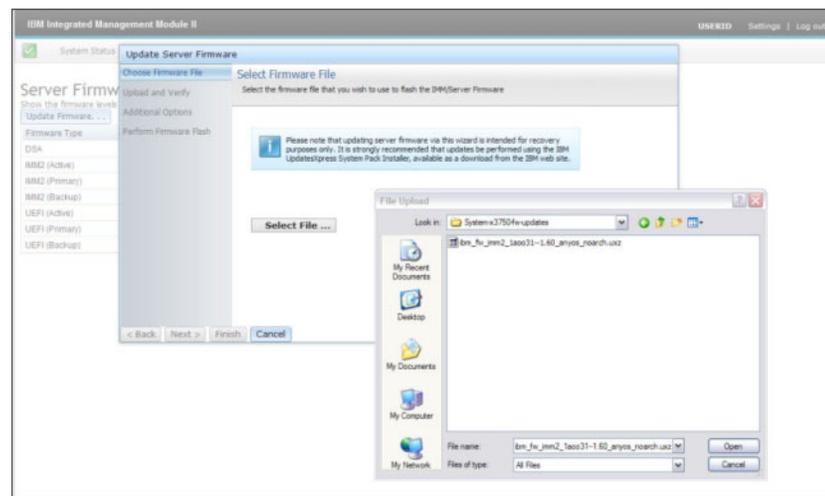
1. Clique em **Firmware do Servidor** na lista de menu Gerenciamento do Servidor.
2. Clique em **Atualizar Firmware**. A janela Atualizar Firmware do Servidor é aberta (conforme mostrado na ilustração a seguir).



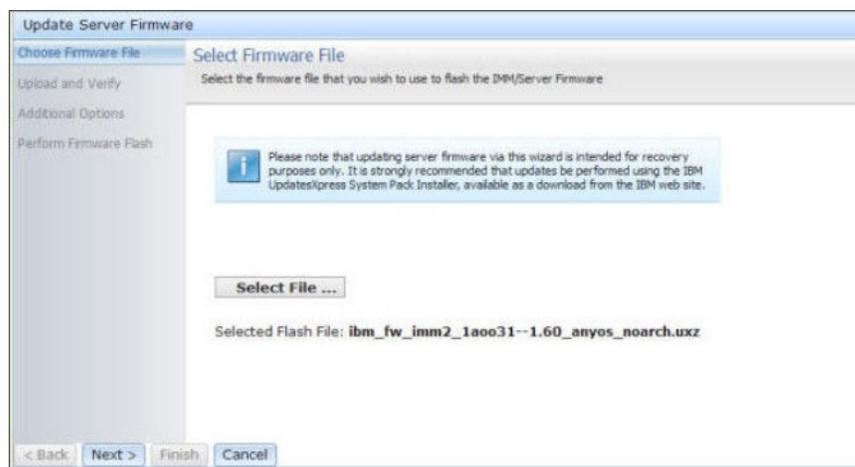
3. Leia o aviso antes de continuar com a próxima etapa.
4. Execute uma das seguintes etapas:
 - Clique em **Cancelar** e retorne à janela Firmware do Servidor anterior.
 - Clique em **Selecionar Arquivo...** para selecionar o arquivo de firmware que você deseja usar para atualizar o firmware do servidor.

Nota: Todas as outras opções ficam esmaecidas quando a janela Atualizar Firmware do Servidor é aberta inicialmente.

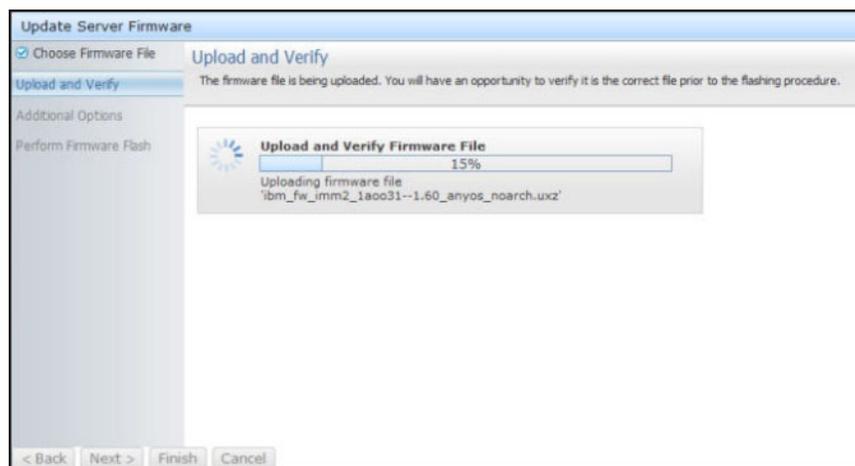
Quando você clica em **Selecionar Arquivo...**, uma janela Upload de Arquivo é aberta (conforme mostrado na ilustração a seguir). Essa janela permite procurar o arquivo desejado.



5. 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 (conforme mostrado na ilustração a seguir).

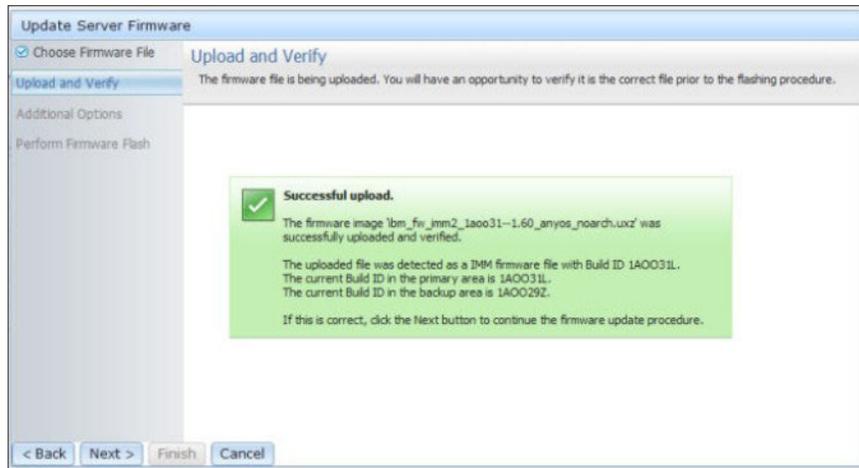


6. Clique em **Avançar >** para começar a fazer upload e verificar o processo no arquivo selecionado. Um medidor de progresso será exibido enquanto o arquivo estiver sendo transferido por upload e verificado (conforme mostrado na ilustração a seguir).

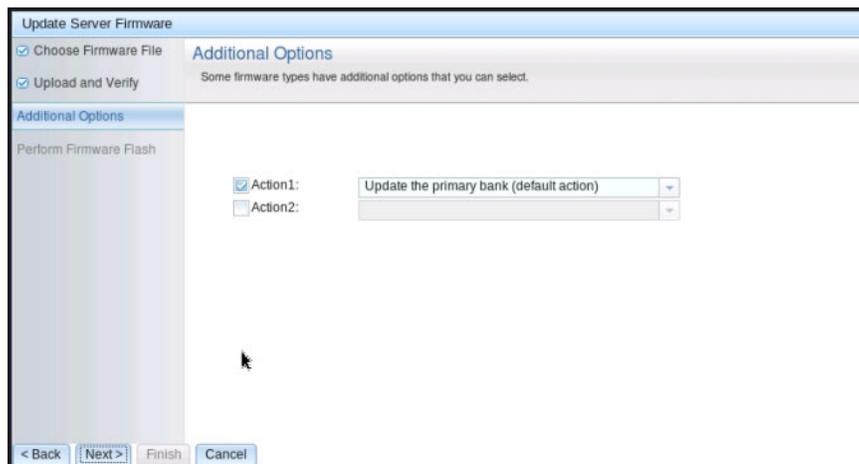


É possível visualizar essa janela de status para verificar se o arquivo selecionado para atualização é o arquivo correto. A janela de status terá informações sobre o tipo de arquivo de firmware que deve ser atualizado, como DSA, IMM ou UEFI.

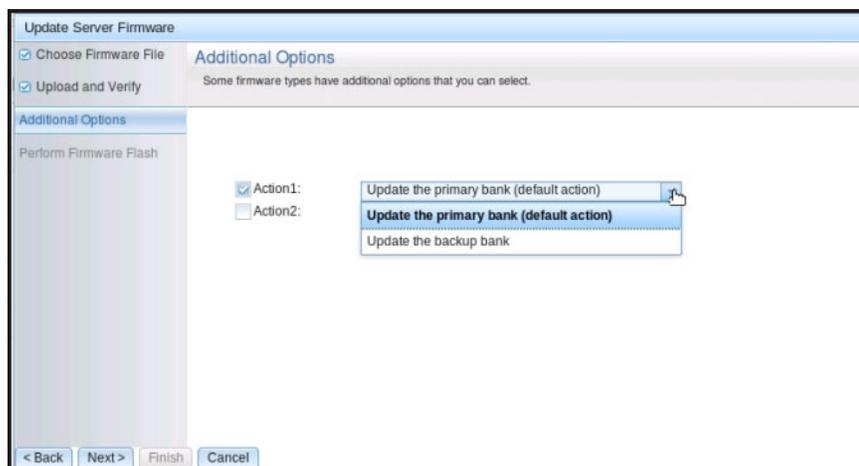
Depois que o arquivo de firmware é transferido por upload e verificado com êxito, uma janela Upload Bem-sucedido é aberta (conforme mostrado na ilustração a seguir).



7. Clique em **Avançar >** se as informações estiverem corretas. Clique em **< Voltar** se você desejar refazer qualquer uma das seleções.
Se você clicar em **Avançar >**, um conjunto de opções adicionais será exibido (conforme mostrado na ilustração a seguir).



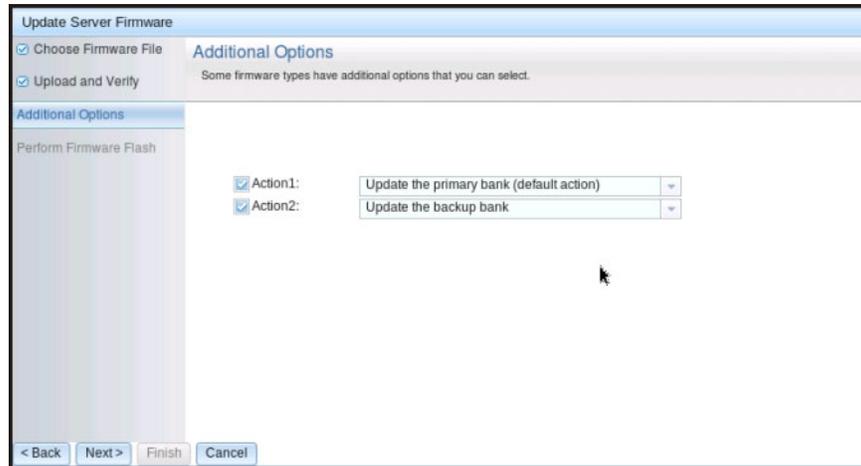
8. O menu suspenso ao lado do campo **Ação 1** fornece a opção para **Atualizar o Banco Primário (ação padrão)** ou **Atualizar o Banco de Backup** (conforme mostrado na ilustração a seguir).



Depois de selecionar uma ação, você é retornado à tela anterior com a ação adicional solicitada exibida.

Depois que a ação selecionada é carregada, essa ação e um novo menu suspenso **Ação 2** são exibidos (conforme mostrado na ilustração a seguir).

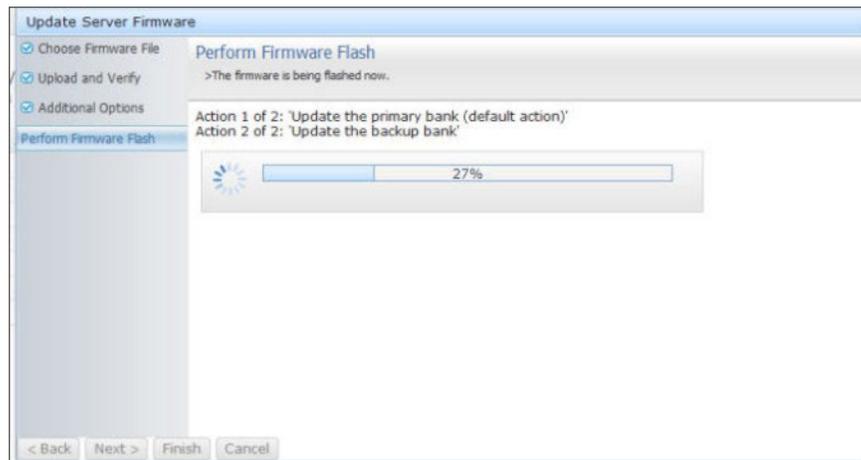
Nota: Para desativar uma ação e iniciar o processo de opção adicional novamente, clique na caixa de seleção ao lado da ação relacionada.



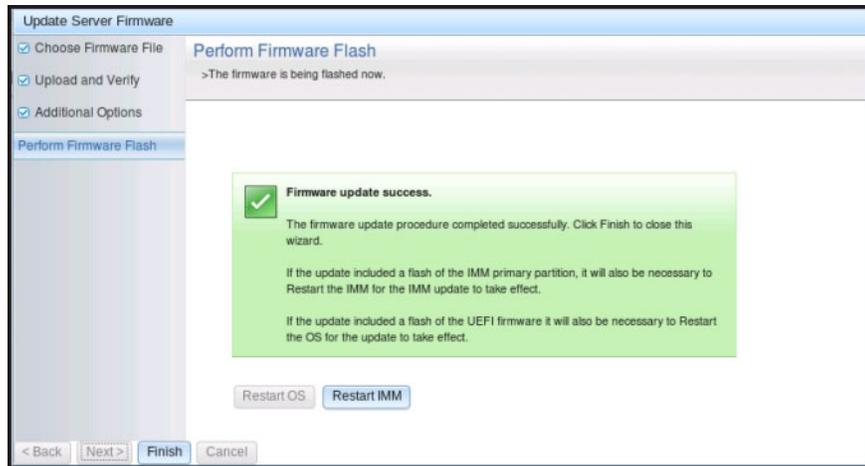
A tela anterior mostra que para a Ação 1, o banco primário é selecionado para ser atualizado. Também é possível selecionar atualizar o banco de backup sob Ação 2 (conforme mostrado na tela anterior). Tanto o banco primário como o banco de backup serão atualizados ao mesmo tempo quando você clicar em **Avançar >**.

Nota: A Ação 1 deve ser diferente da Ação 2.

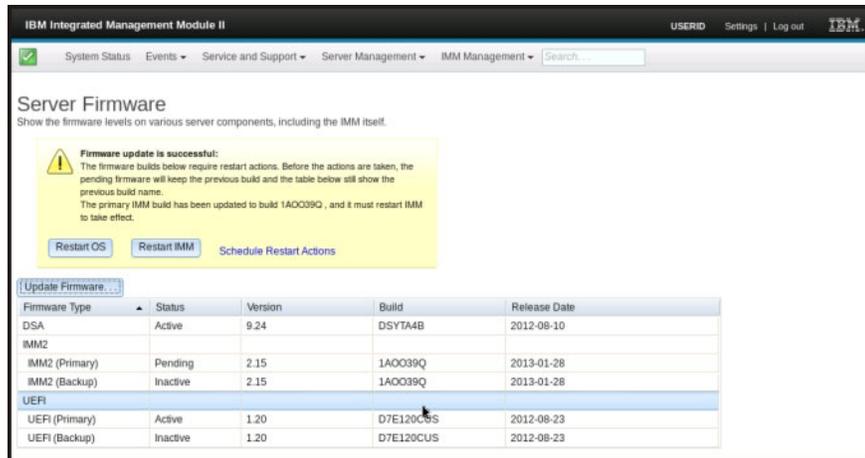
Um medidor de progresso mostra o progresso da atualização para os bancos primário e de backup (conforme mostrado na ilustração a seguir).



Quando a atualização de firmware é concluída com êxito, a janela a seguir é aberta. Seleccione a operação relacionada de acordo com o conteúdo exibido para concluir o processo de atualização.



Se a atualização de firmware primária não foi concluída, a janela a seguir será aberta quando a tela Firmware do Servidor for exibida.



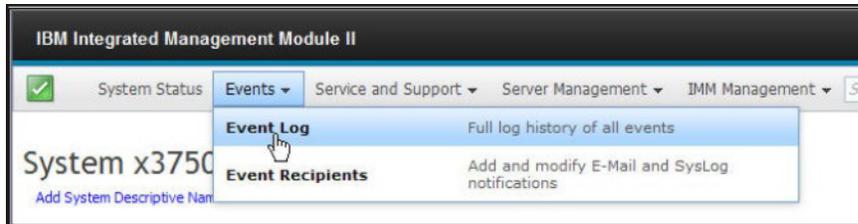
Gerenciando eventos do sistema

O menu **Eventos** permite gerenciar o histórico de Log de Eventos e gerenciar Destinatários de Eventos para notificações por email e syslog.

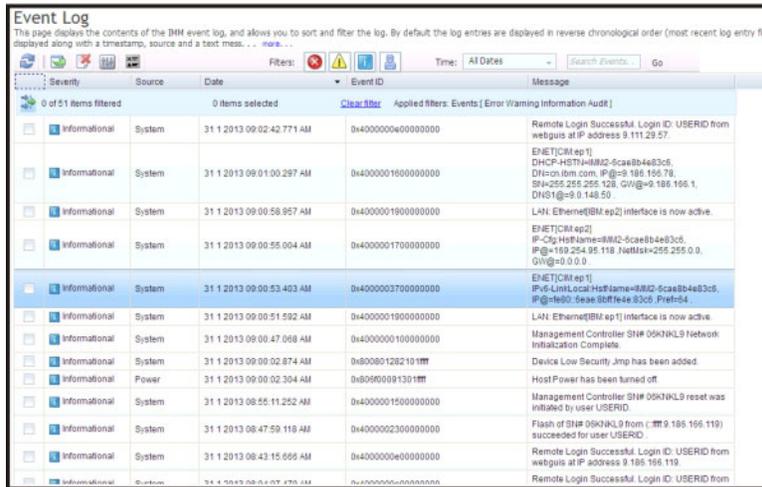
Gerenciando o Log de Eventos

Clique na opção **Log de Eventos** para exibir a janela Log de Eventos. A janela Log de Eventos inclui uma descrição dos eventos que são relatados pelo IMM2 e informações sobre todas as tentativas de acesso remoto e mudanças na configuração. Todos os eventos no log são registrados com data e hora usando as configurações de data e hora do IMM2. Alguns eventos gerarão alertas, se estiverem configurados para isso na página Destinatários de Eventos. Também é possível classificar e filtrar eventos no log de eventos.

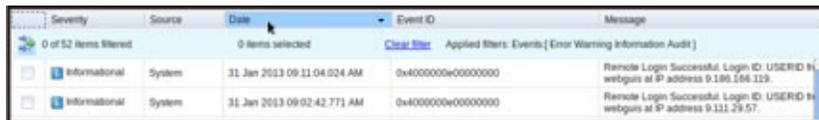
Clique na opção **Log de Eventos**. A seguinte janela é aberta.



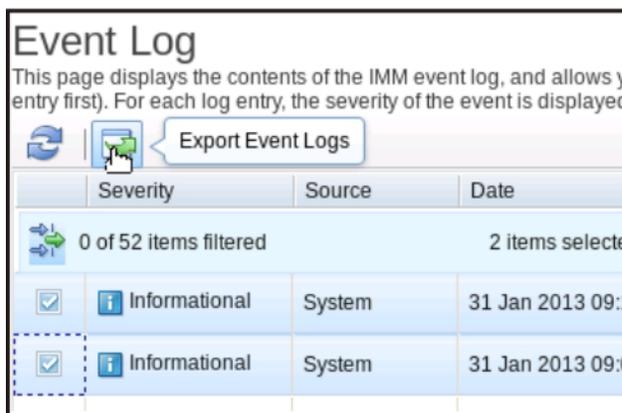
Após a seleção da opção Log de Eventos, a janela a seguir é aberta.



Para classificar e filtrar eventos no log de eventos, selecione o título da coluna (conforme mostrado na ilustração a seguir).

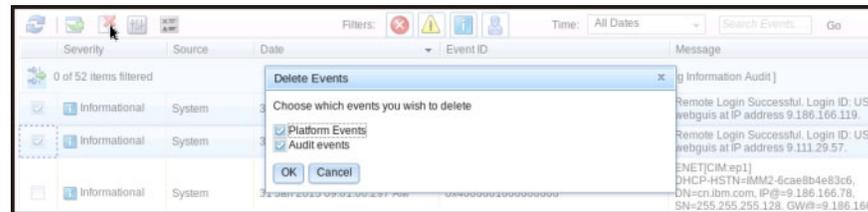


É possível salvar todos os eventos, ou os eventos selecionados, do log de eventos em um arquivo usando o botão **Exportar**. Para selecionar eventos específicos, escolha um ou mais eventos na página Log de Eventos principal e clique com o botão esquerdo no botão **Exportar** (conforme mostrado na ilustração a seguir).

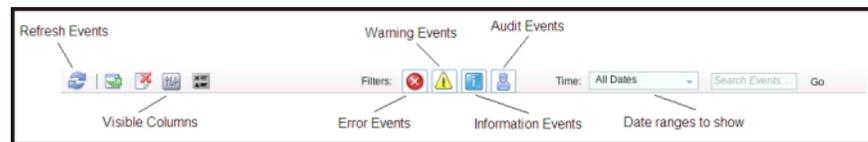


Para escolher qual tipo de evento você deseja excluir, clique em **Excluir Eventos**. Você deve selecionar a categoria de eventos que deseja excluir.

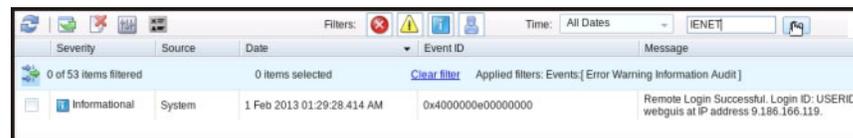
A ilustração a seguir mostra a janela Excluir Eventos.



Para selecionar o tipo de entrada de log de eventos que você deseja exibir, clique no botão apropriado (conforme mostrado na ilustração a seguir).



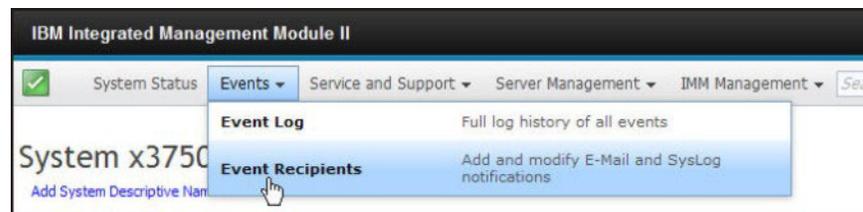
Para procurar tipos específicos de eventos ou palavras-chave, digite o tipo de evento ou palavra-chave no campo **Procurar Eventos** e clique em **Ir** (conforme mostrado na ilustração a seguir).



Notificação de Eventos do Sistema

Selecione a opção **Destinatários de Eventos** para incluir e modificar notificações por email e syslog.

A ilustração a seguir mostra a seleção da opção Destinatários de Eventos.

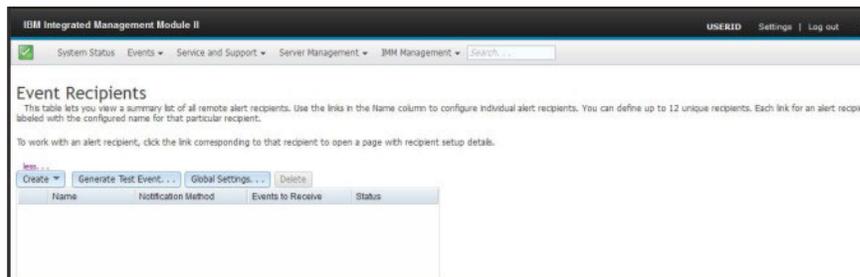


A opção Destinatários de Eventos permite gerenciar quem será notificado sobre eventos do sistema. É possível configurar cada destinatário e gerenciar as configurações que se aplicam a todos os Destinatários de Eventos. Também é possível gerar um evento de teste para verificar a operação do recurso de notificação.

A ilustração a seguir mostra a página Destinatários de Eventos.



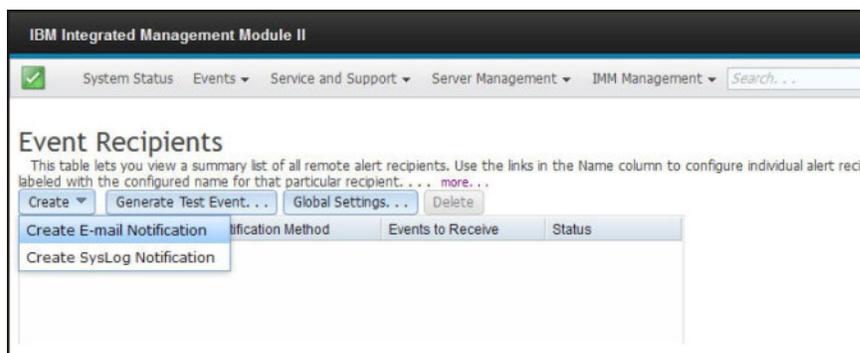
A ilustração a seguir mostra informações adicionais que são exibidas quando você clica no link **mais** na página Destinatários de Eventos.



Criando Notificações por Email e Syslog

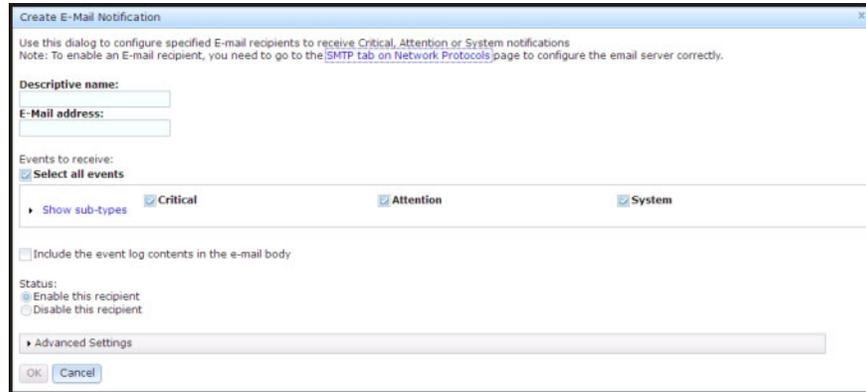
Selecione a guia **Criar** para criar notificações por email e syslog.

A ilustração a seguir mostra as opções disponíveis no menu Criar.

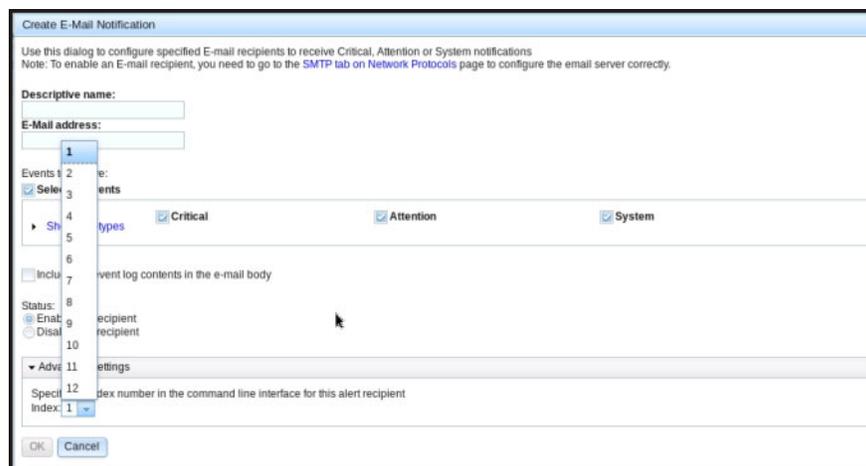


Na opção **Criar Notificação por Email**, é possível configurar um endereço de email de destino e escolher os tipos de eventos sobre os quais você deseja ser notificado. Além disso, é possível clicar em **Configurações Avançadas** para selecionar o número de índice inicial. Para incluir o log de eventos no email, marque a caixa de seleção **Incluir o conteúdo do log de eventos no corpo do email**.

A ilustração a seguir mostra a tela Criar Notificação por Email.

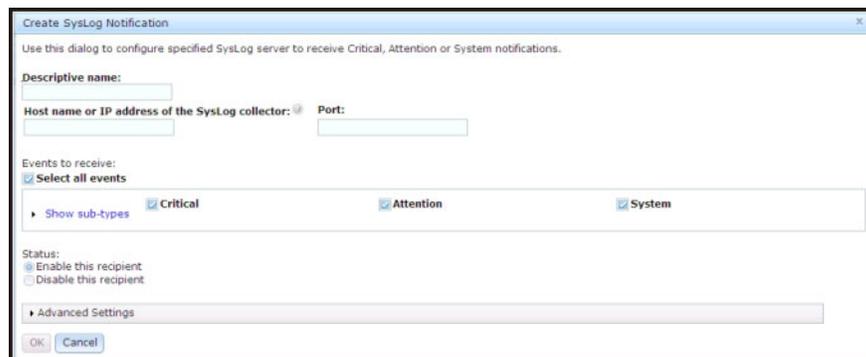


A ilustração a seguir mostra as seleções na área de janela Configurações Avançadas.

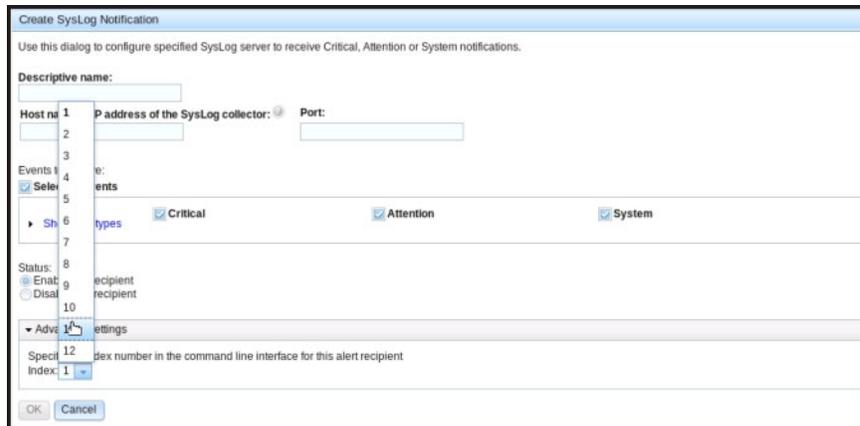


Na opção **Criar Notificação por Syslog**, é possível configurar o nome do host e endereço IP do coletor do syslog e escolher os tipos de eventos sobre os quais você deseja ser notificado. É possível clicar em **Configurações Avançadas** para selecionar o número de índice inicial. Também é possível especificar a porta que você deseja usar para esse tipo de notificação.

A ilustração a seguir mostra a tela Criar Notificação por Syslog.



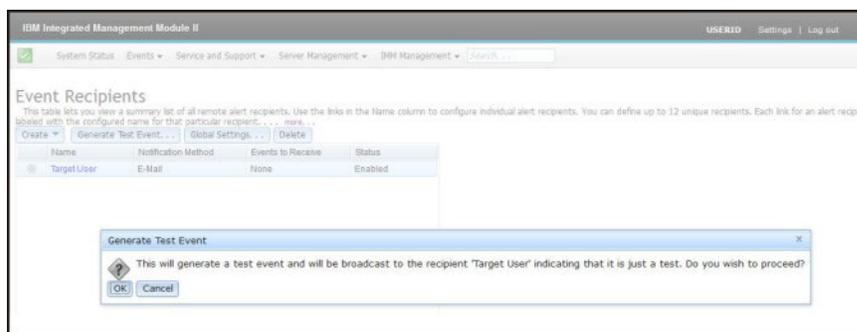
A ilustração a seguir mostra as seleções na área de janela Configurações Avançadas.



Gerando Eventos de Teste

Use a guia **Gerar Evento de Teste...** para enviar um email de teste para um destino de email selecionado. Após a seleção da notificação de eventos, clique em **OK** para gerar o evento de teste. O evento de teste é enviado ao destinatário com a notificação de que este é um teste.

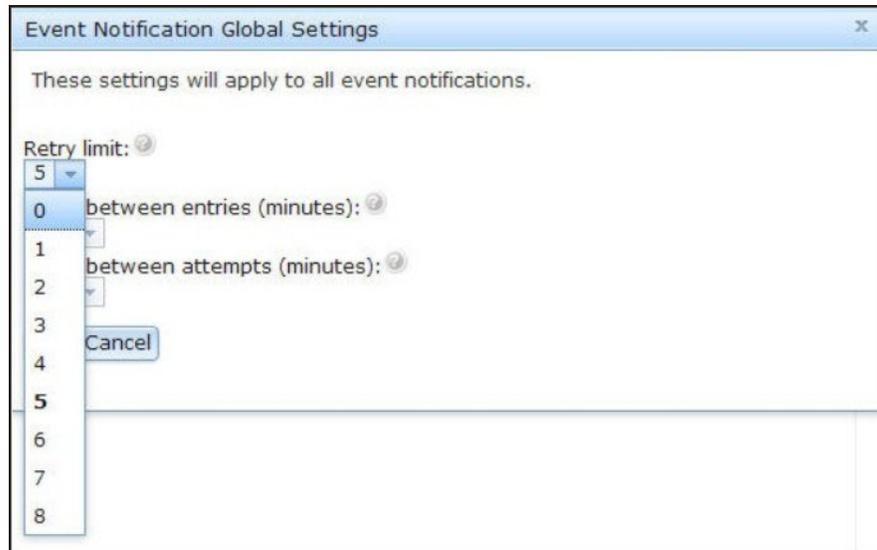
A ilustração a seguir mostra a janela Gerar Evento de Teste.



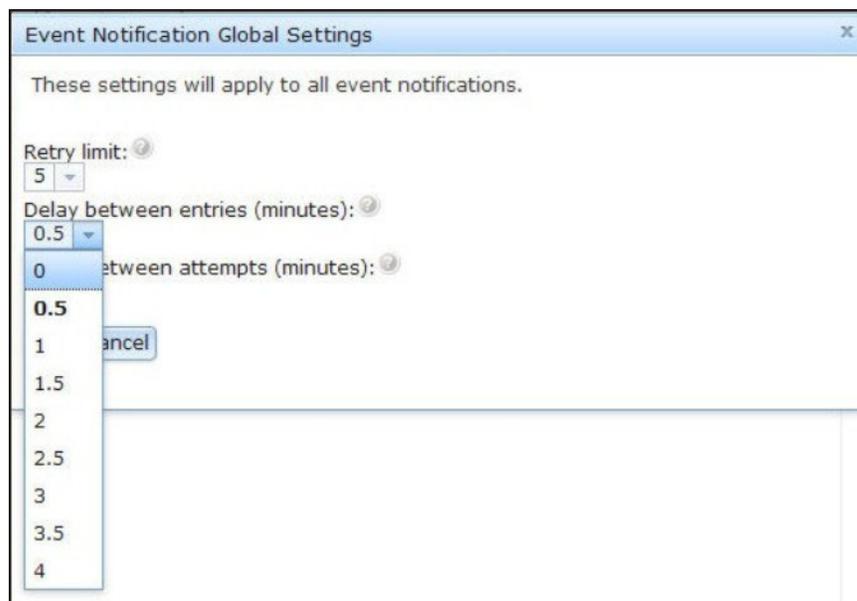
Configurando Limites para Notificações de Nova Tentativa

Use a guia **Configurações Globais...** para configurar um limite para tentar novamente a notificação de eventos, tentar novamente o atraso entre as entradas de notificação de eventos (em minutos) e tentar novamente o atraso entre tentativas (em minutos).

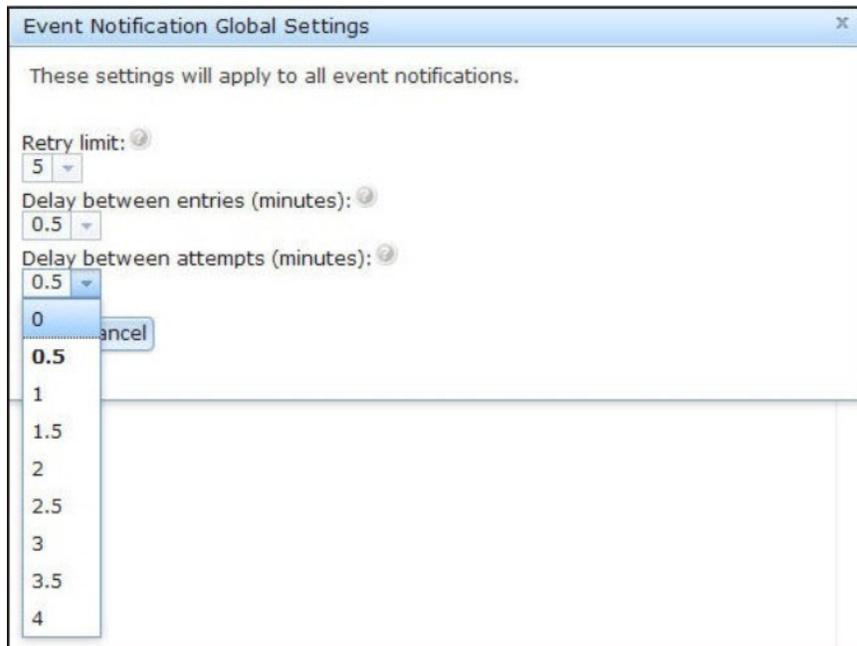
A ilustração a seguir mostra as configurações para a opção Limite de Novas Tentativas.



A ilustração a seguir mostra as configurações para a opção Atraso entre Entradas (Minutos).



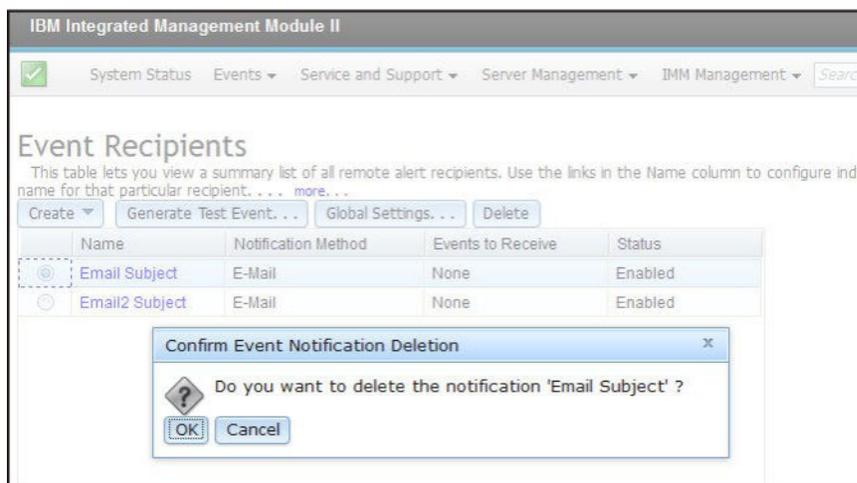
A ilustração a seguir mostra as configurações para a opção Atraso entre Tentativas (Minutos).



Excluindo Notificações por Email ou Syslog

Use a guia **Excluir** para remover um destino de notificação por email ou syslog.

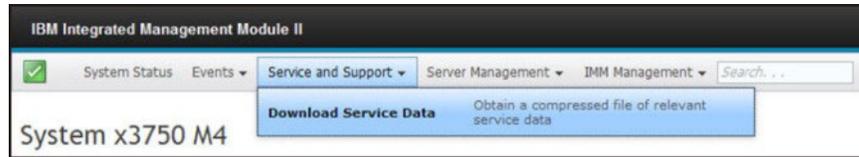
A ilustração a seguir mostra a janela Confirmar Exclusão de Notificação de Eventos.



Coletando Informações de Serviço e Suporte

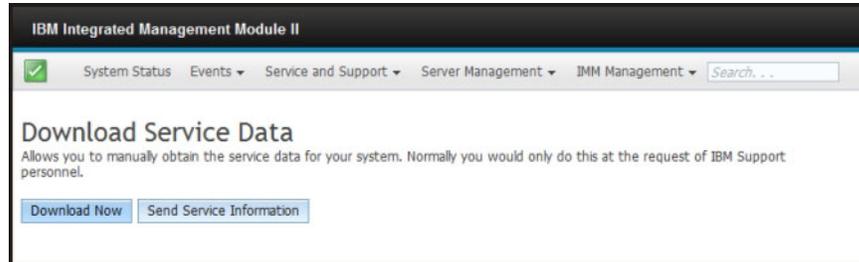
Clique na opção **Fazer o Download de Dados de Serviço** sob o menu **Serviço e Suporte** para coletar informações sobre o servidor que podem ser usadas pelo Suporte IBM para ajudá-lo com seu problema.

A ilustração a seguir mostra a guia **Serviço e Suporte**.



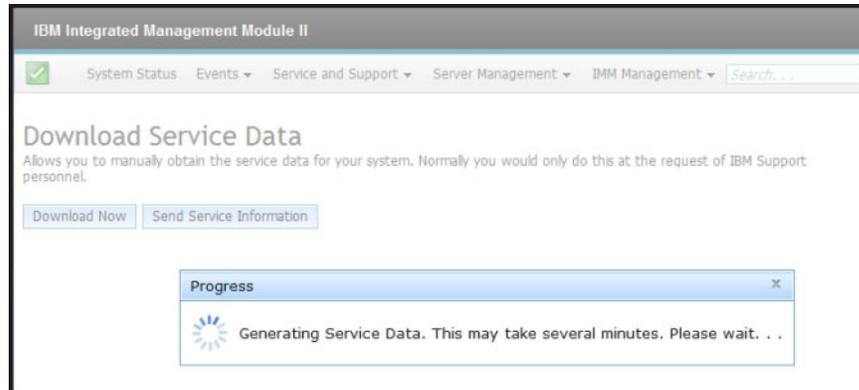
Clique no botão **Fazer o Download Agora** se você desejar fazer o download dos dados de serviço e suporte.

A ilustração a seguir mostra a janela Fazer o Download de Dados de Serviço.

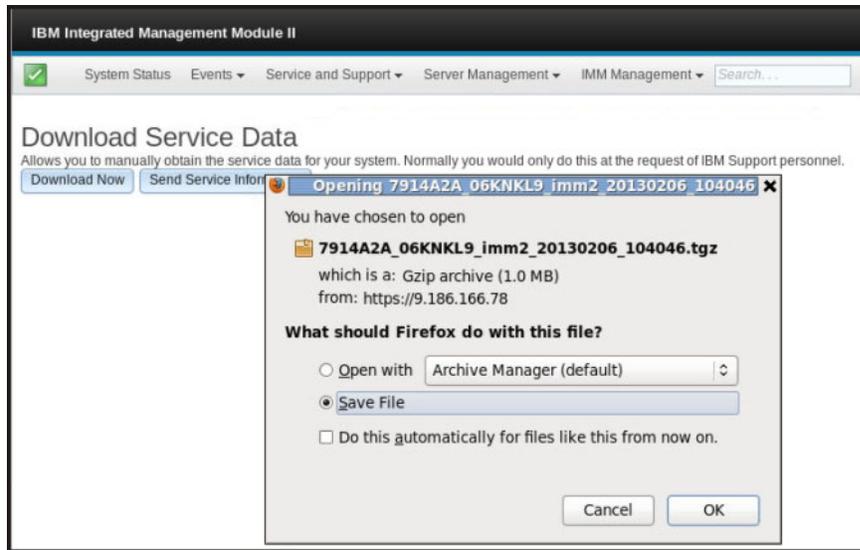


O processo para coletar os dados de serviço e suporte é iniciado. Esse processo demora alguns minutos para gerar os dados de serviço que podem ser salvos em um arquivo.

Você verá a janela Progresso a seguir enquanto os dados do Serviço estiverem sendo gerados.



Quando o processo for concluído, você será solicitado a inserir o local para salvar o arquivo. Consulte a ilustração a seguir para obter um exemplo.



Capturando os Dados da Tela de Falha mais Recente do S.O.

Use a opção Tela de Falha mais Recente do S.O. para capturar os dados da tela de falha do sistema operacional e armazená-los. O IMM2 armazena apenas as informações de eventos de erro mais recentes, sobrescrevendo os dados da tela de falha do S.O. mais antigos quando ocorre um novo evento de erro. O recurso Watchdog do S.O. deve ser ativado para capturar a tela de falha do S.O. Caso ocorra um evento que faça o S.O. parar a execução, o recurso Watchdog do S.O. é acionado. A captura de tela de falha do S.O. está disponível apenas com a funcionalidade Nível Avançado do IMM2. Consulte a documentação para seu servidor para obter informações sobre o nível do IMM2 que está instalado em seu servidor.

Para exibir remotamente uma imagem da Tela de Falha do S.O., selecione uma das opções de menu a seguir:

- **Tela de Falha mais Recente do S.O.** na guia Gerenciamento do Servidor
- Guia **Tela de Falha mais Recente do S.O.** na página Status do Sistema

Nota: Se uma Tela de Falha do S.O. não tiver sido capturada, a guia Tela de Falha mais Recente do S.O. na página Status do Sistema ficará esmaecida e não poderá ser selecionada.

A ilustração a seguir mostra a Tela de Falha do S.O.

```
A problem has been detected and windows has been shut down to prevent damage
to your computer.

The end-user manually generated the crashdump.

If this is the first time you've seen this stop error screen,
restart your computer. If this screen appears again, follow
these steps:

Check to make sure any new hardware or software is properly installed.
If this is a new installation, ask your hardware or software manufacturer
for any windows updates you might need.

If problems continue, disable or remove any newly installed hardware
or software. Disable BIOS memory options such as caching or shadowing.
If you need to use Safe Mode to remove or disable components, restart
your computer, press F8 to select Advanced Startup Options, and then
select Safe Mode.

Technical information:

*** STOP: 0x000000E2 (0x0000000000000000,0x0000000000000000,0x0000000000000000,0
x0000000000000000)

Collecting data for crash dump ...
Initializing disk for crash dump ...
Beginning dump of physical memory.
Dumping physical memory to disk: 100
Physical memory dump complete.
Contact your system admin or technical support group for further assistance.
```

Gerenciando a Energia do Servidor

Use a guia Gerenciamento de Energia para executar as tarefas a seguir:

- Exibir informações sobre as fontes de alimentação instaladas.
- Controlar como a "energia" de fonte de alimentação é gerenciada.
- Controlar a energia total do sistema.
- Exibir informações sobre as fontes de alimentação instaladas e a capacidade da fonte de alimentação atual.
- Exibir o histórico da quantidade de energia usada.

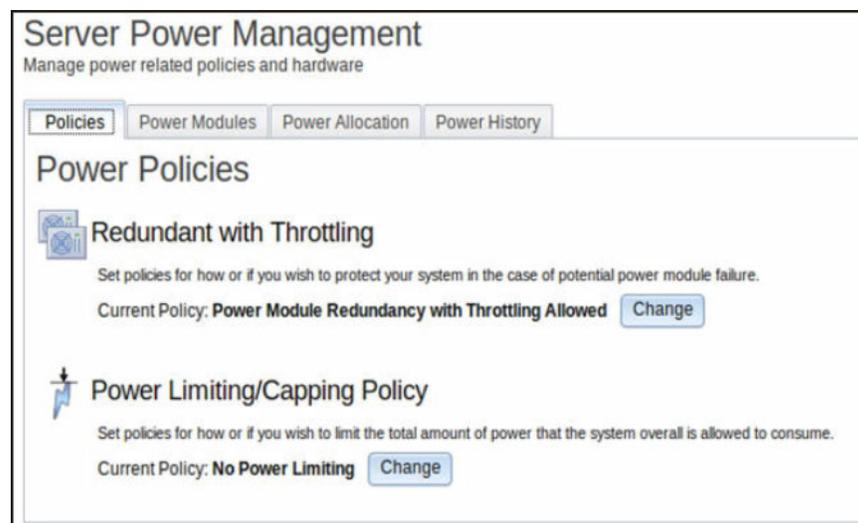
Selecione a opção **Gerenciamento de Energia** sob a guia Gerenciamento do Servidor para visualizar informações de gerenciamento de energia e executar funções de gerenciamento de energia (conforme mostrado na ilustração a seguir).

Server Management ▾	IMM Management ▾	Search
Server Firmware	View firmware levels and update firmware	
Remote Control	Allows you access into the operating system of your system	
Server Properties	Various properties and settings related to your system	
Server Power Actions	Power actions such as power on, power off, and restart	
Cooling Devices	Cooling devices installed in your system	
Power Modules	Power modules installed in your system	
Disks	Hard disk drives installed directly in your system	
Memory	RAM installed in your system	
Processors	Physical CPUs installed in your system	
Server Timeouts	Configure watchdogs, etc.	
PXE Network Boot	Settings for how your system performs boot from PXE server	
Latest OS Failure Screen	Windows systems only. View an image of the most recent failure screen.	
Power Management	Power devices, policies, and consumption	

Controlando a Fonte de Alimentação e a Energia Total do Sistema

Clique na guia **Políticas** para controlar como a fonte de alimentação é gerenciada e, opcionalmente, controlar a energia total do sistema com o Active Energy Manager configurando uma política de limitação (conforme mostrado na ilustração a seguir).

Nota: A guia **Políticas** não está disponível em um IBM Flex System.



Para selecionar a política que você deseja usar para proteger seu servidor no caso de uma potencial falha no módulo de energia, clique no botão **Alterar** da Política Atual para a opção Redundante com Regulagem na janela Políticas de Energia.

Nota: Escolhendo uma política de energia, é possível negociar entre a redundância e a energia disponível.

As seleções de política de energia são as seguintes:

Redundante sem Regulagem

É permitida a inicialização do servidor se houver garantia de que o servidor superará a perda de uma fonte de alimentação e continuará a execução sem regulagem.

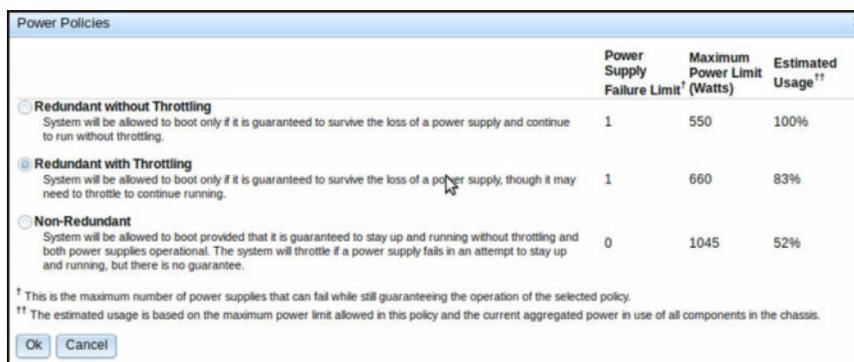
Redundante com Regulagem

É permitida a inicialização do servidor se houver garantia de que o servidor superará a perda de uma fonte de alimentação, embora o servidor possa precisar de regulagem para continuar a execução.

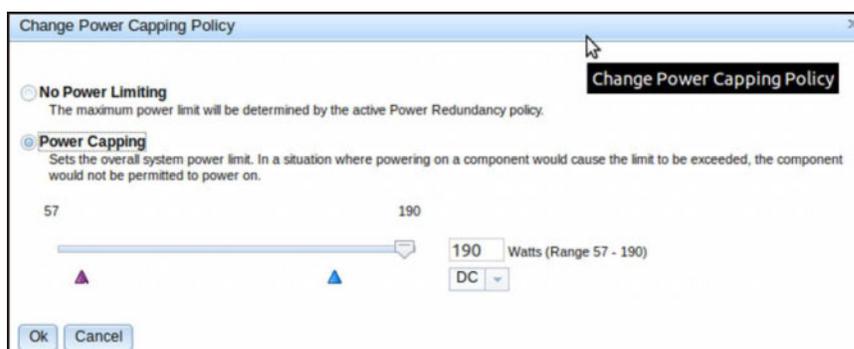
Não Redundante

É permitida a inicialização do servidor desde que haja garantia de que o servidor continuará a execução sem regulagem e ambas as fontes de alimentação estiverem operacionais. O servidor será regulado se uma fonte de alimentação falhar em uma tentativa de continuar a execução; porém, não há nenhuma garantia.

A janela a seguir é aberta quando você seleciona o botão **Alterar** para a opção Redundante com Regulagem.



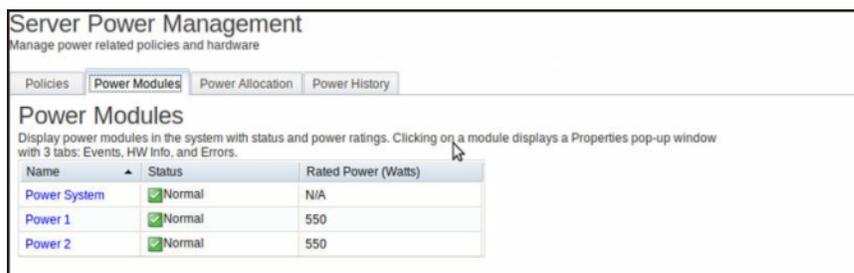
Com o Active Energy Manager, é possível limitar a quantidade total de energia que o servidor é permitido usar. Para configurar um limite para o uso de energia do servidor, clique no botão **Alterar** da Política Atual para a opção Política de Limitação de Energia na janela Políticas de Energia. A janela Alterar Política de Limitação de Energia é aberta (conforme mostrado na ilustração a seguir).



Selecione o botão **Limitação de Energia** e mova a marca da régua de controle para a voltagem desejada. A seta à direita sob a marca da régua de controle indica a configuração mínima que o Active Energy Manager pode garantir. A seta à esquerda sob a marca da régua de controle indica o uso máximo de energia do sistema nas últimas 24 horas. As duas setas fornecem orientação na configuração de um limite de energia.

Exibindo as Fontes de Alimentação Instaladas Atualmente

Clique na guia **Módulos de Energia** para exibir informações sobre as fontes de alimentação instaladas atualmente (conforme mostrado na ilustração a seguir).



O nome de cada módulo de energia no servidor é exibido juntamente com o status e a classificação de energia de cada módulo de energia. Para exibir informações adicionais para um módulo de energia, clique no nome de um módulo de energia.

Uma janela Propriedades que contém três guias é aberta: Eventos, Informações de HW e Erros para esse módulo de energia específico.

Exibindo a Capacidade da Fonte de Alimentação

Clique na guia **Alocação de Energia** para exibir quanta capacidade da fonte de alimentação está sendo usada e para exibir o consumo de energia de corrente contínua atual do servidor (conforme mostrado na ilustração a seguir).



Exibindo o Histórico de Energia

Clique na guia **Histórico de Energia** para exibir a quantia de energia que está sendo usada pelo sistema por um período de tempo selecionado. Na guia **Gráfico** na página Histórico de Energia, é possível selecionar o período de tempo e também a opção para visualizar a energia de corrente alternada ou corrente contínua. O uso de energia médio, mínimo e máximo é exibido (conforme mostrado na ilustração a seguir).



Capítulo 7. Features on Demand

O Features on Demand (FoD) do IMM2 permite instalar e gerenciar recursos opcionais do servidor e do gerenciamento de sistemas.

Há vários níveis de funcionalidade e recursos de firmware do IMM2 disponíveis para seu servidor. O nível de recursos de firmware do IMM2 instalado em seu servidor varia com base no tipo de hardware. Para obter informações sobre o tipo de hardware e recursos do IMM em seu servidor, consulte a documentação fornecida com o servidor.

É possível atualizar a funcionalidade do IMM2 comprando e instalando uma chave de ativação do FoD. Para obter informações detalhadas adicionais sobre o FoD, consulte o *Features on Demand User's Guide* em <http://www.ibm.com/systems/x/fod/>.

Nota: Em servidores com a funcionalidade de nível básico do IMM2, o IBM Integrated Management Module Standard Upgrade é necessário antes de instalar a funcionalidade do IBM Integrated Management Module Advanced Upgrade.

Para pedir uma chave de ativação do FoD, entre em contato com o representante ou parceiro de negócios ou acesse <http://www.ibm.com/systems/x/fod/>.

Use a interface da web do IMM2 ou a CLI do IMM2 para instalar manualmente uma chave de ativação do FoD que permita usar um recurso opcional comprado. Antes de ativar uma chave:

- A chave de ativação do FoD deve estar no sistema que você está usando para efetuar login no IMM2.
- Você deve ter pedido a opção FoD e recebido seu código de autorização via correio ou email.

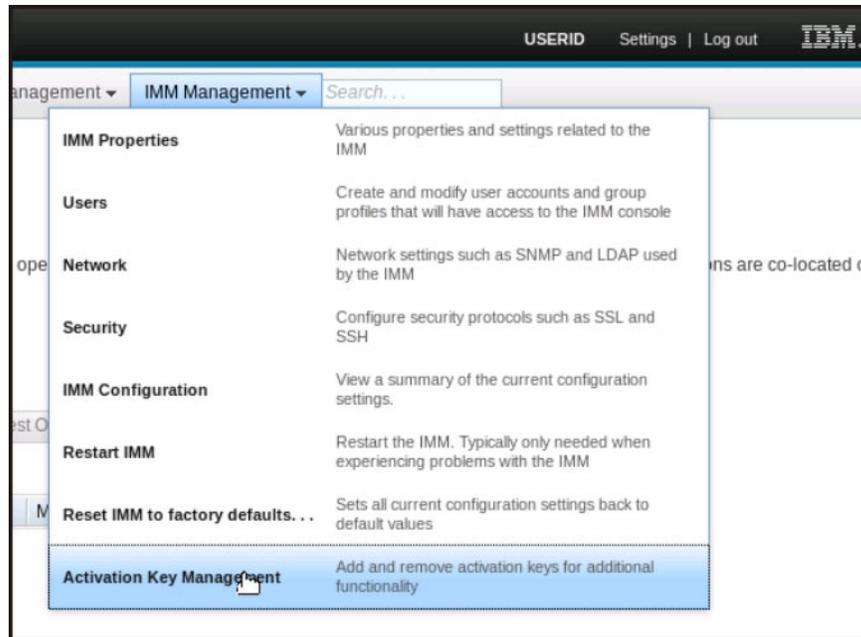
Consulte “Instalando uma Chave de Ativação”, “Removendo uma Chave de Ativação” na página 141 ou “Exportando uma Chave de Ativação” na página 143 para obter informações sobre como gerenciar uma chave de ativação FoD usando a interface da web do IMM2. Consulte “Comando keycfg” na página 172 para obter informações sobre como gerenciar uma chave de ativação do FoD usando a CLI do IMM2.

Instalando uma Chave de Ativação

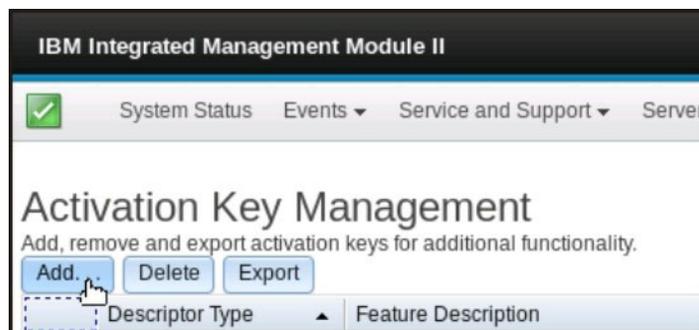
Instale uma chave de ativação de FoD para incluir um recurso opcional em seu servidor.

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

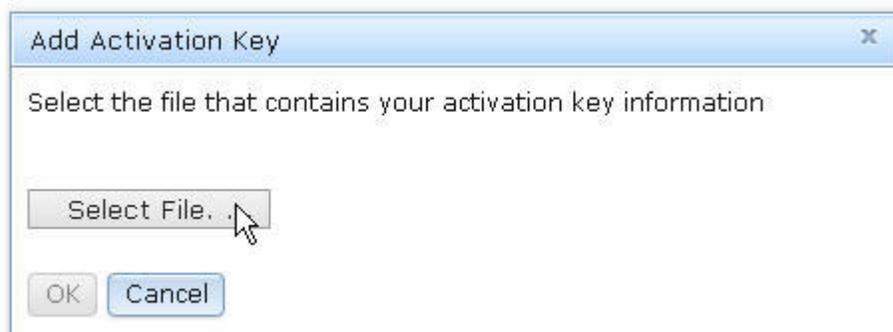
1. Efetue login no IMM2. Para obter informações adicionais, consulte o “Efetuando Login no IMM2” na página 10.
2. Na interface da web do IMM2, clique na guia **Gerenciamento do IMM**; em seguida, clique em **Gerenciamento de Chaves de Ativação**.



3. Na página Gerenciamento de Chaves de Ativação, clique em **Incluir...**



4. Na janela Incluir Chave de Ativação, clique em **Selecionar Arquivo...**; 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.

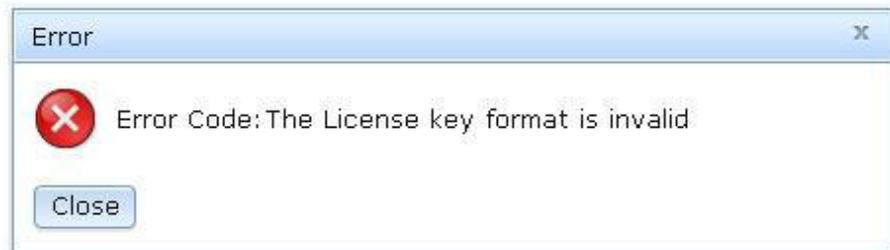


A janela Sucesso indica que a chave de ativação está instalada.

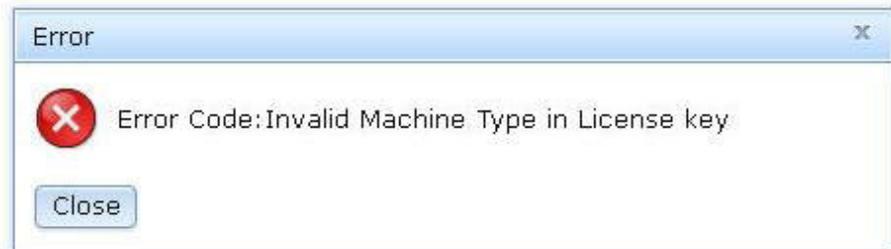


Nota:

- Se a chave de ativação não for válida, você verá a janela de erro a seguir.



- Se estiver tentando instalar a chave de ativação em um tipo de máquina que não suporta o recurso FoD, você verá a janela de erro a seguir.



5. Clique em **OK** para fechar a janela Sucesso.

A chave de ativação selecionada é incluída no servidor e aparece na página Gerenciamento de Chaves de Ativação.

Activation Key Management
Add, remove and export activation keys for additional functionality.

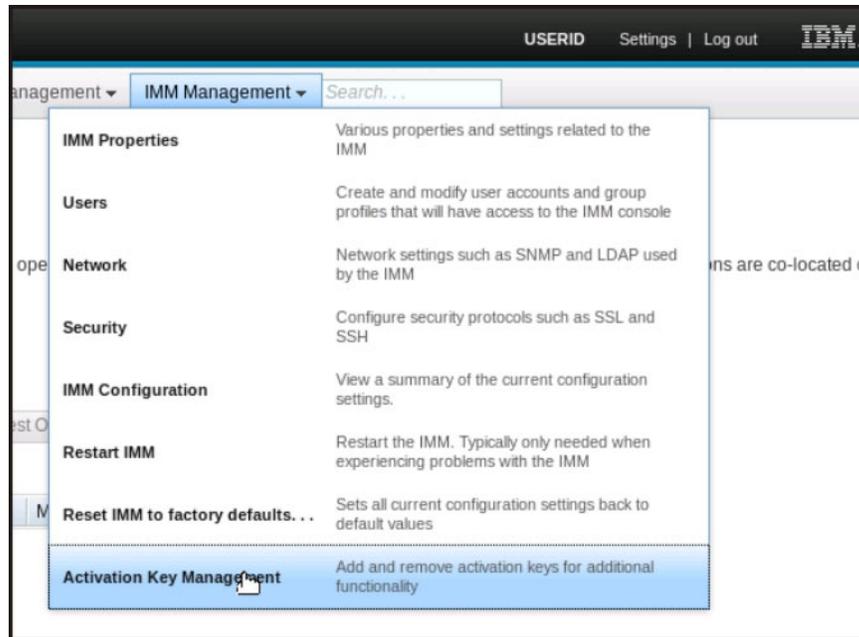
Descriptor Type	Feature Description	Unique IDs	Constraints
1	IBM Integrated Management Module Advanced Upgrade	791406KNKL9	No Constraints

Removendo uma Chave de Ativação

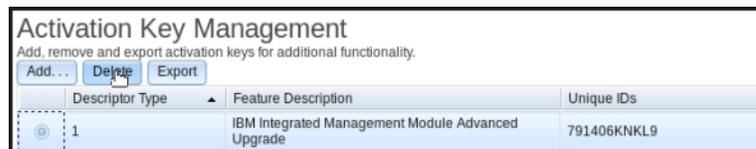
Remova uma chave de ativação de FoD para excluir um recurso opcional de seu servidor.

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

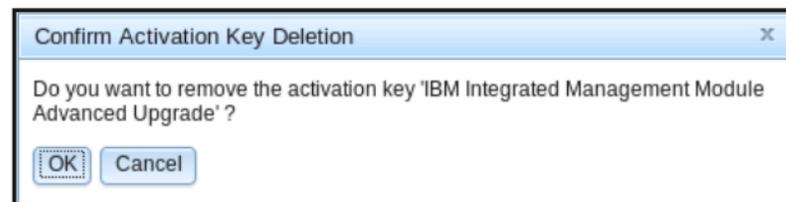
1. Efetue login no IMM2. Para obter informações adicionais, consulte o "Efetuando Login no IMM2" na página 10.
2. Na interface da web do IMM2, clique na guia **Gerenciamento do IMM**; em seguida, clique em **Gerenciamento de Chaves de Ativação**.



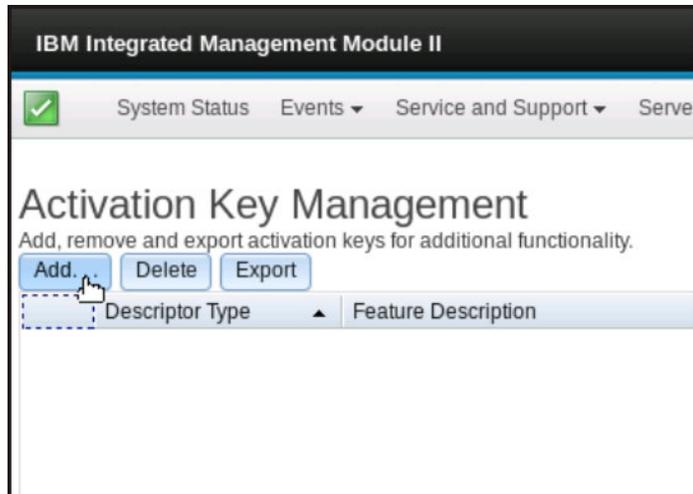
3. Na página Gerenciamento de Chaves de Ativação, selecione a chave de ativação a ser removida; em seguida, clique em **Excluir**.



4. 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 Chaves de Ativação.

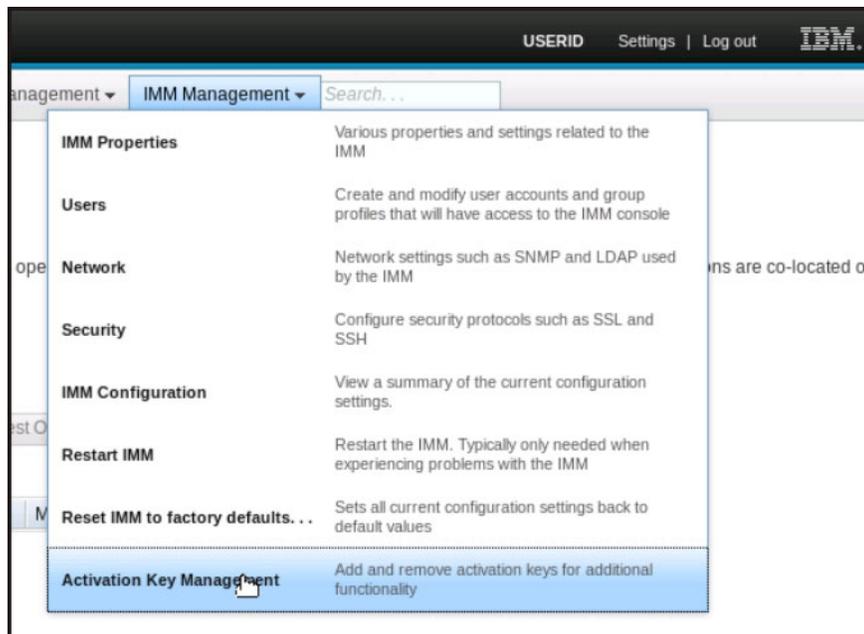


Exportando uma Chave de Ativação

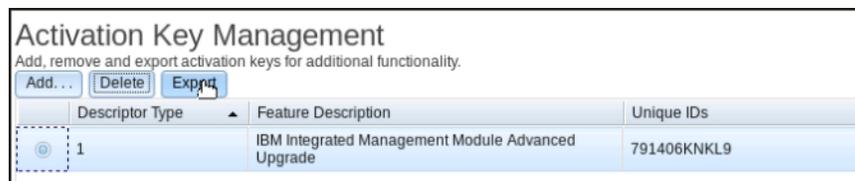
Exporte uma chave de ativação de FoD para exportar m recurso opcional de seu servidor.

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

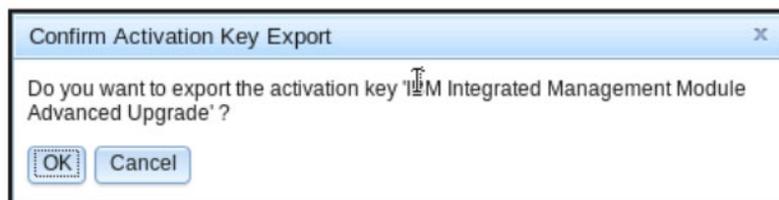
1. Efetue login no IMM2. Para obter informações adicionais, consulte o “Efetue Login no IMM2” na página 10.
2. Na interface da web do IMM2, clique na guia **Gerenciamento do IMM**; em seguida, clique em **Gerenciamento de Chaves de Ativação**.



3. Na página Gerenciamento de Chaves de Ativação, selecione a chave de ativação a ser exportada; em seguida, clique em **Exportar**.



4. Na janela Confirmar Exportação de Chave de Ativação, clique em **OK** para confirmar a exportação da chave de ativação ou clique em **Cancelar** para cancelar a solicitação de exportação de chave.



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

Capítulo 8. Interface da linha de comandos

Use a interface da linha de comandos (CLI) do IMM2 para acessar o IMM2 sem ter que usar a interface da web. Ela fornece um subconjunto das funções de gerenciamento fornecidas pela interface da web.

É possível acessar a CLI por meio de uma sessão Telnet ou SSH. Você deve ser autenticado pelo IMM2 antes de poder emitir quaisquer comandos da CLI.

Gerenciando a IMM2 com o IPMI

O IMM2 é fornecido com o ID do Usuário 1 configurado inicialmente para um nome de usuário USERID e uma senha PASSWORD (com um zero, não a letra O). Esse usuário tem acesso de Supervisor.

Importante: Altere esse nome de usuário e senha durante a configuração inicial para segurança aprimorada.

O IMM2 também fornece os recursos de gerenciamento do servidor remoto IPMI a seguir:

Interfaces da linha de comandos

A CLI 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”.

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”.

Usando o IPMItool

O IPMItool fornece várias ferramentas que podem ser usadas para gerenciar e configurar um sistema IPMI. É possível usar o IPMItool dentro e fora da banda para gerenciar e configurar o IMM2.

Para obter mais informações sobre o IPMItool ou fazer o download do IPMItool, acesse <http://sourceforge.net/>.

Acessando a Interface da Linha de Comandos

Para acessar a CLI, inicie uma sessão Telnet ou SSH para o endereço IP do IMM2 (consulte “Configurando o redirecionamento serial para Telnet ou SSH” na página 146 para obter mais informações).

Efetuando login na sessão de linha de comandos

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

1. Estabeleça uma conexão com o IMM2.
2. No prompt de nome do usuário, digite o ID do usuário.
3. No prompt de senha, digite a senha que você usa para efetuar login no IMM2.
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 Telnet ou SSH

O redirecionamento serial-para-Telnet ou SSH permite que um administrador do sistema use o IMM2 como um servidor de terminal serial. Uma porta serial do servidor pode ser acessada a partir de uma conexão Telnet ou SSH quando o redirecionamento serial é ativado.

Notas:

1. O IMM2 permite no máximo duas sessões Telnet abertas. As sessões Telnet podem acessar as portas seriais independentemente para que vários usuários possam ter uma visualização simultânea de uma porta serial redirecionada.
2. O comando **console 1** da CLI é usado para iniciar uma sessão de redirecionamento serial com a porta COM.

Sessão de Exemplo

```
telnet 192.168.70.125 (Pressione Enter.)
Conectando a 192.168.70.125...
username: USERID (Pressione Enter.)
password: ***** (Pressione Enter.)
system> console 1 (Pressione Enter.)
```

Todo o tráfego da COM2 é agora roteado para a sessão Telnet. Todo o tráfego da sessão Telnet ou SSH é roteado para a COM2.

ESC (

Digite a sequência de teclas de saída para retornar à CLI. Neste exemplo, pressione Esc e, em seguida, digite um parêntese esquerdo. O prompt da CLI é exibido para indicar o retorno à CLI do IMM2.

```
system>
```

Sintaxe de Comandos

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, o argumento 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

A CLI tem os seguintes recursos e limitações:

- Várias sessões de CLI simultâneas são permitidas com diferentes métodos de acesso (Telnet ou SSH). No máximo, duas sessões de linha de comandos Telnet podem estar ativas a qualquer momento.

Nota: O número de sessões Telnet é configurável; os valores válidos são 0, 1 e 2. O valor 0 significa que a interface Telnet está desativada.

- É permitido um comando por linha (limite de 160 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 você pode usar como um atalho para executar um comando, como no exemplo a seguir:

```
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 IMM2A00096B9E003A
-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).
- A saída de um comando é exibida na tela depois que o comando concluiu a execução. Isso impossibilita que os comandos relatem status de execução em tempo real. Por exemplo, no modo detalhado do comando **flashing**, o progresso da atualização não é mostrado em tempo real. É mostrado depois que o comando conclui a execução.
- 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 seria `ifconfig eth0 -i 192.168.70.133`.

- Todos os comandos têm as opções `-h`, `-help` e `?`, que fornecem a 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 que são suportados por sua configuração, use a opção `help` ou `?` conforme mostrado nos seguintes exemplos:

```
system> help
system> ?
```

Listagem Alfabética de Comandos

A lista completa de todos os comandos da CLI do IMM2, em ordem alfabética, é a seguinte:

- “Comando `accsecfg`” na página 159
- “Comando `alertcfg`” na página 160
- “Comando `alertentries`” na página 197
- “Comando `asu`” na página 161
- “Comando `backup`” na página 165
- “Comando `batch`” na página 200
- “Comando `clearcfg`” na página 200
- “Comando `clearlog`” na página 150
- “Comando `clock`” na página 201
- “comando do console” na página 158
- “Comando `dhcpinfo`” na página 166
- “Comando `dns`” na página 167
- “comando `ethtousb`” na página 168
- “comando `exit`” na página 149
- “Comando `fans`” na página 150
- “Comando `ffdc`” na página 150
- “Comando `gprofile`” na página 169
- “comando `help`” na página 149
- “Comando `history`” na página 149
- “Comando `identify`” na página 201
- “Comando `ifconfig`” na página 170
- “Comando `info`” na página 202
- “Comando `keycfg`” na página 172
- “Comando `ldap`” na página 173
- “Comando `led`” na página 152
- “Comando `ntp`” na página 175
- “Comando `passwordcfg`” na página 176
- “Comando `ports`” na página 176

- “Comando portcfg” na página 177
- “Comando power” na página 157
- “Comando pxeboot” na página 157
- “Comando readlog” na página 153
- “Comando reset” na página 158
- “Comando resetsp” na página 202
- “comando restaurar” na página 178
- “Comando restoredefaults” na página 179
- “Comando set” na página 179
- “Comando show” na página 154
- “Comando smtp” na página 180
- “Comando Snmp” na página 181
- “Comando snmpalerts” na página 183
- “Comando spreset” na página 202
- “Comando srcfg” na página 184
- “Comando sshcfg” na página 185
- “Comando ssl” na página 186
- “Comando sslcfg” na página 187
- “Comando syshealth” na página 155
- “Comando telnetcfg” na página 190
- “Comando temps” na página 155
- “Comando thermal” na página 191
- “Comando timeouts” na página 191
- “Comando usbeth” na página 192
- “Comando users” na página 192
- “Comando volts” na página 155
- “Comando vpd” na página 156

Comandos Utilitários

Os comandos de utilitário são os seguintes:

- “comando exit”
- “comando help”
- “Comando history”

comando exit

Use o comando **exit** para efetuar logoff e terminar a sessão da CLI.

comando help

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 comandos.

Comando history

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 de históricos.

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
-g 0.0.0.0
-s 255.255.255.0
-n IMM2A00096B9E003A
-r auto
-d auto
-m 1500
-b 00:09:6B:9E:00:3A
-l 00:00:00:00:00:00
system>
```

Comandos de Monitor

Os comandos de monitor são os seguintes:

- “Comando clearlog”
- “Comando fans”
- “Comando ffdc”
- “Comando led” na página 152
- “Comando readlog” na página 153
- “Comando show” na página 154
- “Comando syshealth” na página 155
- “Comando temps” na página 155
- “Comando volts” na página 155
- “Comando vpd” na página 156

Comando clearlog

Use o comando **clearlog** para limpar o log de eventos do IMM2. Para usar esse comando, você deve ter a autoridade para limpar logs de eventos.

Comando fans

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

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

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.

Opção	Descrição	Valores
-t	Número de tipo	1 (dump do processador) e 4 (dados de serviço). 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 ou 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_imm2_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_imm2_120926-105320.tgz
system>

```

Comando led

Use o comando **led** para exibir e configurar estados de LED.

- A execução do comando **led** sem opções exibe o status de 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.

Opção	Descrição	Valores
-l	Obtenha o status de todos os LEDs no sistema e seus subcomponentes	
-chklog	Desligar o LED de log de verificação	off
-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

Use o comando **readlog** para exibir as entradas de log de eventos do IMM2, cinco 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 do arquivo do arquivo de 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 SERVPROC 12/18/03 10:18:58 Remote Login Successful.  
Login ID: 'USERID' CLI authenticated from 192.168.70.231 (Telnet).'  
2 I SERVPROC 12/18/03 10:12:22 Remote Login successful.  
Login ID: 'USERID' from web browser at IP=192.168.70.231'  
3 E SERVPROC 12/18/03 10:10:37 Failure reading I2C device.  
4 E SERVPROC 12/18/03 10:10:37 Environmental monitor not responding.  
5 E SERVPROC 12/18/03 10:10:37 Failure reading I2C device.  
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 show

Use o comando **show** para exibir configurações simples do IMM2.

- O comando **show** exibe os valores configurados usando o comando **set**.
- As configurações são organizadas como uma árvore de diretórios. Exiba a árvore integral usando a opção de comando **show -r**.
- Algumas dessas configurações, como variáveis de ambiente, são usadas pela CLI.

A tabela a seguir mostra os argumentos das opções.

Opção	Descrição	Valores
<i>valor</i>	Valor de caminho ou configuração a ser exibido	
-r	Exibir configurações recursivamente	

Sintaxe:

```
show [options]
option:
  value
  -r
```

Comando syshealth

Use o comando **syshealth** para exibir um resumo do funcionamento do servidor. O estado da energia, o estado do sistema, a contagem de reinicializações e o status do software do IMM2 são exibidos.

Exemplo:

```
system> syshealth
Power On
State System on/starting UEFI
Restarts 71
system>
```

Comando temps

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.

Exemplo:

```
system> temps
Temperatures are displayed in degrees Fahrenheit/Celsius
      WR      W      T      SS      HS
-----
CPU1  65/18  72/22  80/27  85/29  90/32
CPU2  58/14  72/22  80/27  85/29  90/32
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: reconfiguração de aviso

W: aviso

T: temperatura (valor atual)

SS: encerramento temporário

HS: encerramento permanente

2. Todos os valores de temperatura estão em graus Fahrenheit/Celsius.

Comando volts

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.

Exemplo:

```
system> volts
      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
SSL: encerramento temporário baixo
WL: aviso baixo
WRL: reconfiguração de aviso alta
V: voltagem (valor atual)
WRH: reconfiguração de aviso alta
WH: aviso alto
SSH: encerramento temporário alto
HSH: encerramento permanente alto

Comando vpd

Use o comando **vpd** para exibir dados vitais do produto para o sistema (sys), IMM2 (imm), BIOS do servidor (uefi), servidor Dynamic System Analysis Preboot (dsa), firmware do servidor (fw) e componentes do servidor (comp). As mesmas informações são exibidas como na interface da web.

Sintaxe:

```

vpd [options]
option:
  -sys
  -imm
  -uefi
  -dsa
  -fw
  -comp

```

Use o comando vpd para exibir dados vitais do produto para diferentes partes do servidor.

Opção	Descrição
-sys	Exibe dados vitais do produto para o sistema
-imm	Exibe dados vitais do produto para o controlador IMM2
-uefi	Exibe dados vitais do produto para o BIOS
-dsa	Exibe dados vitais do produto para o Diag
-fw	Exibe dados vitais do produto para o firmware do sistema
-comp	Exibe dados vitais do produto para componentes do sistema

Exemplo:

```

system> vpd -dsa
Type      Version      Build      ReleaseDate
-----
DSA       9,25         DSYTA5A   2012/07/31
system>

```

Comandos de controle de energia e reinicialização do servidor

Os comandos de energia e reinicialização do servidor são os seguintes:

- “Comando power”
- “Comando pxeboot”
- “Comando reset” na página 158

Comando power

Use o comando **power** para controlar a energia do sistema. Para emitir os comandos **power**, você deve ter autoridade de acesso de energia e reinicialização.

power on liga o servidor.

power off desliga o servidor. A opção **-s** encerra o sistema operacional antes de desligar o servidor.

power state exibe o estado da energia do servidor (ligado ou desligado) e o estado atual do servidor.

power cycle desliga o servidor e o liga novamente. A opção **-s** encerra o sistema operacional antes de desligar o servidor.

Sintaxe:

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

Comando pxeboot

Use o comando **pxeboot** para exibir e configurar 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.

Opção	Descrição	Valores
-en	Configura a condição do Ambiente de Execução de Pré-inicialização para a próxima reinicialização do sistema	ativado, desativado

Sintaxe:

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

Exemplo:

```
system> pxeboot
-en disabled
system>
```

Comando reset

Use o comando **reset** para reiniciar o servidor. Para usar esse comando, você deve ter autoridade de acesso de energia e reinicialização. A opção **-s** encerra o sistema operacional antes de reiniciar o servidor.

Sintaxe:

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

Comando de redirecionamento serial

Existe um comando de redirecionamento serial: o “comando do console”.

comando do console

Use o comando **console** para iniciar uma sessão do console de redirecionamento serial para a porta serial designada do IMM2.

Sintaxe:

```
console 1
```

Comandos de configuração

Os comandos de configuração são os seguintes:

- “Comando accsecfg” na página 159
- “Comando alertcfg” na página 160
- “Comando asu” na página 161
- “Comando backup” na página 165
- “Comando dhcpinfo” na página 166
- “Comando dns” na página 167
- “comando ethtousb” na página 168
- “Comando gprofile” na página 169
- “Comando ifconfig” na página 170
- “Comando keycfg” na página 172
- “Comando ldap” na página 173
- “Comando ntp” na página 175
- “Comando passwordcfg” na página 176
- “Comando ports” na página 176
- “Comando portcfg” na página 177
- “comando restaurar” na página 178
- “Comando restoredefaults” na página 179
- “Comando set” na página 179
- “Comando smtp” na página 180
- “Comando Snmp” na página 181
- “Comando snmpalerts” na página 183
- “Comando srcfg” na página 184
- “Comando sshcfg” na página 185
- “Comando ssl” na página 186

- “Comando sslcfg” na página 187
- “Comando telnetcfg” na página 190
- “Comando thermal” na página 191
- “Comando timeouts” na página 191
- “Comando usbeth” na página 192
- “Comando users” na página 192

Comando accsecfg

Use o comando **accsecfg** para exibir e configurar definições de segurança da conta.

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

Opção	Descrição	Valores
-legacy	Configura a segurança da conta como um conjunto legado predefinido de padrões	
-high	Configura a segurança da conta como um conjunto alto predefinido de padrões	
-custom	Configura a segurança da conta para valores definidos pelo usuário	
-am	Configura o método de autenticação do usuário	local, ldap, localldap, ldaplocal
-lp	Período de bloqueio após máximo de falhas de login (minutos)	0, 1, 2, 5, 10, 15, 20, 30, 60, 120, 180 ou 240 minutos. O valor padrão será 60 se "Segurança Alta" estiver ativado e 2 se "Segurança Legada" estiver ativado. Um valor zero desativa esta função.
-pe	Período de tempo de expiração de senha (dias)	0 a 365 dias
-pr	Senha necessária	on, off
-pc	Regras de complexidade de senha	on, off
-pd	Número mínimo de caracteres diferentes da senha	0 a 19 caracteres
-pl	Comprimento da senha	1 a 20 caracteres
-ci	Intervalo mínimo de mudança de senha (horas)	0 a 240 horas
-lf	Número máximo de falhas de login	0 a 10

Opção	Descrição	Valores
-chgdft	Alterar senha padrão após primeiro login	on, off
-chgnew	Alterar nova senha de usuário após primeiro login	on, off
-rc	Ciclo de reutilização de senha	0 a 5
-wt	Tempo limite da sessão de inatividade da web (minutos)	1, 5, 10, 15, 20, none ou user

Sintaxe:

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 o comando **alertcfg** para exibir e configurar os parâmetros de alerta remoto global do IMM2.

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

Opção	Descrição	Valores
-dr	Configura o tempo de espera entre as novas tentativas antes de o IMM2 reenviar um alerta	0 a 4,0 minutos, em incrementos de 0,5 minuto
-da	Configura o tempo de espera antes de o IMM2 enviar um alerta para o próximo destinatário na lista	0 a 4,0 minutos, em incrementos de 0,5 minuto
-rl	Configura o número de vezes adicionais que o IMM2 tenta enviar um alerta, se tentativas anteriores foram malsucedidas	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

Os comandos do Utilitário de Configurações Avançadas são usados para configurar definições de 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 7. Comandos ASU

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.	<i>setting_instance</i>
help	Use esse comando para exibir informações da ajuda para uma ou mais configurações.	<i>setting</i>

Tabela 7. Comandos ASU (continuação)

Comando	Descrição	Valor
set	<p>Use esse comando para alterar o valor de uma configuração. Configure a definição de UEFI para o valor de entrada.</p> <p>Notas:</p> <ul style="list-style-type: none"> • 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." 	<i>setting value</i>
showgroups	<p>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.</p>	<i>setting</i>
show	<p>Use esse comando para exibir o valor atual de uma ou mais configurações.</p>	<i>setting</i>

Tabela 7. Comandos ASU (continuação)

Comando	Descrição	Valor
showvalues	Use esse comando para exibir todos os valores possíveis para uma ou mais configurações. Notas: <ul style="list-style-type: none"> • 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. 	<i>setting</i>
Notas: <ul style="list-style-type: none"> • Na sintaxe de comando, <i>setting</i> é o nome de uma configuração que você deseja visualizar ou alterar e <i>value</i> é o valor que está colocando na configuração. • <i>Setting</i> pode ser mais que um nome, exceto ao usar o comando set. • <i>Setting</i> pode conter curingas, por exemplo, um asterisco (*) ou um ponto de interrogação (?). • <i>Setting</i> pode ser um grupo, um nome de configuração ou all. 		

Alguns exemplos da sintaxe de 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`.

Comando **show values** de exemplo:

```
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.

Opção	Descrição	Valores
-b ¹	Exibir no formato de lote.	

Opção	Descrição	Valores
--help ³	Exibir uso e opções do comando. O ícone --help é colocado antes do comando, por exemplo, asu --help show .	
--help ³	Exibir ajuda para o comando. A opção --help é colocada após o comando, por exemplo, asu show --help .	
-l ¹	Nome de configuração de formato longo (incluir o conjunto de configuração).	
-m ¹	Nome de configuração de formato combinado (usar o ID de configuração).	
-v ²	Saída detalhada.	
<ol style="list-style-type: none"> 1. As opções -b, -l e -m são usadas apenas com o comando show. 2. A opção -v é usada apenas entre asu e o comando. 3. A opção --help pode ser usada com qualquer 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 8. Comandos de Transação

Comando	Descrição	Valor
tropen <i>id</i>	Esse comando cria um novo arquivo de transação contendo várias definições a serem configuradas.	<i>Id</i> é a sequência de identificação, 1 a 3 caracteres alfanuméricos.
trset <i>id</i>	Esse comando inclui uma ou mais configurações ou pares de valores em uma transação.	<i>Id</i> é a sequência de identificação, 1 a 3 caracteres alfanuméricos.

Tabela 8. Comandos de Transação (continuação)

Comando	Descrição	Valor
trlist <i>id</i>	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.	<i>Id</i> é a sequência de identificação, 1 a 3 caracteres alfanuméricos.
trcommit <i>id</i>	Esse comando confirma e executa o conteúdo do arquivo de transação. Os resultados da execução e quaisquer erros serão exibidos.	<i>Id</i> é a sequência de identificação, 1 a 3 caracteres alfanuméricos.
trrm <i>id</i>	Esse comando remove o arquivo de transação após ele ter sido confirmado.	<i>Id</i> 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.Wo1BootOrder "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 o comando **backup** para criar um arquivo de backup que contenha as configurações de segurança do sistema atuais.

A tabela a seguir mostra os argumentos 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 da 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 imm-back.cli -pp xxxxxx -ip 192.168.70.200
ok
system>

```

Comando dhcpinfo

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
```

Exemplo:

```

system> dhcpinfo eth0

-server : 192.168.70.29
-n      : IMM2A-00096B9E003A
-i      : 192.168.70.202
-g      : 192.168.70.29
-s      : 255.255.255.0
-d      : linux-sp.raleigh.ibm.com
-dns1   : 192.168.70.29
-dns2   : 0.0.0.0
-dns3   : 0.0.0.0
-i6     : 0::0
-d6     : *
-dns61  : 0::0
-dns62  : 0::0
-dns63  : 0::0
system>

```

A tabela a seguir descreve a saída do exemplo.

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

Opção	Descrição
-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 o comando **dns** para visualizar e definir a configuração do DNS do IMM2.

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

Opção	Descrição	Valores
-state	Estado do DNS	on, off
-ddns	Estado do DDNS	ativado, desativado
-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 IMM2 na qual o DNS está ativado.

Exemplo:

```
system> dns
-state : enabled
-i1    : 192.168.70.202
-i2    : 192.168.70.208
-i3    : 192.168.70.212
-i61   : fe80::21a:64ff:fee6:4d5
-i62   : fe80::21a:64ff:fee6:4d6
-i63   : fe80::21a:64ff:fee6:4d7
-ddns  : enabled
-ddn   : ibm.com
-ddncur : ibm.com
-dnsrc : dhcp
-p     : ipv6

system>
```

A tabela a seguir descreve a saída do exemplo.

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 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.

Opção	Descrição	Valores
-en	Estado de Ethernet-sobre-USB	enabled, disabled

Opção	Descrição	Valores
-mx	Configurar mapeamento de portas para índice <i>x</i>	O par de portas, separadas por dois-pontos (:), no formato <i>port1:port2</i> Em que: <ul style="list-style-type: none"> • O número de índice de porta, <i>x</i>, é especificado como um número inteiro de 1 a 10 na opção de comando. • <i>port1</i> do par de portas é o número da porta Ethernet externa. • <i>port2</i> 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
  -mx port_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 gprofile

Use o comando **gprofile** para exibir e configurar perfis de grupo para o IMM2.

A tabela a seguir mostra os argumentos das opções.

Opção	Descrição	Valores
-clear	Exclui um grupo	ativado, desativado
-n	O nome do grupo	Sequência de até 63 caracteres para <i>group_name</i> O <i>group_name</i> deve ser exclusivo.
-a	Nível de autoridade baseada em função	supervisor, operator, rbs <lista de funções>: 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	Exibe 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 ifconfig

Use o comando **ifconfig** 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.

A tabela a seguir mostra os argumentos das opções.

Opção	Descrição	Valores
-state	Estado da interface	disabled, enabled
-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
-nic	Endereço NIC	compartilhado, dedicado

Opção	Descrição	Valores
-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 ativados.	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 ativado.	O endereço Local de link é determinado pelo IMM2. 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
-p6	Comprimento de prefixo de endereço	Numérico entre 1 e 128
-g6	Gateway ou rota padrão	Endereço IP para gateway ou rota padrão do canal Ethernet 0 no IPv6
-dhcp6	Estado do DHCPv6	disabled, enabled
-sa6	Estado de configuração automática stateless do IPv6	disabled, enabled

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
-dn domain_name
-auto state
-nic state
-address_table
-ipv6 state
-ipv6static state
-sa6 state
-i6 static_ipv6_ip_address
-g6 ipv6_gateway_address
-p6 length
```

Exemplo:

```
system> ifconfig eth0
-state enabled
-c dthens
-i 192.168.70.125
-g 0.0.0.0
-s 255.255.255.0
-n IMM2A00096B9E003A
```

```

-r auto
-d auto
-m 1500
-b 00:09:6B:9E:00:3A
-l 00:00:00:00:00:00
system> ifconfig eth0 -c static -i 192.168.70.133
These configuration changes will become active after the next reset of the IMM2.
system>

```

Nota: A opção **-b** na exibição `ifconfig` é para o endereço MAC gravado. O endereço MAC gravado é somente leitura e não é configurável.

Comando `keycfg`

Use o comando `keycfg` para exibir, incluir ou excluir chaves de ativação. Essas teclas controlam o acesso a recursos opcionais de Features on Demand (FoD) do IMM2.

- Quando `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.

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 <code>keycfg</code> .
-deltype	Excluir chave de ativação por tipo de chave	Valor de tipo de chave válido.

Sintaxe:

```
keycfg [options]
option:
  -add
    -ip ip_address
    -pn port_number
    -u username
    -pw password
    -f filename
  -del key_index
  -deltype key_type
```

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"
system>
```

Comando ldap

Use o comando **ldap** para exibir e configurar os parâmetros de configuração do protocolo LDAP.

A tabela a seguir mostra os argumentos 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	ativado, desativado
-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 <i>client_dn</i>
-d	Domínio de procura	Sequência de até 63 caracteres para <i>search_domain</i>
-f	Filtro de grupo	Sequência de até 127 caracteres para <i>group_filter</i>
-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 <i>group_search_attr</i>
-l	Atributo de permissão de login	Sequência de até 63 caracteres para <i>string</i>
-p	Senha do cliente	Sequência de até 15 caracteres para <i>client_pw</i>
-pc	Confirmar senha do cliente	Sequência de até 15 caracteres para <i>confirm_pw</i> O uso do comando é: <code>ldap -p client_pw -pc confirm_pw</code> Essa opção é necessária quando você altera a senha do cliente. Ela compara o argumento <i>confirm_pw</i> com o argumento <i>client_pw</i> . O comando falhará se os argumentos não corresponderem.

Opção	Descrição	Valores
-r	Nome distinto (DN) de entrada raiz	Sequência de até 127 caracteres para <i>root_dn</i>
-rbs	Segurança Aprimorada Baseada em Função para usuários do Active Directory	ativado, desativado
-s1ip	Nome do host/endereço IP do servidor 1	Sequência de até 127 caracteres ou um endereço IP para <i>host name/ip_addr</i>
-s2ip	Nome do host/endereço IP do servidor 2	Sequência de até 127 caracteres ou um endereço IP para <i>host name/ip_addr</i>
-s3ip	Nome do host/endereço IP do servidor 3	Sequência de até 127 caracteres ou um endereço IP para <i>host name/ip_addr</i>
-s4ip	Nome do host/endereço IP do servidor 4	Sequência de até 127 caracteres ou um endereço IP para <i>host name/ip_addr</i>
-s1pn	Número da porta do servidor 1	Um número de porta com até 5 dígitos para <i>port_number</i>
-s2pn	Número da porta do servidor 2	Um número de porta com até 5 dígitos para <i>port_number</i>
-s3pn	Número da porta do servidor 3	Um número de porta com até 5 dígitos para <i>port_number</i>
-s4pn	Número da porta do servidor 4	Um número de porta com até 5 dígitos para <i>port_number</i>
-t	Nome de destino do servidor	Quando a opção <code>-rbs</code> está ativada, esse campo especifica um nome de destino que pode ser associado a uma ou mais funções no servidor Active Director por meio da ferramenta Role-Based Security (RBS) Snap-In.
-u	Atributo de procura UID	Sequência de até 63 caracteres para <i>search_attr</i>
-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|locl|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
```

```

-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 o comando **ntp** para exibir e configurar o Network Time Protocol (NTP).

A tabela a seguir mostra os argumentos das opções.

Opção	Descrição	Valores
-en	Ativa ou desativa o Network Time Protocol	ativado, desativado
-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 clock do IMM2 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 passwordcfg

Use o comando **passwordcfg** para exibir e configurar os parâmetros de senha.

Opção	Descrição
-legacy	Configura a segurança da conta como um conjunto legado predefinido de padrões
-high	Configura a segurança da conta como um conjunto alto predefinido de padrões
-exp	Duração máxima da senha (0 a 365 dias). Configure como 0 para não haver expiração.
-cnt	Número de senhas anteriores que não podem ser reutilizadas (0 a 5)
-nul	Permite contas sem senha (yes no)
-h	Exibe o uso e as opções do comando

Sintaxe:

```
passwordcfg [options]
options: {-high}|{-legacy}|{-exp|-cnt|-nul}
-legacy
-high
-exp:
-cnt:
-nul:
-h
```

Exemplo:

```
system> passwordcfg
Security Level: Legacy
system> passwordcfg -exp 365
ok
system> passwordcfg -nul yes
ok
system> passwordcfg -cnt 5
ok
system> passwordcfg
Security Level: Customize
-exp: 365
-cnt: 5
-nul: allowed
```

Comando ports

Use o comando **ports** para exibir e configurar portas do IMM2.

A execução do comando **ports** sem opções exibe informações para todas as portas do IMM2. A tabela a seguir mostra os argumentos das opções.

Opção	Descrição	Valores
-open	Exibir portas abertas	
-reset	Reconfigurar portas para configurações padrão	
-http	Número da porta HTTP	Número da porta padrão: 80
-https	Número da porta HTTPS	Número da porta padrão: 443

Opção	Descrição	Valores
-telnetp	Número da porta da CLI legada do Telnet	Número da porta padrão: 23
-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
  -http port_number
  -https port_number
  -telnetp port_number
  -sshp port_number
  -snmpap port_number
  -snmptp port_number
  -rpp port_number
  -cimhp port_number
  -cimhsp port_number
```

Exemplo:

```
system> ports
-http 80
-https 443
-rpp 3900
-snmppap 161
-snmptp 162
-sshp 22
-telnetp 23
-cimhp 5988
-cimhsp 5989
system>
```

Comando portcfg

Use o comando **portcfg** para configurar o IMM2 para o recurso de redirecionamento serial.

O IMM2 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 IMM2 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.

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 Em que: <ul style="list-style-type: none"> • 0 = none: A CLI é desativada • 1 = cliems: A CLI é ativada com sequências de pressionamento de tecla compatíveis com o EMS • 2 = cliuser: A CLI é ativada 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 com sequência de pressionamento de tecla definida pelo usuário)
-p      : even
-s      : 1
system> portcfg -b 38400
ok
system>
```

comando restaurar

Use o comando **restore** para restaurar as configurações do sistema a partir de um arquivo de backup.

A tabela a seguir mostra os argumentos 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

Opção	Descrição	Valores
-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:

```
restore [options]
```

option:

```
-f filename
-pp password
-ip ip_address
-pn port_number
-u username
-pw password
```

Exemplo:

```
system> restore -f imm-back.cli -pp xxxxxx -ip 192.168.70.200
ok
system>
```

Comando restoredefaults

Use o comando **restoredefaults** para restaurar todas as configurações do IMM2 para o padrão de factory.

- 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 set

Use o comando **set** para alterar as configurações do IMM2.

- Algumas configurações do IMM2 podem ser alteradas com um comando **set** simples.
- Algumas dessas configurações, como variáveis de ambiente, são usadas pela CLI.
- Use o comando **show** para exibir valores configurados usando o comando **set**.

A tabela a seguir mostra os argumentos das opções.

Opção	Descrição	Valores
<i>valor</i>	Configurar valor para caminho ou configuração especificada	Valor apropriado para o caminho ou configuração especificada.

Sintaxe:

```
set [options]
option:
  valor
```

Comando smtp

Use o comando **smtp** para exibir e configurar definições para 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.

Opção	Descrição	Valores
-auth	Suporte de autenticação SMTP	ativado, desativado
-authpw	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
  -authpw 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 o comando **snmp** 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.

Opção	Descrição	Valores
-a	Agente SNMPv1	on, off Nota: Para ativar o agente do SNMPv1, os critérios a seguir devem ser atendidos: <ul style="list-style-type: none">• Contato do IMM2 especificado usando a opção de comando -cn.• Local do IMM2 especificado usando a opção de comando -l.• Pelo menos um nome de comunidade SNMP especificado usando uma das opções de comando -cx.• Pelo menos um endereço IP válido é especificado para cada comunidade SNMP usando uma das opções de comando -cxiy.
-a3	Agente do SNMPv3	on, off Nota: Para ativar o agente do SNMPv3, os critérios a seguir devem ser atendidos: <ul style="list-style-type: none">• Contato do IMM2 especificado usando a opção de comando -cn.• Local do IMM2 especificado usando a opção de comando -l.
-t	Traps SNMP	on, off
-l	Local do IMM2	Sequência (limitada a 47 caracteres). Nota: <ul style="list-style-type: none">• Argumentos contendo espaços devem ser colocados entre aspas. Nenhum espaço à esquerda ou direita é permitido nos argumentos.• Limpe o local do IMM2 especificando nenhum argumento ou especificando uma sequência vazia como o argumento, tal como "".
-cn	Nome de contato do IMM2	Sequência (limitada a 47 caracteres). Nota: <ul style="list-style-type: none">• Argumentos contendo espaços devem ser colocados entre aspas. Nenhum espaço à esquerda ou direita é permitido nos argumentos.• Limpe o nome do contato do IMM2 especificando nenhum argumento ou especificando uma sequência vazia como o argumento, tal como "".

Opção	Descrição	Valores
-cx	Nome da comunidade SNMP <i>x</i>	Sequência (limitada a 15 caracteres). Nota: <ul style="list-style-type: none"> <i>x</i> é especificado como 1, 2 ou 3 na opção de comando para indicar o número da comunidade. Argumentos contendo 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 "".
-cxiy	Endereço IP ou nome do host <i>y</i> da comunidade SNMP <i>x</i>	Endereço IP ou nome do host válido (limitado a 63 caracteres). Nota: <ul style="list-style-type: none"> <i>x</i> é especificado como 1, 2 ou 3 na opção de comando para indicar o número da comunidade. <i>y</i> é especificado como 1, 2 ou 3 na opção de comando para indicar o número do endereço IP ou nome do host. Um endereço IP ou nome do host só pode conter pontos, sublinhados, sinais de menos, 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.
-cax	Tipo de acesso da comunidade SNMPv3 <i>x</i>	get, set, trap Nota: <i>x</i> é especificado como 1, 2 ou 3 na opção de comando para indicar o número da comunidade.

Sintaxe:

```
snmp [options]
option:
  -a state
  -a3 state
  -t state
  -l location
  -cn contact_name
  -c1 snmp_community_1_name
  -c2 snmp_community_2_name
  -c3 snmp_community_3_name
  -cli1 community_1_ip_address_or_hostname_1
  -cli2 community_1_ip_address_or_hostname_2
  -cli3 community_1_ip_address_or_hostname_3
  -c2i1 community_2_ip_address_or_hostname_1
  -c2i2 community_2_ip_address_or_hostname_2
  -c2i3 community_2_ip_address_or_hostname_3
  -c3i1 community_3_ip_address_or_hostname_1
  -c3i2 community_3_ip_address_or_hostname_2
  -c3i3 community_3_ip_address_or_hostname_3
  -ca1 community_1_access_type
  -ca2 community_2_access_type
  -ca3 community_3_access_type
```

Exemplo:

```
system> snmp
-a Enabled
-a3 Enabled
```

```

-t Enabled
-l RTC,NC
-cn Snmp Test
-c1 public
-c1i1 192.44.146.244
-c1i2 192.44.146.181
-c1i3 192.44.143.16
-ca1 set
-ch1 specific
-c2 private
-c2i1 192.42.236.4
-c2i2
-c2i3
-ca2 get
-ch2 specific
-c3
-c3i1
-c3i2
-c3i3
-ca3 get
-ch3 ipv4only
system>

```

Comando snmpalerts

Use o comando **snmpalerts** 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.

Opção	Descrição	Valores
-status	Status de alerta de SNMP	on, off
-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: <ul style="list-style-type: none"> • 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	enabled, disabled

Opção	Descrição	Valores
-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: <ul style="list-style-type: none"> • 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	enabled, disabled
-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: <ul style="list-style-type: none"> • 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	enabled, disabled

Sintaxe:

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

Comando srcfg

Use o comando **srcfg** 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 IMM2 não fornece um recurso de passagem de porta serial para porta serial. Portanto, as opções `-passthru` e `entercli seq` 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 de comando `srcfg -entercli seq`.

Opção	Descrição	Valores
<code>-entercli seq</code>	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, <code>^[</code> para a tecla de escape e <code>^M</code> 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 <code>^(</code> que é Esc seguido por (.

Sintaxe:

```
srcfg [options]
options:
-entercli seq entercli_keyseq
```

Exemplo:

```
system> srcfg
-entercli seq ^[Q
system>
```

Comando sshcfg

Use o comando `sshcfg` para exibir e configurar parâmetros de SSH.

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

Opção	Descrição	Valores
<code>-cstatus</code>	Estado da CLI do SSH	ativado, desativado
<code>-hk gen</code>	Gerar chave privada do servidor SSH	
<code>-hk rsa</code>	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 o comando **ssl** para exibir e configurar os parâmetros de SSL.

Nota: Para poder ativar 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.

Opção	Descrição	Valores
-ce	Ativa ou desativa um cliente SSL	on, off
-se	Ativa ou desativa um servidor SSL	on, off
-cime	Ativa ou desativa o CIM sobre HTTPS no servidor SSL	on, off

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 o comando `sslcfg` para exibir e configurar SSL para o IMM2 e gerenciar certificados.

A execução do comando `sslcfg` sem opções exibe todas as informações de configuração do SSL. A tabela a seguir mostra os argumentos das opções.

Opção	Descrição	Valores
-server	Status do servidor SSL	enabled, disabled Nota: O servidor SSL poderá ser ativado apenas se houver um certificado válido no local.
-client	Status do cliente SSL	enabled, disabled Nota: O cliente SSL poderá ser ativado apenas se houver um certificado de servidor ou cliente válido no local.
-cim	Status do CIM sobre HTTPS	enabled, disabled Nota: O CIM sobre HTTPS poderá ser ativado apenas se houver um certificado de servidor ou cliente válido no local.

Opção	Descrição	Valores
-cert	Gerar certificado autoassinado	server, client, sysdir Nota: <ul style="list-style-type: none"> 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.
-csr	Gerar CSR	server, client, sysdir Nota: <ul style="list-style-type: none"> 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 .
-tcx	Certificado de confiança <i>x</i> para cliente SSL	import, download, remove Nota: O número do certificado de confiança, <i>x</i> , 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.

Opção	Descrição	Valores
-cl	Cidade ou localidade	Sequência delimitada por aspas (máximo 50 caracteres) Nota: Necessário ao gerar um certificado autoassinado ou CSR.
-on	Organization name	Sequência delimitada por aspas (máximo 60 caracteres) Nota: Necessário ao gerar um certificado autoassinado ou CSR.
-hn	Nome do host do IMM2	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.
-s	Sobrenome	Sequência delimitada por aspas (máximo 60 caracteres) Nota: Opcional ao gerar um certificado autoassinado ou CSR.
-gn	Primeiro 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
  -pn port_number
```

```

-u username
-pw password
-l filename
-dnld
-upld
-tcx action
-c country_code
-sp state_or_province
-cl city_or_locality
-on organization_name
-hn imm_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

```

Exemplo:

```

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
system>

```

Comando telnetcfg

Use o comando **telnetcfg** para exibir e configurar as configurações de Telnet.

A execução do comando **telnetcfg** sem opções exibe o estado do Telnet. A tabela a seguir mostra os argumentos das opções.

Opção	Descrição	Valores
-en	Estado do Telnet	disabled, 1, 2 Nota: Se não desativado, o Telnet será ativado para um ou dois usuários.

Sintaxe:

```

telnetcfg [options]
option:
-en state

```

Exemplo:

```

system> telnetcfg
-en 1
system>

```

Comando thermal

Use o comando **thermal** 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.

Opção	Descrição	Valores
-mode	Seleção de modo térmico	normal, desempenho

Sintaxe:

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

Exemplo:

```
system> thermal
-mode normal
system>
```

Comando timeouts

Use o comando **timeouts** para exibir os valores de tempo limite ou alterá-los. Para exibir os tempos limites, 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.

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

Sintaxe:

```
timeouts [options]
options:
  -f power_off_delay_watchdog_option
  -o OS_watchdog_option
  -l loader_watchdog_option
```

Exemplo:

```
system> timeouts
-o disabled
-l 3.5
system> timeouts -o 2.5
```

```
ok
system> timeouts
-o 2.5
-l 3.5
```

Comando **usbeth**

Use o comando **usbeth** para ativar ou desativar 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 **users**

Use o comando **users** 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.

Opção	Descrição	Valores
- <i>user_index</i>	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.

Opção	Descrição	Valores
-a	Nível de autoridade do usuário	super, ro, custom Em que: <ul style="list-style-type: none"> • super (supervisor) • ro (somente leitura) • custom é seguido por dois-pontos e uma lista de valores separados por uma barra vertical (), no formato custom:am rca. Esses valores podem ser usados em qualquer combinação. <ul style="list-style-type: none"> am (acesso de gerenciamento da conta do usuário) rca (acesso ao console remoto) rcvma (acesso ao console remoto e 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)
-ep	Senha de criptografia (para backup/restauração)	Senha válida
-clear	Apagar conta do usuário especificada	O número de índice da conta do usuário a ser apagado deve ser especificado, seguindo o formato: users -clear -user_index
-curr	Exibir usuários atualmente com login efetuado	
-sauth	Protocolo de autenticação SNMPv3	HMAC-MD5, HMAC-SHA, none
-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

Opção	Descrição	Valores
-pk	Exibir chave pública SSH para o usuário	Número de índice da conta do usuário. Nota: <ul style="list-style-type: none"> Cada chave SSH designada ao usuário é exibida, juntamente com um número de índice de identificação. Ao usar as opções de chave pública SSH, a opção -pk deve ser usada após o índice de usuário (opção <i>-userindex</i>), no formato: users -2 -pk. Todas as chaves estão no formato OpenSSH.
-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 <i>-userindex</i>), no formato: users -2 -pk -e.
-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 <i>-key_index</i> ou -all específico para todas as chaves designadas ao usuário. Nota: Ao usar as opções de chave pública SSH, a opção -pk deve ser usada após o índice de usuário (opção <i>-userindex</i>), no formato: users -2 -pk -remove -1.
-add	Incluir chave pública SSH para o usuário (opção de chave pública SSH)	Chave delimitada por aspas no formato OpenSSH Nota: <ul style="list-style-type: none"> A opção -add é usada exclusiva 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 <i>-userindex</i>), no formato: users -2 -pk -add "AAAAB3NzC1yc2EAAAABlWAAQQAFAvfnTUzRF7pdBuaBy4d0/aIFasa/Gtc+o/wlZnuC4aDHMA1UmnMyLOCiIaN0y400ICEKcQjKEhrYymtAoVtFKApvY39GpnSGRC/qcLGWLM4cmi rKL5kxHNOqIcwbT1NPceoKHj46X7E+mq1fWnAhhjDpcVFjagM3Ek2y7w/tBGrwGn7DPHJU1tzcJy68mEAnIrzjUoR98Q3/B9cJD77ydGKe8rPdI2hIEpXR5dNUiupA1Yd8PSSMgdukASKEd3eRRZTB13SAtMucUsTkYj1Xcqex10Qz4+N50R6MbNcw1sx+mTEAvvcPjhuga70UNPGhLJM16k7jeJiQ8Xd2p Xb0ZQ=="
-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. Nota: <ul style="list-style-type: none"> A opção -upld é usada exclusiva de todas as outras opções de comando users -pk (exceto para -i e -l). Para substituir por uma nova chave, você deve especificar um <i>-key_index</i>. 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 <i>-userindex</i>), no formato: users -2 -pk -upld -i tftp://9.72.216.40/ -l file.key.

Opção	Descrição	Valores
-dnld	Fazer o download de uma chave pública SSH especificada <i>(opção de chave pública SSH)</i>	Requer um <i>-key_index</i> para especificar a chave para fazer o download e as opções <i>-i</i> e <i>-l</i> para especificar o local de download em outro computador que esteja executando um servidor TFTP. Nota: <ul style="list-style-type: none"> A opção <i>-dnld</i> é usada exclusiva de todas as outras opções de comando <i>users -pk</i> (exceto para <i>-i</i>, <i>-l</i> e <i>-key_index</i>). Ao usar as opções de chave pública SSH, a opção <i>-pk</i> deve ser usada após o índice de usuário (opção <i>-userindex</i>), no formato: <i>users -2 -pk -dnld -l -i tftp://9.72.216.40/ -l file.key</i>.
-i	Endereço IP do servidor TFTP/SFTP para fazer upload ou fazer o downloading de um arquivo-chave <i>(opção de chave pública SSH)</i>	Endereço IP válido Nota: A opção <i>-i</i> é requerida pelas opções de comando <i>users -pk -upld</i> e <i>users -pk -dnld</i> .
-pn	Número da porta do servidor TFTP/SFTP <i>(opção de chave pública SSH)</i>	Número da porta válido (padrão 69/22) Nota: Um parâmetro opcional para as opções de comando <i>users -pk -upld</i> e <i>users -pk -dnld</i> .
-u	Nome de usuário para o servidor SFTP <i>(opção de chave pública SSH)</i>	Nome de usuário válido Nota: Um parâmetro opcional para as opções de comando <i>users -pk -upld</i> e <i>users -pk -dnld</i> .
-pw	Senha para o servidor SFTP <i>(opção de chave pública SSH)</i>	Senha válida Nota: Um parâmetro opcional para as opções de comando <i>users -pk -upld</i> e <i>users -pk -dnld</i> .
-l	Nome do arquivo para fazer upload ou fazer download de um arquivo-chave via TFTP ou SFTP <i>(opção de chave pública SSH)</i>	Nome do arquivo válido Nota: A opção <i>-l</i> é requerida pelas opções de comando <i>users -pk -upld</i> e <i>users -pk -dnld</i> .
-af	Aceitar conexões do host <i>(opção de chave pública SSH)</i>	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 <i>(opção de chave pública SSH)</i>	Sequência limitada por aspas de até 255 caracteres. Nota: Ao usar as opções de chave pública SSH, a opção <i>-pk</i> deve ser usada após o índice de usuário (opção <i>-userindex</i>), no formato: <i>users -2 -pk -cm "This is my comment."</i> .

Sintaxe:

```

users [options]
options:
  -user_index
  -n username
  -p password
  -a authority_level
  -ep encryption_password
  -clear
  -curr
  -sauth protocol
  -spriv protocol
  -spw password
  -sepw password
  -sacc state
  -strap hostname

```

```

users -pk [options]
options:
  -e
  -remove index
  -add key
  -upld
  -dnld
  -i ip_address
  -pn port_number
  -u username
  -pw password
  -l filename
  -af list
  -cm comment

```

Exemplo:

```

system> users
1. USERID Read/Write
Password Expires: no expiration
2. manu Read Only
Password Expires: no expiration
3. eliflippen Read Only
Password Expires: no expiration
4. <not used>
5. jacobyaackenovic custom:cel|ac
Password Expires: no expiration
system> users -7 -n sptest -p PASSWORD -a custom:am|rca|cel|nsc|ac
ok
system> users
1. USERID Read/Write
Password Expires: no expiration
2. test Read/Write
Password Expires: no expiration
3. test2 Read/Write
Password Expires: no expiration
4. <not used>
5. jacobyaackenovic custom:cel|ac
Password Expires: no expiration
6. <not used>
7. sptest custom:am|rca|cel|nsc|ac
Password Expires: no expiration
8. <not used>
9. <not used>
10. <not used>
11. <not used>
12. <not used>
system>

```

Comandos de Controle do IMM2

Os comandos de controle do IMM2 são os seguintes:

- “Comando alertentries”
- “Comando batch” na página 200
- “Comando clearcfg” na página 200
- “Comando clock” na página 201
- “Comando identify” na página 201
- “Comando info” na página 202
- “Comando resetsp” na página 202
- “Comando spreset” na página 202

Comando alertentries

Use o comando **alertentries** para gerenciar receptores de alertas.

- **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.

Opção	Descrição	Valores
-number	Número de índice do receptor de alertas para exibir, incluir, modificar ou excluir	1 a 12
-status	Status do receptor de alertas	on, off
-type	Tipo de alerta	email, syslog
-log	Incluir log de eventos no email de alerta	on, off
-n	Nome do receptor de alertas	Sequência
-e	Endereço de email do receptor de alertas	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	

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: <ul style="list-style-type: none"> • 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	ativado, desativado
-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: <ul style="list-style-type: none"> • 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	ativado, desativado

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: <ul style="list-style-type: none"> • 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	ativado, desativado

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 o comando **batch** para executar um ou mais comandos de 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.

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
  -u 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 o comando **clearcfg** para definir a configuração do IMM2 para seus padrões de factory. Você deve ter pelo menos autoridade de Configuração de Adaptador Avançada para emitir esse comando. Depois que a configuração do IMM2 estiver limpa, o IMM2 será reiniciado.

Comando clock

Use o comando **clock** para exibir a data e hora atuais de acordo com o clock do IMM2 e o deslocamento GMT. Você pode definir as configurações de data, hora, deslocamento GMT e horário de verão.

Observe as seguintes informações:

- Para um deslocamento GMT de +2, -7, -6, -5, -4 ou -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), mik (Minsk), 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), moo (Montevidéu), bre (Brasil - Leste).
- O ano deve ser de 2000 a 2089, inclusive.
- O mês, data, horas, minutos e segundos podem ser valores de dígito único (por exemplo, 9:50:25 em vez de 09:50:25).
- O deslocamento GMT pode estar no formato de +2:00, +2, ou 2 para deslocamentos positivos, e -5:00 ou -5, para deslocamentos negativos.

Sintaxe:

```
clock [options]
options:
-d mm/dd/yyyy
-t hh:mm:ss
-g gmt offset
-dst on/off/special case
```

Exemplo:

```
system> clock
12/12/2011 13:15:23 GMT-5:00 dst on
system> clock -d 12/31/2011
ok
system> clock
12/31/2011 13:15:30 GMT-5:00 dst on
```

Comando identify

Use o comando **identify** para ligar e desligar, ou fazer piscar, o LED de identificação do chassi. A opção -d poderá ser usada com -s para ligar o LED apenas durante o número de segundos especificado com o parâmetro -d. O LED então 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 o comando **info** para exibir e configurar informações sobre o IMM2.

A execução do comando **info** sem opções exibe todas as informações de local e contato do IMM2. A tabela a seguir mostra os argumentos das opções.

Opção	Descrição	Valores
-name	Nome do IMM2	Sequência
-contact	Nome da pessoa de contato do IMM2	Sequência
-location	Local do IMM2	Sequência
-room ¹	Identificador de espaço do IMM2	Sequência
-rack ¹	Identificador de rack do IMM2	Sequência
-rup ¹	Posição do IMM2 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 reconfigurado se o IMM2 residir em um IBM Flex System.

Sintaxe:

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

Comando resetsp

Use o comando **resetsp** para reiniciar o IMM2. Você deve ter pelo menos autoridade de Configuração de Adaptador Avançada para poder emitir esse comando.

Comando spreset

Use o comando **spreset** para reiniciar o IMM2. Você deve ter pelo menos autoridade de Configuração de Adaptador Avançada para poder emitir esse comando.

Apêndice A. Obtendo ajuda e assistência técnica

Se você precisar de ajuda, serviço ou assistência técnica ou apenas desejar mais informações sobre produtos IBM, encontrará uma ampla variedade de fontes disponíveis da IBM para ajudá-lo.

Use estas informações para obter informações adicionais sobre a IBM e os produtos IBM, determinar o que fazer se tiver um problema com o sistema ou dispositivo opcional IBM e determinar quem chamar para manutenção, se for necessário.

Antes de ligar

Antes de ligar, certifique-se de que tenha executado estas etapas para tentar resolver o problema sozinho.

Se você achar que precisa de ajuda da IBM para executar serviço de garantia em seu produto IBM, os técnicos de serviço da IBM poderão auxiliá-lo com mais eficácia se você se preparar antes de ligar.

- Verifique se todos os cabos estão conectados.
- Verifique as chaves de energia para assegurar-se de que o sistema e os dispositivos opcionais estejam ligados.
- Verifique software, firmware e drivers de dispositivo de sistema operacional atualizados para o seu produto IBM. Os termos e condições da Garantia IBM indicam que você, o proprietário do produto IBM, 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). O seu técnico de serviço IBM solicitará que você faça upgrade de seu software e firmware se o problema tiver uma solução documentada dentro de um upgrade de software.
- Se você tiver instalado um novo hardware ou software em seu ambiente, verifique o <http://www.ibm.com/systems/info/x86servers/serverproven/compat/us> para se certificar de que o hardware e o software sejam suportados por seu produto IBM.
- Acesse <http://www.ibm.com/supportportal> para verificar se há informações para ajudá-lo a resolver o problema.
- Reúna as seguintes informações para fornecer ao Suporte IBM. Esses dados ajudarão o Suporte IBM a fornecer rapidamente uma solução para seu problema e a assegurar que você receba o nível de serviço para o qual pode ter contratado.
 - Números dos contratos de Manutenção de Hardware e Software, se aplicável
 - Número do tipo de máquina (identificador de máquina da IBM, com quatro dígitos)
 - Número do modelo
 - Número de série
 - Níveis de UEFI e firmware do sistema atual
 - Outras informações pertinentes, como mensagens e logs de erro
- Acesse http://www.ibm.com/support/entry/portal/Open_service_request para enviar uma Solicitação de Serviço Eletrônica. O envio de uma Solicitação de Serviço Eletrônica iniciará o processo de determinação de uma solução para o seu problema disponibilizando as informações pertinentes para o Suporte IBM

de maneira rápida e eficiente. Os técnicos de serviço IBM podem começar a trabalhar em sua solução assim que você preencher e enviar uma Solicitação de Serviço Eletrônica.

É possível solucionar vários problemas sem assistência externa seguindo os procedimentos de resolução de problemas que a IBM fornece na ajuda online ou na documentação fornecida com o produto IBM. A documentação fornecida com os sistemas IBM também descreve os testes de diagnóstico que é possível executar. A maioria dos sistemas, sistemas operacionais e programas vem com documentação que contém procedimentos de resolução de problemas e explicações sobre mensagens e códigos de erro. Se você suspeitar de um problema de software, consulte a documentação do sistema operacional ou programa.

Usando a documentação

As informações sobre sistema e software pré-instalado IBM, se houver, ou sobre dispositivo opcional estão disponíveis na documentação fornecida com o produto. Essa documentação pode incluir documentos impressos, documentos online, arquivos leia-me e arquivos de ajuda.

Consulte as informações de resolução de problemas em sua documentação do sistema para obter instruções de como usar os programas de diagnóstico. As informações de resolução de problemas ou os programas de diagnóstico instruem se você precisa de drivers de dispositivo adicionais ou atualizados ou outro software. A IBM mantém páginas na World Wide Web em que é possível obter informações técnicas mais recentes e fazer download de drivers de dispositivo e atualizações. Para acessar essas páginas, acesse <http://www.ibm.com/supportportal>.

Obtendo ajuda e informações na World Wide Web

Informações atualizadas sobre os produtos e o suporte IBM estão disponíveis na World Wide Web.

Na World Wide Web, informações atualizadas sobre sistemas IBM, dispositivos opcionais, serviços e suporte estão disponíveis em <http://www.ibm.com/supportportal>. As informações do IBM System x estão em <http://www.ibm.com/systems/x>. As informações do IBM BladeCenter estão em <http://www.ibm.com/systems/bladecenter>. As informações do IBM IntelliStation estão em <http://www.ibm.com/systems/intellistation>.

Como enviar dados do DSA para a IBM

Use o IBM Enhanced Customer Data Repository para enviar dados diagnósticos à IBM.

Antes de enviar dados diagnósticos para a IBM, leia os termos de uso em <http://www.ibm.com/de/support/ecurep/terms.html>.

É possível usar qualquer um dos métodos a seguir para enviar dados diagnósticos à IBM:

- **Upload padrão:** http://www.ibm.com/de/support/ecurep/send_http.html
- **Upload padrão com o número de série do sistema:** http://www.ecurep.ibm.com/app/upload_hw

- **Upload seguro:**http://www.ibm.com/de/support/ecurep/send_http.html#secure
- **Upload seguro com o número de série do sistema:** https://www.ecurep.ibm.com/app/upload_hw

Criando uma página da web de suporte personalizada

É possível criar uma página da web de suporte personalizada identificando os produtos IBM que são de seu interesse.

Para criar uma página da web de suporte personalizada, acesse <http://www.ibm.com/support/mynotifications>. Nessa página personalizada, é possível assinar notificações semanais por email sobre novos documentos técnicos, procurar informações e downloads e acessar vários serviços administrativos.

Serviço e Suporte de Software

Por meio da Linha de Suporte IBM, é possível obter assistência por telefone, mediante uma taxa, com relação a problemas de uso, configuração e software em seus produtos IBM.

Para obter informações adicionais sobre Linha de Suporte e outros serviços IBM, consulte <http://www.ibm.com/services> ou consulte <http://www.ibm.com/planetwide> para obter os números de telefone de suporte. Nos EUA e no Canadá, ligue 1-800-IBM-SERV (1-800-426-7378).

Serviço e suporte de hardware

É possível receber serviço de hardware através do seu revendedor IBM ou dos Serviços IBM.

Para localizar um revendedor autorizado pela IBM a fornecer serviço de garantia, acesse <http://www.ibm.com/partnerworld> e clique em **Localizar Parceiros de Negócios** do lado direito da página. Para números de telefone de suporte IBM, consulte <http://www.ibm.com/planetwide>. Nos EUA e no Canadá, ligue 1-800-IBM-SERV (1-800-426-7378).

Nos Estados Unidos e no Canadá, o serviço e suporte de hardware estão disponíveis 24 horas por dia, 7 dias por semana. No Reino Unido, esses serviços estão disponíveis de segunda a sexta, das 9h às 18h.

Serviço do Produto da IBM Taiwan

Use estas informações para entrar em contato com a assistência ao produto IBM Taiwan.

台灣 IBM 產品服務聯絡方式：
台灣國際商業機器股份有限公司
台北市松仁路7號3樓
電話：0800-016-888

Informações de contato da assistência ao produto IBM Taiwan:

IBM Taiwan Corporation
3F, No 7, Song Ren Rd.
Taipei, Taiwan
Telephone: 0800-016-888

Apêndice B. Avisos

Estas informações foram desenvolvidas para produtos e serviços oferecidos nos Estados Unidos.

É possível que a IBM não ofereça os produtos, serviços ou recursos discutidos nesta publicação em outros países. Consulte um representante IBM local para obter informações sobre produtos e serviços disponíveis atualmente em sua área. Qualquer referência a produtos, programas ou serviços IBM não significa que apenas produtos, programas ou serviços IBM possam ser utilizados. Qualquer produto, programa ou serviço funcionalmente equivalente, que não infrinja nenhum direito de propriedade intelectual da IBM poderá ser utilizado em substituição a este produto, programa ou serviço. Contudo, é de responsabilidade do usuário avaliar e verificar o funcionamento de qualquer produto, programa ou serviço que não seja da IBM.

A IBM pode ter patentes ou solicitações de patentes pendentes relativas a assuntos tratados nesta publicação. O fornecimento deste documento não garante ao Cliente nenhum direito sobre tais patentes. Pedidos de licença devem ser enviados, por escrito, para:

Gerência de Relações Comerciais e Industriais da IBM Brasil
Av. Pasteur, 138-146
Botafogo
Rio de Janeiro, RJ
CEP 22290-240

A INTERNATIONAL BUSINESS MACHINES CORPORATION 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, esta disposição pode não se aplicar ao Cliente.

Essas informações podem conter imprecisões técnicas ou erros tipográficos. Alterações são periodicamente realizadas nas informações aqui constantes; essas alterações serão incorporadas em novas edições da publicação. A IBM pode fazer aperfeiçoamentos e/ou modificações nos produtos e/ou nos programas descritos nesta publicação a qualquer momento, sem aviso.

Todas as referências nestas informações a websites sites não IBM são fornecidas apenas por conveniência e não representam de forma alguma um endosso a estes websites sites. Os materiais contidos nesses websites não fazem parte dos materiais deste produto IBM e o uso desses websites é de inteira responsabilidade do Cliente.

A IBM pode utilizar ou distribuir as informações fornecidas da forma que julgar apropriada sem incorrer em qualquer obrigação para com o Cliente.

Marcas registradas

IBM, o logotipo IBM e `ibm.com` são marcas registradas da International Business Machines Corp., registradas em diversas jurisdições em todo o mundo. Outros nomes de produtos e serviços podem ser marcas registradas da IBM ou de outras empresas.

Uma lista atual de marcas registradas da IBM está disponível na web em <http://www.ibm.com/legal/us/en/copytrade.shtml>.

Adobe e PostScript são marcas registradas da Adobe Systems Incorporated nos Estados Unidos e/ou em outros países.

Cell Broadband Engine é uma marca registrada da Sony Computer Entertainment, Inc., nos Estados Unidos e/ou em outros países, e é usada sob licença a partir de agora.

Intel, Intel Xeon, Itanium e Pentium são marcas registradas da Intel Corporation ou de suas subsidiárias nos Estados Unidos e em outros países.

Java e todas as marcas registradas e logotipos baseados em Java são marcas registradas da Oracle e/ou suas afiliadas.

Linux é uma marca registrada de Linus Torvalds nos Estados Unidos e/ou em outros países.

Microsoft, Windows e Windows NT são marcas registradas da Microsoft Corporation nos Estados Unidos e/ou em outros países.

UNIX é marca registrada do The Open Group nos Estados Unidos e/ou em outros países.

Notas importantes

A velocidade do processador indica a velocidade do clock interno do microprocessador; outros fatores também afetam o desempenho do aplicativo.

A velocidade da unidade de CD ou DVD é a taxa de leitura variável. As velocidades reais variam e muitas vezes são inferiores ao máximo possível.

Ao se referir a armazenamento de processador, armazenamento real e virtual ou volume de canal, KB representa 1024 bytes, MB representa 1.048.576 bytes e GB representa 1.073.741.824 bytes.

Ao se referir à capacidade de unidade de disco rígido ou volume de comunicações, MB representa 1.000.000 de bytes e GB representa 1.000.000.000 de bytes. A capacidade total acessível pelo usuário pode variar dependendo dos ambientes operacionais.

A capacidade máxima interna da unidade de disco rígido assume a substituição de qualquer unidade de disco rígido padrão e a ocupação de todos os compartimentos de unidade de disco rígido com as maiores unidades suportadas atualmente disponíveis na IBM.

A memória máxima pode requerer a substituição da memória padrão por um módulo de memória opcional.

Cada célula de memória em estado sólido tem um número intrínseco e finito de ciclos de gravação que a célula pode incorrer. Portanto, um dispositivo de estado sólido tem um número máximo de ciclos de gravação ao qual ele pode estar sujeito, expresso como “total de bytes gravados” (TBW). Um dispositivo que tenha excedido esse limite poderá falhar em responder aos comandos gerados pelo sistema ou poderá ser incapaz de ser gravado. A IBM não é responsável pela substituição de um dispositivo que excedeu seu número máximo garantido de ciclos de programa/apagamento, conforme documentado nas Especificações Oficiais Publicadas para o dispositivo.

A IBM não faz declarações ou fornece garantias referentes a produtos e serviços não IBM que sejam ServerProven, incluindo mas não se limitando às garantias implícitas de comercialização e adequação a um determinado propósito. Esses produtos são oferecidos e garantidos exclusivamente por terceiros.

A IBM não faz representações ou garantias com relação a produtos não IBM. O suporte (se disponível) a produtos não IBM é fornecido por terceiros, não pela IBM.

Alguns softwares podem ser diferentes de sua versão de varejo (se disponível) e podem não incluir manuais do usuário ou toda a funcionalidade do programa.

Contaminação por partículas

Atenção: Partículas do ar (incluindo faíscas ou partículas de metal) e gases reativos agindo sozinhos ou em combinação com outros fatores ambientais, como umidade ou temperatura, podem expor o dispositivo a riscos, descritos neste documento.

Os riscos apresentados pela presença de níveis excessivos de partículas ou concentrações de gases perigosos incluem danos que podem levar ao mau funcionamento do dispositivo ou cessar completamente o funcionamento. Esta especificação estabelece limites de partículas e gases com o propósito de evitar tais danos. Os limites não devem ser vistos ou usados como limites definitivos, pois vários outros fatores, como temperatura ou umidade do ar, podem influenciar no impacto da transferência contaminante de partículas ou gases e corrosivos ambientais. Na ausência de limites específicos que são estabelecidos neste documento, deve-se implementar práticas que mantenham os níveis de gás e de partículas consistentes com a proteção da saúde e segurança das pessoas. Se a IBM determinar que os níveis de partículas ou gases de seu ambiente causaram danos ao dispositivo, ela poderá condicionar a provisão de reparo ou substituição de dispositivos ou peças à implementação de medidas reparatórias apropriadas para atenuar essa contaminação do ambiente. A implementação dessas medidas reparatórias é de responsabilidade do cliente.

Tabela 9. Limites para partículas e gases

Contaminante	Limites
Partículas	<ul style="list-style-type: none"> O ar do ambiente deve ser filtrado continuamente a 40% de eficiência de marca de poeira atmosférica (MERV 9) de acordo com o ASHRAE Standard 52.2¹. O ar que entra em um datacenter deve ser filtrado com 99,97% de eficiência ou mais, usando filtros de partículas do ar de alta eficiência (HEPA) que atendam ao padrão MIL-STD-282. A umidade relativa deliquescente da contaminação de partículas deve ser maior que 60%². O ambiente deve estar livre de contaminação condutora, como pó de zinco.
Gases	<ul style="list-style-type: none"> Cobre: Classe G1 conforme ANSI/ISA 71.04-1985³ 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 Ar de Ventilação para Eficiência da Remoção por Tamanho de Partícula*. Atlanta: American Society of Heating, Refrigerating and Air-Conditioning Engineers, Inc.

² A umidade relativa deliquescente da contaminação de partícula é a umidade relativa na qual a poeira absorve água suficiente para se tornar úmida e promover condução iônica.

³ ANSI/ISA-71.04-1985. *Condições ambientais para medição de processo e sistemas de controle: contaminantes do ar*. Instrument Society of America, Research Triangle Park, North Carolina, U.S.A.

Formato da documentação

As publicações deste produto estão em Adobe Portable Document Format (PDF) e devem ser compatíveis com os padrões de acessibilidade. Se você encontrar dificuldades ao usar os arquivos PDF e desejar solicitar um formato baseado na web ou documento PDF acessível para uma publicação, envie uma mensagem para o endereço a seguir:

Information Development
Av. Pasteur, 138-146
205/A015
3039 E. Cornwallis Road
P.O. Box 12195
Research Triangle Park, North Carolina 27709-2195
CEP 22290-240

Na solicitação, certifique-se de incluir o número de peça da publicação e o título.

Ao enviar suas informações para a IBM, o Cliente concede à IBM o direito não exclusivo de usar ou distribuir as informações da maneira que julgar apropriada, sem incorrer em qualquer obrigação para com o Cliente.

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. Pode ser necessária certificação adicional por lei antes de fazer qualquer conexão desse tipo. Entre em contato com um representante ou revendedor IBM para esclarecer qualquer dúvida.

Avisos de emissão eletrônica

Ao conectar um monitor ao equipamento, você deverá usar o cabo de monitor designado e qualquer dispositivo de supressão de interferência fornecido com o monitor.

Declaração da Federal Communications Commission (FCC)

Nota: Este equipamento foi testado e aprovado segundo os critérios estabelecidos para dispositivos digitais da Classe A, em conformidade com a Parte 15 das Normas da FCC. Esses critérios têm a finalidade de assegurar um nível adequado de proteção contra interferências prejudiciais, quando o equipamento estiver funcionando em uma instalação comercial. Este equipamento gera, utiliza e pode emitir energia de frequência de rádio e, se não for instalado e utilizado de acordo com o manual de instruções, pode provocar interferência prejudicial nas comunicações de rádio. A operação deste equipamento em área residencial pode causar interferência prejudicial e, nesse caso, o usuário será obrigado arcar com o custo da correção da interferência.

Devem ser usados cabos e conectores devidamente blindados e aterrados para que os limites de emissão da FCC sejam respeitados. A IBM não se responsabiliza por qualquer interferência na recepção de rádio ou televisão provocada pela utilização de cabos e conectores que não sejam os recomendados ou por alterações ou modificações não autorizadas neste equipamento. Mudanças ou modificações não autorizadas podem anular a autoridade do usuário para operar o equipamento.

Este dispositivo está em conformidade com a Parte 15 das Normas da FCC. A operação está sujeita às duas seguintes condições: (1) este dispositivo não pode provocar interferência prejudicial e (2) este dispositivo deve aceitar qualquer interferência recebida, incluindo as que possam provocar operação indesejada.

Declaração de conformidade de emissão de Classe A do segmento de mercado do Canadá

Este equipamento digital Classe A está em conformidade com o ICES-003 canadense.

Avis de conformité à la réglementation d'Industrie Canada

Cet appareil numérique de la classe A est conforme à la norme NMB-003 du Canada.

Declaração de Classe A da Austrália e Nova Zelândia

Atenção: Este é um produto Classe A. Em um ambiente doméstico, este produto pode causar interferência de rádio; em tal caso, o usuário poderá ser obrigado a tomar as medidas adequadas.

Declaração de conformidade com a Diretiva EMC da União Europeia

Este produto está em conformidade com os requisitos de proteção da Diretiva 2004/108/EC do Conselho da UE, que trata da aproximação das leis dos Países Membros sobre compatibilidade eletromagnética. A IBM não pode aceitar a responsabilidade por qualquer falha em satisfazer aos requisitos de proteção resultantes de uma modificação não recomendada do produto, incluindo o ajuste de placas opcionais não IBM.

Atenção: Este é um produto da Classe A EN 55022. Em um ambiente doméstico, este produto pode causar interferência de rádio; em tal caso, o usuário poderá ser obrigado a tomar as medidas adequadas.

Fabricante responsável:

International Business Machines Corp.
New Orchard Road
Armonk, New York 10504
914-499-1900

Contato na Comunidade Europeia:

IBM Deutschland GmbH
Technical Regulations, Department M372
IBM-Allee 1, 71139 Ehningen, Germany
Telephone: +49 7032 15 2941
Email: lugi@de.ibm.com

Declaração de Classe A da Alemanha

Deutschsprachiger EU Hinweis: Hinweis für Geräte der Klasse A EU-Richtlinie zur Elektromagnetischen Verträglichkeit

Dieses Produkt entspricht den Schutzanforderungen der EU-Richtlinie 2004/108/EG zur Angleichung der Rechtsvorschriften über die elektromagnetische Verträglichkeit in den EU-Mitgliedsstaaten und hält die Grenzwerte der EN 55022 Klasse A ein.

Um dieses sicherzustellen, sind die Geräte wie in den Handbüchern beschrieben zu installieren und zu betreiben. Des Weiteren dürfen auch nur von der IBM empfohlene Kabel angeschlossen werden. IBM übernimmt keine Verantwortung für die Einhaltung der Schutzanforderungen, wenn das Produkt ohne Zustimmung der IBM verändert bzw. wenn Erweiterungskomponenten von Fremdherstellern ohne Empfehlung der IBM gesteckt/eingebaut werden.

EN 55022 Klasse A Geräte müssen mit folgendem Warnhinweis versehen werden: "Warnung: Dieses ist eine Einrichtung der Klasse A. Diese Einrichtung kann im Wohnbereich Funk-Störungen verursachen; in diesem Fall kann vom Betreiber verlangt werden, angemessene Maßnahmen zu ergreifen und dafür aufzukommen."

Deutschland: Einhaltung des Gesetzes über die elektromagnetische Verträglichkeit von Geräten

Dieses Produkt entspricht dem "Gesetz über die elektromagnetische Verträglichkeit von Geräten (EMVG)". Dies ist die Umsetzung der EU-Richtlinie 2004/108/EG in der Bundesrepublik Deutschland.

Zulassungsbescheinigung laut dem Deutschen Gesetz über die elektromagnetische Verträglichkeit von Geräten (EMVG) (bzw. der EMC EG Richtlinie 2004/108/EG) für Geräte der Klasse A

Dieses Gerät ist berechtigt, in Übereinstimmung mit dem Deutschen EMVG das EG-Konformitätszeichen - CE - zu führen.

Verantwortlich für die Einhaltung der EMV Vorschriften ist der Hersteller:

International Business Machines Corp.
New Orchard Road
Armonk, New York 10504
914-499-1900

Der verantwortliche Ansprechpartner des Herstellers in der EU ist:

IBM Deutschland GmbH
Technical Regulations, Abteilung M372
IBM-Allee 1, 71139 Ehningen, Germany
Telephone: +49 7032 15 2941
Email: lugi@de.ibm.com

Generelle Informationen:

Das Gerät erfüllt die Schutzanforderungen nach EN 55024 und EN 55022 Klasse A.

Declaração de Classe A VCCI do Japão

この装置は、クラス A 情報技術装置です。この装置を家庭環境で使用すると電波妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求されることがあります。 VCCI-A

Este é um produto de Classe A baseado no padrão do Voluntary Control Council for Interference (VCCI). Se este equipamento for usado em um ambiente doméstico, pode ocorrer interferência de rádio, em tal caso, o usuário poderá ser obrigado a tomar ações corretivas.

Instrução da Korea Communications Commission (KCC)

이 기기는 업무용(A급)으로 전자파적합기기로
서 판매자 또는 사용자는 이 점을 주의하시기
바라며, 가정외의 지역에서 사용하는 것을 목
적으로 합니다.

Esse é um equipamento de compatibilidade de onda eletromagnética para empresas (Tipo A). Os vendedores e usuários precisam prestar atenção a isso. Ele se destina a quaisquer áreas, exceto residenciais.

Declaração de Classe A de Interferência Eletromagnética (EMI) da Rússia

ВНИМАНИЕ! Настоящее изделие относится к классу А.
В жилых помещениях оно может создавать радиопомехи, для
снижения которых необходимы дополнительные меры

Declaração de emissão eletrônica de Classe A da República Popular da China

中华人民共和国“A类”警告声明

声明

此为A级产品，在生活环境中，该产品可能会造成无线电干扰。在这种情况下，可能需要用户对其干扰采取切实可行的措施。

Declaração de conformidade de Classe A de Taiwan

警告使用者：
這是甲類的資訊產品，在居住的環境中使用時，可能會造成射頻干擾，在這種情況下，使用者會被要求採取某些適當的對策。

Índice Remissivo

A

acesso
 controle remoto 116
 Telnet 57, 190
acesso remoto 2
ações de energia 104
Active Energy Manager
 guia políticas 134
Advanced Settings Utility (ASU) 1
ajuda
 da World Wide Web 204
 enviando dados diagnósticos à
 IBM 204
 origens de 203
applet ActiveX
 atualizando 106
Applet Java
 atualizando 106
as informações do sistema
 visualizando 97
assistência, obtendo 203
assistência ao produto, IBM Taiwan 205
assistência ao produto IBM Taiwan 205
assistente de configuração
 IMM2 58
atributo de permissão de login
 LDAP 57, 173
atributo de procura do grupo
 LDAP 57, 173
Atributo de procura UID
 Servidor LDAP 57, 173
atualizando
 o applet ActiveX 106
 o applet Java 106
atualizando o firmware 106
aviso de Classe A da FCC 211
aviso de Classe A da FCC nos Estados
 Unidos 211
aviso de emissão eletrônica da Classe
 A 211
avisos 207
 emissão eletrônica 211
 FCC, Classe A 211
avisos e instruções 5
avisos importantes 208

B

backup da configuração
 IMM2 58
baseboard management controller
 (BMC) 1
BIOS (sistema BIOS) 1
BladeCenter 1, 4, 7

C

captura de tela azul 106
captura de tela do sistema
 operacional 106

centro de informações 204
chave de ativação
 exportar 143
 gerenciar 58, 172
 instalar 139, 172
 remover 141, 172
chaves SSH
 usuário 56, 192
CIM sobre HTTPS
 gerenciamento de certificado 57, 186,
 187
 segurança 57, 186, 187
coletando dados de serviço e
 suporte 130
Comando accsecfg 159
Comando alertcfg 160
Comando alertentries 197
comando asu 161
Comando backup 165
comando batch 200
Comando clearcfg 200
Comando clearlog 150
Comando clock 201
comando de redirecionamento serial 158
Comando dhcpinfo 166
Comando dns 167
comando do console 158
comando ethtousb 168
comando exit 149
Comando fans 150
comando ffdc 150
Comando gprofile 169
comando help 149
Comando history 149
Comando identify 201
Comando ifconfig 170
Comando info 202
comando keycfg 172
Comando ldap 173
Comando led 152
Comando ntp 175
Comando passwordcfg 176
Comando portcfg 177
comando ports 176
Comando power 157
comando pxeboot 157
Comando readlog 153
Comando reset 158
Comando resetsp 202
comando restaurar 178
comando restoredefaults 179
Comando set 179
comando show 154
Comando smtp 180
Comando Snmp 181
comando snmpalerts 183
comando spreset 202
Comando srcfg 184
comando sshcfg 185
Comando ssl 186
Comando sslcfg 187

Comando syshealth 155
comando telnetcfg 190
Comando temps 155
comando thermal 191
Comando timeouts 191
Comando usbeth 192
Comando users 192
Comando volts 155
Comando vpd 156
comandos
 accsecfg 159
 ajuda 149
 alertcfg 160
 alertentries 197
 asu 161
 backup 165
 clearcfg 200
 clearlog 150
 clock 201
 configurar 179
 console 158
 dhcpinfo 166
 dns 167
 ethtousb 168
 exit 149
 fans 150
 ffdc 150
 gprofile 169
 history 149
 identify 201
 ifconfig 170
 informativo 202
 keycfg 172
 ldap 173
 led 152
 Lote 200
 ntp 175
 passwordcfg 176
 portas 176
 portcfg 177
 power 157
 pxeboot 157
 readlog 153
 reset 158
 resetsp 202
 restaurar 178
 restoredefaults 179
 show 154
 smtp 180
 snmp 181
 snmpalerts 183
 spreset 202
 srcfg 184
 sshcifg 185
 ssl 186
 sslcifg 187
 syshealth 155
 telnetcfg 190
 temps 155
 thermal 191
 timeouts 191

- comandos (*continuação*)
 - usbeth 192
 - users 192
 - volts 155
 - vpd 156
- comandos, lista alfabética 148
- comandos, tipos de
 - configuração 158
 - controle do IMM2 197
 - energia e reinicialização do servidor 157
 - monitor 150
 - redirecionamento serial 158
 - utilitário 149
- comandos de configuração 158
- comandos de controle do IMM2 197
- comandos de monitor 150
- comandos de utilitário 149
- comunidades de SNMPv1
 - gerenciar 56
 - manage 181
- conexão de rede 8
 - endereço IP, estático padrão 8
 - endereço IP estático, padrão 8
 - endereço IP estático padrão 8
- configuração de backup
 - IMM2 58
- configuração de visualização
 - IMM2 58
- configuração padrão
 - IMM 179
 - IMM2 58
- configurações
 - alerta SNMP 74
 - avançada 72
 - CIM sobre HTTPS 86
 - DDNS 76
 - designações de porta 84
 - DNS 75
 - Ethernet 72
 - HTTPS 85
 - LDAP 77
 - login global 67
 - guia geral 67
 - guia nível de segurança de conta 69
 - para a sessão da web 17
 - protocolo do cliente LDAP 87
 - segurança 85
 - servidor ssh 89
 - SMTP 76
 - Telnet 82
 - USB 83
- configurações de login global
 - guia geral 67
 - guia nível de segurança de conta 69
- configurações de sessão da web 17
- configurações de SNMPv3
 - usuário 56, 192
- configurações de Telnet
 - configurar 57
- configurando
 - configurações de login global 67
 - destinatários de alertas 30
 - redirecionamento serial para SSH 146
- configurando (*continuação*)
 - redirecionamento serial para Telnet 146
- configurando o IMM2
 - opções para configurar o IMM2 55
- configurando tempos limites do servidor 58
- configurar
 - configurações de alerta SNMP 74
 - configurações de LDAP 77
 - configurações de segurança 85
 - configurações de SMTP 76
 - configurações de Telnet 57, 82
 - configurações de USB 83
 - configurações do DDNS 76
 - configurações do DNS 75
 - configurações Ethernet 72
 - contas de usuário de SNMPv3 56, 192
 - contato de SNMPv1 56, 181
 - contato de SNMPv3 56, 181
 - dados 55, 201
 - DDNS 56, 167
 - designações de porta 84
 - DNS 56, 167
 - Ethernet 56, 170
 - Ethernet sobre USB 57, 168
 - hora 55, 201
 - IMM2 58
 - IPv4 56, 170
 - IPv6 56, 170
 - LDAP 56, 173
 - método de autenticação do usuário 56, 159
 - MTU 56, 170
 - negociação automática 56, 170
 - níveis de segurança da conta do usuário 56, 159
 - nome do host 56, 170
 - porta da CLI SSH 57, 176
 - porta da CLI Telnet 57, 176
 - porta de Controle Remoto 57, 176
 - porta de Traps SNMP 57, 176
 - porta do agente do SNMP 57, 176
 - porta do CIM sobre HTTP 57, 176
 - porta do CIM sobre HTTPS 57, 176
 - Porta do Servidor LDAP 57, 173
 - Porta HTTP 57, 176
 - porta HTTPS 57, 176
 - porta serial 55, 61, 177
 - portas 57, 176
 - protocolo CIM sobre HTTPS 86
 - protocolo do cliente LDAP 87
 - protocolo HTTPS 85
 - protocolos de rede 71
 - segurança 57
 - sequência-chave da CLI 55, 177
 - Servidor LDAP 56, 173
 - servidor ssh 89
 - SMTP 56, 180
 - SNMPv1 56, 181
 - Telnet 190
 - tempo limite de inatividade da web 56, 159
 - traps SNMPv1 56, 181
- configurar (*continuação*)
 - unidade de transmissão máxima 56, 170
 - USB 57, 168
- configurar números de porta 57, 176
- conta do usuário
 - criar 55, 192
 - gerenciamento 63
 - perfil do grupo 66
- contaminação, partículas e gases 209
- contaminação de gases 209
- contaminação por partículas 209
- contas de usuário
 - configurando 62
- contas de usuário de SNMPv3
 - configurar 56, 192
- contato de SNMPv1
 - configurar 56, 181
- contato de SNMPv3
 - configurar 56, 181
- controlando o status de energia do servidor 104
- controle de mouse
 - absoluto 110
 - relativa com aceleração padrão Linux 110
 - relativo 110
- controle de mouse absoluto 110
- controle de mouse relativo 110
- controle de mouse relativo para Linux (aceleração padrão Linux) 110
- controle remoto
 - acessando 116
 - captura de tela 106
 - comandos de energia e reinicialização 112
 - controle de mouse absoluto 110
 - controle de mouse relativo 110
 - controle de mouse relativo para Linux (aceleração padrão Linux) 110
 - estatísticas de desempenho 112
 - modo de cursor único 111
 - modo de passagem do teclado 110
 - saindo 117
 - sessão de mídia virtual 105
 - Sessão de Mídia Virtual 115
 - suporte de mouse 110
 - suporte de teclado 108
 - suporte de teclado internacional 109
 - visualizador de vídeo 105
 - Visualizador de Vídeo 107, 108
- controle remoto, janelas
 - sessão de mídia virtual 40
 - visualizador de vídeo 40
- controle remoto de energia 112
- criando uma página da web de suporte personalizada 205
- criar
 - conta do usuário 55, 192
 - notificação por email 125
 - notificação por syslog 125

D

- dados
 - configurar 55, 201

- dados da tela de falha do S.O.
 - capturar 132
- dados de serviço e suporte
 - coletando 130
 - fazendo o download 130
- data e hora, IMM2
 - definição 59
- DDNS
 - configurar 56, 167
 - gerenciar 56
 - manage 167
 - nome de domínio customizado 56, 167
 - nome de domínio especificado pelo servidor DHCP 56, 167
 - origem de nome de domínio 56, 167
- declaração de Classe A da Alemanha 212
- declaração de Classe A da Austrália 211
- declaração de Classe A da Nova Zelândia 211
- declaração de conformidade com a Diretiva EMC da União Europeia 212
- declaração de emissão eletrônica de Classe A da China 214
- declaração de emissão eletrônica de Classe A da República Popular da China 214
- declaração regulamentar de telecomunicação 210
- definição
 - a data e hora do IMM2 59
- destinatário do evento 30
- destinatários de email
 - configurando 30
- destinatários de eventos
 - manage 123
- disco, remoto 115
- disco remoto 115, 116
- DNS
 - configurar 56, 167
 - endereçamento do servidor 56, 167
 - endereçamento IPv4 56, 167
 - endereçamento IPv6 56, 167
 - Servidor LDAP 56, 173
- documentação
 - formato 210
 - usando 204
- documentação acessível 210
- domínio de procura
 - Servidor LDAP 57, 173
- DSA, enviando dados à IBM 204

E

- efetuando login no IMM2 10
- efetuando logout da sessão do IMM2 20
- encaminhamento de porta
 - Ethernet sobre USB 57, 168
- endereçamento do servidor
 - DNS 56, 167
- endereçamento IPv4
 - DNS 56, 167
- endereçamento IPv6
 - DNS 56, 167
- Endereço IP
 - configurando 7

- Endereço IP (*continuação*)
 - IPv4 7
 - IPv6 7
 - Servidor LDAP 57, 173
 - servidor SMTP 56, 180
- endereço IP, estático padrão 8
- endereço IP estático, padrão 8
- endereço IP estático padrão 8
- endereço MAC
 - gerenciar 56
 - manage 170
- energia do servidor
 - controle 104
- energia e reinicialização do servidor
 - comandos 157
- enviando dados diagnósticos à IBM 204
- Ethernet
 - configurar 56, 170
- Ethernet avançada
 - configurações 72
- Ethernet sobre USB
 - configurar 57, 168
 - encaminhamento de porta 57, 168
- evento
 - log 123
- evento do sistema
 - notificação 125
 - tentar novamente a notificação 125
- eventos
 - destinatários 125
- eventos de teste
 - gerar 125
- excluir
 - notificação por email 125
 - notificação por syslog 125
 - usuário 56, 192
- excluir grupo
 - ativar, desativar 169
- executando
 - tarefas do IMM2 103
- exportar
 - chave de ativação 143
- exportar recurso
 - Features on Demand 143
 - FoD 143

F

- fazer o download de dados de serviço
 - opção, visão geral 33
- Features on Demand 139
 - exportar recurso 143
 - gerenciar 58, 172
 - instalar recurso 139, 172
 - remover recurso 141, 172
- ferramentas
 - IPMItool 145
- filtro de grupo
 - LDAP 57, 173
- firmware
 - servidor de visualização 55, 156
- firmware, servidor
 - atualizando 118
- firmware do servidor
 - atualizando 118
- FoD 139
 - exportar recurso 143

- FoD (*continuação*)
 - gerenciar 58, 172
 - instalar recurso 139, 172
 - remover recurso 141, 172
- fonte de alimentação
 - capacidade 137
- fontes de alimentação instaladas
 - gerenciamento de energia 136
 - guia módulos de energia 136
- funcionalidade de presença remota 105
 - ativando 106
- funcionamento do hardware 99
- funcionamento do sistema 98

G

- gerenciamento de certificado
 - CIM sobre HTTPS 57, 186, 187
 - LDAP 57, 186, 187
 - servidor HTTPS 57, 186, 187
 - servidor SSH 57, 185
- gerenciamento de energia
 - Active Energy Manager 134
 - guia alocação de energia 137
 - guia gráfico 137
 - guia histórico de energia 137
 - guia módulos de energia 136
 - guia políticas 134
- Gerenciamento de Servidores
 - opção de processadores 51
 - opção de tela de falha mais recente do S.O. 52
 - opção discos 49
- gerenciamento do IMM
 - chave de gerenciamento de ativação 94
 - configuração do IMM
 - restaurar e modificar configuração do IMM 92
 - configurações de segurança 85
 - configurando contas de usuário 62
 - configurar o protocolo de rede 71
 - propriedades do IMM
 - configurações de porta serial 61
 - reiniciar o IMM2 92
 - usuário
 - contas 63
 - perfis de grupo 66
- gerenciamento do IMM2
 - propriedades do IMM
 - data e hora 59
 - reconfigurar IMM2 93
- gerenciamento do servidor
 - dados da tela de falha do S.O. 132
 - firmware do servidor 118
 - inicialização da rede PXE 117
 - tempos limites do servidor, configurando 58
- Gerenciamento do Servidor
 - opção de ações de energia do servidor 49
 - opção de firmware do servidor 35
 - opção de inicialização da rede PXE 52
 - opção de memória 50
 - opção de propriedades do servidor 45

- Gerenciamento do Servidor (*continuação*)
 - opção tempos limites do servidor 52
- gerenciar
 - chave de ativação 58, 172
 - comunidades de SNMPv1 56
 - DDNS 56
 - endereço MAC 56
 - Features on Demand 58, 172
 - FoD 58, 172
 - usuário 56
- guia alocação de energia
 - fonte de alimentação 137
 - gerenciamento de energia 137
- guia evento
 - log 28
- guia eventos
 - visão geral 27
- guia Gerenciamento do IMM 53
- guia gerenciamento do servidor 34
- guia serviço e suporte
 - visão geral 33
- guia status do sistema
 - visão geral 21

H

- hora
 - configurar 55, 201

I

- IBM BladeCenter 1, 4, 7
- IBM System x Server Firmware
 - descrição 1
 - utilitário de Configuração 8
- IMM
 - configuração padrão 179
 - configurar 58
 - reconfigurar 202
 - redefinir configuração 179
 - reiniciar 202
 - reset 202
 - restaurar configuração 178
 - spreset 202
- IMM2
 - assistente de configuração 58
 - backup da configuração 58
 - chave de gerenciamento de ativação 94
 - conexão de rede 8
 - configuração de backup 58
 - configuração de visualização 58
 - configuração padrão 58
 - descrição 1
 - descrições de ações 11
 - interface da web 7
 - nível avançado do IMM2 2
 - nível básico do IMM2 2
 - nível padrão do IMM2 2
 - novas funções 1
 - opções de configuração 55
 - reconfigurar 58, 93
 - recursos 2
 - redefinir configuração 58
 - redirecionamento serial 146
 - reiniciar 58, 92

- IMM2 (*continuação*)
 - restauração de configuração 58, 178
 - restaurar configuração 58
 - visão geral da interface com o usuário da web 17
 - visualização de configuração 58
 - visualização do status de backup 58
 - visualização do status de restauração 58
 - visualizar o status de backup 58
 - visualizar o status de restauração 58
- Indicadores Luminosos Virtuais 11
- informações do sistema 97
- inicialização da rede PXE
 - configurando 117
- inicialização remota 115
- instalar
 - chave de ativação 139, 172
- instalar recurso
 - Features on Demand 139, 172
 - FoD 139, 172
- instrução de emissão eletrônica de Classe A da Coreia 213
- instrução de emissão eletrônica de Classe A da Rússia 213
- instrução de emissão eletrônica de Classe A de Taiwan 214
- instrução de emissão eletrônica de Classe A do Canadá 211
- instrução de emissão eletrônica de Classe A do Japão 213
- interface com o usuário da web do IMM2
 - guia eventos
 - visão geral de opções 27
 - guia serviço e suporte
 - visão geral de opções 33
 - guia status do sistema
 - visão geral 21
 - visão geral 17
- interface da linha de comandos (CLI)
 - acessando 145
 - descrição 145
 - efetuando login 146
 - recursos e limitações 147
 - sintaxe de comando 146
- interface da web
 - efetuando login na interface da web 10
- interface da web, abrindo e usando 7
- IPMI
 - gerenciamento de servidor remoto 145
- IPMItool 145
- IPv4
 - configurar 56, 170
- IPv6 7
 - configurar 56, 170

J

- Java 4, 115

L

- LDAP
 - atributo de permissão de login 57, 173
 - atributo de procura do grupo 57, 173
 - configurar 56, 173
 - filtro de grupo 57, 173
 - gerenciamento de certificado 57, 186, 187
 - nome de destino do servidor 57, 173
 - segurança 57, 186, 187
 - segurança aprimorada baseada em função 57, 192
 - segurança baseada em função, aprimorada 57, 192
 - Usuários do Active Directory 57, 192
- lista alfabética de comandos 148
- log de eventos 28
 - gerenciar 123
- login global
 - configurações 67

M

- manage
 - comunidades de SNMPv1 181
 - DDNS 167
 - endereço MAC 170
 - usuário 192
- manipulação de certificado
 - CIM sobre HTTPS 86
 - cliente LDAP seguro 87
- mapeando unidades 116
- marcas registradas 208
- máximo de sessões
 - Telnet 57, 190
- menu eventos 123
- método de autenticação do usuário
 - configurar 56, 159
- método de ligação
 - Servidor LDAP 57, 173
- modo de cor de vídeo no controle remoto 108
- modo de cursor único 111
- modo de passagem do teclado no controle remoto 110
- modos de visualização no controle remoto 107
- módulo de gerenciamento avançado 1, 4, 7
- monitorando o status de servidor 95
- MTU
 - configurar 56, 170

N

- negociação automática
 - configurar 56, 170
- níveis baseados em função
 - operador 169
 - rbs 169
 - supervisor 169
- níveis de segurança da conta do usuário
 - configurar 56, 159
- nome de destino, servidor
 - LDAP 57, 173

- nome de destino do servidor
 - LDAP 57, 173
- nome de domínio, customizado
 - DDNS 56, 167
- nome de domínio, especificado pelo servidor DHCP
 - DDNS 56, 167
- nome distinto, cliente
 - Servidor LDAP 57, 173
- nome distinto, raiz
 - Servidor LDAP 57, 173
- nome distinto raiz
 - Servidor LDAP 57, 173
- nome do host
 - configurar 56, 170
 - Servidor LDAP 57, 173
 - servidor SMTP 56, 180
- notas, importantes 208
- notificação de eventos 30
- notificação de eventos do sistema 30
- número de porta
 - Servidor LDAP 57, 173
 - servidor SMTP 56, 180
- números de porta
 - configurar 57
- números de portas
 - configurar 176
- números de telefone 205
- números de telefone do serviço e suporte a software 205
- números de telefone do serviço e suporte de hardware 205

O

- opção atualização automática de página 17
- opção de ações de energia do servidor
 - na guia Gerenciamento do Servidor 49
- opção de firmware do servidor
 - na guia Gerenciamento do Servidor 35
- opção de gerenciamento de energia
 - na guia Gerenciamento do Servidor
 - consumo de energia 133
 - dispositivos de energia 133
 - políticas de energia 133
- opção de inicialização da rede PXE
 - na guia Gerenciamento do Servidor 52
- opção de memória
 - na guia Gerenciamento do Servidor 50
- opção de mensagem de infração 19
- opção de processadores
 - na guia Gerenciamento do Servidor 51
- opção de propriedades do servidor
 - na guia Gerenciamento do Servidor 45
- opção de tela de falha mais recente do S.O.
 - na guia Gerenciamento do Servidor 52

- opção discos
 - na guia Gerenciamento do Servidor 49
- opção tempos limites do servidor
 - na guia Gerenciamento do Servidor 52
- opções na
 - guia Gerenciamento do IMM 53
 - guia gerenciamento do servidor 34
- origem de nome de domínio
 - DDNS 56, 167

P

- página da web de suporte, customizada 205
- página da web de suporte customizada 205
- página status do sistema, visão geral 21
- perfil do grupo
 - gerenciamento 66
- porta da CLI SSH
 - configurar 57, 176
- porta da CLI Telnet
 - configurar 57, 176
- porta de Controle Remoto
 - configurar 57, 176
- porta de Traps SNMP
 - configurar 57, 176
- porta do agente do SNMP
 - configurar 57, 176
- porta do CIM sobre HTTP
 - configurar 57, 176
- porta do CIM sobre HTTPS
 - configurar 57, 176
- Porta do Servidor LDAP
 - configurar 57, 173
- Porta HTTP
 - configurar 57, 176
- porta HTTPS
 - configurar 57, 176
- porta serial
 - configuração 61
 - configurar 55, 177
- portas
 - configurar 57, 176
 - configurar números 57, 176
 - visualizar abertas 57, 176
- pré-configurado
 - Servidor LDAP 56, 173
- propriedade de servidor
 - guia ambientes 45
 - guia atividade de hardware 45
 - guia configurações gerais 45
 - guia informações do hardware
 - guia hardware de rede 45
 - guia informações do componente do sistema 45
 - guia informações do sistema 45
 - guia LED 45
- propriedades do protocolo de rede
 - configurações de alerta SNMP 74
 - configurações Ethernet 72
 - DDNS 76
 - designações de porta 84
 - DNS 75
 - LDAP 77

- propriedades do protocolo de rede (*continuação*)
 - SMTP 76
 - Telnet 82
 - USB 83
- publicações on-line
 - informações de atualização da documentação 1
 - informações de atualização de firmware 1
 - informações de código de erro 1
- PXE Boot Agent 11

R

- reconfigurar
 - IMM 202
 - IMM2 58
- recurso
 - knock knock 112
- recurso de controle remoto 40, 105
- recurso knock knock
 - ativar 112
 - Modo de usuário
 - múltiplo 112
 - único 112
 - solicitar sessão remota 112
- recursos de nível avançado 3
- recursos de nível básico 2
- recursos do IMM2 2
 - nível avançado 3
 - nível básico 2
- recursos do IMM2recursos de nível padrão
 - nível padrão 3
- redefinir configuração
 - IMM 179
 - IMM2 58
- redirecionamento serial para SSH 146
- redirecionamento serial para Telnet 146
- reiniciar
 - IMM 202
 - IMM2 58
- Remote Desktop Protocol (RDP)
 - ativação 112
- Remote Supervisor Adapter II 1
- removendo o mapeamento de unidades 116
- remove
 - chave de ativação 141, 172
- remover recurso
 - Features on Demand 141, 172
 - FoD 141, 172
- requisitos
 - navegador da web 4
 - Windows de 32 bits 4
- requisitos de navegador 4
- requisitos de navegador da web 4
- requisitos de sistema operacional 4
- reset
 - IMM 202
- restauração de configuração
 - IMM2 58, 178
- restaurar configuração
 - IMM2 58, 178
- resumo da configuração, visualizando 11

S

- segurança
 - CIM sobre HTTPS 57, 186, 187
 - cliente LDAP 87
 - configurar 57
 - gerenciamento de certificado SSL 90
 - LDAP 57, 186, 187
 - manipulação de certificado ssl 90
 - protocolo CIM sobre HTTPS 86
 - protocolo HTTPS 85
 - servidor HTTPS 57, 186, 187
 - servidor ssh 89
 - servidor SSH 57, 185
 - visão geral de ssl 90
- segurança aprimorada baseada em função LDAP 57, 192
- segurança baseada em função, aprimorada LDAP 57, 192
- senha
 - Servidor LDAP 57, 173
 - usuário 56, 192
- sequência-chave da CLI
 - configurar 55, 177
- sequência de inicialização, alterando 11
- sequência de inicialização do servidor
 - host, alterando 11
- Serial over LAN 145
- serviço e suporte
 - antes de ligar 203
 - hardware 205
 - software 205
- servidor HTTPS
 - gerenciamento de certificado 57, 186, 187
 - segurança 57, 186, 187
- Servidor LDAP
 - Atributo de procura UID 57, 173
 - configurar 56, 173
 - DNS 56, 173
 - domínio de procura 57, 173
 - Endereço IP 57, 173
 - método de ligação 57, 173
 - nome distinto do cliente 57, 173
 - nome distinto raiz 57, 173
 - nome do host 57, 173
 - número de porta 57, 173
 - pré-configurado 56, 173
 - senha 57, 173
- servidor SSH
 - gerenciamento de certificado 57, 185
 - segurança 57, 185
- servidores blade 1, 4, 7
- servidores blade IBM 1, 4, 7
- sessão da web do IMM2
 - efetuando logout 20
- Sessão de Mídia Virtual
 - disco remoto 115
 - launch 116
 - mapear unidades 116
 - remover mapeamento de unidades 116
 - saindo 117
- sessões, máximo
 - Telnet 57, 190
- SMTP
 - configurar 56, 180

SMTP (continuação)

- endereço IP do servidor 56, 180
- nome do host do servidor 56, 180
- número da porta do servidor 56, 180
- testar 56

SNMPv1

- configurar 56, 181

SSL

- gerenciamento de certificado 90
- manipulação de certificado 90

status de servidor

- monitorar 95

status do sistema 95

suporte de mouse de controle remoto 110

suporte de mouse no controle remoto 110

suporte de teclado internacional no controle remoto 109

suporte de teclado no controle remoto 108

T

tarefas do IMM2 103

Telnet

- acesso 57, 190
- configurar 190
- máximo de sessões 57, 190

tempo limite de inatividade da web

- configurar 56, 159

tempo limite do servidor

- seleções 58

testar

- SMTP 56

trabalhando com

- eventos no log de eventos 28

traps SNMPv1

- configurar 56, 181

U

unidade de transmissão máxima

- configurar 56, 170

unidades

- mapeamento 116
- remoção de mapeamento 116

usando

- cliente ActiveX 40
- Java client 40

USB

- configurar 57, 168

users

- visualizar atuais 192

usuário

- chaves SSH 56, 192
- configurações de SNMPv3 56, 192
- excluir 56, 192
- gerenciar 56
- manage 192
- senha 56, 192

usuários

- visualizar atuais 56

Usuários do Active Directory

- LDAP 57, 192

V

visão geral

- fazer o download de dados de serviço 33
- ssl 90

visualização de configuração

- IMM2 58

visualização do status de backup

- IMM2 58

visualização do status de restauração

- IMM2 58

Visualizador de Vídeo

- captura de tela 106
- comandos de energia e reinicialização 112
- controle de mouse absoluto 110
- controle de mouse relativo 110
- controle de mouse relativo para Linux (aceleração padrão Linux) 110
- estatísticas de desempenho 112
- modo de cor de vídeo 108
- modo de cursor único 111
- modo de passagem do teclado 110
- modos de visualização 107
- saindo 117
- suporte de mouse 110
- suporte de teclado internacional 109

visualizando

- o funcionamento do hardware 99
- o funcionamento do sistema 98
- o status do sistema 95

visualizar atuais

- usuários 56, 192

visualizar informações do firmware

- servidor 55, 156

visualizar o status de backup

- IMM 58

visualizar o status de restauração

- IMM2 58

visualizar portas abertas 57, 176



Número da Peça: 47C9123

Impresso no Brasil

(1P) P/N: 47C9123

