



Integrated Management Module I

Guia do Usuário





Integrated Management Module I
Guia do Usuário

Índice

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

Capítulo 1. Introdução.	1
--	----------

Recursos do IMM.	3
Fazendo Upgrade do IMM Standard para o IMM Premium	5
Comparando o IMM com outro hardware de gerenciamento de sistemas em servidores System x	5
Usando o IMM com um módulo de gerenciamento avançado BladeCenter	9
Requisitos de navegador da web e sistema operacional	9
Avisos usados neste manual	10

Capítulo 2. Abrindo e usando a interface da web do IMM	11
---	-----------

Acessando a interface da web do IMM	11
Configurando a Conexão de Rede do IMM por meio do Utilitário de Configuração do IBM System x Server Firmware	11
Efetuando login no IMM	14
Descrições das ações do IMM	15

Capítulo 3. Configurando o IMM	19
---	-----------

Configurando informações do sistema	20
Configurando tempos limites do servidor	21
Configurando a data e hora do IMM	22
Sincronizando clocks em uma rede	23
Desativando a interface USB dentro da banda	24
Criando um perfil de login	25
Excluindo um perfil de login	30
Configurando as definições globais de login	30
Configurando definições de alerta remoto	31
Configurar receptores de alerta remoto	32
Configurando definições globais de alerta remoto	33
Configurando definições de alerta SNMP	34
Configurando definições de porta serial	34
Configurando o redirecionamento serial para Telnet ou SSH	36
Configurando designações de porta	36
Configurando as interfaces de rede	38
Definindo as configurações de Ethernet	38
Definindo as configurações de IPv4	41
Definindo as configurações de IPv6	42
Configurando protocolos de rede	43
Configurando o SNMP	43
Configurando o DNS	45
Configurando Telnet	46
Configurando o SMTP.	46
Configurando o LDAP.	46
Exemplo de esquema do usuário	47
Visualização de Esquema do Novell eDirectory	48
Navegando no servidor LDAP	56

Visualização do esquema do Microsoft Windows Server 2003 Active Directory.	58
Configurando o cliente LDAP	63
Configurando a segurança	80
Ativando a Criptografia de Dados.	82
Protegendo o servidor da web, IBM Systems Director e LDAP seguro	82
Certificado SSL	83
Gerenciamento de certificado do servidor SSL	83
Ativando SSL para o servidor da web seguro ou IBM Systems Director sobre HTTPS	88
Gerenciamento de certificado de cliente SSL	88
Gerenciamento de certificado confiável do cliente SSL	88
Ativando SSL para o cliente LDAP	89
Gerenciamento de Criptografia	89
Configurando o servidor Shell Seguro	89
Gerando uma chave do servidor Shell Seguro	90
Ativando o Servidor Shell Seguro	90
Usando o Servidor Shell Seguro	90
Restaurando e modificando a configuração do IMM	91
Usando o arquivo de configuração	92
Fazendo backup da sua configuração atual	92
Restaurando e modificando a configuração do IMM.	92
Restaurando padrões	93
Reiniciando o IMM.	94
Partição escalável	94
Recurso de Consultor de Serviço	94
Configurando o Consultor de Serviço.	94
Usando o Consultor de Serviço.	97
Encerrando sessão	99

Capítulo 4. Monitorando o status do servidor.	101
--	------------

Visualizando o status do sistema	101
Visualizando Indicadores Luminosos Virtuais.	105
Visualizando os logs de eventos	106
Visualizando o log de eventos do sistema a partir da interface da web	107
Visualizando logs de eventos do utilitário de configuração.	108
Visualizando logs de eventos sem reiniciar o servidor	108
Visualizando dados vitais do produto	110

Capítulo 5. Executando tarefas do IMM	113
--	------------

Visualizando a atividade de energia e reinicialização do servidor	113
Controlando o status de energia de um servidor	114
Presença remota	115
Atualizando o firmware do IMM e o applet Java ou ActiveX	115
Ativando a função de presença remota	116
Controle remoto	116

Captura de tela de controle remoto	118
Modos de visualização do Visualizador de Vídeo de controle remoto	118
Modo de cor de vídeo do controle remoto	119
Suporte a teclado de controle remoto	120
Suporte a mouse de controle remoto.	121
Controle de energia remota.	123
Visualizando Estatísticas de Desempenho	123
Iniciando o Remote Desktop Protocol	123
Disco remoto	123
Configurando a inicialização da rede PXE	126
Atualizando o Firmware.	126
Reconfigurando o IMM com o utilitário de Configuração	127
Gerenciando ferramentas e utilitários com o IMM e IBM System x Server Firmware	128
Usando o IPMITool	129
Usando o OSA System Management Bridge	129
Usando o IBM Advanced Settings Utility	129
Usando os Utilitários de Atualização IBM	129
Outros métodos para gerenciar o IMM	130

Capítulo 6. LAN sobre USB 131

Potenciais conflitos com a interface LAN sobre USB	131
Resolvendo conflitos com a interface LAN sobre USB do IMM	131
Configurando a interface LAN sobre USB manualmente	132
Instalando drivers de dispositivo.	132
Instalando o driver de dispositivo IPMI do Windows.	132
Instalando o driver de dispositivo LAN sobre USB Windows	132
Instalando o driver de dispositivo LAN sobre USB Linux	133

Capítulo 7. Interface da linha de comandos. 135

Gerenciando a IPMI com o IMM	135
Acessando a linha de comandos	135
Efetuando login na sessão de linha de comandos	135
Sintaxe do comando	136
Recursos e limitações.	136
Comandos Utilitários.	137
comando exit	137
comando help	137
Comando history	138
Comandos de Monitor	138
Comando clearlog.	138
Comando fans	138
Comando readlog	138
Comando syshealth	139
Comando temps	139
Comando volts	140
Comando vpd	140
Comandos de controle de energia e reinicialização do servidor	141
Comando power	141
Comando reset	141
Comando de redirecionamento serial	141

comando do console	141
Comandos de configuração.	141
Comando dhcpinfo	142
Comando dns	143
Comando gprofile	143
Comando ifconfig	144
Comando ldap	146
Comando ntp	148
Comando passwordcfg	148
Comando portcfg	149
Comando portcontrol.	150
Comando srcfg	150
Comando ssl	151
Comando timeouts	152
Comando usbeth	152
Comando users.	153
Comandos de controle do IMM	154
Comando clearcfg	154
Comando clock.	154
Comando identify	155
Comando resetsp	155
comando update	155
Comandos do Consultor de Serviço	156
Comando autoftp	156
Comando chconfig	157
Comando chlog	158
Comando chmanual	159
Comandos events	159
Comando sdemail	160

Apêndice A. Obtendo ajuda e assistência técnica 161

Antes de ligar	161
Usando a documentação.	162
Obtendo ajuda e informações na World Wide Web	162
Como enviar dados do DSA para a IBM	162
Criando uma página da web de suporte personalizada	163
Serviço e Suporte de Software	163
Serviço e suporte de hardware	163
Serviço do Produto da IBM Taiwan	163

Apêndice B. Avisos 165

Marcas registradas.	166
Notas importantes.	166
Contaminação por partículas	167
Formato da documentação	168
Declaração Regulamentar de Telecomunicação	169
Avisos de emissão eletrônica	169
Declaração da Federal Communications Commission (FCC)	169
Declaração de conformidade de emissão de Classe A do segmento de mercado do Canadá	169
Avis de conformité à la réglementation d'Industrie Canada	169
Declaração de Classe A da Austrália e Nova Zelândia	169
Declaração de conformidade com a Diretiva EMC da União Europeia.	170
Declaração de Classe A da Alemanha	170

Declaração de Classe A VCCI do Japão	171
Instrução da Korea Communications Commission (KCC)	171
Declaração de Classe A de Interferência Eletromagnética (EMI) da Rússia	172
Declaração de emissão eletrônica de Classe A da República Popular da China	172

Declaração de conformidade de Classe A de Taiwan	172
---	-----

Índice Remissivo 173

Tabelas

1. Comparação dos recursos do IMM e recursos do BMC e Remote Supervisor Adapter II combinados em servidores System x	5
2. Ações do IMM	15
3. Números de porta reservados	37
4. Configurações na página Configuração Ethernet Avançada	40
5. Mapeamento de Usuário para Grupo	48
6. Bits de permissão	52
7. Exemplo de atributos UserLevelAuthority e descrições	53
8. Designações UserAuthorityLevel a grupos de usuários.	55
9. Verificando níveis de autoridade e associação ao grupo	63
10. Parâmetros diversos.	66
11. Informações de perfis de grupos	68
12. Parâmetros diversos.	73
13. Bits de permissão	78
14. Suporte de conexão SSL do IMM	82
15. Informações de Contato	95
16. Métodos para visualizar logs de eventos	109
17. Dados vitais do produto do nível da máquina	110
18. Dados vitais do produto do nível de componente	111
19. Log de atividades do componente.	111
20. Dados vitais do produto do firmware do IMM, UEFI e DSA	111
21. Limites para partículas e gases.	168

Capítulo 1. Introdução

O módulo de gerenciamento integrado (IMM) consolida a funcionalidade do processador de serviço, Super E/S, controladora de vídeo e recursos de presença remota em um único chip na placa-mãe do servidor. O IMM substitui o Baseboard Management Controller (BMC) e o Remote Supervisor Adapter II em servidores IBM® System x.

Antes que o IMM fosse usado em servidores IBM, o Baseboard Management Controller (BMC) e o sistema BIOS eram o hardware e o firmware padrão de gerenciamento de sistemas. Os servidores System x usavam processadores de serviços BMC para gerenciar a interface entre o software de gerenciamento de sistemas e a plataforma de hardware. O Remote Supervisor Adapter II e o Remote Supervisor Adapter II Slimline eram os controladores opcionais para gerenciamento do servidor fora da banda.

Importante: Embora o IMM seja padrão em alguns produtos IBM BladeCenter e servidores blade IBM, o módulo de gerenciamento avançado BladeCenter permanece o módulo de gerenciamento principal para funções de gerenciamento de sistemas e multiplexação de teclado/vídeo/mouse (KVM) para servidores BladeCenter e blade. O conteúdo relacionado à Interface da Web do IMM e à Interface da Linha de Comandos não se aplica ao IBM BladeCenter e aos servidores blade. Os usuários que desejam configurar as definições do IMM nos servidores blade devem usar o Advanced Settings Utility (ASU) no servidor blade para executar essas ações.

O IMM oferece diversas melhorias na funcionalidade combinada do BMC e o do Remote Supervisor Adapter II:

- Opção de conexão Ethernet dedicada ou compartilhada. A conexão Ethernet dedicada não está disponível em servidores blade ou em alguns servidores System x.

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 IMM disponível.

- Um endereço IP para a Intelligent Platform Management Interface (IPMI) e a interface do processador de serviço. O recurso não se aplica a servidores blade.
- Dynamic System Analysis (DSA) Integrada.
- Capacidade para atualizar local ou remotamente outras entidades sem precisar reiniciar o servidor para iniciar o processo de atualização.
- Configuração remota com o Advanced Settings Utility (ASU). O recurso não se aplica a servidores blade.
- Capacidade de aplicativos e ferramentas acessarem o IMM, dentro da banda ou fora da banda. Apenas a conexão do IMM dentro da banda é suportada nos servidores blade.
- Recursos aprimorados de presença remota. O recurso não se aplica a servidores blade.

O IBM System x® Server Firmware é a implementação da IBM do Unified Extensible Firmware Interface (UEFI). Ele substitui o BIOS nos servidores System x

e nos servidores blade IBM. 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 2.1, 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.

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

Este documento não contém explicações de erros ou mensagens. Os erros e as mensagens do IMM são descritos no *Guia de Determinação de Problemas e Serviços* que é fornecido com o servidor. Para localizar a versão mais recente deste documento ou do IBM white paper *Transitioning to UEFI and IMM* no IBM® Support Portal, conclua as etapas a seguir.

Nota: A primeira vez que você acessar o IBM Support Portal, escolha a categoria do produto, a família de produtos e os números do modelo para seu servidor. 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 **Documentação**.
5. Em **Ver os resultados**, clique em **Visualizar sua página**.
6. Na caixa Documentação, clique em **Mais resultados**.
7. Na caixa Categoria, marque a caixa de seleção **Integrated Management Module (IMM)**. Links para a documentação do IMM e UEFI aparecem.

Se atualizações de firmware estiverem disponíveis, será possível fazer download delas no website da IBM. O IMM pode ter recursos que não são descritos na documentação; e a documentação pode ser ocasionalmente atualizada para incluir informações sobre esses recursos, ou atualizações técnicas podem estar disponíveis para fornecer informações adicionais que não estão incluídas na documentação do IMM.

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

Nota: A primeira vez que você acessar o IBM Support Portal, escolha a categoria do produto, a família de produtos e os números do modelo para seu servidor. 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 do IMM

O IMM fornece as seguintes funções:

- Acesso remoto e gerenciamento ininterruptos do servidor
- Gerenciamento remoto independente do status do servidor gerenciado
- Controle remoto de hardware e sistemas operacionais
- Gerenciamento baseado na web com navegadores da web padrão

O IMM fornece dois tipos de funcionalidade: recursos do IMM Standard e do IMM Premium. Para obter informações sobre o tipo de hardware IMM no servidor, consulte a documentação fornecida com o servidor.

Recursos do IMM Standard

Nota: Alguns dos seguintes recursos não se aplicam a servidores blade.

- Acesso a configurações críticas do servidor
- Acesso a dados vitais do produto (VPD) do servidor
- Suporte a Predictive Failure Analysis (PFA) avançado
- Notificação e alertas automáticos
- Monitoramento e controle contínuos de funcionamento
- Opção de uma conexão Ethernet dedicada ou compartilhada (se aplicável).

Nota: Uma porta de rede de gerenciamento de sistemas dedicada pode não estar disponível em seu servidor.

- Suporte ao servidor do Sistema de Nomes de Domínio (DNS)
- Suporte ao Protocolo de Configuração de Host Dinâmico (DHCP)
- Alertas de email
- Dynamic System Analysis (DSA) Integrada
- Níveis aprimorados de autoridade do usuário

- LAN sobre USB para comunicações dentro da banda com o IMM
- Logs de eventos com registro de data e hora, salvos no IMM e podem ser anexados a alertas de email
- Interfaces e protocolos padrão de mercado
- Watchdogs do S.O.
- Configuração remota por meio do Advanced Settings Utility (ASU)
- Atualização de firmware remota
- Controle de energia remota
- Gráficos acelerados remotos contínuos
- Interface com o usuário do servidor da web seguro
- Serial over LAN
- Redirecionamento do console do servidor
- Suporte ao Protocolo Simples de Gerenciamento de Rede (SNMP)
- Autenticação do usuário utilizando uma conexão segura com um servidor Lightweight Directory Access Protocol(LDAP)

Recursos do IMM Premium

Nota: Alguns dos seguintes recursos não se aplicam a servidores blade.

- Acesso a configurações críticas do servidor
- Acesso a dados vitais do produto (VPD) do servidor
- Suporte a Predictive Failure Analysis (PFA) avançado
- Notificação e alertas automáticos
- Monitoramento e controle contínuos de funcionamento
- Opção de uma conexão Ethernet dedicada ou compartilhada (se aplicável).

Nota: Uma porta de rede de gerenciamento de sistemas dedicada pode não estar disponível em seu servidor.

- Suporte ao servidor do Sistema de Nomes de Domínio (DNS)
- Suporte ao Protocolo de Configuração de Host Dinâmico (DHCP)
- Alertas de email
- Dynamic System Analysis (DSA) Integrada
- Níveis aprimorados de autoridade do usuário
- LAN sobre USB para comunicações dentro da banda com o IMM
- Logs de eventos com registro de data e hora, salvos no IMM e podem ser anexados a alertas de email
- Interfaces e protocolos padrão de mercado
- Watchdogs do S.O.
- Configuração remota por meio do Advanced Settings Utility (ASU)
- Atualização de firmware remota
- Controle de energia remota
- Gráficos acelerados remotos contínuos
- Interface com o usuário do servidor da web seguro
- Serial over LAN
- Redirecionamento do console do servidor
- Suporte ao Protocolo Simples de Gerenciamento de Rede (SNMP)

- Autenticação do usuário utilizando uma conexão segura com um servidor Lightweight Directory Access Protocol(LDAP)
- Presença remota, incluindo o controle remoto de um servidor
- Captura de tela de falha do sistema operacional e exibição por meio da interface da web
- Disco remoto, que permite a conexão de uma unidade de disquete, unidade de CD/DVD, unidade flash USB ou imagem de disco com um servidor

Nota: Os seguintes recursos do Remote Supervisor Adapter II não estão no IMM:

- Exibição de endereços MAC do servidor
- Diversas entradas do servidor NTP

Fazendo Upgrade do IMM Standard para o IMM Premium

Se o seu servidor tiver a funcionalidade IMM Standard, será possível fazer upgrade para o IMM Premium, adquirindo e instalando uma chave de mídia virtual na placa-mãe do servidor. Nenhum firmware novo é necessário.

Para solicitar uma chave de mídia virtual, acesse <http://www.ibm.com/systems/x/newgeneration>.

Nota: Para obter informações sobre como instalar a chave de mídia virtual, consulte a documentação fornecida com o servidor.

Se você precisar de ajuda para seu pedido, ligue para o número de ligação gratuita listado na página de peças de varejo ou entre em contato com o representante IBM local para obter assistência.

Comparando o IMM com outro hardware de gerenciamento de sistemas em servidores System x

A tabela a seguir compara os recursos do IMM com os recursos do BMC e Remote Supervisor Adapter II em servidores System x.

Nota: Como o BMC, o IMM usará a especificação IPMI padrão.

Tabela 1. Comparação dos recursos do IMM e recursos do BMC e Remote Supervisor Adapter II combinados em servidores System x

Descrição	BMC com Remote Supervisor Adapter II	IMM
Conexões de rede	O BMC usa uma conexão de rede que é compartilhada com um servidor e um endereço IP que é diferente do endereço IP do Remote Supervisor Adapter II. O Remote Supervisor Adapter II usa uma conexão de rede de gerenciamento de sistemas dedicada e um endereço IP que é diferente do endereço IP do BMC.	O IMM oferece a funcionalidade do BMC e Remote Supervisor Adapter II por meio da mesma conexão de rede. Um endereço IP é usado para ambos. Se o servidor tiver uma porta de rede de gerenciamento de sistemas dedicada, será possível escolher uma conexão de rede dedicada ou compartilhada. 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 <i>compartilhada</i> será a única configuração do IMM disponível.

Tabela 1. Comparação dos recursos do IMM e recursos do BMC e Remote Supervisor Adapter II combinados em servidores System x (continuação)

Descrição	BMC com Remote Supervisor Adapter II	IMM
Recursos de atualização	Cada servidor requer uma atualização exclusiva para BMC e Remote Supervisor Adapter II. O BIOS e as ferramentas de diagnóstico podem ser atualizados dentro da banda.	Uma imagem de firmware do IMM pode ser usada para todos os servidores aplicáveis. Os firmwares do IMM, do servidor System x e do Dynamic System Analysis (DSA) podem ser atualizados dentro e fora da banda. O IMM pode atualizar a si mesmo, o firmware do servidor e o firmware do DSA local ou remotamente sem requerer que o servidor seja reiniciado para iniciar o processo de atualização.
Recursos de configuração	As mudanças na configuração com o ASU estão disponíveis apenas dentro da banda. O sistema requer configurações separadas para BMC, Remote Supervisor Adapter II e BIOS.	O ASU pode executar dentro ou fora da banda e pode configurar o IMM e o firmware do servidor. Com o ASU, é possível também modificar ordem de inicialização, iSCSI e VPD (tipo de máquina, número de série, UUID e ID do ativo). As definições de configuração do firmware do servidor são mantidas pelo IMM. Portanto, é possível fazer mudanças na configuração do firmware do servidor enquanto o servidor está desligado ou enquanto o sistema operacional está em execução; e essas mudanças são efetivadas na próxima vez que o servidor for iniciado. As definições de configuração do IMM podem ser configuradas dentro ou fora da banda por meio das seguintes interfaces com o usuário do IMM: • Interface da web • Interface da linha de comandos • Interface do IBM Systems Director • SNMP
Captura de tela do sistema operacional	As capturas de tela são executadas pelo Remote Supervisor Adapter II quando ocorrem falhas do sistema operacional. A exibição de capturas de tela requer um applet Java.	Esse recurso está disponível apenas com o IMM Premium. Para obter informações sobre o upgrade do IMM Standard para o IMM Premium, consulte “Fazendo Upgrade do IMM Standard para o IMM Premium” na página 5. As capturas de tela são exibidas diretamente pelo navegador da web sem a necessidade de um applet Java.

Tabela 1. Comparação dos recursos do IMM e recursos do BMC e Remote Supervisor Adapter II combinados em servidores System x (continuação)

Descrição	BMC com Remote Supervisor Adapter II	IMM
Criação de log de erro	O BMC fornece um log de eventos do sistema BMC (log de eventos do IPMI). O Remote Supervisor Adapter II fornece um log baseado em texto que inclui descrições de eventos que são relatadas pelo BMC. Esse log também contém qualquer informação ou eventos detectados pelo próprio Remote Supervisor Adapter II.	O IMM tem dois logs de eventos: 1. O log de eventos do sistema está disponível por meio da interface IPMI. 2. O log de eventos do chassi está disponível por meio de outras interfaces do IMM. O log de eventos do chassi exibe mensagens de texto que são geradas usando as especificações da Distributed Management Task Force, DSP0244 e DSP8007. Nota: Para obter uma explicação de um determinado evento ou mensagem, consulte o <i>Guia de Determinação de Problema e Serviço</i> que é fornecido com o servidor.
Monitoramento	O BMC com o Remote Supervisor Adapter II tem os seguintes recursos de monitoramento: • Monitoramento de servidor e voltagem da bateria, temperatura do servidor, ventiladores, fontes de alimentação e status de processador e DIMM • Controle de velocidade do ventilador • Suporte a Análise Preditiva de Falhas (PFA) • Controle de LED de diagnóstico do sistema (energia, unidade de disco rígido, atividade, alertas, pulsação) • Reinicialização Automática de Servidor(ASR) • Recuperação Automática do BIOS (ABR)	O IMM fornece os mesmos recursos de monitoramento que o BMC e o Remote Supervisor Adapter II. Quando usado em uma configuração RAID, o status expandido da unidade de disco rígido, incluindo PFA de unidade de disco, é suportado pelo IMM.

Tabela 1. Comparação dos recursos do IMM e recursos do BMC e Remote Supervisor Adapter II combinados em servidores System x (continuação)

Descrição	BMC com Remote Supervisor Adapter II	IMM
Presença remota	O BMC com o Remote Supervisor Adapter II tem os seguintes recursos de presença remota: • Redirecionamento de console gráfico sobre LAN • Disquete virtual remoto e CD-ROM • Redirecionamento remoto de alta velocidade de vídeo PCI, teclado e mouse • Resolução de vídeo de até 1024 x 768, a 70 Hz, é suportada • Criptografia de dados	Esse recurso está disponível apenas com o IMM Premium. Para obter informações sobre o upgrade do IMM Standard para o IMM Premium, consulte “Fazendo Upgrade do IMM Standard para o IMM Premium” na página 5. Além dos recursos de presença remota do Remote Supervisor Adapter II, o IMM também tem os recursos a seguir. Nota: O IMM requer o Java Runtime Environment 1.5 ou posterior, ou ActiveX, se o Internet Explorer for utilizado no Windows. • Resolução de vídeo de até 1280 x 1024, a 75 Hz, é suportada • Suporte de USB 2.0 para teclado virtual, mouse e dispositivos de armazenamento em massa • Intensidade de cor de 15 bits • Opção de modo de mouse absoluto ou relativo • Suporte a unidade flash USB • Controle de energia e reinicialização do servidor na janela de Controle Remoto • Vídeo na janela de Controle Remoto pode ser salvo em um arquivo O IMM fornece duas janelas do cliente separadas. Uma para interação de vídeo, teclado e mouse e outra para mídia virtual. A interface da web do IMM 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. A interface do Remote Supervisor Adapter II tem uma régua de controle da largura de banda.
Segurança	O Remote Supervisor Adapter II tem recursos avançados de segurança, incluindo Secure Sockets Layer (SSL) e criptografia.	O IMM tem os mesmos recursos de segurança que o Remote Supervisor Adapter II.

Tabela 1. Comparação dos recursos do IMM e recursos do BMC e Remote Supervisor Adapter II combinados em servidores System x (continuação)

Descrição	BMC com Remote Supervisor Adapter II	IMM
Redirecionamento serial	A função IPMI Serial over LAN (SOL) é um recurso padrão do BMC. O Remote Supervisor Adapter II oferece a capacidade de redirecionar dados seriais do servidor para uma sessão Telnet ou SSH. Nota: Esse recurso não está disponível em alguns servidores.	A porta COM1 é utilizada para SOL em servidores System x. A COM1 é configurável apenas por meio da interface IPMI. A porta COM2 é utilizada para redirecionamento serial por meio de Telnet ou SSH. A COM2 é configurável por meio de todas as interfaces do IMM exceto a interface IPMI. A porta COM2 é usada para SOL nos servidores blade. Ambas as configurações de porta COM são limitadas a 8 bits de dados, paridade nula, 1 bit de parada e uma opção de taxa de bauds de 9600, 19200, 38400, 57600, 115200 ou 230400. Em servidores blade, a porta COM2 é uma porta COM interna sem acesso externo. O compartilhamento de porta serial IPMI não é possível em servidores blade. Em servidores montados em rack e torre, a porta COM2 do IMM é uma porta COM interna sem acesso externo.
SNMP	O suporte SNMP é limitado a SNMPv1.	O IMM suporta SNMPv1 e SNMPv3.

Usando o IMM com um módulo de gerenciamento avançado BladeCenter

O módulo de gerenciamento avançado BladeCenter é a interface de gerenciamento de sistemas padrão no IBM BladeCenter e em servidores blade IBM. Embora o IMM agora esteja incluído em alguns servidores IBM BladeCenter e IBM blade, o módulo de gerenciamento avançado permanece o módulo de gerenciamento para funções de gerenciamento de sistemas e multiplexação de teclado, vídeo e mouse (KVM) para servidores BladeCenter e blade. As interfaces de rede externas para o IMM não estão disponíveis no BladeCenter.

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

Requisitos de navegador da web e sistema operacional

A interface da web do IMM requer o Plug-in Java™ 1.5 ou posterior (para o recurso de presença remota) e um dos seguintes navegadores da web:

- Microsoft Internet Explorer versão 6.0, 7.0 ou 8.0 com o Service Pack mais recente. As versões posteriores à 8.0 não são suportadas.
- Mozilla Firefox versão 1.5 ou posterior

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

- Microsoft Windows Server 2008 R2
- 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

Nota: A interface da web do IMM não suporta os idiomas de conjunto de caracteres de duplo byte (DBCS).

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 IMM

O IMM combina funções de processador de serviço, uma controladora de vídeo e função de presença remota (quando uma chave de mídia virtual opcional está instalada) em um único chip. Para acessar o IMM remotamente usando a interface da web do IMM, 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 IMM.

Acessando a interface da web do IMM

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

O IMM também suporta IPv6, mas não tem um endereço IP IPv6 estático fixo por padrão. Para acesso inicial ao IMM em um ambiente IPv6, é possível usar o endereço IP IPv4 ou o endereço local de link IPv6. O IMM gera um único endereço IPv6 local de link exclusivo, que é mostrado na interface da web do IMM 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 IMM, 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 IMM fornece a opção de utilizar 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.

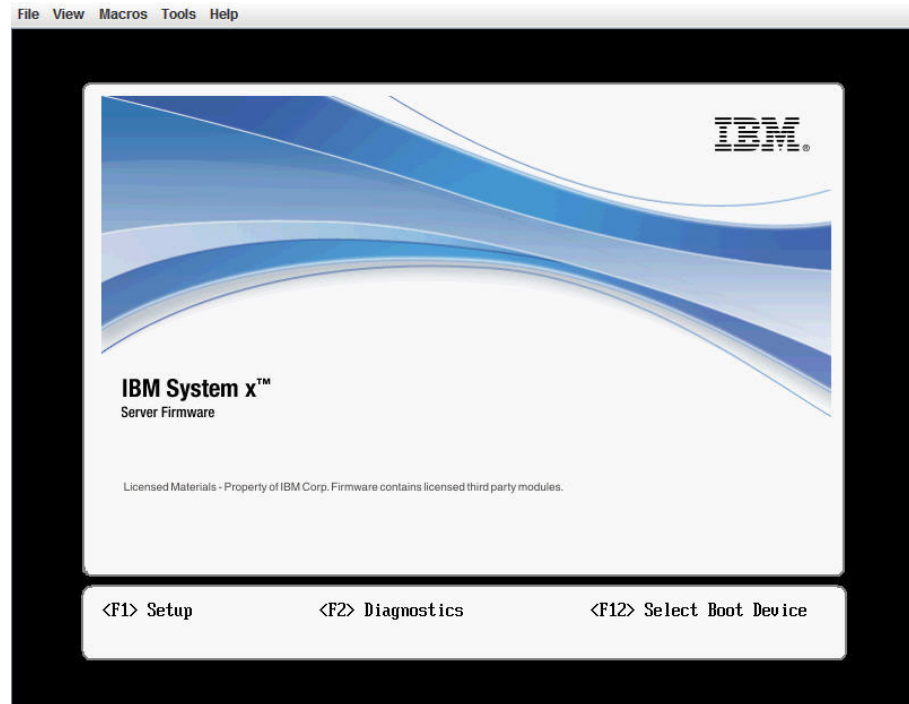
Nota: Uma porta de rede de gerenciamento de sistemas dedicada pode não estar disponível em seu servidor. Se o hardware não tiver uma porta de rede dedicada, a configuração *compartilhada* será a única configuração do IMM disponível.

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

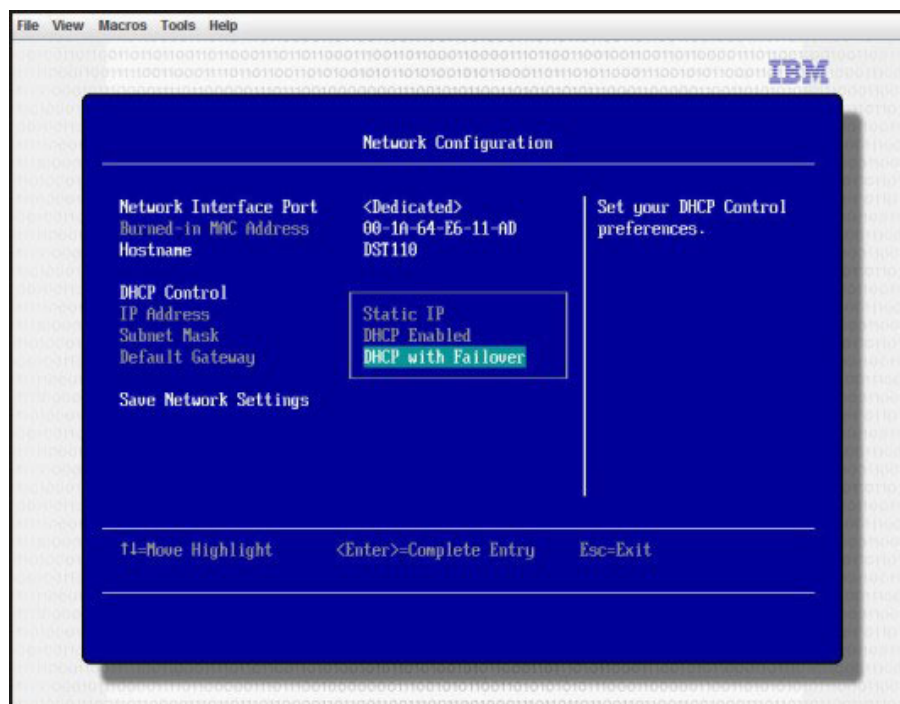
Depois de iniciar o servidor, é possível usar o utilitário de Configuração para selecionar uma conexão de rede do IMM. O servidor com o hardware do IMM deve estar conectado a um servidor Protocolo de Configuração de Host Dinâmico (DHCP), ou a rede do servidor deve estar configurada para usar o endereço IP estático do IMM. Para configurar a conexão de rede do IMM 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 2 minutos após o servidor ser conectado à energia de corrente alternada, o botão liga/desliga 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 IMM 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 IMM 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 IMM disponível. Na tela **Configuração de Rede**, selecione **Dedicada** (se aplicável) ou **Compartilhada** no campo **Porta da Interface de Rede**.
- Para encontrar os locais dos conectores Ethernet em seu servidor que são usados pelo IMM, consulte a documentação fornecida com seu servidor.

10. Selecione **Salvar Configurações de Rede**.

11. Saia do utilitário de Configuração.

Notas:

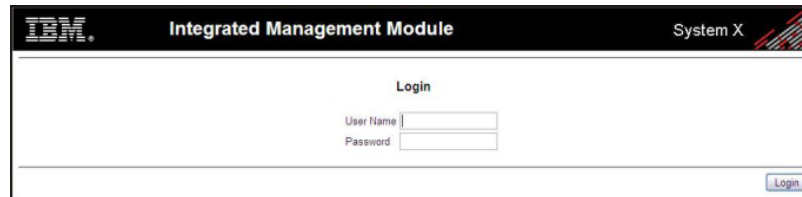
- É preciso aguardar aproximadamente 1 minuto para que as mudanças entrem em vigor antes que o firmware do servidor esteja funcional novamente.
- É possível também configurar a conexão de rede do IMM por meio da interface da web do IMM. Para obter mais informações, consulte “Configurando as interfaces de rede” na página 38.

Efetuando login no IMM

Importante: O IMM é configurado inicialmente com um nome de usuário USERID e uma senha PASSWORD (com um zero, não a letra O). Essa configuração de usuário padrão tem acesso de Supervisor. Altere essa senha padrão durante a configuração inicial para uma maior segurança.

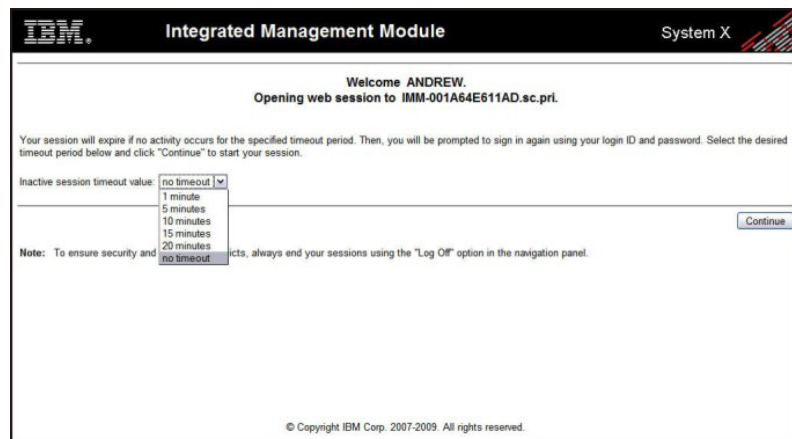
Para acessar o IMM por meio da interface da web do IMM, conclua as etapas a seguir:

1. Abra um navegador da web. No campo de endereço ou URL, digite o endereço IP ou o nome do host do servidor IMM ao qual você deseja se conectar.

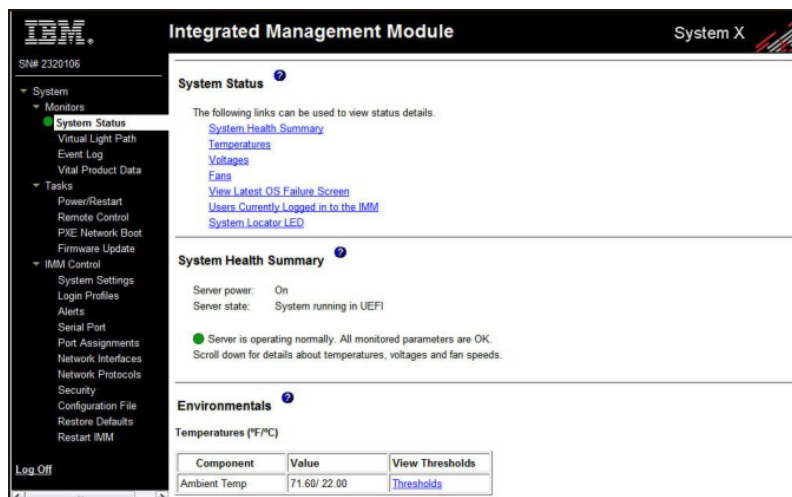


2. Digite seu nome de usuário e senha na janela Login do IMM. Se você estiver usando o IMM pela primeira vez, poderá obter o nome do usuário e a senha do administrador do sistema. Todas as tentativas de login são documentadas no log de eventos. Dependendo de como o seu administrador do sistema configurou o ID do usuário, talvez seja necessário inserir uma nova senha.
3. Na página da web Bem-vindo, selecione um valor de tempo limite na lista suspensa do campo que é fornecido. Se o navegador ficar inativo durante esse número de minutos, o IMM efetuará logoff da interface da web.

Nota: Dependendo de como o seu administrador do sistema configurou as definições de login global, o valor de tempo limite poderá ser um valor fixo.



4. Clique em **Continuar** para iniciar a sessão. O navegador abre a página Status do Sistema, que fornece a você uma visualização rápida do status do servidor e do resumo de funcionamento do servidor.



Para obter descrições das ações que podem ser executadas a partir dos links na área de janela de navegação esquerda da interface da web do IMM, consulte “Descrições das ações do IMM”. Em seguida, acesse Capítulo 3, “Configurando o IMM”, na página 19.

Descrições das ações do IMM

Tabela 2 lista as ações que estão disponíveis quando você está com login efetuado no IMM.

Tabela 2. Ações do IMM

Link	Ação	Descrição
Status do Sistema	Visualizar o funcionamento do sistema para um servidor, visualizar a captura de tela de falha do sistema operacional e visualizar os usuários que estão com login efetuado no IMM	É possível monitorar a energia e o estado de funcionamento do servidor, bem como temperatura, voltagem e status dos ventiladores do seu servidor na página Funcionamento do Sistema. É possível também visualizar a imagem da última captura de tela de falha do sistema operacional e os usuários que estão com login efetuado no IMM.
Indicadores Luminosos Virtuais	Visualizar o nome, a cor e o status de cada LED nos indicadores luminosos do servidor	A página Indicadores Luminosos Virtuais exibe o status atual do LEDs no servidor.
Log de Eventos	Visualizar logs de eventos para servidores remotos	A página Log de Eventos contém entradas que estão atualmente armazenadas no log de eventos do chassi. O log inclui uma descrição de texto dos eventos que são relatados pelo BMC, além de informações sobre todas as tentativas de acesso remoto e mudanças na configuração. Todos os eventos no log têm registro de data e hora, usando as configurações de data e hora do IMM. Alguns eventos também gerarão alertas, se estiverem configurados para isso na página Alertas. É possível classificar e filtrar eventos no log de eventos.
Dados Vitais do Produto	Visualizar os dados vitais do produto (VPD) do servidor	O IMM coleta informações do servidor, informações do firmware do servidor e VPD do componente do servidor. Esses dados estão disponíveis na página Dados Vitais do Produto.

Tabela 2. Ações do IMM (continuação)

Link	Ação	Descrição
Energia/ Reinicialização	Ligar ou reiniciar remotamente um servidor	O IMM fornece controle remoto total de energia sobre o servidor com as ações ligar, desligar e reiniciar. Além disso, as estatísticas de ligação e reinicialização são capturadas e exibidas para mostrar a disponibilidade do hardware do servidor.
Controle Remoto	Redirecionar o console de vídeo do servidor e usar a imagem de disco ou unidade de disco do computador como uma unidade no servidor	Na página Controle Remoto, é possível iniciar o recurso de Controle Remoto. Com o Controle Remoto, é possível visualizar o console do servidor a partir de seu computador, possibilitando montar uma das unidades de disco do computador, como a unidade de CD-ROM ou a unidade de disquete, no servidor. É possível usar o mouse e o teclado para interagir e controlar o 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.
Inicialização da Rede PXE	Alterar a sequência de inicialização (boot) do servidor host para a próxima reinicialização para tentar uma inicialização da rede de Ambiente de Execução de Pré-inicialização (PXE)/Protocolo de Configuração de Host Dinâmico (DHCP)	Se o firmware do servidor e o utilitário do agente de inicialização PXE estiverem definidos corretamente, na página Inicialização da Rede PXE, você poderá alterar a sequência de inicialização (boot) do servidor host para a próxima reinicialização para tentar uma inicialização da rede PXE/DHCP. A sequência de inicialização do host será alterada apenas se o host não estiver sob Proteção de Acesso Privilegiado (PAP). Depois de ocorrer a próxima reinicialização, a caixa de seleção na página Inicialização da Rede PXE será desmarcada.
Atualização de Firmware	Atualizar firmware no IMM	Use as opções na página Atualização de Firmware para atualizar o firmware do IMM, o firmware do servidor e o firmware do DSA.
Configurações do Sistema	Visualizar e alterar as configurações do servidor IMM	É possível configurar o local do servidor e informações gerais, como o nome do IMM, as configurações de tempo limite do servidor e as informações de contato para o IMM, na página Configurações do Sistema.
	Configurar o clock do IMM	É possível configurar o clock do IMM que é usado para registro de data e hora das entradas no log de eventos.
	Ativar ou desativar a interface dentro da banda USB	É possível ativar ou desativar a interface USB dentro da banda (ou LAN sobre USB).
Perfis de Login	Configurar os perfis de login do IMM e as definições globais de login	É possível definir até 12 perfis de login que permitam o acesso ao IMM. É possível também definir configurações globais de login que se aplicam a todos os perfis de login, incluindo ativar a autenticação do servidor do Protocolo LDAP e customizar o nível de segurança de conta.
Alertas	Configurar alertas remotos e receptores de alertas remotos	É possível configurar o IMM para gerar e encaminhar alertas para eventos diferentes. Na página Alertas, é possível configurar os alertas que são monitorados e os destinatários que são notificados.
	Configurar eventos do Protocolo Simples de Gerenciamento de Rede (SNMP)	É possível configurar as categorias de eventos para os quais os traps SNMP são enviados.
	Configurar definições de alerta	É possível estabelecer configurações globais que se apliquem a todos os receptores de alertas remotos, como o número de novas tentativas de alerta e o atraso entre elas.

Tabela 2. Ações do IMM (continuação)

Link	Ação	Descrição
Porta Serial	Configurar as definições de porta serial do IMM	Na página Porta Serial, é possível configurar a taxa de bauds da porta serial que é usada pela função de redirecionamento serial. É possível também configurar a sequência-chave que é usada para alternar entre os modos de redirecionamento serial e interface da linha de comandos (CLI).
Designações de porta	Alterar os números de porta dos protocolos do IMM	Na página Designações de Porta, é possível visualizar e alterar os números de porta designados aos protocolos do IMM (por exemplo, HTTP, HTTPS, Telnet e SNMP).
Interfaces de Rede	Configurar as interfaces de rede do IMM	Na página Interfaces de Rede, é possível configurar as definições de acesso à rede para a conexão Ethernet no IMM.
Protocolos de Rede	Configurar os protocolos de rede do IMM	É possível configurar as definições de Protocolo Simples de Gerenciamento de Rede (SNMP), Sistema de Nomes de Domínio (DNS) e Protocolo Simples de Transporte de Correio (SMTP) que são usadas pelo IMM na página Protocolos de Rede. É possível também configurar os parâmetros LDAP.
Segurança	Configurar o Secure Sockets Layer (SSL)	É possível ativar ou desativar o SSL e gerenciar os certificados SSL que são usados. Pode-se também ativar ou desativar o uso de uma conexão SSL para conectar-se a um servidor LDAP.
	Ativar o acesso de Shell Seguro (SSH)	É possível ativar o acesso SSH ao IMM.
Arquivo de Configuração	Fazer backup e restaurar a configuração do IMM	É possível fazer backup, modificar e restaurar a configuração do IMM, bem como visualizar um resumo de configuração, na página Arquivo de Configuração.
Restaurar Configurações Padrão	Restaurar as configurações padrão do IMM	Atenção: Quando você clica em Restaurar Padrões , todas as modificações feitas no IMM são perdidas. É possível redefinir a configuração do IMM para os padrões de fábrica.
Reiniciar IMM	Reiniciar o IMM	É possível reiniciar o IMM.
Partição Escalável	Configurar o servidor como uma partição em um complexo escalável.	Se o servidor estiver configurado em um complexo escalável, o IMM permitirá que você controle o sistema em um complexo. Se houver um problema com o servidor sendo escalável, o IMM relatará um erro.
Consultor de Serviço	Encaminha códigos de evento que permite manutenção para o suporte IBM	Quando ativado, o Consultor de Serviço permite que o IMM encaminhe códigos de evento que permite manutenção para o suporte IBM para posterior resolução de problemas. Nota: Consulte a documentação de seu servidor para ver se ele suporta esse recurso.
Efetuar Logoff	Efetuar logoff do IMM	É possível efetuar logoff da sua conexão com o IMM.

Você pode clicar no link **Visualizar Resumo da Configuração**, que está no canto superior direito na maioria das páginas, para visualizar rapidamente a configuração do IMM.

Capítulo 3. Configurando o IMM

Utilize os links em **Controle do IMM** na área de janela de navegação para configurar o IMM.

Na página Configurações do Sistema, é possível:

- Configurar as informações do servidor
- Configurar os tempos limites do servidor
- Configurar a data e hora do IMM
- Ativar ou desativar comandos na interface USB

Na página Perfis de Login, é possível:

- Configurar perfis de login para controlar o acesso ao IMM
- Configurar definições globais de login, como período de bloqueio após tentativas malsucedidas de login
- Configurar o nível de segurança de conta

Na página Alertas, é possível:

- Configurar os destinatários de alerta remoto
- Configurar o número de tentativas de alerta remoto
- Selecionar o atraso entre os alertas
- Selecionar quais alertas são enviados e como são encaminhados

Na página Porta Serial, é possível:

- Configurar a taxa de bauds da porta serial 2 (COM2) para redirecionamento serial
- Especificar a sequência de pressionamento de tecla que é usada para alternar entre o redirecionamento serial e a interface da linha de comandos (CLI)

Na página Designações de Porta, é possível alterar os números de porta de serviços do IMM.

Na página Interfaces de Rede, é possível configurar a conexão Ethernet para o IMM.

Na página Protocolos de Rede, é possível configurar:

- Configuração SNMP
- Configuração do DNS
- Protocolo Telnet
- Configuração de SMTP
- Configuração de LDAP
- Protocolo de localização de serviço

Na página Segurança, é possível instalar e configurar as definições de Secure Sockets Layer (SSL).

Na página Arquivo de Configuração, é possível fazer backup, modificar e restaurar a configuração do IMM.

Na página Restaurar Padrões, é possível redefinir a configuração do IMM para os padrões de fábrica.

Na página Reiniciar IMM, é possível reiniciar o IMM.

Configurando informações do sistema

Para configurar as informações do sistema IMM, conclua as etapas a seguir:

1. Efetue login no IMM no qual você deseja configurar as informações do sistema. Para obter mais informações, consulte Capítulo 2, “Abrindo e usando a interface da web do IMM”, na página 11.
2. Na área de janela de navegação, clique em **Configurações do Sistema**. Uma página semelhante à da ilustração a seguir é exibida.

Nota: Os campos disponíveis na página Configurações do Sistema são determinados pelo servidor remoto acessado.

The screenshot shows the IBM Integrated Management Module (IMM) web interface. The top header includes the IBM logo, the title 'Integrated Management Module', and 'System X'. A sidebar on the left contains a navigation menu with options like System, Monitors, Tasks, and IMM Control. The main content area is titled 'IMM Information' and contains several sections: 'IMM Information' with fields for Name, Contact, and Location; 'Server Timeouts' with dropdowns for OS watchdog and Loader watchdog; 'IMM Date and Time' showing the current date and time, and a link to 'Set IMM Date and Time'; and 'Miscellaneous' with a checkbox for 'Do not allow commands on USB interface'.

3. No campo **Nome** na área de **Informações do IMM**, digite o nome do IMM. Use o campo **Nome** para especificar um nome para o IMM nesse servidor. O nome é incluído com notificações de alerta por email e SNMP para identificar a origem do alerta.

Nota: O nome do IMM (no campo **Nome**) e o nome do host IP do IMM (no campo **Nome do Host** na página Interfaces de Rede) não compartilham automaticamente o mesmo nome porque o campo **Nome** está limitado a 16 caracteres. O campo **Nome do Host** pode conter até 63 caracteres. Para minimizar a confusão, defina o campo **Nome** como a parte não completa do nome do host IP. O nome do host IP não completo inclui até o primeiro ponto de um nome de host IP completo. Por exemplo, para o nome completo do host IP imm1.us.company.com, o nome do host IP não completo é imm1. Para obter informações sobre o nome do host, consulte “Configurando as interfaces de rede” na página 38.

4. No campo **Contato**, digite as informações de contato. Por exemplo, é possível especificar o nome e o número do telefone da pessoa a ser contatada se houver um problema com esse servidor. Você pode digitar no máximo 47 caracteres nesse campo.

5. No campo **Local**, digite o local do servidor. Nesse campo, inclua detalhes suficientes para localizar rapidamente o servidor para manutenção ou outros propósitos. Você pode digitar no máximo 47 caracteres nesse campo.
6. Role para a parte inferior da página e clique em **Salvar**.

Configurando tempos limites do servidor

Nota: Os tempos limites do servidor exigem que a interface USB dentro da banda (ou LAN sobre USB) seja ativada para permitir comandos. Para obter mais informações sobre os comandos de ativação e desativação da interface USB, consulte “Desativando a interface USB dentro da banda” na página 24. Para obter informações sobre a instalação dos drivers de dispositivo necessários, consulte “Instalando drivers de dispositivo” na página 132.

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

1. Efetue login no IMM no qual você deseja configurar os tempos limites do servidor. Para obter mais informações, consulte Capítulo 2, “Abrindo e usando a interface da web do IMM”, na página 11.
2. Na área de janela de navegação, clique em **Configurações do Sistema** e role para baixo até a área **Tempos Limites do Servidor**.
É possível configurar o IMM para responder automaticamente aos seguintes eventos:
 - Sistema operacional parado
 - Falha ao carregar sistema operacional
3. Ative os tempos limites do servidor que correspondam aos eventos que o IMM deve responder automaticamente.

Watchdog do S.O.

Use o campo **Watchdog do S.O.** para especificar o número de minutos entre as verificações do sistema operacional pelo IMM. Se o sistema operacional falhar em responder a uma dessas verificações, o IMM 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 sistema operacional, selecione um intervalo de tempo no menu. Para desativar esse watchdog, selecione **0.0** no menu. Para capturar telas de falha do sistema operacional, você deve ativar o watchdog no campo **Watchdog do S.O.**.

Watchdog do carregador

Use o campo **Watchdog do carregador** para especificar o número de minutos que o IMM aguarda entre a conclusão do POST e o início do sistema operacional. Se esse intervalo for excedido, o IMM 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 IMM aguarda para que a inicialização do sistema operacional seja concluída. Para desativar esse watchdog, selecione **0.0** no menu.

Atraso de desligamento

Use o campo **Atraso de desligamento** para especificar o número de minutos que o IMM aguarda o encerramento do sistema operacional antes de desligar a energia do servidor (se a energia não foi desligada pelo próprio sistema operacional). Se você configurar o atraso de desligamento, será possível certificar-se de que o sistema operacional tenha tempo suficiente para um encerramento ordenado antes de a energia do servidor ser desligada. Para determinar o atraso de desligamento do servidor, encerre-o e observe quanto tempo ele leva para ser encerrado. Inclua um buffer de tempo nesse valor e use o número resultante como a configuração de atraso de desligamento.

Para configurar o valor do atraso de desligamento, selecione o valor do tempo desejado no menu. Um valor X'0' significa que o sistema operacional, não o IMM, desliga a energia do servidor.

4. Role para a parte inferior da página e clique em **Salvar**.

Configurando a data e hora do IMM

O IMM usa seu próprio clock de tempo real para registrar a data e hora de todos os eventos registrados no log de eventos.

Nota: A configuração de data e hora do IMM afeta apenas o clock do IMM, não o do servidor. O clock de tempo real do IMM e o do servidor são separados, independentes e podem ser configurados com horários diferentes. Para sincronizar o clock do IMM com o do servidor, acesse a área **Network Time Protocol** da página e configure o nome do host ou endereço IP do servidor NTP com o mesmo nome de host ou endereço IP do servidor que é usado para configurar o clock do servidor. Consulte “Sincronizando clocks em uma rede” na página 23 para obter mais informações.

Os alertas enviados por email e SNMP usam a configuração do clock de 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 (DST) 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.

Para verificar as configurações de data e hora do IMM, conclua as etapas a seguir:

1. Efetue login no IMM no qual você deseja configurar os valores de data e hora do IMM. Para obter mais informações, consulte Capítulo 2, “Abrindo e usando a interface da web do IMM”, na página 11.
2. Na área de janela de navegação, clique em **Configurações do Sistema** e role para baixo até a área **Data e Hora do IMM**, que mostra a data e hora em que a página da web foi gerada.
3. Para substituir as configurações de data e hora e ativar o horário de verão (DST) e os deslocamentos da Hora de Greenwich (GMT), clique em **Configurar Data e Hora do IMM**. É exibida uma página semelhante à da ilustração a seguir.

4. No campo **Data**, digite os números do mês, dia e ano atuais.
5. No campo **Hora**, digite os números que correspondem à hora, minutos e segundos atuais nos campos de entrada aplicáveis. A hora (hh) deve ser um número de 00 a 23 conforme representado em um relógio de 24 horas. Os minutos (mm) e segundos (ss) devem ser números de 00 a 59.
6. No campo **Deslocamento GMT**, selecione o número que especifica o deslocamento, em horas, da Hora de Greenwich (GMT), correspondente ao fuso horário no qual o servidor está localizado.
7. Marque ou desmarque a caixa de seleção **Ajustar automaticamente para mudanças de horário de verão** para especificar se o clock do IMM é ajustado automaticamente quando o horário local é alterado entre horário padrão e horário de verão.
8. Clique em **Salvar**.

Sincronizando clocks em uma rede

O Network Time Protocol (NTP) fornece uma maneira de sincronizar clocks em toda uma rede de computadores, permitindo que qualquer cliente NTP obtenha a hora correta de um servidor NTP.

O recurso NTP do IMM fornece uma maneira de sincronizar o clock de tempo real do IMM com a hora fornecida por um servidor NTP. É possível especificar o servidor NTP que deve ser usado, especificar a frequência com a qual o IMM é sincronizado, ativar ou desativar o recurso NTP e solicitar sincronização de hora imediata.

O recurso NTP não fornece a segurança estendida e a autenticação que são fornecidas por meio de algoritmos de criptografia no NTP Versão 3 e NTP Versão

4. O recurso NTP do IMM suporta apenas o Simple Network Time Protocol (SNTP) sem autenticação.

Para configurar as definições de recursos NTP do IMM, conclua as etapas a seguir:

1. Efetue login no IMM em que você deseja sincronizar os clocks na rede. Para obter mais informações, consulte Capítulo 2, “Abrindo e usando a interface da web do IMM”, na página 11.
2. Na área de janela de navegação, clique em **Configurações do Sistema** e role para baixo até a área **Data e Hora do IMM**.
3. Clique em **Configurar data e hora do IMM**. É exibida uma página semelhante à da ilustração a seguir.



4. Em **Network Time Protocol (NTP)**, é possível selecionar entre as configurações a seguir:

Serviço de sincronização automática do NTP

Use essa seleção para ativar ou desativar a sincronização automática do clock do IMM com um servidor NTP.

Nome do host ou endereço IP do NTP

Use esse campo para especificar o nome do servidor NTP a ser usado para a sincronização de clock.

Frequência de atualização do NTP

Use esse campo para especificar o intervalo aproximado (em minutos) entre as solicitações de sincronização. Insira um valor entre 3 e 1440 minutos.

Sincronizar Clock Agora

Clique nesse botão para solicitar uma sincronização imediata em vez de aguardar o término do tempo de intervalo.

5. Clique em **Salvar**.

Desativando a interface USB dentro da banda

Importante: Se você desativar a interface USB dentro da banda, não será possível executar uma atualização dentro da banda do firmware do IMM, 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 Atualização de Firmware na interface da web do IMM para atualizar o firmware. Para obter mais informações, consulte “Atualizando o Firmware” na página 126.

Se você desativar a interface USB dentro da banda, desative também os tempos limites de watchdog para evitar que o servidor seja reiniciado inesperadamente. Para obter mais informações, consulte “Configurando tempos limites do servidor” na página 21.

A interface USB dentro da banda, ou LAN sobre USB, é usada para comunicação dentro da banda com o IMM. Para impedir que qualquer aplicativo que está em execução no servidor solicite ao IMM que execute tarefas, você deve desativar a interface USB dentro da banda. Para obter mais informações a respeito de LAN sobre USB, consulte Capítulo 6, “LAN sobre USB”, na página 131.

Para desativar a interface USB dentro da banda, conclua as etapas a seguir:

1. Efetue login no IMM no qual você deseja desativar a interface do driver de dispositivo USB. Para obter mais informações, consulte Capítulo 2, “Abrindo e usando a interface da web do IMM”, na página 11.
2. Na área de janela de navegação, clique em **Configurações do Sistema** e role para a área **Diversos**. É exibida uma página semelhante à da ilustração a seguir.



3. Para desativar a interface USB dentro da banda, selecione **Desativado** na lista **Permitir comandos na interface USB**. A seleção dessa opção não afeta as funções de presença remota USB (por exemplo, teclado, mouse e armazenamento em massa). Ao desativar a interface USB dentro da banda, os aplicativos de gerenciamento de sistemas dentro da banda, como o Advanced Settings Utility (ASU), e os utilitários de pacote de atualização de firmware podem não funcionar.

Nota: O ASU funcionará com uma interface USB dentro da banda desativada se um driver de dispositivo IPMI estiver instalado.

Se você tentar usar os aplicativos de gerenciamento de sistemas enquanto a interface dentro da banda estiver desativada, eles poderão não funcionar.

4. Clique em **Salvar**.

Para ativar a interface do driver de dispositivo USB após ela ter sido desativada, desmarque a caixa de seleção **Não permitir comandos na interface USB** e clique em **Salvar**.

Nota:

1. A interface USB dentro da banda também é chamada de "LAN sobre USB" e é descrita com mais detalhes em Capítulo 6, "LAN sobre USB", na página 131.
2. Quando você tentar uma instalação de rede de algumas distribuições do Linux, a instalação poderá falhar se a interface USB do IMM dentro da banda estiver ativada. Para obter mais informações, consulte <http://rhn.redhat.com/errata/RHBA-2009-0127.html>.
3. Se você estiver executando uma instalação de rede que não contém a atualização no website do Red Hat descrito na nota anterior 2, será necessário desativar a interface USB dentro da banda antes de executar a instalação e ativá-la depois que a instalação for concluída.
4. Para obter informações a respeito da configuração da interface LAN sobre USB, consulte "Configurando a interface LAN sobre USB manualmente" na página 132.

Criando um perfil de login

Use a tabela Perfis de Login para visualizar, configurar ou alterar perfis de login individuais. Use os links na coluna ID de Login para configurar perfis de login individuais. Você pode definir até 12 perfis exclusivos. Cada link na coluna ID de Login é rotulado com o ID de login configurado do perfil associado.

Determinados perfis de login são compartilhados com os IDs de usuário IPMI, fornecendo um conjunto único de contas de usuário local (nome de usuário/senha) que funcionam com todas as interfaces com o usuário do IMM, incluindo IPMI. As regras que pertencem a esses perfis de login compartilhados são descritas na lista a seguir:

- O ID do usuário IPMI 1 é sempre o usuário nulo.

- O ID do usuário IPMI 2 é mapeado para o ID de login 1, o ID do usuário IPMI 3 para o ID de login 2 e assim por diante.
- O usuário padrão do IMM é definido como USERID e PASSWORD (com um zero, não a letra O) para o ID do usuário IPMI 2 e o ID de login 1.

Por exemplo, se um usuário for incluído por meio de comandos IPMI, as informações desse usuário também estarão disponíveis para autenticação pela web, Telnet, SSH e outras interfaces. Por outro lado, se um usuário for incluído na web ou em outras interfaces, as informações desse usuário estarão disponíveis para iniciar uma sessão IPMI.

Como as contas de usuário são compartilhadas com a IPMI, algumas restrições são impostas para fornecer uma base comum entre as interfaces que utilizam essas contas. A lista a seguir descreve as restrições de perfil de login do IMM e da IPMI:

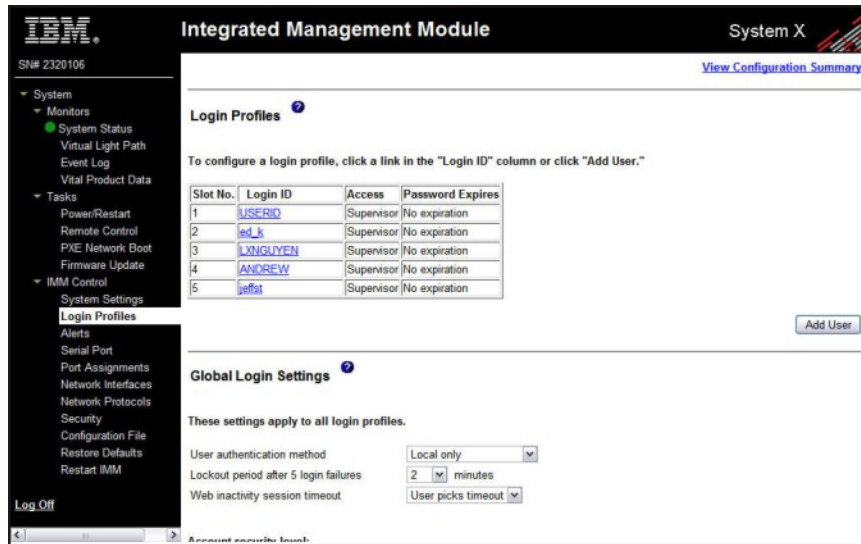
- A IPMI permite no máximo 64 IDs de usuário. A implementação da IPMI do IMM permite apenas 12 contas de usuário.
- A IPMI permite logins anônimos (nome de usuário nulo e senha nula), mas o IMM não.
- A IPMI permite vários IDs de usuário com os mesmos nomes de usuários, mas o IMM não.
- A IPMI solicita alterar o nome de usuário do nome atual para o mesmo nome atual retornar um código de conclusão de parâmetro inválido porque o nome de usuário solicitado já está em uso.
- O comprimento máximo da senha da IPMI para o IMM é 16 bytes.
- As palavras a seguir são restritas e não estão disponíveis para uso como nomes de usuário local do IMM:
 - immroot
 - nobody
 - ldap
 - lighttpd
 - sshd
 - daemon
 - immftp

Para configurar um perfil de login, conclua as etapas a seguir:

1. Efetue login no IMM no qual você deseja criar um perfil de login. Para obter mais informações, consulte Capítulo 2, “Abrindo e usando a interface da web do IMM”, na página 11.
2. Na área de janela de navegação, clique em **Perfis de Login**.

Nota: Se você não configurou um perfil, ele não aparecerá na tabela Perfis de Login.

A página Perfis de Login exibe cada ID de login, o nível de acesso do login e as informações de expiração de senha, conforme mostrado na ilustração a seguir.



Importante: Por padrão, o IMM é configurado com um perfil de login que ativa o acesso remoto usando um ID de usuário de login USERID e uma senha PASSWORD (0 é um zero, não a letra O). Para evitar uma potencial exposição da segurança, altere esse perfil de login padrão durante a configuração inicial do IMM.

3. Clique em **Incluir Usuário**. Uma página de perfil individual semelhante à da ilustração a seguir é exibida.

4. No campo **ID de Login**, digite o nome do perfil. É possível digitar no máximo 16 caracteres no campo **ID de Login**. Os caracteres válidos são letras maiúsculas e minúsculas, números, pontos e sublinhados.

Nota: Esse ID de login é usado para conceder acesso remoto ao IMM.

5. No campo **Senha**, designe uma senha ao ID de login. Uma senha deve conter no mínimo cinco caracteres, um dos quais deve ser um caractere não alfabético. Senhas nulas ou vazias são aceitas.

Nota: Essa senha é usada com o ID de login para conceder acesso remoto ao IMM.

6. No campo **Confirmar senha**, digite a senha novamente.

7. Na área **Nível de autoridade**, selecione uma das opções a seguir para definir os direitos de acesso para esse ID de login:

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

Se você selecionar a opção Customizado, deverá selecionar um ou mais dos seguintes níveis de autoridade customizados:

- **Gerenciamento de Conta do Usuário:** Um usuário pode incluir, modificar ou excluir usuários e alterar as configurações globais de login na página Perfis de Login.
- **Acesso ao Console Remoto:** Um usuário pode acessar o console remoto.
- **Acesso a Console Remoto e Mídia Virtual:** Um usuário pode acessar o console remoto e o recurso de mídia virtual.
- **Acesso a Energia/Reinicialização do Servidor Remoto:** Um usuário pode acessar as funções de ligação e reinicialização do servidor remoto. Essas funções estão disponíveis na página Energia/Reinicialização.
- **Capacidade para Limpar Logs de Eventos:** Um usuário pode limpar os logs de eventos. Todos podem examinar os logs de eventos, mas essa permissão específica é necessária para limpar os logs.
- **Configuração de Adaptador - Básica:** Um usuário pode modificar parâmetros de configuração nas páginas Configurações do Sistema e Alertas.
- **Configuração de Adaptador - Rede & Segurança:** Um usuário pode modificar parâmetros de configuração nas páginas Segurança, Protocolos de Rede, Interface de Rede, Designações de Porta e Porta Serial.
- **Configuração de Adaptador - Avançada:** Um usuário não tem restrições ao configurar o IMM. Além disso, diz-se que usuário tem acesso administrativo ao IMM, o que significa que o usuário também pode executar as seguintes funções avançadas: atualizar o firmware, inicializar a rede PXE, restaurar os padrões de fábrica do IMM, modificar e restaurar a configuração do IMM a partir de um arquivo de configuração, bem como reiniciar e reconfigurar o IMM.

Quando um usuário configura o nível de autoridade de um ID de login do IMM, o nível de privilégio da IPMI resultante do ID do Usuário IPMI correspondente é configurado de acordo com estas prioridades:

- Se o usuário configurar o nível de autoridade do ID de login do IMM como Supervisor, o nível de privilégio da IPMI será configurado como Administrador.
- Se o usuário configurar o nível de autoridade do ID de login do IMM como Somente Leitura, o nível de privilégio da IPMI será configurado como Usuário.
- Se o usuário configurar o nível de autoridade do ID de login do IMM para ter qualquer um dos seguintes tipos de acesso, o nível de privilégio da IPMI será configurado como Administrador:

- Acesso ao Gerenciamento de Conta do Usuário
- Acesso ao Console Remoto
- Acesso ao Console Remoto e Disco Remoto
- Configuração de Adaptador - Rede & Segurança
- Configuração de Adaptador - Avançada
- Se o usuário configurar o nível de autoridade do ID de login do IMM para ter Acesso a Energia/Reinicialização do Servidor Remoto ou Capacidade para Limpar Logs de Eventos, o nível de privilégio da IPMI será configurado como Operador.
- Se o usuário configurar o nível de autoridade do ID de login do IMM como Configuração de Adaptador (Básica), o nível de privilégio da IPMI será configurado como Usuário.

Nota: Para retornar os perfis de login para os padrões de fábrica, clique em **Limpar Perfis de Login**.

8. Na área **Configurar Usuário SNMPv3**, marque a caixa de seleção se o usuário precisar ter acesso ao IMM usando o protocolo SNMPv3. Depois que você clicar na caixa de seleção, uma área da página semelhante à da ilustração a seguir será exibida.

Use os campos a seguir para configurar as definições de SNMPv3 para o perfil do usuário:

Protocolo de Autenticação

Use esse campo para especificar **HMAC-MD5** ou **HMAC-SHA** como o protocolo de autenticação. Esses são algoritmos hash usados pelo modelo de segurança do SNMPv3 para a autenticação. A senha para a conta Linux será usada para autenticação. Se você escolher **Nenhum**, o protocolo de autenticação não 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 só será válido se o protocolo de autenticação for definido como HMAC-MD5 ou HMAC-SHA.

Senha de Privacidade

Use esse campo para especificar a senha de criptografia.

Confirmar Senha de Privacidade

Use esse campo para confirmar a senha de criptografia.

Tipo de Acesso

Use esse campo para especificar **Get** ou **Set** como o tipo de acesso. Os usuários SNMPv3 com o tipo de acesso Get somente podem executar operações de consulta. Com o tipo de acesso Set, os usuários SNMPv3

podem executar operações de consulta e modificar configurações (por exemplo, configurar a senha para um usuário).

Nome do host/endereço IP para traps

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

9. Clique em **Salvar** para salvar suas configurações de ID de login.

Excluindo um perfil de login

Para excluir um perfil de login, conclua as etapas a seguir:

1. Efetue login no IMM para o qual você deseja criar um perfil de login. Para obter mais informações, consulte Capítulo 2, “Abrindo e usando a interface da web do IMM”, na página 11.
2. Na área de janela de navegação, clique em **Perfis de Login**. A página Perfis de Login exibe cada ID de login, o nível de acesso do login e as informações de expiração de senha.
3. Clique no perfil de login que você deseja excluir. A página Perfil de Login para esse usuário é exibida.
4. Clique em **Limpar Perfil de Login**.

Configurando as definições globais de login

Conclua as etapas a seguir para configurar as condições que se aplicam a todos os perfis de login para o IMM:

1. Efetue login no IMM para o qual você deseja definir as configurações globais de login. Para obter mais informações, consulte Capítulo 2, “Abrindo e usando a interface da web do IMM”, na página 11.
2. Na área de janela de navegação, clique em **Perfis de Login**.
3. Role para baixo até a área **Configurações Globais de Login**. É exibida uma página semelhante à da ilustração a seguir.

Global Login Settings

These settings apply to all login profiles.

User authentication method: Local only

Lockout period after 5 login failures: 2 minutes

Web inactivity session timeout: User picks timeout

Account security level:

☒ Legacy security settings	No password required No password expiration No password re-use restrictions
☐ High security settings	Password required Passwords expire in 90 days Password reuse checking enabled (last 5 passwords kept in history)
☐ Custom security settings	User login password required: Disabled Number of previous passwords that cannot be used: 5 Maximum Password Age: 90 days

Save

4. No campo **Método de autenticação do usuário**, especifique como os usuários que estão tentando efetuar login serão autenticados. Selecione um dos métodos de autenticação a seguir:
 - **Somente local:** Os usuários são autenticados por uma procura de uma tabela que é local para o IMM. Se não houver correspondência do ID do usuário e

senha, o acesso será negado. Os usuários autenticados com êxito são designados ao nível de autoridade configurado em “Criando um perfil de login” na página 25.

- **Somente LDAP:** O IMM tenta autenticar o usuário usando o servidor LDAP. As tabelas do usuário local no IMM nunca são procuradas com esse método de autenticação.
- **Local primeiro, depois LDAP:** A autenticação local é tentada primeiro. Se a autenticação local falhar, será tentada a autenticação LDAP.
- **LDAP primeiro, depois Local:** A autenticação LDAP é tentada primeiro. Se a autenticação LDAP falhar, será tentada a autenticação local.

Nota:

- a. Apenas contas administradas localmente são compartilhadas com a interface IPMI porque a IPMI não suporta autenticação LDAP.
 - b. Mesmo que o campo **Método de autenticação do usuário** esteja configurado como **Somente LDAP**, os usuários poderão efetuar login na interface IPMI usando as contas administradas localmente.
5. No campo **Período de bloqueio após 5 falhas de login**, especifique por quanto tempo, em minutos, o IMM proíbe tentativas de login remoto se mais de cinco falhas sequenciais para efetuar login remotamente forem detectadas. O bloqueio de um usuário não impede que outros usuários efetuem login.
 6. No campo **Tempo limite de inatividade da sessão da web**, especifique 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** se o usuário selecionará o período limite durante o processo de login.
 7. (Opcional) Na área **Nível de segurança da conta**, selecione um nível de segurança de senha. As **Configurações de segurança legada** e **Configurações de alta segurança** definem os valores padrão conforme indicados na lista de requisitos.
 8. Para customizar a configuração de segurança, selecione **Configurações de segurança customizada** para visualizar e alterar a configuração de gerenciamento da segurança de conta.

Senha de login de usuário necessária

Use esse campo para indicar se um ID de login sem senha é permitido.

Número de senhas anteriores que não podem ser usadas

Use esse campo para indicar 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.

Expiração de senha

Use esse campo para indicar a duração máxima da senha que é permitida antes de ser necessário alterar a senha. Os valores de 0 a 365 dias são suportados. Selecione **0** para desativar a verificação de expiração de senha.

9. Clique em **Salvar**.

Configurando definições de alerta remoto

É possível configurar os destinatários de alerta remoto, o número de tentativas de alerta, os incidentes que acionam alertas remotos e os alertas locais a partir do link **Alertas** na área de janela de navegação.

Depois de configurar um destinatário de alerta remoto, o IMM envia um alerta para esse destinatário por meio de uma conexão de rede quando ocorre qualquer evento selecionado do grupo Alertas Monitorados. O alerta contém informações sobre a natureza do evento, a hora e data do evento e o nome do sistema que gerou o alerta.

Nota: Se os campos **Agente SNMP** ou **Traps SNMP** não forem configurados como **Ativado**, nenhum trap SNMP será enviado. Para obter informações sobre esses campos, consulte “Configurando o SNMP” na página 43.

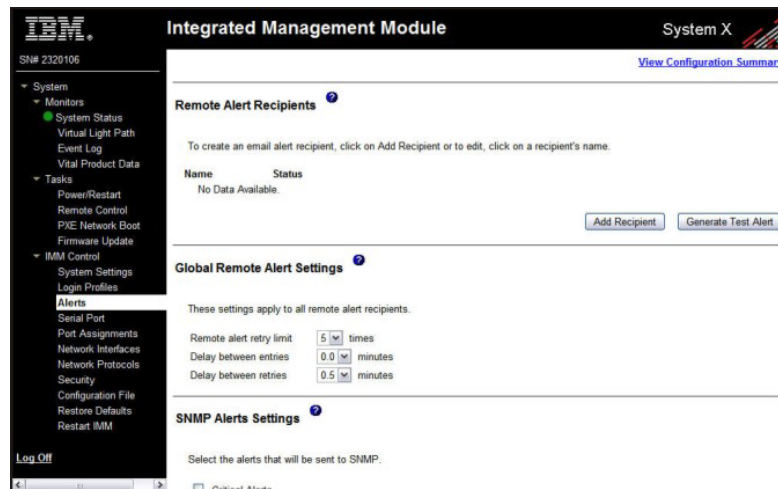
Configurar receptores de alerta remoto

É possível definir até 12 receptores de alertas remotos exclusivos. Cada link para um receptor de alertas é rotulado com o nome do destinatário e o status do alerta.

Nota: Se você não tiver configurado um perfil de receptor de alertas, o perfil não aparecerá na lista de receptores de alertas remotos.

Para configurar um receptor de alertas remotos, conclua as etapas a seguir:

1. Efetue login no IMM no qual você deseja configurar definições de alerta remoto. Para obter mais informações, consulte Capítulo 2, “Abrindo e usando a interface da web do IMM”, na página 11.
2. Na área de janela de navegação, clique em **Alertas**. A página Receptores de Alertas Remotos é exibida. É possível ver o método de notificação e o status do alerta para cada destinatário, se eles estiverem configurados.



3. Clique em um dos links de receptor de alertas remotos ou clique em **Incluir Destinatário**. É aberta uma janela de destinatário individual, semelhante à da ilustração a seguir.

4. No campo **Status**, clique em **Ativado** para ativar o receptor de alertas remotos.
5. No campo **Nome**, digite o nome do destinatário ou outro identificador. O nome digitado aparece como o link para o destinatário na página Alertas.
6. No campo **Endereço de email**, insira o endereço de email do receptor de alertas.
7. Use a caixa de seleção para incluir logs de eventos com alertas de email.
8. No campo **Alertas Monitorados**, selecione o tipo de alertas que são enviados para o receptor de alertas. Os alertas remotos são categorizados pelos seguintes níveis de severidade:

Alertas críticos

São gerados para eventos que indicam que um componente do servidor não está mais funcionando.

Alertas de aviso

São gerados para eventos que podem evoluir para um nível crítico.

Alertas de sistema

São gerados para eventos que ocorrem como resultado de erros no sistema ou para eventos que ocorrem como resultado de mudanças na configuração.

Todos os alertas são armazenados no log de eventos e enviados para todos os receptores de alertas remotos configurados.

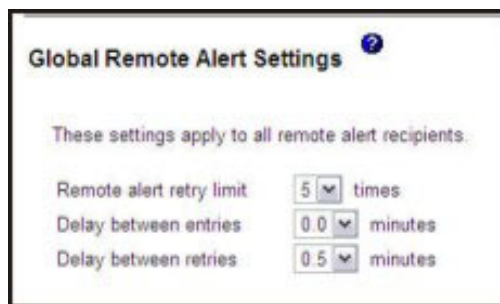
9. Clique em **Salvar**.

Configurando definições globais de alerta remoto

As configurações globais de alerta remoto se aplicam apenas a alertas encaminhados.

Conclua as etapas a seguir para configurar o número de vezes que o IMM tenta enviar um alerta:

1. Efetue login no IMM no qual você deseja configurar tentativas de alerta remoto. Para obter mais informações, consulte Capítulo 2, “Abrindo e usando a interface da web do IMM”, na página 11.
2. Na área de janela de navegação, clique em **Alertas** e role para baixo até a área **Configurações Globais de Alerta Remoto**.



Use essas configurações para definir o número de tentativas de alerta remoto e o tempo entre as tentativas. As configurações se aplicam a todos os receptores de alerta remoto configurados.

Limite de novas tentativas de alerta remoto

Use o campo **Limite de nova tentativa de alerta remoto** para especificar o número de vezes adicionais que o IMM tenta enviar um

alerta para um destinatário. O IMM não envia diversos alertas; tentativas de alerta adicionais ocorrerão apenas se houver uma falha quando o IMM tentar enviar o alerta inicial.

Nota: Essa configuração de alerta não se aplica a alertas SNMP.

Atraso entre as entradas

Use o campo **Atraso entre as entradas** para especificar o intervalo de tempo (em minutos) que o IMM aguarda antes de enviar um alerta para o próximo destinatário na lista.

Atraso entre novas tentativas

Use o campo **Atraso entre novas tentativas** para especificar o intervalo de tempo (em minutos) que o IMM aguarda entre novas tentativas de enviar um alerta para um destinatário.

3. Role para a parte inferior da página e clique em **Salvar**.

Configurando definições de alerta SNMP

O agente do SNMP notifica o IMM sobre eventos por meio de traps SNMP. É possível configurar o SNMP para filtrar os eventos com base no tipo de evento. As categorias de eventos que estão disponíveis para filtragem são Crítico, Aviso e Sistema. As configurações de alerta SNMP são globais para todos os traps SNMP.

Nota:

1. O IMM fornece dois arquivos Management Information Base (MIB) para uso com aplicativos SNMP. O arquivos MIB estão incluídos nos pacotes de atualização de firmware do IMM.
2. O IMM suporta os padrões SNMPv1 e SNMPv3.

Conclua as etapas a seguir para selecionar o tipo ou tipos de alertas que são enviados para SNMP:

1. Efetue login no IMM no qual você deseja configurar tentativas de alerta remoto. Para obter mais informações, consulte Capítulo 2, “Abrindo e usando a interface da web do IMM”, na página 11.
2. Na área de janela de navegação, clique em **Alertas** e role para baixo até a área **Configurações de Alertas SNMP**.
3. Selecione o(s) tipo(s) de alertas. Os alertas remotos são categorizados pelos seguintes níveis de severidade:
 - Crítico
 - Aviso
 - Sistema
4. Role para a parte inferior da página e clique em **Salvar**.

Configurando definições de porta serial

O IMM fornece duas portas seriais que são usadas para redirecionamento serial.

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.

Em servidores blade, a porta serial 2 (COM2) é usada SOL. Em servidores System x, 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.

Ambas as portas seriais usam 8 bits de dados, paridade nula e 1 de parada. Uma opção de taxa de bauds de 9600, 19200, 38400, 57600, 115200 e 230400 está disponível.

É possível configurar o redirecionamento serial e a interface da linha de comandos para a porta COM2 no IMM.

Para configurar a taxa de transferência de dados serial e redirecionamento, conclua as etapas a seguir:

1. Efetue login no IMM no qual você deseja configurar a porta serial. Para obter mais informações, consulte Capítulo 2, “Abrindo e usando a interface da web do IMM”, na página 11.
2. Na área de janela de navegação, clique em **Porta Serial**. Uma página semelhante à da ilustração a seguir é exibida.



3. No campo **Taxa de bauds**, selecione a taxa de transferência de dados para corresponder à taxa da porta COM do servidor que você deseja usar para redirecionamento serial. Use o campo **Taxa de bauds** para especificar a taxa de transferência de dados de sua conexão de porta serial. Para definir a taxa de bauds de dados, selecione a taxa de transferência de dados, em bits por segundo, que corresponda à sua conexão de porta serial.
4. No campo **Modo de CLI**, na área **Configurações de Redirecionamento Serial/CLI**, selecione **CLI com sequências de pressionamento de tecla compatíveis com EMS** se você quiser usar a sequência de teclas compatível com Microsoft Windows Server 2003 Emergency Management Services (EMS) para sair da operação de redirecionamento serial, ou selecione **CLI com sequências de pressionamento de tecla definidas pelo usuário** se quiser usar sua própria sequência de teclas.

Nota: Se você selecionar **CLI com sequências de pressionamento de tecla definidas pelo usuário**, deverá definir a sequência de teclas.

Após o início do redirecionamento serial, ele continua até que o usuário digite a sequência de teclas de saída. Quando a sequência de teclas de saída é digitada, o redirecionamento serial para e o usuário é retornado para o modo de comando na sessão Telnet ou SSH. Use esse campo para especificar a sequência de teclas de saída.

5. Clique em **Salvar**.

Configurando o redirecionamento serial para Telnet ou SSH

O redirecionamento serial para Telnet ou SSH permite que um administrador do sistema use o IMM como 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 IMM 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 interface da linha de comandos 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 Q

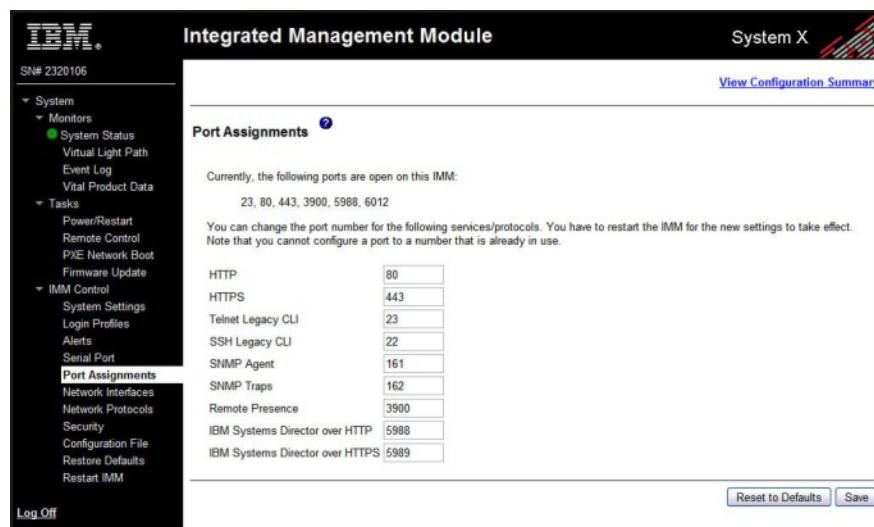
Digite a sequência de teclas de saída para retornar à interface da linha de comandos. Nesse exemplo, pressione Esc e, em seguida, digite q.

Voltar para o console LegacyCLI....

Configurando designações de porta

Para alterar os números de porta de serviços do IMM, conclua as etapas a seguir:

1. Efetue login no IMM no qual você deseja configurar as designações de porta. Para obter mais informações, consulte Capítulo 2, “Abrindo e usando a interface da web do IMM”, na página 11.
2. Na área de janela de navegação, clique em **Designações de Porta**. É exibida uma página semelhante à da ilustração a seguir.



3. Use as informações a seguir para designar valores para os campos:

HTTP Esse é o número da porta para o servidor HTTP do IMM. O número da porta padrão é 80. Os outros valores válidos estão no intervalo de 1 a 65535. Se você alterar esse número de porta, deverá incluir esse número, precedido por dois-pontos, no final do endereço da web. Por exemplo, se a porta HTTP for alterada para 8500, digite `http://hostname:8500/` para abrir a interface da web do IMM. Observe que você deve digitar o prefixo `http://` antes do endereço IP e do número da porta.

HTTPS

Esse é o número da porta que é usada para o tráfego HTTPS (SSL) da interface da web. O valor padrão é 443. Os outros valores válidos estão no intervalo de 1 a 65535.

CLI Legada Telnet

Esse é o número da porta da CLI Legada para efetuar login usando o serviço Telnet. O valor padrão é 23. Os outros valores válidos estão no intervalo de 1 a 65535.

CLI Legada SSH

Esse é o número da porta configurada para CLI Legada para efetuar login usando o SSH. O padrão é 22.

Agente do SNMP

Esse é o número da porta do agente do SNMP executado no IMM. O valor padrão é 161. Os outros valores válidos estão no intervalo de 1 a 65535.

Traps SNMP

Esse é o número da porta usado para traps SNMP. O valor padrão é 162. Os outros valores válidos estão no intervalo de 1 a 65535.

Presença Remota

Esse é o número da porta que o recurso de controle remoto usa para visualizar e interagir com o console do servidor. O padrão é 3900 para servidores torre e montado em rack.

Nota: O recurso Teclado, Vídeo e Mouse Simultâneos (cKVM) no BladeCenter requer que o número da porta seja 2068. Não altere este número de porta em um servidor blade.

IBM Systems Director sobre HTTP

Esse é o número da porta que o IBM Systems Director usa para interagir com o console do servidor. O padrão é 5988.

IBM Systems Director sobre HTTPS

Esse é o número da porta que o IBM Systems Director usa para interagir com o console do servidor por meio de SSL. O padrão é 5989.

Os números de porta a seguir são reservados e só podem ser usados para os serviços correspondentes.

Tabela 3. Números de porta reservados

Número da porta	Serviços usados para
427	SLP
7070 a 7077	Gerenciamento de partições

4. Clique em **Salvar**.

Configurando as interfaces de rede

Na página Interfaces de Rede, é possível definir o acesso ao IMM, configurando uma conexão Ethernet com o IMM. Para definir a configuração de Ethernet para o IMM, modifique as configurações nas áreas Ethernet, IPv4 ou IPv6 da página Interfaces de Rede conforme necessário. As configurações em cada área são descritas nas seções a seguir.

Nota: Os valores na imagem a seguir são exemplos. Suas configurações serão diferentes.

The screenshot shows the 'Ethernet' configuration page. At the top, there's a section for the Ethernet interface, which is currently 'Enabled'. Below this, there's a checkbox for 'IPv6 Enabled' which is checked. The 'Hostname' field contains 'IMM-001A64E604D5', and the 'Domain name' field is empty. The 'DDNS Status' is set to 'Enabled', and the 'Domain Name Used' is set to 'DHCP'. There are links for 'Advanced Ethernet Setup' and 'View Automatic Configuration'. Below the Ethernet section, there's a section for 'IPv4' configuration. It has a dropdown for 'DHCP' set to 'Try DHCP server. If it fails, use static IP config.'. Below this, there's a note: '*** The IP configuration for this interface is assigned by a DHCP server. Follow the link *** "IP Configuration Assigned by DHCP Server" to see the assigned configuration.' Underneath, there's a 'Static IP Configuration' section with fields for 'IP address' (192.168.70.125), 'Subnet mask' (255.255.255.0), and 'Gateway address' (0.0.0.0). Below this, there's a link 'IP Configuration Assigned by DHCP Server'. At the bottom, there's a section for 'IPv6' configuration. It shows the 'Link local address' as 'fe80::21a:64ff:fe66:4d5'. There are checkboxes for 'IPv6 static IP configuration' (Disabled), 'DHCPv6' (Enabled), and 'Stateless Auto-configuration' (Enabled). There is also a link 'View Automatic Configuration'.

Para ver um resumo de todas as definições de configuração, clique em **Visualizar Resumo da Configuração** nas páginas Interfaces de Rede. Antes de configurar as definições na página Interfaces de Rede, revise as informações nas seções a seguir,

Nota: Você também pode configurar a conexão de rede do IMM por meio do utilitário de configuração. Para obter mais informações, consulte “Configurando a Conexão de Rede do IMM por meio do Utilitário de Configuração do IBM System x Server Firmware” na página 11.

Definindo as configurações de Ethernet

As configurações a seguir podem ser modificadas na área Ethernet da página Interfaces de Rede.

Interface

Use esse campo para ativar ou desativar essa interface de rede. Para permitir conexões de rede por meio dessa interface de rede, selecione **Ativado**.

IPv6 Ativado

Use essa caixa de seleção para ativar ou desativar o suporte IPv6 no IMM.

Nota: Se você desmarcar a caixa de seleção **IPv6 Ativado**, a caixa de seleção **Ocultar todos os campos de configuração do IPv6 quando o IPv6 estiver desativado** será exibida. Se a nova caixa de seleção estiver marcada, a área do IPv6 na página Interfaces de Rede estará oculta na interface da web.

Nome do Host

Use esse campo para definir um nome de host exclusivo para o subsistema do IMM. É possível digitar no máximo 63 caracteres nesse campo. O nome do host pode consistir apenas em caracteres alfanuméricos, hífens e sublinhados.

Nota: O nome do host por padrão é IMM-, seguido pelo endereço MAC gravado.

Nome de domínio

Use esse campo para definir um nome de domínio DNS.

Status do DDNS

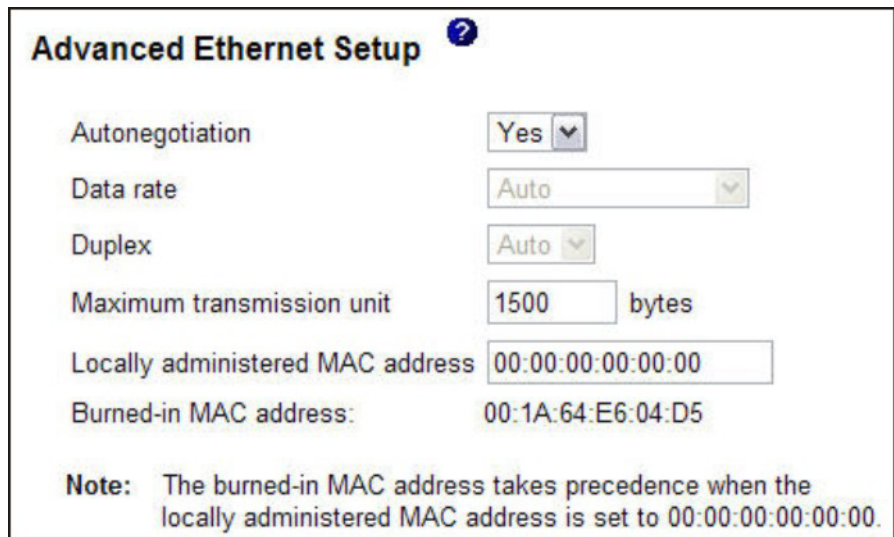
Use esse campo para ativar ou desativar o DNS Dinâmico (DDNS). O DDNS permite que o IMM notifique um servidor DNS para alterar, em tempo real, a configuração do DNS ativo de seus nomes de host configurados, endereços ou outras informações armazenadas no DNS. Quando o DDNS é ativado, IMM notifica o servidor DNS do endereço IP que foi recebido de um servidor DHCP ou por meio de autoconfiguração.

Nome de Domínio Usado

Use esse campo para selecionar se o nome de domínio DHCP ou designado manualmente é enviado para o DNS quando o DDNS é ativado. O valor será configurado como DHCP ou Manual.

Configuração de Interface Avançada

Clique nesse link para abrir a página Configuração de Interface Avançada, que é semelhante à imagem a seguir.



The screenshot shows the 'Advanced Ethernet Setup' configuration page. It includes several settings: Autonegotiation set to 'Yes', Data rate set to 'Auto', Duplex set to 'Auto', Maximum transmission unit set to '1500 bytes', Locally administered MAC address set to '00:00:00:00:00:00', and Burned-in MAC address set to '00:1A:64:E6:04:D5'. A note at the bottom states: 'Note: The burned-in MAC address takes precedence when the locally administered MAC address is set to 00:00:00:00:00:00.'

Nessa página, é possível visualizar e alterar configurações adicionais da interface. A tabela a seguir descreve as configurações na página Configuração Ethernet Avançada.

Tabela 4. Configurações na página Configuração Ethernet Avançada

Configuração	Função
Negociação automática	Use essa configuração para escolher se as definições Taxa de dados e Rede duplex são configuráveis ou não. Se a Negociação Automática estiver configurada como Sim , as definições Taxa de dados e Duplex estarão configuradas como Auto e não serão configuráveis. Se a Negociação Automática estiver configurada como Não , o usuário poderá configurar as definições Taxa de dados e Duplex.
Taxa de dados	Use esse campo para especificar a quantidade de dados a serem transferidos por segundo por meio de sua conexão de LAN. Para configurar a taxa de dados, selecione a taxa de transferência de dados em Megabits (Mb) que corresponde à sua capacidade de rede. Para detectar a taxa de transferência de dados automaticamente, selecione Auto .
Duplex	Use esse campo para especificar o tipo de canal de comunicação que é utilizado em sua rede. Para configurar o modo duplex, selecione Full ou Half . Full duplex permite que dados sejam transferidos em ambas as direções de uma vez. Um canal half duplex permite que dados sejam transferidos em uma direção ou em outra, mas não em ambas ao mesmo tempo. Para detectar o tipo duplex automaticamente, selecione Auto .
Unidade de transmissão máxima (MTU)	Use esse campo para especificar o tamanho máximo de um pacote (em bytes) para sua interface de rede. Para configurar o valor de MTU, insira o número desejado no campo de texto. Para Ethernet, o intervalo válido de MTU é de 68 a 1.500.
Endereço MAC administrado localmente	Use esse campo para especificar um endereço físico para esse subsistema do IMM. Se um valor for especificado, o endereço localmente administrado substituirá o endereço MAC gravado. O endereço localmente administrado deve ser um valor hexadecimal entre 000000000000 e FFFFFFFF. Esse valor deve estar no formato XX:XX:XX:XX:XX:XX, em que X é um número entre 0 e 9 e de A a F. O IMM não permite o uso de um endereço multicast. Um endereço multicast tem o bit menos significativo do primeiro byte configurado como 1. Portanto, o primeiro byte deve ser um número par.
Endereço MAC gravado	O endereço MAC gravado é um endereço físico exclusivo designado ao IMM pelo fabricante.

Definindo as configurações de IPv4

As configurações a seguir podem ser modificadas na área IPv4 da página Interfaces de Rede.

DHCP Use esse campo para especificar se você deseja que as definições de TCP/IP da porta Ethernet do subsistema do IMM sejam configuradas por meio de um servidor de Protocolo de Configuração de Host Dinâmico (DHCP) em sua rede. Para usar a configuração DHCP, selecione **Ativado - Obter configuração de IP do servidor DHCP**. Para configurar suas definições de TCP/IP manualmente, selecione **Desativado - Usar configuração de IP estático**. Se você quiser tentar um servidor DHCP e, em seguida, reverter para a configuração de IP estático se um servidor DHCP não puder ser atingido, selecione **Tentar servidor DHCP. Se falhar, usar a configuração de IP estático**.

Se a configuração IP for designada por um servidor DHCP, clique no link **Configuração de IP Designada pelo servidor DHCP** para visualizar os detalhes de configuração.

Nota:

1. Deve haver um servidor DHCP acessível, ativo e configurado em sua rede se você selecionar a opção **Ativado - Obter a configuração de IP do servidor DHCP**.
2. A configuração designada por um servidor DHCP substituirá qualquer configuração de IP estático.
3. A opção **Tentar servidor DHCP. Se falhar, usar a configuração de IP estático** não é suportada em todos os IMM.

Configuração de IP Estático

Os campos a seguir contêm a configuração de IP estático para esta interface. Essas configurações só serão usadas se o DHCP estiver desativado. Se o DHCP estiver ativado, a configuração de IP dinâmico designada pelo servidor DHCP substituirá essas configurações estáticas.

- **Endereço IP:** Use esse campo para definir o endereço IP do subsistema do IMM acessado por meio dessa interface de rede. Para configurar o endereço IP, digite o endereço na caixa de texto. O endereço IP deve conter quatro números inteiros (de 0 a 255) separados por pontos e sem espaços.

Nota: O valor padrão para esse campo é 192.168.70.125.

- **Máscara de sub-rede:** Use esse campo para definir a máscara de sub-rede que será usada pelo subsistema do IMM. Para definir a máscara de sub-rede, digite a máscara de bits na caixa de texto. A máscara de sub-rede contém quatro números inteiros (de 0 a 255) separados por pontos e sem espaços. Os bits que são definidos de forma contígua começando com o bit mais à esquerda. Por exemplo, 0.255.0.0 não é uma máscara de sub-rede válida. Esse campo não pode ser configurado como 0.0.0.0 ou 255.255.255.255.

Nota: O padrão para esse campo é 255.255.255.0.

- **Endereço do gateway:** Use esse campo para identificar o endereço IP de seu gateway padrão. Para configurar o endereço do gateway, digite o endereço na caixa de texto. O endereço do gateway deve conter quatro números inteiros (de 0 a 255) separados por pontos e sem espaços ou pontos consecutivos.

Nota: O padrão para esse campo é 0.0.0.0.

Configuração de IP Designada pelo Servidor DHCP

Clique nesse link para visualizar a configuração de IP designada pelo servidor DHCP. A página Configuração de IP Designada pelo Servidor DHCP, semelhante à imagem a seguir, é exibida.

Nota: Essa opção está disponível somente quando o DHCP está ativado.

IP Configuration Assigned by DHCP Server ?	
Host name	IMM-001A64E604D5
IP address	9.44.146.191
Gateway address	9.44.146.129
Subnet mask	255.255.255.128
Domain name	raleigh.ibm.com
DNS Server IP Addresses	
Primary	9.0.6.1
Secondary	9.0.7.1
Tertiary	N/A

Definindo as configurações de IPv6

As configurações a seguir podem ser modificadas na área IPv6 da página Interfaces de Rede.

Nota: Pelo menos uma das opções de configuração de IPv6 descritas nesta seção (Configuração Estática de IPv6, DHCPv6 ou Configuração Automática Stateless) deve ser ativada.

Endereço local de link

O endereço local de link é o endereço IPv6 que é designado ao IMM. O endereço local de link tem um formato semelhante ao seguinte exemplo:
fe80::21a:64ff:fee6:4d5

Configuração Estática de IPv6

Use esse campo para ativar ou desativar as definições de configuração estática para IPv6. Quando a caixa de seleção **Configuração Estática de IPv6** é selecionada, as seguintes opções estão disponíveis:

- **Endereço IP:** Use esse campo para definir o endereço IPv6 do IMM que é acessado por meio dessa interface de rede. Para configurar o endereço IP, digite o endereço IPv6 na caixa de texto. O valor nesse campo deve ser um endereço IPv6 válido.

Nota: O padrão para esse campo é 0::0.

- **Comprimento de prefixo do endereço (1 a 128):** Use esse campo para configurar o comprimento de prefixo para o endereço IPv6 estático.

- **Rota padrão:** Use esse campo para configurar o endereço IPv6 da sua rota padrão. Para configurar a rota padrão, digite o endereço IPv6 na caixa correspondente. O valor nesse campo deve ser um endereço IPv6 válido.

Nota: O valor padrão para esse campo é 0::0.

DHCPv6

Use esse campo para ativar ou desativar a configuração designada DHCPv6 no IMM.

Configuração Automática Stateless

Use esse campo para ativar ou desativar a configuração automática stateless no IMM.

Visualizar Configuração Automática (link)

Para visualizar a configuração de IPv6 designada pelo servidor DHCP, clique nesse link. A página Configuração Automática de IPv6 é exibida.

Configurando protocolos de rede

Na página Protocolos de Rede, você pode executar as funções a seguir:

- Configurar o Protocolo Simples de Gerenciamento de Rede (SNMP)
- Configurar o Sistema de Nomes de Domínio (DNS)
- Configurar o Protocolo Telnet
- Configurar o Protocolo Simples de Transporte de Correio (SMTP)
- Configurar o Protocolo LDAP
- Configurar o Protocolo de Localização de Serviço (SLP)

As mudanças nas configurações do protocolo de rede requerem que o IMM seja reiniciado para que as mudanças entrem em vigor. Se você estiver alterando mais de um protocolo, poderá aguardar até que todas as mudanças de protocolo tenham sido feitas e salvas antes de reiniciar o IMM.

Configurando o SNMP

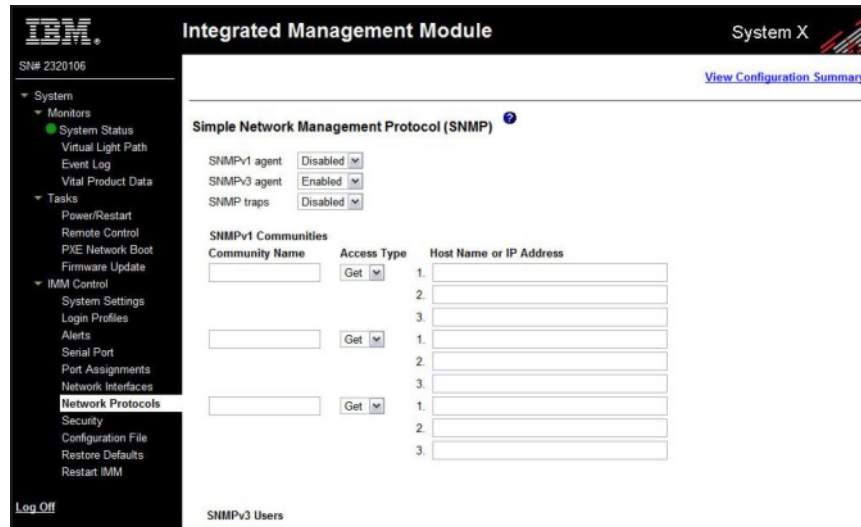
É possível usar o agente do SNMP para coletar informações e controlar o servidor. O IMM também pode ser configurado para enviar alertas SNMP para os nomes de host ou endereços IP configurados.

Nota:

1. O IMM fornece dois arquivos Management Information Base (MIB) para uso com aplicativos SNMP. Os arquivos MIB estão incluídos nos pacotes de atualização de firmware do IMM.
2. O IMM suporta os padrões SNMPv1 e SNMPv3.

Para configurar o SNMP, conclua as etapas a seguir:

1. Efetue login no IMM no qual você deseja configurar o SNMP. Para obter mais informações, consulte Capítulo 2, “Abrindo e usando a interface da web do IMM”, na página 11.
2. Na área de janela de navegação, clique em **Protocolos de Rede**. É exibida uma página semelhante à da ilustração a seguir.



3. Selecione **Ativado** no campo **Agente do SNMPv1** ou **Agente do SNMPv3**.

Nota: Se você ativou o agente SNMPv3, deverá configurar as definições de SNMPv3 para perfis de login ativos para que a interação entre o gerenciador e o agente do SNMPv3 funcione corretamente. É possível configurar essas definições na parte inferior da configurações de perfil de login individual na página Perfis de Login (consulte “Criando um perfil de login” na página 25 para obter mais informações). Clique no link para o perfil de login a ser configurado, role para a parte inferior da página e, em seguida, clique na caixa de seleção **Configurar Usuário SNMPv3**.

4. Selecione **Ativado** no campo **Traps SNMP** para encaminhar alertas para comunidades SNMP em sua rede. Para ativar o agente do SNMP, os critérios a seguir devem ser atendidos:
 - Um contato do sistema deve ser especificado na página Configurações do Sistema. Para obter informações sobre as definições da página Configurações do Sistema, consulte “Configurando informações do sistema” na página 20.
 - O local do sistema deve ser especificado na página Configurações do Sistema.
 - Pelo menos um nome de comunidade deve ser especificado.
 - Pelo menos um endereço IP ou nome de host válido (se o DNS estiver ativado) deve ser especificado para essa comunidade.

Nota: Os receptores de alertas cujo método de notificação seja SNMP não poderão receber alertas a menos que os campos **Agente SNMPv1** ou **Agente SNMPv3** e **Traps SNMP** estejam configurados como **Ativado**.

5. Configure uma comunidade para definir o relacionamento administrativo entre agentes SNMP e gerenciadores SNMP. Você deve definir pelo menos uma comunidade. Cada definição de comunidade consiste nos seguintes parâmetros:
 - Nome da Comunidade
 - Tipo de Acesso
 - Endereço IP

Se qualquer um desses parâmetros não estiver correto, o acesso de gerenciamento de SNMP não será concedido.

Nota: Se uma janela de mensagem de erro for exibida, faça os ajustes necessários nos campos listados na janela de erro. Em seguida, role para a parte inferior da página e clique em **Salvar** para salvar suas informações corretas. Você deve configurar pelo menos uma comunidade para ativar esse agente do SNMP.

6. No campo **Nome da Comunidade**, insira um nome ou sequência de autenticação para especificar a comunidade.
7. No campo **Tipo de Acesso**, selecione um tipo de acesso. Selecione **Trap** para permitir que todos os hosts na comunidade recebam traps; selecione **Get** para permitir que todos os hosts na comunidade recebam traps e consultem objetos MIB; selecione **Set** para permitir que todos os hosts na comunidade recebam traps, consultem e configurem objetos MIB.
8. No campo **Nome do Host ou Endereço IP** correspondente, insira o nome do host ou endereço IP de cada gerenciador de comunidade.
9. Role para a parte inferior da página e clique em **Salvar**.
10. Na área de janela de navegação, clique em **Reiniciar IMM** para ativar as mudanças.

Configurando o DNS

É possível configurar o Sistema de Nomes de Domínio (DNS) para especificar se endereços adicionais do servidor DNS devem ser incluídos na ordem de procura para resolução de endereço de nome de host para IP. A consulta de DNS é sempre ativada, e outros endereços DNS podem ser designados automaticamente pelo servidor DHCP quando a funcionalidade DHCP está ativada.

Para que endereços de DNS adicionais sejam ativados, pelo menos um deles deve ser um valor diferente de zero. Os servidores DNS adicionais são incluídos no início da lista de procura, para que a consulta de nome do host seja feita nesses servidores antes que ela ocorra em um servidor DNS que é designado automaticamente por um servidor DHCP.

Para configurar o DNS, conclua as etapas a seguir:

1. Efetue login no IMM no qual você deseja configurar o DNS. Para obter mais informações, consulte Capítulo 2, “Abrindo e usando a interface da web do IMM”, na página 11.
2. Na área de janela de navegação, clique em **Protocolos de Rede** e role para baixo até a área **Designações de Endereço do Sistema de Nomes de Domínio (DNS)** da página. Uma seção da página semelhante à da ilustração a seguir é exibida.

Order	IPv4	IPv6
Primary		
Secondary		
Tertiary		

3. Se um servidor (ou servidores) DNS estiver disponível em sua rede, selecione **Ativado** no campo **DNS**. O campo **DNS** especifica se você usa um servidor DNS em sua rede para converter nomes de host em endereços IP.
4. Se você tiver endereços do servidor DNS IPv4 e IPv6, selecione **IPv4** ou **IPv6** na lista de **Servidores DNS Preferenciais** para especificar quais endereços do servidor são preferenciais.
5. Se você ativou o DNS, use o s campos de texto Primário, Secundário e Terciário para especificar os endereços IP de até seis servidores DNS em sua rede. Para configurar os três endereços do servidor DNS IPv4 ou IPv6, digite os endereços nos campos de texto aplicáveis. Certifique-se de que os endereços IPv4 ou IPv6 estejam nos formatos válidos.
6. Role para a parte inferior da página e clique em **Salvar**.
7. Na área de janela de navegação, clique em **Reiniciar IMM** para ativar as mudanças.

Configurando Telnet

Para configurar o Telnet, conclua as seguintes etapas:

1. Efetue login no IMM no qual você deseja configurar o Telnet. Para obter mais informações, consulte Capítulo 2, “Abrindo e usando a interface da web do IMM”, na página 11.
2. Na área de janela de navegação, clique em **Protocolos de Rede** e role para baixo para a área **Protocolo Telnet** da página. É possível configurar o número máximo de usuários Telnet simultâneos, ou desativar o acesso Telnet.
3. Role para a parte inferior da página e clique em **Salvar**.
4. Na área de janela de navegação, clique em **Reiniciar IMM** para ativar as mudanças.

Configurando o SMTP

Para especificar o endereço IP ou nome do host do servidor Protocolo Simples de Transporte de Correio (SMTP), conclua as etapas a seguir.

1. Efetue login no IMM no qual você deseja configurar o SMTP. Para obter mais informações, consulte Capítulo 2, “Abrindo e usando a interface da web do IMM”, na página 11.
2. Na área de janela de navegação, clique em **Protocolos de Rede** e role para baixo para a área **SMTP** da página.
3. No campo **Nome do Host ou Endereço IP do Servidor SMTP**, 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.
4. Role para a parte inferior da página e clique em **Salvar**.
5. Na área de janela de navegação, clique em **Reiniciar IMM** para ativar as mudanças.

Configurando o LDAP

Usando um servidor LDAP, o IMM pode autenticar um usuário consultando ou procurando um diretório LDAP em um servidor LDAP, em vez de passar pelo banco de dados de usuário local. Em seguida, o IMM pode autenticar remotamente qualquer acesso do usuário por meio de um servidor LDAP central. Isso requer o suporte a clientes LDAP no IMM. Você também pode designar níveis de autoridade de acordo com as informações encontradas no servidor LDAP.

É possível também usar o LDAP para designar usuários e IMMs aos grupos e executar a autenticação do grupo, além da autenticação normal do usuário (verificação de senha). Por exemplo, um IMM pode ser associado a um ou mais grupos; e um usuário só aprovaria a autenticação do grupo se o usuário pertencesse a pelo menos um grupo que está associado ao IMM.

As informações sobre como configurar os dois servidores LDAP a seguir são fornecidas nesta seção:

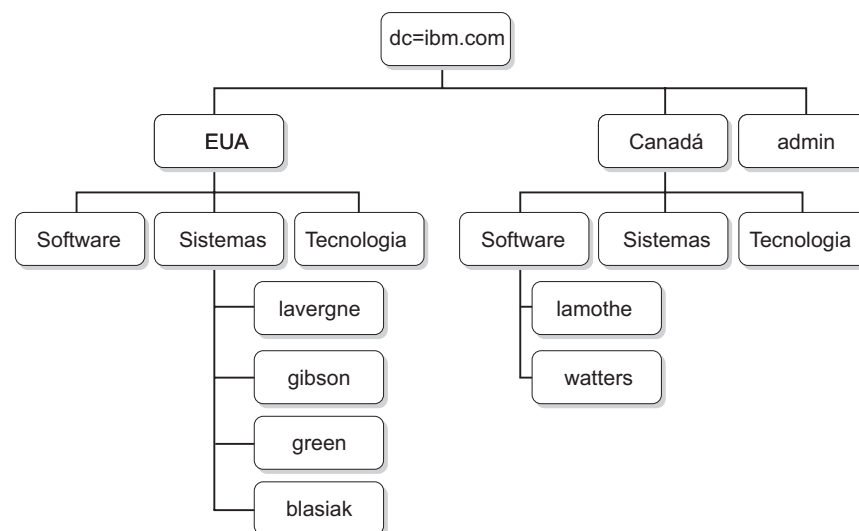
- Novell eDirectory versão 8.7.1
- Microsoft Windows Server 2003 Active Directory

Exemplo de esquema do usuário

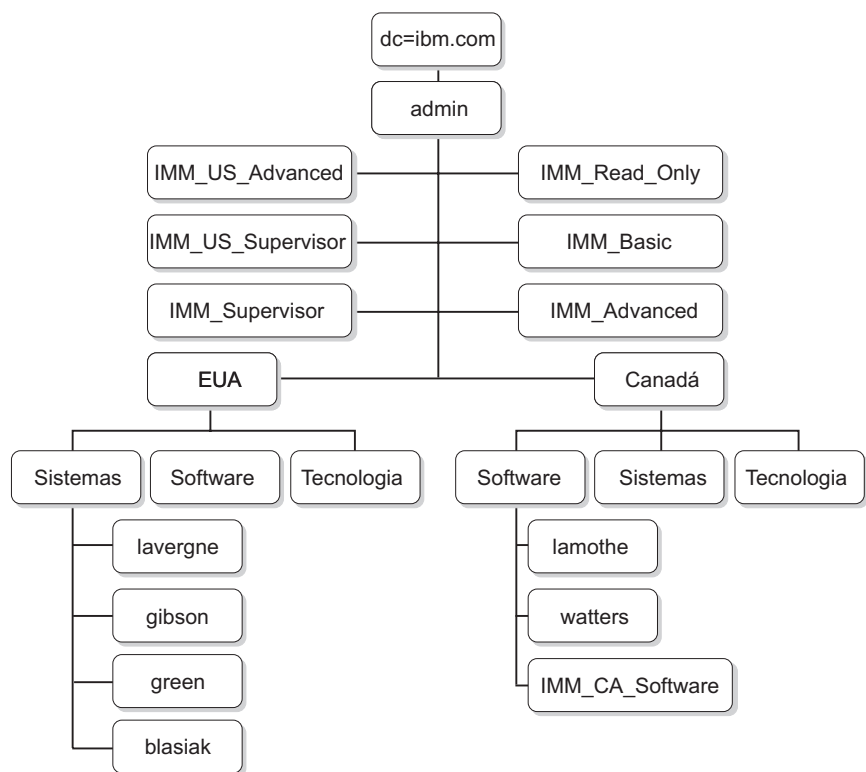
Um exemplo de esquema de usuário simples é descrito nesta seção. Esse exemplo de esquema é usado em todo o documento para ilustrar a configuração no cliente LDAP e no servidor LDAP.

A raiz do exemplo de esquema do usuário está em um componente de domínio chamado `ibm.com`. Ou seja, cada objeto nessa árvore tem um nome distinto raiz igual a `dc=ibm,dc=com`. Agora suponha que essa árvore represente uma empresa que deseja classificar usuários e grupos de usuários com base no país e na organização. A hierarquia seria raiz → país → organização → pessoas.

A ilustração a seguir mostra uma visualização simplificada do esquema usado neste documento. Observe o uso de uma conta de usuário (`userid=admin`) diretamente abaixo da raiz. Este é o administrador.



A ilustração a seguir mostra a inclusão de grupos de usuários. Seis grupos de usuários são definidos e incluídos no primeiro nível, e outro grupo de usuários é incluído na organização `Software`, no país `Canadá`.



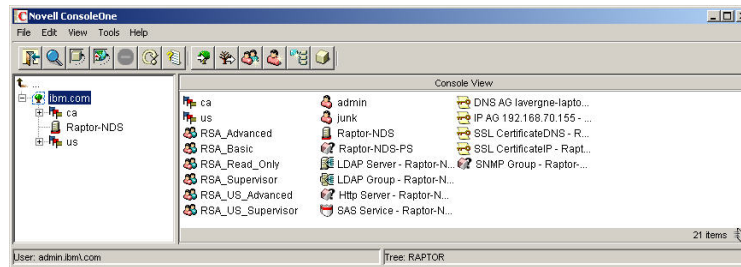
Os usuários e grupos de usuários associados em Tabela 5 são usados para concluir o esquema.

Tabela 5. Mapeamento de Usuário para Grupo

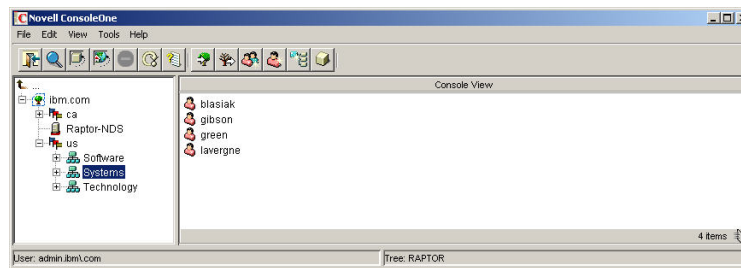
Nome distinto do usuário	Associação de grupo
cn=lavergne, o=Systems, c=us, dc=ibm.com	cn=IMM_Supervisor, dc=ibm.com cn=IMM_US_Supervisor, dc=ibm.com
cn=blasiak, o=Systems, c=us, dc=ibm.com	cn=IMM_US_Advanced, dc=ibm.com
cn=gibson, o=Systems, c=us, dc=ibm.com	cn=IMM_Basic, dc=ibm.com
cn=green, o=Systems, c=us, dc=ibm.com	cn=IMM_Read_Only, dc=ibm.com
cn=watters, o=Systems, c=ca, dc=ibm.com	cn=IMM_CA_Software, o=Software, c=ca, dc=ibm.com
cn=lamothe, o=Systems, c=ca, dc=ibm.com	cn=IMM_CA_Software, o=Software, c=ca, dc=ibm.com

Visualização de Esquema do Novell eDirectory

Usando a ferramenta Novell ConsoleOne, o esquema descrito em “Exemplo de esquema do usuário” na página 47 foi obtido no Novell eDirectory. A ilustração a seguir mostra a visualização de nível superior do esquema, conforme vista na ferramenta ConsoleOne.



A ilustração a seguir captura os usuários em o=Systems, c=us, dc=ibm.com.



Associação de grupo

O Novell eDirectory utiliza um atributo chamado **GroupMembership** para identificar os grupos dos quais um usuário é membro. A classe de objeto de Usuário utiliza especificamente esse atributo. O cliente LDAP usa um valor padrão **memberOf** na sua solicitação de procura ao servidor LDAP ao consultar os grupos dos quais um usuário é membro.

É possível configurar o cliente LDAP para consultas de associação usando um dos métodos a seguir:

- Configure o valor **GroupMembership** no campo **Atributo de Procura de Grupo** no cliente LDAP.
- Crie um mapeamento de atributo entre **GroupMembership** e **memberOf** no servidor LDAP Novell eDirectory.

Conclua as etapas a seguir para configurar o atributo padrão no cliente LDAP:

1. Na interface da web do IMM, na área de janela de navegação esquerda, clique em **Protocolos de Rede**.
2. Role para a área **Atributos de Procura LDAP**.
3. No campo **Atributo de Procura de Grupo**, digite o atributo padrão que você deseja.

Se o campo **Atributo de Procura de Grupo** estiver em branco, ele será padronizado como **memberOf** e você precisará configurar o servidor Novell eDirectory para mapear o atributo **GroupMembership** para **memberOf**. Conclua as etapas a seguir para configurar o servidor Novell eDirectory para mapear o atributo **GroupMembership** para **memberOf**.

1. Usando a ferramenta ConsoleOne, clique com o botão direito do mouse no ícone **Grupo LDAP** e clique em **Propriedades**. A janela Propriedades do Grupo LDAP é aberta.
2. Clique na guia **Mapeamentos de Atributo**.
3. Clique em **Incluir** e, em seguida, crie um mapeamento entre **Associação ao Grupo** e **memberOf**.

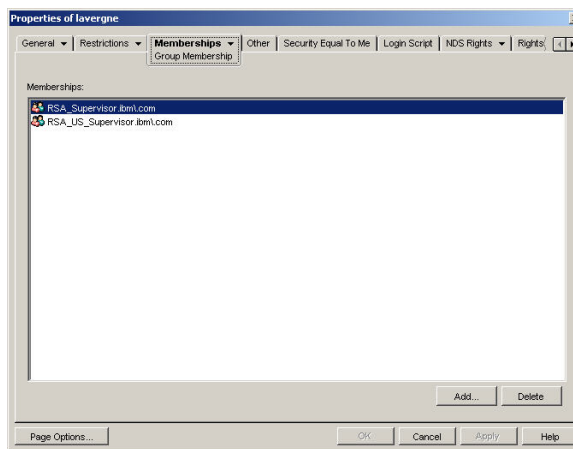
4. Clique em **OK**. Uma página que mostra as propriedades do grupo LDAP é aberta.

Incluindo usuários nos grupos de usuários

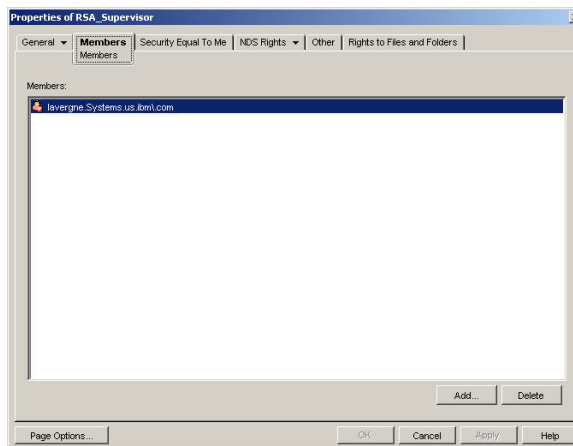
É possível incluir usuários nos grupos de usuários apropriados, ao incluir os grupos no perfil de um usuário, ou incluir usuários no perfil de um grupo. O resultado final é idêntico.

Por exemplo, no exemplo de esquema de usuário anterior, o usuário **lavergne** é membro de **IMM_US_Supervisor** e **IMM_Supervisor**. Utilizando uma ferramenta do navegador, como Novell ConsoleOne, é possível verificar o esquema (clique duas vezes em **usuário lavergne** e selecione a guia **Associações**).

É exibida uma página semelhante à da ilustração a seguir.



Da mesma forma, se as propriedades do grupo **IMM_Supervisor** forem exibidas, e você selecionar a guia **Membros**, uma página semelhante à da ilustração a seguir será aberta.

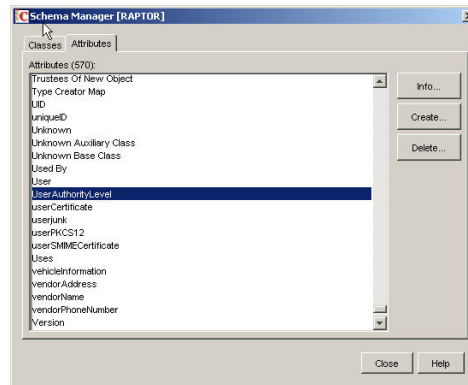


Níveis de autoridade

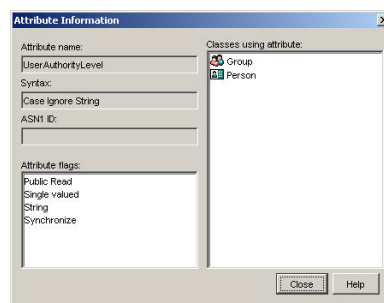
Para usar o recurso de níveis de autoridade, use o ConsoleOne para criar um novo atributo com o rótulo **UserAuthorityLevel** no Novell eDirectory. Esse novo atributo será usado para suportar níveis de autoridade.

1. Na ferramenta Novell ConsoleOne, clique em **Ferramentas > Schema Manager**.

2. Clique na guia **Atributos** e clique em **Criar**.
3. Rotule o atributo **UserAuthorityLevel**. Deixe **ID ASN1** em branco ou consulte o administrador do LDAP para determinar o valor a ser usado. Clique em **Avançar**.
4. Configure a sintaxe como **Sequência Ignora Maiúsculas e Minúsculas**. Clique em **Avançar**.
5. Configure os sinalizadores conforme aplicável. Consulte o administrador do LDAP para certificar-se de que eles estejam configurados corretamente. Clique na caixa de seleção **Leitura Pública**; em seguida, clique em **Avançar**.
6. Clique em **Concluir**. Uma página semelhante à da ilustração a seguir é aberta.



7. Retorne para a janela Schema Manager e clique na guia **Classes**.
8. Clique na classe **Pessoa** e clique em **Incluir**. Observe que você pode usar a classe do objeto de Usuário.
9. Role para baixo até o atributo **UserAuthorityLevel**, selecione-o e inclua-o nos atributos para essa classe. Clique em **OK**.
10. Clique na classe **Grupo** e clique em **Incluir**.
11. Role para baixo até o atributo **UserAuthorityLevel**, selecione-o e inclua-o nos atributos para essa classe. Clique em **OK**.
12. Para verificar se o atributo foi incluído com êxito na classe, na janela Schema Manager, selecione a classe **Atributos**.
13. Role para o atributo **UserAuthorityLevel**; em seguida, clique em **Informações**. Uma página semelhante à da ilustração a seguir é aberta.



Configurando níveis de autoridade

Esta seção explica como interpretar e usar o atributo **UserAuthorityLevel**. O valor designado ao atributo **UserAuthorityLevel** determina as permissões (ou níveis de autoridade) designada a um usuário após uma autenticação bem-sucedida.

O atributo UserAuthorityLevel é lido como uma sequência de bits ou 0s e 1s. Os bits são numerados da esquerda para a direita. O primeiro bit é o da posição 0. O segundo da posição 1, e assim por diante.

A tabela a seguir fornece uma explicação de cada posição de bit.

Tabela 6. Bits de permissão

Posição do Bit	Função	Explicação
0	Negar Sempre	Se configurado, 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	Se configurado, privilégios de administrador foram 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	Se configurado, um usuário terá acesso somente leitura e não poderá executar nenhum procedimento de manutenção (por exemplo, reinicialização, ações remotas ou atualizações de firmware). Nada pode ser modificado, usando salvar, limpar ou restaurar funções. A posição de bit 2 e todos os demais bits são mutuamente exclusivos, com a posição de bit 2 tendo a precedência mais baixa. Se algum outro bit for configurado, esse bit será ignorado.
3	Rede & Segurança	Se configurado, um usuário poderá modificar a configuração nos painéis Segurança, Protocolos de Rede, Interface de Rede, Designações de Porta e Porta Serial.
4	Gerenciamento de Conta do Usuário	Se configurado, um usuário poderá incluir, modificar ou excluir usuários e alterar as Configurações Globais de Login no painel Perfis de Login.
5	Acesso ao Console Remoto	Se configurado, um usuário poderá acessar o console do servidor remoto e modificar a configuração no painel Porta Serial.
6	Acesso ao Console Remoto e Disco Remoto	Se configurado, um usuário poderá acessar o console do servidor remoto e as funções de disco remoto para o servidor remoto. O usuário também pode modificar a configuração no painel Porta Serial.
7	Acesso a Energia/Reinicialização do Servidor Remoto	Se configurado, um usuário poderá acessar as funções de ligação, reinicialização e tempo limite do servidor remoto.

Tabela 6. Bits de permissão (continuação)

Posição do Bit	Função	Explicação
8	Configuração de Adaptador Básica	Se configurado, um usuário poderá modificar parâmetros de configuração nos painéis Configurações do Sistema e Alertas (exclui os parâmetros Contato, Local e Tempo Limite do Servidor).
9	Capacidade para Limpar Logs de Eventos	Se configurado, um usuário poderá 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.
10	Configuração de Adaptador Avançada	Se configurado, um usuário não terá restrições ao configurar o adaptador e terá acesso administrativo ao IMM. O usuário pode executar as seguintes funções avançadas: atualizar o firmware, inicializar a rede PXE, restaurar os padrões de fábrica do adaptador, modificar e restaurar a configuração de adaptador a partir de um arquivo de configuração e reiniciar/reconfigurar o adaptador. Isso exclui as funções de tempo limite e Controle de Energia/Reinicialização do Servidor.
11	Reservado	Essa posição de bit está reservada para uso futuro (atualmente ignorada).
Notas: • Se não forem utilizados bits, o padrão será definido como Somente Leitura para o usuário. • É dada prioridade às permissões de login recuperadas diretamente do registro do usuário. Se o registro do usuário não contiver um nome no campo Atributo de Permissão de Login, será feita uma tentativa de recuperar as permissões do grupo ao qual o usuário pertence e que correspondem ao filtro de grupo. Nesse caso, é designado ao usuário o OR inclusivo de todos os bits para todos os grupos. • Se o bit Negar Sempre (posição de bit zero) for configurado para qualquer um dos grupos, o usuário terá o acesso recusado. O bit Negar Sempre tem precedência sobre todos os bits. • Se um usuário tiver a capacidade de modificar os parâmetros de configuração de adaptador básico, rede, ou relacionado à segurança, você deverá considerar fornecer a esse usuário a capacidade de reiniciar o IMM (posição de bit dez). Sem essa capacidade, um usuário pode ser capaz de alterar um parâmetro; mas, o parâmetro não entrará em vigor.		

A tabela a seguir contém exemplos e suas descrições:

Tabela 7. Exemplo de atributos UserLevelAuthority e descrições

Exemplo de atributo UserLevelAuthority	Descrição
IBMRBSPermissions=010000000000	Acesso de Supervisor (a posição de bit 1 é configurada)

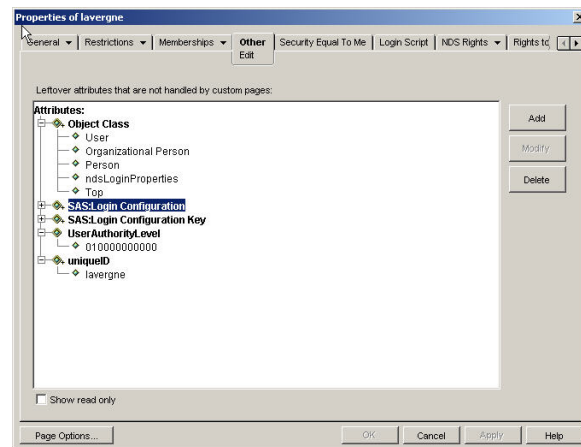
Tabela 7. Exemplo de atributos UserLevelAuthority e descrições (continuação)

Exemplo de atributo UserLevelAuthority	Descrição
IBMRBSPermissions=001000000000	Acesso Somente Leitura (a posição de bit 2 é configurada)
IBMRBSPermissions=100000000000	Sem Acesso (a posição de bit 0 é configurada)
IBMRBSPermissions=000011111100	Todas as autoridades, exceto Configuração de Adaptador Avançada
IBMRBSPermissions=000011011110	Todas as autoridades, exceto acesso a mídia virtual

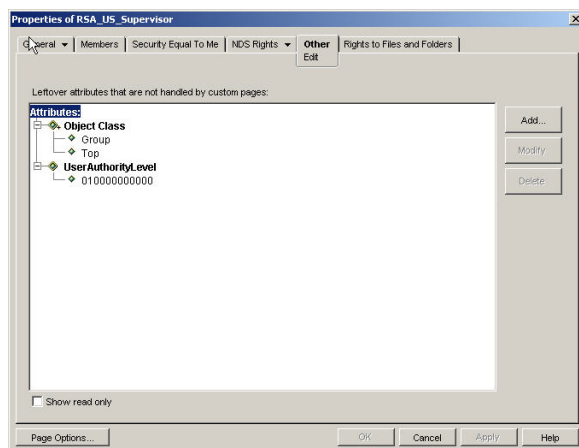
Conclua as etapas a seguir para incluir o atributo UserAuthorityLevel no usuário *lavergne* e em cada um dos grupos de usuários:

1. Clique com o botão direito do mouse no usuário **lavergne** e clique em **Propriedades**.
2. Clique na guia **Outro**. Clique em **Incluir**.
3. Role para baixo até **UserAuthorityAttribute** e clique em **OK**.
4. Preencha o valor que você deseja para o atributo. Por exemplo, se você deseja designar o acesso de Supervisor, configure o atributo como **IBMRBSPermissions=010000000000**. Clique em **OK**.
5. Repita as etapas de 1 a 4 para cada grupo de usuários e configure **UserAuthorityLevel** conforme apropriado.

A ilustração a seguir mostra as propriedades do usuário *lavergne*.



A ilustração a seguir mostra as propriedades de IMM_US_Supervisor.



A tabela a seguir mostra o **UserAuthorityLevel** designado a cada um dos grupos de usuários no exemplo de esquema do usuário.

Tabela 8. Designações UserAuthorityLevel a grupos de usuários

Grupo de Usuários	UserAuthorityLevel	Tradução
IMM_Basic	IBMRBSPermissions=000100000000	Rede e segurança
IMM_CA_Software	IBMRBSPermissions=000101111010	Rede e segurança Acesso ao console remoto e mídia virtual / Acesso a energia e reinicialização do servidor remoto Configuração de adaptador básica Configuração de adaptador avançada
IMM_Advanced	IBMRBSPermissions=000110111100	Rede e segurança Acesso ao console remoto e mídia virtual / Acesso a energia e reinicialização do servidor remoto Configuração de adaptador básica Configuração de adaptador avançada Capacidade para limpar logs de eventos
IMM_Supervisor	IBMRBSPermissions=010000000000	Acesso de Supervisor
IMM_Read_Only	IBMRBSPermissions=001000000000	Acesso somente leitura
IMM_US_Advanced	IBMRBSPermissions=000110111100	Rede e segurança Gerenciamento de conta do usuário Acesso ao console remoto e mídia virtual / Acesso a energia e reinicialização do servidor remoto Configuração de adaptador básica Capacidade para limpar logs de eventos
IMM_US_Supervisor	IBMRBSPermissions=010000000000	Acesso de Supervisor

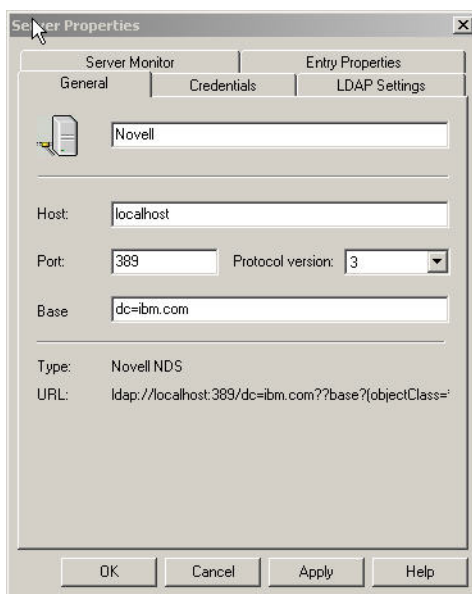
Navegando no servidor LDAP

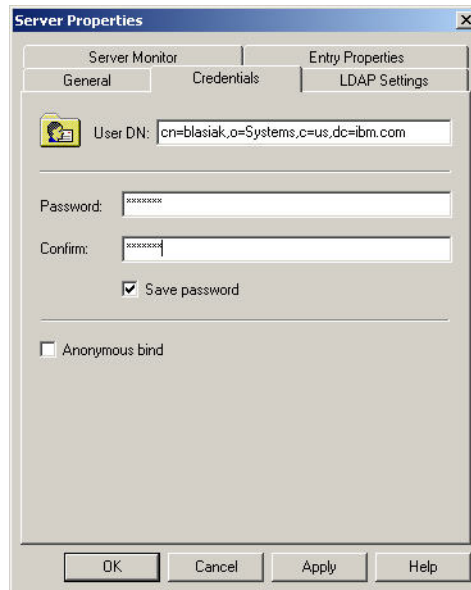
Antes de tentar se conectar do cliente LDAP no IMM com o seu servidor LDAP, conecte-se ao seu servidor LDAP usando um navegador LDAP de terceiros de sua escolha. Por exemplo, há uma ferramenta de procura de diretório disponível em <http://www.ldapbrowser.com>.

Usar o navegador LDAP antes de tentar usar o cliente LDAP do IMM tem as seguintes vantagens:

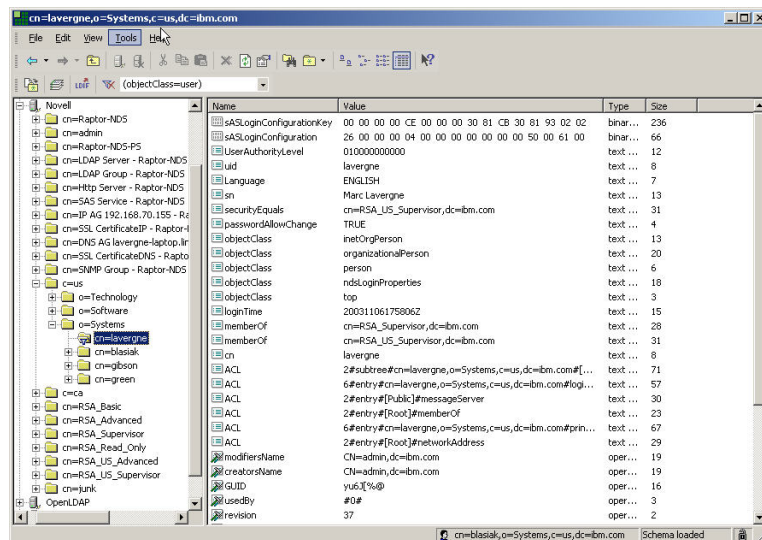
- A capacidade de conectar-se a um servidor usando várias credenciais. Isso mostrará se as contas do usuário no servidor LDAP estão configuradas corretamente. Se você puder conectar-se ao servidor usando o navegador, mas não puder conectar-se ao servidor usando o cliente LDAP do IMM, o cliente LDAP estará configurado incorretamente. Se não for possível conectar-se usando o navegador, você não conseguirá conectar com o cliente LDAP no IMM.
- Depois de conectar-se com êxito ao servidor, será possível navegar pelo banco de dados do servidor LDAP e emitir rapidamente consultas de procura. Isso confirmará se o servidor LDAP está configurado da maneira desejada, com relação ao acesso a diversos objetos. Por exemplo, você pode descobrir que não é possível visualizar um atributo específico ou pode não ver todos os objetos que esperava ver em uma solicitação de procura específica. Isso indica que as permissões designadas aos objetos (por exemplo, o que é visível publicamente ou o que está oculto) não estão configuradas corretamente. Entre em contato com o administrador do servidor LDAP para corrigir o problema. É importante observar que as credenciais que você usa para conexão determinam quais privilégios você terá no servidor.
- Verifique a associação ao grupo para todos os usuários. Verifique o atributo **UserAuthorityLevel** designado a usuários e grupos de usuários.

As ilustrações a seguir mostram várias consultas e resultados da procura feitos para um servidor Novell eDirectory configurado com o “Exemplo de esquema do usuário” na página 47. Nesse caso, a ferramenta do navegador Softerra LDAP foi usada. A conexão inicial com o servidor foi feita com as propriedades e credenciais que são mostradas na ilustração.

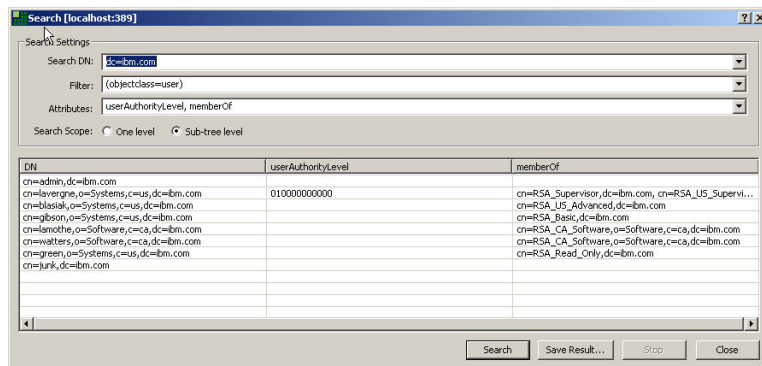




Após a conexão inicial com êxito, a seguinte visualização do esquema no Novell eDirectory é exibida.



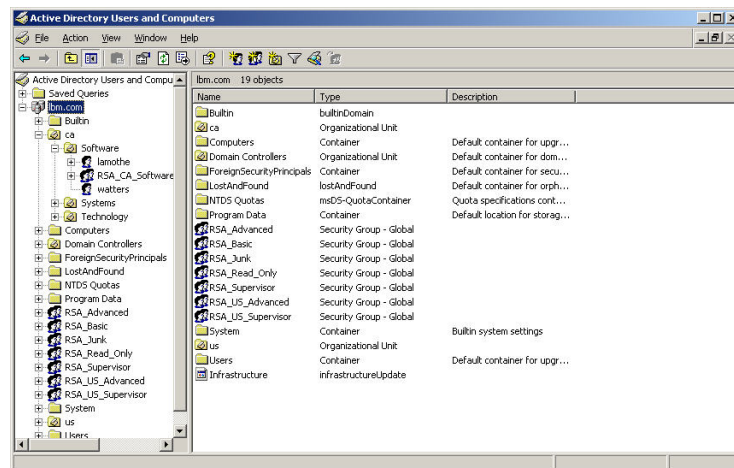
A ilustração a seguir mostra uma consulta de todos os usuários, com uma solicitação para recuperar os atributos **userAuthorityLevel** e **memberOf**.



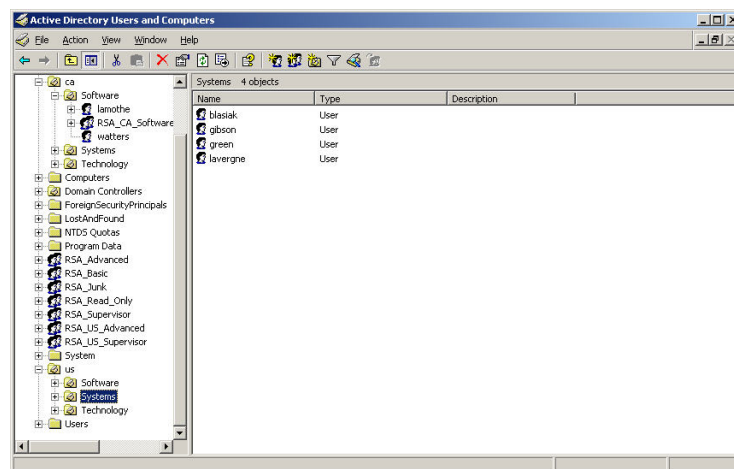
Visualização do esquema do Microsoft Windows Server 2003 Active Directory

Esta seção descreve alguns dos aspectos de configuração relativos à captura de informações no “Exemplo de esquema do usuário” na página 47no Microsoft Windows Server 2003 Active Directory.

A ilustração a seguir mostra a visualização de nível superior do esquema, conforme vista na ferramenta de gerenciamento de Usuários e Computadores do Active Directory.



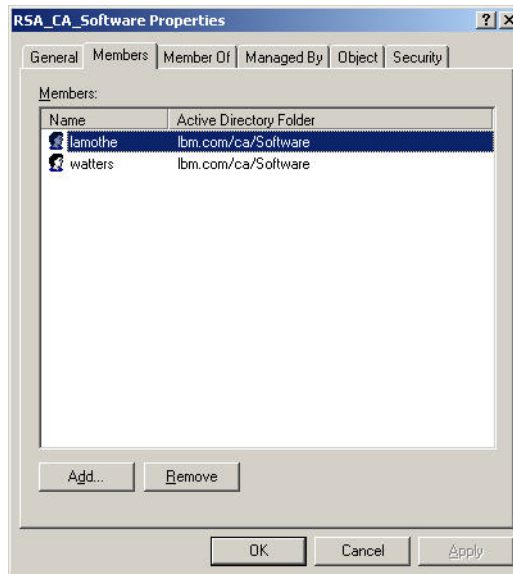
A ilustração a seguir mostra os usuários em ou=Systems, ou=us, dc=ibm, dc=com.



Incluindo usuários em grupos de usuários

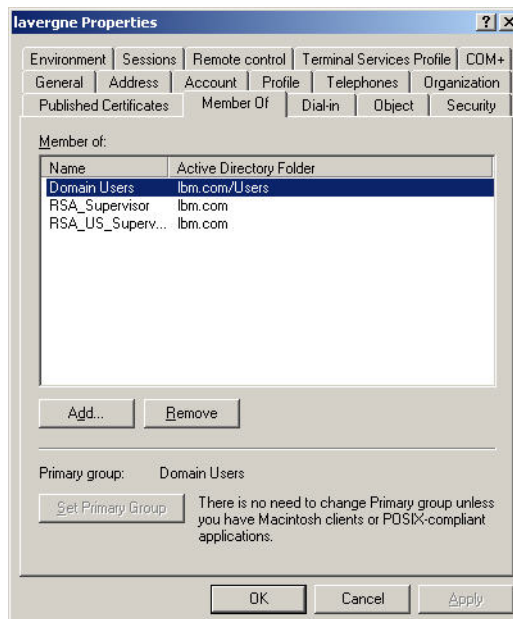
No Active Directory, é possível incluir grupos em um usuário específico, ou incluir usuários em um grupo específico. Clique com o botão direito do mouse no objeto usuário ou grupo de usuários; em seguida, clique em **Propriedades**.

Se você selecionar um grupo de usuários e, em seguida, clicar na guia **Membros**, uma página semelhante à da ilustração a seguir será aberta.



Para incluir ou excluir usuários do grupo de usuários, clique em **Incluir** ou **Remover**.

Se você selecionar um usuário e, em seguida, clicar na guia **MembersOf**, uma página semelhante à da ilustração a seguir será aberta.



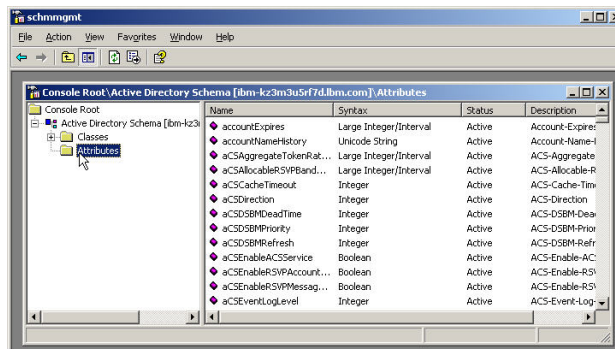
Para incluir ou excluir usuários do grupo de usuários, clique em **Incluir** ou **Remover**.

Níveis de autoridade

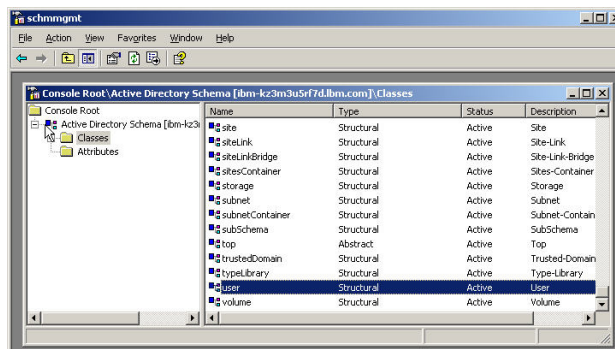
A seção “Níveis de autoridade” na página 50 descreve como criar um novo atributo com o servidor Novell eDirectory para apoiar o conceito de níveis de autoridade, e como eles são designados a usuários que se autenticam em um servidor LDAP a partir de um IMM. O atributo criado foi chamado de **UserAuthorityLevel**. Nesta seção, você criará esse atributo no Active Directory.

1. Instale a ferramenta de Snap-In de Esquema do Active Directory. Para obter mais informações, consulte a documentação fornecida com o Active Directory.

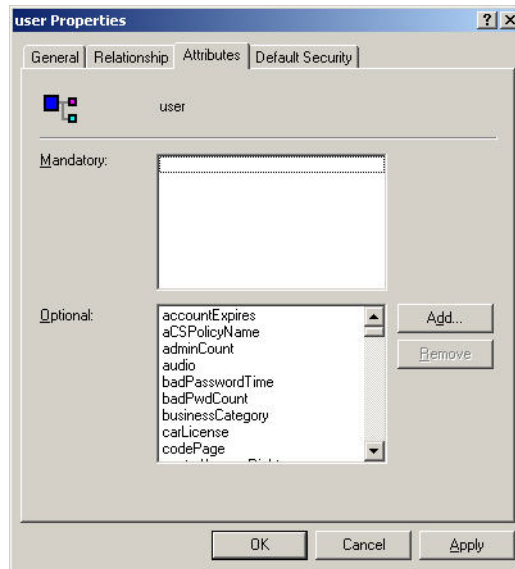
2. Inicie o Esquema do Active Directory.
3. Clique em **Ação > Criar Atributo**. Preencha os campos a seguir:
 - a. Configure o Nome Comum como **UserAuthorityLevel**
 - b. Configure a Sintaxe como **Sequência sem Distinção entre Maiúsculas e Minúsculas**
 - c. Configure Mínimo e Máximo como **12**
4. Entre em contato com o administrador do sistema para designar um novo OID X.500. Se você não desejar definir um novo OID X.500, use um atributo existente em vez de criar um novo atributo para o nível de autoridade.



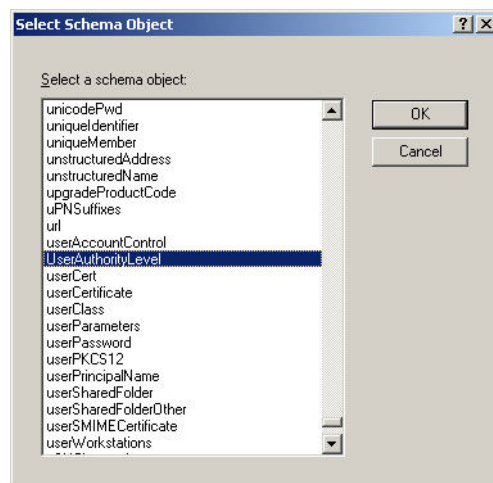
5. Depois que o atributo for salvo, selecione a pasta **Classes**.



6. Clique duas vezes na classe **usuário**. A janela Propriedades do usuário é aberta.

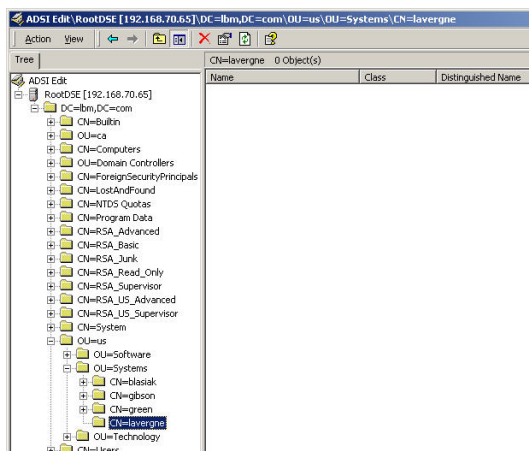


7. Selecione a guia **Atributos** e, em seguida, clique em **Incluir**. A janela Selecionar Objeto de Esquema é aberta.

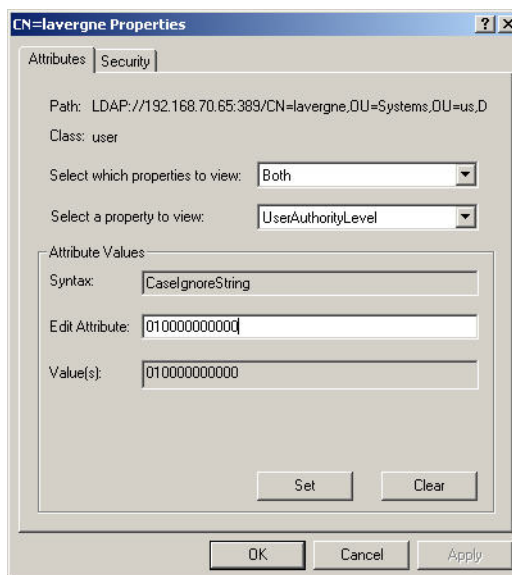


8. Role para baixo até **UserAuthorityLevel** e clique em **OK**. Esse atributo agora aparecerá na lista de atributos opcionais para a classe de objeto do usuário.
9. Repita a etapa 6 na página 60 até a etapa 8 para a classe grupos. Isso permite que o atributo **UserAuthorityLevel** seja designado a um usuário ou grupo de usuários. Essas são as duas únicas classes de objeto que precisam usar esse novo atributo.
10. Designe o atributo **UserAuthorityLevel** aos usuários e grupos de usuários apropriados. Para corresponder o esquema definido no servidor Novell eDirectory, use os mesmos valores conforme em “Configurando níveis de autoridade” na página 51. É possível usar a ferramenta ADSI Edit para fazer isso. A ferramenta de suporte Microsoft ADSI Edit é um snap-in do Microsoft Management Console (MMC) usado para visualizar todos os objetos no diretório (incluindo informações de esquema e configuração), modificar objetos e configurar listas de controle de acesso em objetos.
11. Para esse exemplo, suponha que você deseja incluir o atributo **UserAuthorityLevel** no usuário lavergne. Use o ADSI Edit para fazer isso. Você deve fornecer as credenciais apropriadas para conectar-se ao Active Directory; caso contrário, poderá não ter os privilégios de usuário corretos

para modificar objetos no servidor. A ilustração a seguir mostra o esquema, conforme visto pelo ADSI, após a conexão com o servidor.



12. Clique com o botão direito do mouse em **lavergne** e clique em **Propriedades**. Uma janela semelhante à da ilustração a seguir é aberta.



13. No campo **Selecionar quais propriedades visualizar**, selecione **UserAuthorityLevel**.
14. No campo **Editar Atributo**, digite **IBMRBSPermissions=010000000000**, que é convertido em Acesso de Supervisor. Clique em **Definir**.
15. Clique em **OK**.
16. É possível incluir esse atributo nos grupos de usuários seguindo as mesmas etapas para o objeto de grupo de usuários que você deseja modificar.

Verificando a Configuração do Active Directory

Antes de tentar conectar o cliente LDAP com o Active Directory (para autenticar usuários), procure o esquema do Active Directory com um navegador LDAP. No mínimo, emita as consultas listadas na tabela a seguir para verificar os níveis de autoridade e a associação ao grupo.

Tabela 9. Verificando níveis de autoridade e associação ao grupo

Nome distinto de procura	Filtro	Atributos
DC=ibm, DC=com	(objectclass=user)	memberOf, userAuthorityLevel
DC=ibm, DC=com	(objectclass=group)	member, userAuthorityLevel

Configurando o cliente LDAP

É possível configurar o LDAP para autenticar usuários do módulo de gerenciamento. O IMM suporta autenticação de usuário local e remota. A autenticação local usa as informações fornecidas na página Perfis de Login para autenticar usuários. Utilizando um servidor LDAP, um módulo de gerenciamento pode autenticar um usuário, consultando ou procurando um diretório LDAP em um servidor LDAP remoto, em vez de passar por seu banco de dados do usuário local.

Quando for usado qualquer tipo de autenticação remota, será possível escolher que as permissões para cada usuário autenticado com êxito sejam autorizadas localmente ou com base em informações armazenadas no servidor LDAP usado para autenticação remota. As permissões autorizadas para um usuário especificam as ações que cada usuário pode executar enquanto está conectado ao IMM. Os métodos de autenticação remota são descritos nos tópicos a seguir:

- Autenticação do Active Directory com autorização local
- Autenticação e autorização baseadas em função do Active Directory
- Autenticação e autorização LDAP legadas

Autenticação do Active Directory com autorização local

É possível configurar a autenticação LDAP remota para usuários, com autorização do usuário local, usando a autenticação do Active Directory.

Nota: A autenticação do Active Directory com autorização local aplica-se apenas a um servidor usado em um ambiente do Active Directory.

Ao usar a autenticação do Active Directory com autorização local, os servidores Active Directory são usados apenas para autenticar usuários verificando as credenciais de um usuário. Não há informações de autorização armazenadas no servidor Active Directory para um determinado usuário; os perfis de grupos armazenados pelo IMM devem ser configurados com informações de autorização. As informações de autorização usadas para configurar os perfis de grupos podem ser obtidas recuperando informações de associação para um usuário a partir do servidor Active Directory. Essas informações de associação fornecem a lista de grupos aos quais um usuário pertence (grupos aninhados são suportados). Os grupos especificados no servidor Active Directory são então comparados com os nomes de grupos configurados localmente no IMM. Para cada grupo do qual o usuário é membro, são designadas permissões ao usuário desse grupo. Para cada nome de grupo localmente configurado no IMM, há um perfil de autorização correspondente que também é configurado para esse grupo.

O IMM suporta até 16 nomes de grupos configurados localmente. Cada nome de grupo é limitado a 63 caracteres. Um dos seguintes atributos deve ser configurado como o nome do grupo para corresponder às informações de associação ao grupo recuperadas dos servidores Active Directory:

- Nome distinto (DN)

- Atributo "cn"
- Atributo "name"
- Atributo "sAMAccountName"

Para configurar a autenticação do Active Directory com autorização local para o IMM, conclua as etapas a seguir:

1. Na área de janela de navegação, clique em **Protocolos de Rede**.
2. Role para baixo até a seção **Cliente Lightweight Directory Access Protocol (LDAP)**.
3. Selecione **Usar Servidores LDAP apenas para Autenticação (com autorização local)**.
4. Selecione uma das opções a seguir, para configurar manualmente ou descobrir dinamicamente os controladores de domínio:
 - Selecione **Usar DNS para Localizar Servidores LDAP** para descobrir dinamicamente os controladores de domínio com base em registros DNS SVR.
 - Selecione **Usar Servidores LDAP Pré-configurados** (seleção padrão) para configurar manualmente os controladores de domínio.
5. Se você estiver usando o DNS para descobrir dinamicamente os controladores de domínio, defina as configurações a seguir; em seguida, continue com a etapa 7 na página 65.

Nota: Se usando o DNS para descobrir dinamicamente o controlador de domínio, você deverá especificar o nome completo do domínio do controlador de domínio.

- Procurar Domínio
 - Insira o nome de domínio do controlador de domínio no campo **Procurar Domínio**.
- Nome da Floresta do Active Directory
 - Esse campo opcional é usado para descobrir catálogos globais. Os catálogos globais são necessários para usuários pertencentes a grupos universais em domínios cruzados. Em ambientes nos quais a associação ao grupo de domínio cruzado não é aplicável, esse campo pode ser deixado em branco.

A ilustração a seguir mostra a janela Cliente LDAP ao usar o DNS para descobrir dinamicamente os controladores de domínio.

Lightweight Directory Access Protocol (LDAP) Client ?

☐ Use LDAP Servers for Authentication and Authorization

☒ Use LDAP Servers for Authentication Only (with local authorization)

☒ Use DNS to Find LDAP Servers

Active Directory Forest Name

Search Domain

☐ Use Pre-configured LDAP Servers

Active Directory Settings

View or set up authorization: [Group Profiles](#)

Miscellaneous Parameters

Root DN

UID Search Attribute

Binding Method

Client DN

Password

Confirm password

6. Se estiver configurando manualmente controladores de domínio e catálogos globais, utilize a seleção **Usar Servidores LDAP Pré-configurados** (padrão); em seguida, configure os campos **Nome do Host ou Endereço IP do Servidor LDAP** e **Porta**.

Até quatro controladores de domínio podem ser configurados usando um endereço IP ou um nome completo de host. Os servidores de catálogo global são identificados usando os números de porta 3268 ou 3269. O uso de qualquer outro número de porta indica que um controlador de domínio está sendo configurado.

7. Se você estiver usando perfis de autorização de grupo, clique em **Perfis de Grupo** na seção Configurações do Active Directory para visualizá-los e configurá-los (consulte “Perfis de grupos para usuários do Active Directory” na página 68 para obter informações adicionais).
8. Retorne à página Protocolos de Rede. Clique no link **Seção do Cliente LDAP da página Protocolos de Rede** que está na página Perfis de Grupos para Usuários do Active Directory; em seguida, role para a seção **Cliente Lightweight Directory Access Protocol (LDAP)**.
9. Configure os Parâmetros Diversos do IMM. Consulte a tabela a seguir para obter informações sobre os parâmetros.

Tabela 10. Parâmetros diversos

Campo	Descrição	Opção
DN Raiz	O IMM usa o campo DN Raiz em formato DN como entrada raiz da árvore de diretórios. Esse DN será usado como objeto base para todas as procuras. Um exemplo poderia ser semelhante a dc=mycompany,dc=com.	

Tabela 10. Parâmetros diversos (continuação)

Campo	Descrição	Opção
Método de ligação	O campo Método de Ligação é usado para ligações iniciais com o servidor de controlador de domínio; selecione uma opção.	- Com credenciais configuradas: Insira o DN e a Senha do cliente que devem ser usados para a ligação inicial. Se essa ligação falhar, o processo de autenticação também falhará. Se a ligação for bem-sucedida, uma procura tentará localizar um registro do usuário que corresponda ao DN do cliente digitado no campo DN do Cliente. A procura geralmente pesquisa atributos comuns que correspondam ao ID do usuário apresentado durante o processo de login. Esses atributos incluem displayName, sAMAccountName e userPrincipalName. Se o campo Atributo de Procura UID estiver configurado, a procura também incluirá esse atributo. Se a procura for bem-sucedida, será tentada uma segunda ligação, desta vez com o DN do usuário (recuperado da procura) e a senha apresentados durante o processo de login. Se a segunda tentativa de ligação for bem-sucedida, a parte de autenticação terá sido bem-sucedida e as informações de associação ao grupo para o usuário serão recuperadas e correspondidas com relação aos grupos configurados localmente no IMM. Os grupos correspondidos definirão as permissões de autorização designadas ao usuário. - Com credenciais de login: A ligação inicial com o servidor de controlador de domínio é feita usando as credenciais apresentadas durante o processo de login. Se essa ligação falhar, o processo de autenticação também falhará. Se a ligação for bem-sucedida, uma procura tentará localizar o registro do usuário. Depois de localizado, as informações de associação ao grupo para o usuário serão recuperadas e correspondidas com relação aos grupos configurados localmente no IMM. Os grupos correspondidos definirão as permissões de autorização designadas ao usuário. - Anonimamente: A ligação inicial com o servidor de controlador de domínio será feita sem um DN ou senha. Essa opção não é recomendável, pois a maioria dos servidores é configurada para desaprovar solicitações de procura em registros de usuário específicos.

Perfis de grupos para usuários do Active Directory

Os perfis de grupos são configurados para fornecer especificações de autorização local para grupos de usuários. Cada perfil de grupo inclui autorização expressa como Nível de Autoridade (Funções), exatamente da mesma maneira que em perfis de login. Para configurar perfis de grupos, os usuários devem ter autorização de gerenciamento de conta do usuário. Para associar usuários a perfis de grupos, são necessários servidores de autenticação LDAP.

Lista de perfis de grupos

A lista de perfis de grupos é acessada clicando em **Controle do IMM > Perfis de Login**. O resumo de ID e função do grupo é exibido para cada perfil de grupo (como com perfis de login). Nessa lista, novos grupos podem ser incluídos e grupos existentes podem ser selecionados para edição ou para serem excluídos.

A ilustração a seguir mostra a janela Perfis de Grupos para Usuários do Active Directory.



Para editar um perfil de grupo, clique em **Editar**. Uma página Perfil do Grupo é aberta para esse grupo. Para excluir um perfil de grupo, clique em **Excluir**. Você deve confirmar a exclusão de um perfil de grupo. Para incluir um novo perfil de grupo, clique no link **Incluir um grupo**. Uma página Perfil do Grupo é aberta para você inserir as informações do novo perfil de grupo. 16 perfis de grupos no máximo podem ser incluídos. Os nomes de perfis de grupos não precisam ser exclusivos.

A tabela a seguir descreve os campos na página Perfil do Grupo.

Tabela 11. Informações de perfis de grupos

Campo	Opção	Descrição
ID do Grupo		Esse campo é usado para especificar o ID do grupo para o perfil do grupo. É possível digitar no máximo 63 caracteres. O ID do grupo deve ser igual aos de suas contrapartes nos servidores LDAP. Exemplos de nomes de grupo são Grupo de Administradores do IMM e IMM/Robert.
Função		Selecione as funções (níveis de autoridade) associadas a este ID de login e transfira-as para a caixa Funções designadas . A tecla Enter ou um clique do mouse pode ser usado para transferir itens selecionados de uma caixa para a outra.
	Supervisor	O usuário não tem restrições, exceto escopo designado.

Tabela 11. Informações de perfis de grupos (continuação)

Campo	Opção	Descrição
	Operador	O usuário só tem permissão de acesso somente leitura e não pode executar nenhuma mudança, por exemplo, salvar, modificar e limpar. Isso também inclui estado que afeta operações como reiniciar o IMM, restaurar padrões e atualizar firmware.
Função	Customizado	O usuário pode ou não ter alguma restrição, dependendo do nível de autoridade customizado que é designado para ele. Se você selecionar a opção Customizado, deverá selecionar um ou mais dos seguintes níveis de autoridade do cliente: • Rede e Segurança – O usuário pode modificar a configuração nos painéis Segurança, Protocolos de Rede, Interface de Rede, Designações de Porta e Porta Serial. • Gerenciamento de conta do usuário – O usuário pode incluir, modificar ou excluir usuários e alterar as configurações de Login Global no painel Perfis de Login. • Acesso ao Console Remoto – Os usuários podem acessar o console do servidor remoto. • Acesso ao Console Remoto e Disco Remoto – O usuário pode acessar o console do servidor remoto e as funções de disco remoto para o servidor remoto. • Acesso a Energia/Reinicialização do Servidor Remoto – O usuário pode acessar as funções de ligação, reinicialização e tempo limite do servidor remoto. • Configuração de Adaptador Básica – O usuário pode modificar parâmetros de configuração nos painéis Configurações do Sistema (excluindo Contato, Local e Tempos Limites do Servidor) e Alertas. • Capacidade para Limpar Logs de Eventos – O usuário pode limpar os logs de eventos. Nota: Todos podem visualizar os logs de eventos; mas, esse parâmetro é obrigatório para limpar os logs. • Configuração de Adaptador Avançada – O usuário não tem restrições ao configurar o adaptador e tem acesso administrativo ao IMM. O usuário pode executar as seguintes funções avançadas: atualizar o firmware, inicializar a rede do Ambiente de Execução de Pré-inicialização (PXE), restaurar os padrões de fábrica do adaptador, modificar e restaurar a configuração de adaptador a partir de um arquivo de configuração e reiniciar/reconfigurar o adaptador. Nota: Esse nível de autoridade exclui as funções de tempo limite e Controle de Energia/Reinicialização do Servidor.

Tabela 11. Informações de perfis de grupos (continuação)

Campo	Opção	Descrição
Nota: Para evitar uma situação em que não há usuário que tenha acesso de leitura/gravação, o perfil de login número um deve ser configurado com pelo menos a capacidade de modificar os perfis de login. Deve ser concedido a esse usuário acesso de Supervisor ou de Gerenciamento de Contas do Usuário. Isso garante que pelo menos um usuário possa executar ações, fazer mudanças na configuração e incluir usuários nos perfis de login que também podem executar ações ou fazer mudanças na configuração.		

A ilustração a seguir mostra a janela Perfil do Grupo.

Autenticação e autorização baseadas em função do Active Directory

É possível configurar autenticação e autorização LDAP remotas para usuários, utilizando o Active Directory.

Notas:

- A autenticação e autorização baseadas em função do Active Directory se aplicam apenas a um servidor usado em um ambiente do Active Directory.
- A ferramenta Snap-in de Segurança baseada em função aprimorada é necessária para autenticação e autorização baseadas em função do Active Directory.

A autenticação e autorização baseadas em função do Active Directory usa as informações de configuração armazenadas em um servidor Active Directory para autenticar um usuário e, em seguida, associar permissões ao usuário. Antes de ativar a autenticação e autorização baseadas em função do Active Directory, utilize a ferramenta Snap-in de Segurança baseada em função aprimorada para armazenar as informações de configuração no servidor Active Directory que associa permissões aos usuários. Essa ferramenta é executada em qualquer cliente Microsoft Windows e pode ser transferida por download no site <http://www.ibm.com/systems/support/>.

A ferramenta Snap-in de Segurança baseada em função aprimorada permite que você configure funções em um servidor Active Directory e associe o IMM, usuários

e grupos a essas funções. Consulte a documentação da ferramenta Snap-in de Segurança baseada em função aprimorada para obter informações e instruções. As funções identificam as permissões designadas aos usuários e grupos e identificam os destinos de comandos, como o IMM ou um servidor blade, aos quais uma função está conectada. Antes de ativar a autenticação e autorização baseadas em função do Active Directory, as funções devem ser configuradas no servidor Active Directory.

O nome opcional configurado no campo **Nome de Destino do Servidor** identifica um determinado IMM e pode ser associado a uma ou mais funções no servidor Active Directory por meio da ferramenta Snap-in de Segurança baseada em função aprimorada. Isso é feito criando destinos gerenciados, fornecendo aos destinos nomes específicos e associando os destinos às funções apropriadas. Se um Nome de Destino do Servidor estiver configurado, ele poderá definir funções específicas para usuários e destinos do IMM que são membros da mesma função. Quando um usuário efetua login no IMM e é autenticado por meio do Active Directory, as funções para esse usuário são recuperadas do diretório. As permissões designadas ao usuário são extraídas das funções que têm um destino como membro com um nome que corresponde a esse IMM, ou um destino que corresponde a qualquer IMM. O IMM pode receber um nome exclusivo, ou mais de um IMM podem compartilhar o mesmo nome de destino. A designação de mais de um IMM ao mesmo nome de destino, agrupa-os e designa-os à mesma função.

Para configurar a autenticação e autorização baseadas em função do Active Directory para o IMM, conclua as etapas a seguir:

1. Na área de janela de navegação, clique em **Protocolos de Rede**.
2. Role para baixo até a seção **Cliente Lightweight Directory Access Protocol (LDAP)**.
3. Selecione **Usar Servidores LDAP para Autenticação e Autorização**.
4. Selecione **Ativado** para o campo **Segurança aprimorada baseada em função para Usuários do Active Directory**.
5. Selecione uma das seguintes opções para descobrir dinamicamente ou configurar manualmente os controladores de domínio:
 - Selecione **Usar DNS para Localizar Servidores LDAP** para descobrir dinamicamente os controladores de domínio com base em registros DNS SVR.
 - Selecione **Usar Servidores LDAP Pré-configurados** (seleção padrão) para configurar manualmente os controladores de domínio.
6. Se você estiver usando o DNS para descobrir dinamicamente os controladores de domínio, configure o nome de domínio do controlador de domínio; em seguida, continue com a etapa 8 na página 73. Você deve especificar o nome completo do domínio do controlador de domínio. Insira o nome de domínio do controlador de domínio no campo **Procurar Domínio**.

A janela a seguir exibe a janela Cliente LDAP ao usar o DNS para descobrir dinamicamente os controladores de domínio.

Lightweight Directory Access Protocol (LDAP) Client ?

☒ Use LDAP Servers for Authentication and Authorization
☐ Use LDAP Servers for Authentication Only (with local authorization)

☒ Use DNS to Find LDAP Servers

Search Domain

☐ Use Pre-configured LDAP Servers

Active Directory Settings

Enhanced role-based security for Active Directory Users

Server Target Name

Miscellaneous Parameters

Root DN

UID Search Attribute

Binding Method

Client DN

Password

Confirm password

- Se você estiver configurando manualmente os controladores de domínio, configure os campos **Nome do Host ou Endereço IP do Servidor LDAP e Porta**.

Nota: Até quatro controladores de domínio podem ser configurados usando um endereço IP ou um nome completo de host.

A ilustração a seguir mostra a janela Cliente LDAP ao configurar manualmente os controladores de domínio.

Lightweight Directory Access Protocol (LDAP) Client ?

☒ Use LDAP Servers for Authentication and Authorization
 ☐ Use LDAP Servers for Authentication Only (with local authorization)

☐ Use DNS to Find LDAP Servers
 ☒ Use Pre-configured LDAP Servers

LDAP Server Fully Qualified Host Name or IP Address

Port

1.

2.

3.

4.

Active Directory Settings

Enhanced role-based security for Active Directory Users

Enabled ▾

Server Target Name

Miscellaneous Parameters

Root DN

UID Search Attribute

Binding Method

With configured credentials ▾

Client DN

Password

Confirm password

- Defina as Configurações do Active Directory, selecionando **Ativado** no menu **Segurança aprimorada baseada em função para Usuários do Active Directory**.
- Configure os Parâmetros Diversos. Consulte a tabela a seguir para obter informações sobre os parâmetros.

Tabela 12. Parâmetros diversos

Campo	Descrição	Opção
DN Raiz	O IMM usa o campo DN Raiz em formato DN como entrada raiz da árvore de diretórios. Esse DN será usado como objeto base para todas as procuras. Um exemplo poderia ser semelhante a dc=mycompany,dc=com.	

Tabela 12. Parâmetros diversos (continuação)

Campo	Descrição	Opção
Método de ligação	O campo Método de Ligação é usado para ligações iniciais com o servidor de controlador de domínio; selecione uma opção.	• Anonimamente: A ligação inicial com o servidor de controlador de domínio será feita sem um DN ou senha. Essa opção não é recomendável, pois a maioria dos servidores é configurada para desaprovar solicitações de procura em registros de usuário específicos. • Com credenciais configuradas: Insira o DN e a Senha do cliente que devem ser usados para a ligação inicial. • Com credenciais de login: A ligação inicial com o servidor de controlador de domínio é feita usando as credenciais apresentadas durante o processo de login. O ID do usuário pode ser fornecido utilizando um DN, um DN parcial, um nome de domínio completo, ou por meio de um ID do usuário que corresponda ao campo Atributo de Procura de UID configurado no IMM. Se as credenciais forem semelhantes a um DN parcial (por exemplo, cn=joe), esse DN parcial será prefixado ao DN Raiz configurado em uma tentativa de criar um DN que corresponda ao registro do usuário. Se a tentativa de ligação falhar, uma tentativa de ligação final ocorrerá incluindo o prefixo cn= na credencial de login; em seguida, inclua os resultados da sequência no DN Raiz configurado.

Autenticação e autorização LDAP legadas

Autenticação e autorização LDAP legadas é o modelo original usado com o IMM. A autenticação e autorização LDAP legadas suportam os ambientes Active Directory, Novell eDirectory e OpenLDAP e dependem das informações de configuração armazenadas em um servidor LDAP para permissões associadas a um usuário. A autenticação e autorização LDAP legadas são utilizadas para autenticar e autorizar usuários por meio de um servidor LDAP. Se a Segurança Aprimorada Baseada em Função para Usuários do Active Directory estiver desativada em um IMM, você terá permissão para configurar os atributos de procura LDAP para o IMM.

Para configurar a autenticação e autorização LDAP legadas para o IMM, conclua as etapas a seguir:

1. Na área de janela de navegação, clique em **Protocolos de Rede**.
2. Role para baixo até a seção **Cliente Lightweight Directory Access Protocol (LDAP)**.
3. Selecione **Usar Servidores LDAP para Autenticação e Autorização**.
4. Selecione **Desativado** para o campo **Segurança aprimorada baseada em função para Usuários do Active Directory**.

5. Selecione uma das opções a seguir, para descobrir dinamicamente ou configurar manualmente os servidores LDAP a serem usados para autenticação:
 - Selecione **Usar DNS para Localizar Servidores LDAP** para descobrir dinamicamente os servidores LDAP nos registros DNS SVR.
 - Selecione **Usar Servidores LDAP Pré-configurados** (seleção padrão) para configurar manualmente os servidores LDAP.
6. Se você estiver usando o DNS para descobrir dinamicamente os servidores LDAP, configure o nome de domínio do servidor LDAP; em seguida, continue com a etapa 8 na página 76. Você deve especificar o nome completo do domínio do servidor LDAP. Insira o nome de domínio do servidor LDAP no campo **Procurar Domínio**.

A janela a seguir exibe a janela Cliente LDAP ao usar o DNS para descobrir dinamicamente os servidores LDAP.

Lightweight Directory Access Protocol (LDAP) Client ?

☒ Use LDAP Servers for Authentication and Authorization
☐ Use LDAP Servers for Authentication Only (with local authorization)

☒ Use DNS to Find LDAP Servers

Search Domain

☐ Use Pre-configured LDAP Servers

Active Directory Settings

Enhanced role-based security for Active Directory Users

Miscellaneous Parameters

Root DN

UID Search Attribute

Binding Method

Client DN

Password

Confirm password

Group Filter

Group Search Attribute

Login Permission Attribute

7. Se você estiver configurando manualmente os servidores LDAP, configure os campos **Nome do Host ou Endereço IP do Servidor LDAP** e **Porta**; em seguida, continue com a etapa 8 na página 76.

Nota: Até quatro servidores LDAP podem ser configurados usando um endereço IP ou um nome completo do host.

A janela a seguir exibe a janela Cliente LDAP ao configurar manualmente os servidores LDAP.

Lightweight Directory Access Protocol (LDAP) Client ?

☒ Use LDAP Servers for Authentication and Authorization
☐ Use LDAP Servers for Authentication Only (with local authorization)

☐ Use DNS to Find LDAP Servers
☒ Use Pre-configured LDAP Servers

	LDAP Server Fully Qualified Host Name or IP Address	Port
1.		
2.		
3.		
4.		

Active Directory Settings

Enhanced role-based security for Active Directory Users Disabled ▾

Miscellaneous Parameters

Root DN	
UID Search Attribute	
Binding Method	With configured credentials ▾
Client DN	
Password	
Confirm password	
Group Filter	
Group Search Attribute	
Login Permission Attribute	

8. Defina as Configurações do Active Directory, selecionando **Desativado** no menu **Segurança aprimorada baseada em função para Usuários do Active Directory**.
9. Configure os Parâmetros Diversos. Consulte a lista a seguir para obter uma descrição dos campos de parâmetros necessários.
 - O IMM usa o campo **DN Raiz** em formato DN como entrada raiz da árvore de diretórios. Esse DN será usado como objeto base para todas as procuras. Um exemplo poderia ser semelhante a `dc=mycompany,dc=com`.
 - O campo **Método de Ligação** é usado para ligações iniciais com o servidor de controlador de domínio. Use uma das seguintes opções de ligação:
 - Anonimamente:
A ligação inicial com o servidor de controlador de domínio será feita sem um DN ou senha. Essa opção não é recomendável, pois a maioria dos servidores é configurada para desaprovar solicitações de procura em registros de usuário específicos.

- Com credenciais configuradas:

Insira o DN e a Senha do cliente que devem ser usados para a ligação inicial.

- Com credenciais de login:

Ligue com as credenciais fornecidas durante o processo de login. O ID do usuário pode ser fornecido utilizando um DN, um DN parcial, um nome de domínio completo, ou por meio de um ID do usuário que corresponda às informações no campo **Atributo de Procura de UID** configurado no IMM. Se as credenciais forem semelhantes a um DN parcial (por exemplo, cn=joe), esse DN parcial será prefixado ao DN Raiz configurado em uma tentativa de criar um DN que corresponda ao registro do usuário. Se a tentativa de ligação falhar, uma tentativa de ligação final ocorrerá incluindo o prefixo cn= na credencial de login; em seguida, inclua os resultados da sequência no DN Raiz configurado.

- O campo **Filtro de Grupo** é usado para autenticação de grupo. Ele especifica o grupo ao qual o IMM pertence. Se o filtro de grupo for deixado em branco, a autenticação do grupo terá êxito automaticamente. A autenticação do grupo, se ativada, ocorrerá após a autenticação do usuário. Foi feita uma tentativa de corresponder pelo menos um grupo no Filtro de Grupo com 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 do grupo será aprovada. As comparações fazem distinção entre maiúsculas e minúsculas.

Quando a autenticação de grupo está desativada, próprio registro do usuário deve conter o atributo de permissão; caso contrário, o acesso será negado.

Para cada grupo que corresponde ao filtro, as permissões associadas a esse grupo são designadas ao usuário. As permissões associadas a um grupo são localizadas ao recuperar as informações do **Atributo de Permissão de Login**.

O filtro é limitado a 511 caracteres e consiste em um ou mais nomes de grupos. O caractere de dois-pontos (:) deve ser usado para especificar diversos nomes de grupo. Os espaços iniciais e finais são ignorados, enquanto todos os demais espaços são tratados como parte do nome do grupo. 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 igual a cn=adminGroup,dc=mycompany,dc=com pode ser especificado utilizando o DN real ou com adminGroup.

Nota: O símbolo de asterisco (*) usado anteriormente não é mais tratado como um símbolo curinga. O conceito de curinga foi removido por motivos de segurança.

- O campo **Atributo de Procura de Grupo** é usado pelo algoritmo de procura para localizar informações de associação ao grupo para um usuário específico. Quando o nome do filtro de grupo estiver configurado, a lista de grupos aos quais o usuário pertence deverá ser recuperada do servidor LDAP. Essa lista é necessária para executar autenticação de grupo. Para recuperar essa lista, o filtro de procura enviado para o servidor LDAP deve especificar o nome do atributo que está associado aos grupos. O campo **Atributo de Procura de Grupo** especifica o nome do atributo.

Em um ambiente Active Directory ou Novell eDirectory, o campo **Atributo de Procura de Grupo** especifica o nome do atributo que identifica os grupos aos quais um usuário pertence. Em um Active Directory, o atributo **memberOf** é usado e, com o Novell eDirectory, o atributo **groupMembership** é usado. Em um ambiente do servidor OpenLDAP, os usuários geralmente são designados a grupos cujo objectClass é PosixGroup.

Nesse contexto, o parâmetro **Atributo de Procura de Grupo** especifica o nome do atributo que identifica os membros de um determinado PosixGroup, que geralmente é **memberUid**. Se o campo **Atributo de Procura de Grupo** for deixado em branco, o nome do atributo no filtro será padronizado como **memberOf**.

- O campo **Atributo de Permissão de Login** especifica o nome do atributo associado às permissões de login do usuário. Quando um usuário é autenticado com êxito usando um servidor LDAP, é necessário recuperar as permissões de login do usuário.

Nota: Esse campo **Atributo de Permissão de Login** não deve ficar em branco; caso contrário, será impossível recuperar as permissões do usuário. Sem permissões verificadas, a tentativa de login falhará.

O valor de atributo retornado pelo servidor LDAP é procurado usando a sequência de palavra-chave **IBMRBSPermissions=**. Essa palavra-chave deve ser seguida imediatamente por uma sequência de bits (até 12 0s ou 1s consecutivos). Cada bit representa um conjunto específico de funções. Os bits são numerados de acordo com sua posição. O bit mais à esquerda é o da posição 0, e o bit mais à direita, o da posição 11. Um valor 1 em uma determinada posição ativa essa função específica. Um valor 0 desativa essa função. A sequência **IBMRBSPermissions=010000000000** é um exemplo.

A palavra-chave **IBMRBSPermissions=** pode ser colocada em qualquer lugar no campo **Atributo de Permissão de Login**. Isso permite que o administrador de LDAP reutilize um atributo existente; portanto, impedindo uma extensão para o esquema LDAP e permitindo que o atributo seja usado para seu propósito original. O usuário pode agora incluir a sequência de palavra-chave no início, no final ou em qualquer local nesse campo. O atributo usado permitirá uma sequência de formatação livre.

A tabela a seguir fornece uma explicação de cada posição de bit.

Tabela 13. Bits de permissão

Posição do Bit	Função	Explicação
0	Negar Sempre	Se configurado, 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	Se configurado, privilégios de administrador foram 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.

Tabela 13. Bits de permissão (continuação)

Posição do Bit	Função	Explicação
2	Acesso Somente Leitura	Se configurado, um usuário terá acesso somente leitura e não poderá executar nenhum procedimento de manutenção (por exemplo, reinicialização, ações remotas ou atualizações de firmware). Nada pode ser modificado, usando salvar, limpar ou restaurar funções. A posição de bit 2 e todos os demais bits são mutuamente exclusivos, com a posição de bit 2 tendo a precedência mais baixa. Se algum outro bit for configurado, esse bit será ignorado.
3	Rede & Segurança	Se configurado, um usuário poderá modificar a configuração nos painéis Segurança, Protocolos de Rede, Interface de Rede, Designações de Porta e Porta Serial.
4	Gerenciamento de Conta do Usuário	Se configurado, um usuário poderá incluir, modificar ou excluir usuários e alterar as Configurações Globais de Login no painel Perfis de Login.
5	Acesso ao Console Remoto	Se configurado, um usuário poderá acessar o console do servidor remoto e modificar a configuração no painel Porta Serial.
6	Acesso ao Console Remoto e Disco Remoto	Se configurado, um usuário poderá acessar o console do servidor remoto e as funções de disco remoto para o servidor remoto. O usuário também pode modificar a configuração no painel Porta Serial.
7	Acesso a Energia/Reinicialização do Servidor Remoto	Se configurado, um usuário poderá acessar as funções de ligação, reinicialização e tempo limite do servidor remoto.
8	Configuração de Adaptador Básica	Se configurado, um usuário poderá modificar parâmetros de configuração nos painéis Configurações do Sistema e Alertas (exclui os parâmetros Contato, Local e Tempo Limite do Servidor).
9	Capacidade para Limpar Logs de Eventos	Se configurado, um usuário poderá 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 13. Bits de permissão (continuação)

Posição do Bit	Função	Explicação
10	Configuração de Adaptador Avançada	Se configurado, um usuário não terá restrições ao configurar o adaptador e terá acesso administrativo ao IMM. O usuário pode executar as seguintes funções avançadas: atualizar o firmware, inicializar a rede PXE, restaurar os padrões de fábrica do adaptador, modificar e restaurar a configuração de adaptador a partir de um arquivo de configuração e reiniciar/reconfigurar o adaptador. Isso exclui as funções de tempo limite e Controle de Energia/Reinicialização do Servidor.
11	Reservado	Essa posição de bit está reservada para uso futuro (atualmente ignorada).
Notas: • Se não forem utilizados bits, o padrão será definido como Somente Leitura para o usuário. • É dada prioridade às permissões de login recuperadas diretamente do registro do usuário. Se o registro do usuário não contiver um nome no campo Atributo de Permissão de Login, será feita uma tentativa de recuperar as permissões do grupo ao qual o usuário pertence e que correspondem ao filtro de grupo. Nesse caso, é designado ao usuário o OR inclusivo de todos os bits para todos os grupos. • Se o bit Negar Sempre (posição de bit zero) for configurado para qualquer um dos grupos, o usuário terá o acesso recusado. O bit Negar Sempre tem precedência sobre todos os bits. • Se um usuário tiver a capacidade de modificar os parâmetros de configuração de adaptador básico, rede, ou relacionado à segurança, você deverá considerar fornecer a esse usuário a capacidade de reiniciar o IMM (posição de bit dez). Sem essa capacidade, um usuário pode ser capaz de alterar um parâmetro; mas, o parâmetro não entrará em vigor.		

Configurando a segurança

É possível usar o procedimento geral nesta seção para configurar a segurança para criptografia de dados sensíveis, o servidor da web IMM, a conexão entre o IMM e o IBM Systems Director, a conexão entre o IMM e um servidor LDAP e para gerenciamento de criptografia. Se você não estiver familiarizado com o uso de certificados SSL, leia as informações em “Certificado SSL” na página 83.

Para configurar a segurança do IMM, faça o seguinte:

1. Configurando a criptografia de dados sensíveis:
 - a. Na área de janela de navegação, clique em **Segurança**. Role para a seção **Ativar Criptografia de Dados** e selecione **Ativar** para habilitar a criptografia de dados. Para desativar a criptografia de dados, selecione **Desativar**.
2. Configurando o servidor da web seguro:
 - a. Na área de janela de navegação, clique em **Segurança**. Role para a seção **Configuração do Servidor HTTPS para Servidor da Web** e selecione **Desativar** para desativar o servidor SSL.

- b. Para gerar ou importar um certificado, clique em **Segurança** na área de janela de navegação e role para a seção **Gerenciamento de Certificado do Servidor HTTPS**. Consulte “Gerenciamento de certificado do servidor SSL” na página 83 para obter mais informações sobre como gerenciar certificados.
 - c. Para ativar o servidor SSL, clique em **Segurança** na área de janela de navegação e role para a seção **Configuração do Servidor HTTPS para Servidor da Web**. Consulte “Ativando SSL para o servidor da web seguro ou IBM Systems Director sobre HTTPS” na página 88 para obter mais informações sobre como ativar SSL.
3. Configurando a conexão do IBM Systems Director:
 - a. Para desativar a configuração do **Systems Director sobre HTTPS**, clique em **Segurança** na área de janela de navegação e role para a seção **Configuração do IBM Systems Director sobre Servidor HTTPS**.
 - b. Para gerar ou importar um certificado, clique em **Segurança** na área de janela de navegação e role para a seção **Gerenciamento de Certificado do IBM Systems Director sobre Servidor HTTPS**. Consulte “Gerenciamento de certificado do servidor SSL” na página 83 para obter mais informações.
 - c. Para ativar o servidor SSL, clique em **Segurança** na área de janela de navegação e role para a seção **Configuração do IBM Systems Director sobre Servidor HTTPS**. Consulte “Ativando SSL para o servidor da web seguro ou IBM Systems Director sobre HTTPS” na página 88 para obter mais informações sobre como ativar SSL.
4. Configurando a segurança SSL para conexões LDAP:
 - a. Para desativar o cliente SSL, clique em **Segurança** na área de janela de navegação e role para a seção **Configuração do Cliente SSL para Cliente LDAP**.
 - b. Para gerar ou importar um certificado, clique em **Segurança** na área de janela de navegação e role para a seção **Gerenciamento de Certificado do Cliente SSL**. Consulte “Gerenciamento de certificado do servidor SSL” na página 83 para obter mais informações.
 - c. Para importar um ou mais certificados confiáveis, clique em **Segurança** na área de janela de navegação e role para a seção **Gerenciamento de Certificado Confiável do Cliente SSL**. Consulte Gerenciamento de certificado confiável do cliente SSL para obter mais informações.
 - d. Para ativar o cliente SSL, clique em **Segurança** na área de janela de navegação e role para a seção **Configuração do Cliente SSL para Cliente LDAP**. Consulte “Ativando SSL para o servidor da web seguro ou IBM Systems Director sobre HTTPS” na página 88 para obter mais informações.
5. Configurando gerenciamento de criptografia:
 - a. Na área de janela de navegação, clique em **Segurança** e role para a seção **Gerenciamento de Criptografia**. Selecione **Modo Compatível Básico**.
 - b. Na área de janela de navegação, clique em **Segurança** e role para a seção **Gerenciamento de Criptografia**. Selecione **Modo de Alta Segurança**.
6. Reinicie o IMM para que as mudanças na configuração do servidor SSL sejam aplicadas. Para obter mais informações, consulte “Reiniciando o IMM” na página 94.

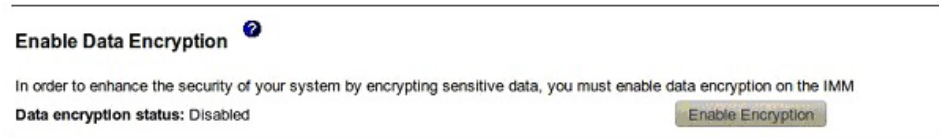
Nota: As mudanças na configuração de criptografia de dados e do cliente SSL entram em vigor imediatamente e não exigem uma reinicialização do IMM.

Ativando a Criptografia de Dados

Por padrão, dados sensíveis são salvos sem criptografia para permanecerem compatíveis com a versão anterior. Para aprimorar a segurança do sistema, você deve ativar a criptografia de dados no IMM.

Para ativar a criptografia de dados, conclua o procedimento a seguir:

1. Na área de janela de navegação, clique em **Segurança**.



2. Clique em **Ativar Criptografia** para ativar a criptografia de dados.

Nota:

- Se você precisar fazer downgrade do firmware do IMM versão 1.42 para a versão anterior, que não fornece criptografia de dados, será necessário desativar a criptografia de dados antes de fazer o downgrade. Se a criptografia de dados não for desativada antes do downgrade, os dados da conta serão perdidos.
- Se você precisar desativar a criptografia de dados no futuro, selecione **Desativar Criptografia** para desativar a criptografia de dados.

Protegendo o servidor da web, IBM Systems Director e LDAP seguro

Secure Sockets Layer (SSL) é um protocolo de segurança que fornece privacidade de comunicação. O SSL permite que aplicativos cliente/servidor se comuniquem de uma maneira que evita intrusões, violações e falsificação de mensagens.

É possível configurar o IMM para usar o suporte SSL para dois tipos de conexões: servidor seguro (HTTPS) e conexão LDAP segura (LDAPS). O IMM age como cliente ou servidor SSL, dependendo do tipo de conexão.

A tabela a seguir mostra as funções do IMM para conexões seguras do servidor da web e conexões LDAP seguras.

Tabela 14. Suporte de conexão SSL do IMM

Tipo de conexão	Cliente SSL	Servidor SSL
Servidor da web seguro (HTTPS)	Navegador da web (Por exemplo: Microsoft Internet Explorer)	Servidor da web do IMM
Conexão segura do IBM Systems Director	IBM Systems Director	Servidor IMM Systems Director
Conexão LDAP segura (LDAPS)	Cliente LDAP do IMM	Um servidor LDAP

É possível visualizar ou alterar as configurações SSL na página Segurança, incluindo ativar ou desativar o SSL, bem como gerenciar certificados obrigatórios para SSL.

Certificado SSL

É possível usar o SSL com um certificado autoassinado ou com um certificado assinado por uma autoridade de certificação de terceiros.

O certificado autoassinado é o método mais simples de usar SSL, mas cria um risco de segurança. Quando você usa o método autoassinado, o cliente SSL não tem como validar a identidade do servidor SSL para a primeira tentativa de conexão entre o cliente e o servidor. É possível a um terceiro personificar o servidor e interceptar os dados que fluem entre o IMM e o navegador da web. Se o certificado autoassinado for importado no armazenamento de certificados do navegador no momento da conexão inicial entre o navegador e o IMM, todas as futuras comunicações serão seguras para o navegador; supondo que a conexão inicial não tenha sido comprometida por um ataque.

Para melhor segurança, use um certificado assinado por uma autoridade de certificação. Para obter um certificado assinado, use a página Gerenciamento de Certificado SSL para gerar uma solicitação de assinatura de certificado. Você deve enviar a solicitação de assinatura de certificado para uma autoridade de certificação e fazer acordos para obter um certificado. Depois de recebido, o certificado será então importado no IMM por meio do link **Importar um Certificado Assinado**; em seguida, o SSL poderá ser ativado.

A função da autoridade de certificação é verificar a identidade do IMM. Um certificado contém assinaturas digitais para a autoridade de certificação e o IMM. Se uma autoridade de certificação reconhecida emitir o certificado ou o certificado da autoridade de certificação já tiver sido importado para o navegador da web, o navegador poderá validar o certificado e identificar positivamente o servidor da web do IMM.

O IMM requer um certificado para o servidor da web seguro e um para o cliente LDAP seguro. Além disso, o cliente LDAP seguro requer um ou mais certificados confiáveis. O certificado confiável é usado pelo cliente LDAP seguro para identificar positivamente o servidor LDAP. O certificado confiável é o certificado da autoridade de certificação 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.

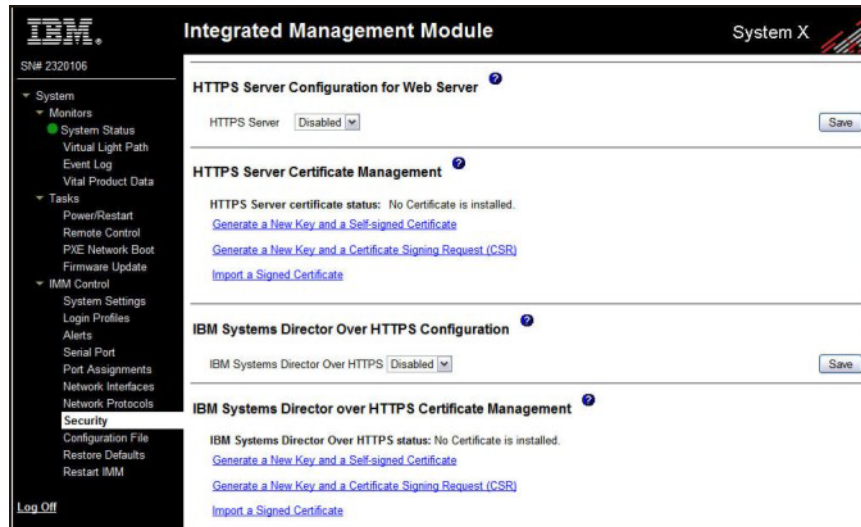
Gerenciamento de certificado do servidor SSL

O servidor SSL requer que um certificado válido e uma chave de criptografia privada correspondente sejam instalados antes da ativação do SSL. Dois métodos estão disponíveis para gerar a chave privada e o certificado requerido: usando um certificado autoassinado ou um certificado assinado por uma autoridade de certificação. Se você deseja usar um certificado autoassinado para o servidor SSL, consulte “Gerando um certificado autoassinado” para obter mais informações. Consulte “Gerando uma solicitação de assinatura de certificado” na página 85, para obter mais informações sobre como usar um certificado assinado por autoridade de certificação para o servidor SSL.

Gerando um certificado autoassinado

Para gerar uma nova chave de criptografia privada e um certificado autoassinado, conclua as etapas a seguir:

1. Clique em **Segurança**, localizado na área de janela de navegação, e a página a seguir será exibida.



2. Na área **Configuração do Servidor SSL para Servidor da Web** ou **Configuração do IBM Systems Director sobre HTTPS**, certifique-se de que a configuração seja **Desativado**. Se não estiver desativado, selecione **Desativado** e depois clique em **Salvar**.

Nota:

- a. O IMM deve ser reiniciado para que o valor selecionado (**Ativado** ou **Desativado**) entra em vigor.
 - b. Para poder ativar o SSL, um certificado SSL válido deve estar em vigor.
 - c. Para usar SSL, você deve configurar um navegador da web do cliente para utilizar SSL3 ou TLS. Os navegadores export-grade mais antigos com apenas o suporte SSL2 não podem ser usados.
3. Na área **Gerenciamento de Certificado do Servidor SSL**, selecione **Gerar uma Nova Chave e um Certificado Autoassinado**. Uma página semelhante à da ilustração a seguir é exibida.

4. Digite as informações nos campos obrigatórios e em qualquer campo opcional aplicável à sua configuração. Para obter uma descrição dos campos, consulte "Dados Obrigatórios do Certificado". 85. Depois de inserir as informações, clique em **Gerar Certificado**. As novas chaves de criptografia e o certificado são

gerados. Esse processo pode levar alguns minutos. Você verá a confirmação se um certificado autoassinado estiver instalado.

Gerando uma solicitação de assinatura de certificado

Para gerar uma nova chave de criptografia privada e solicitação de assinatura de certificado, conclua as etapas a seguir:

1. Na área de janela de navegação, clique em **Segurança**.
2. Na área **Configuração do Servidor SSL para Servidor da Web**, certifique-se de que o servidor SSL esteja desativado. Se ele não estiver desativado, selecione **Desativado** no campo **Servidor SSL** e, em seguida, clique em **Salvar**.
3. Na área **Gerenciamento de Certificado do Servidor SSL**, selecione **Gerar uma Nova Chave e uma Solicitação de Assinatura de Certificado**. Uma página semelhante à da ilustração a seguir é exibida.

SSL Certificate Signing Request (CSR)

Certificate Request Data

Country (2 letter code)

State or Province

City or Locality

Organization Name

IMM Host Name

Optional Certificate Data

Contact Person

Email Address

Organizational Unit

Surname

Given Name

Initials

DN Qualifier

CSR Attributes and Extension Attributes

Challenge Password

Unstructured Name

4. Digite as informações nos campos obrigatórios e em qualquer campo opcional aplicável à sua configuração. Os campos são idênticos aos do certificado autoassinado, com alguns campos adicionais.

Leia as informações nas seções a seguir para obter uma descrição de cada um dos campos comuns.

Dados obrigatórios do certificado Os seguintes campos de entrada do usuário são necessários para gerar um certificado autoassinado ou uma solicitação de assinatura de certificado:

País Use esse campo para indicar o país no qual o IMM está fisicamente localizado. Esse campo deve conter o código de país de 2 caracteres.

Estado ou Município

Use esse campo para indicar o estado ou o município onde o IMM está fisicamente localizado. Esse campo pode conter no máximo 30 caracteres.

Cidade ou Localidade

Use esse campo para indicar a cidade ou a localidade onde o IMM está fisicamente localizado. Esse campo pode conter no máximo 50 caracteres.

Nome da Organização

Use esse campo para indicar a empresa ou organização que possui o IMM. Quando utilizado para gerar uma solicitação de assinatura de certificado, a autoridade de certificação emissora pode verificar se a organização que está solicitando o certificado está legalmente

autorizada a reivindicar a propriedade do nome da empresa ou organização fornecida. Esse campo pode conter no máximo 60 caracteres.

Nome do Host do IMM

Use esse campo para indicar o nome do host do IMM que aparece atualmente na barra de endereço da web do navegador.

Certifique-se de que o valor digitado nesse campo corresponda exatamente ao nome do host como ele é conhecido pelo navegador da web. O navegador compara o nome do host no endereço da web resolvido com o nome que aparece no certificado. Para evitar avisos de certificado do navegador, o valor que é usado nesse campo deve corresponder ao nome do host que é utilizado pelo navegador para conectar-se ao IMM. Por exemplo, se o endereço na barra de endereços da web for `http://mm11.xyz.com/private/main.ssi`, o valor utilizado para o campo Nome do Host IMM deverá ser `mm11.xyz.com`. Se o endereço da web for `http://mm11/private/main.ssi`, o valor usado deverá ser `mm11`. Se o endereço da web for `http://192.168.70.2/private/main.ssi`, o valor usado deverá ser `192.168.70.2`.

Esse atributo de certificado geralmente é referido como o nome comum.

Esse campo pode conter no máximo 60 caracteres.

Pessoa de Contato

Use esse campo para indicar o nome de uma pessoa de contato responsável pelo IMM. Esse campo pode conter no máximo 60 caracteres.

Endereço de Email

Use esse campo para indicar o endereço de email de uma pessoa de contato responsável pelo IMM. Esse campo pode conter no máximo 60 caracteres.

Dados opcionais do certificado Os seguintes campos de entrada do usuário são opcionais para gerar um certificado autoassinado ou uma solicitação de assinatura de certificado:

Unidade Organizacional

Use esse campo para indicar a unidade dentro da empresa ou organização que possui o IMM. Esse campo pode conter no máximo 60 caracteres.

Sobrenome

Use esse campo para informações adicionais, como o sobrenome de uma pessoa que é responsável pelo IMM. Esse campo pode conter no máximo 60 caracteres.

Nome Dado

Use esse campo para informações adicionais, como o nome dado de uma pessoa que é responsável pelo IMM. Esse campo pode conter no máximo 60 caracteres.

Iniciais

Use esse campo para informações adicionais, como as iniciais de uma pessoa que é responsável pelo IMM. Esse campo pode conter no máximo 20 caracteres.

Qualificador de DN

Use esse campo para informações adicionais, como um qualificador de nome distinto para o IMM. Esse campo pode conter no máximo 60 caracteres.

Atributos de solicitação de assinatura de certificado Os campos a seguir são opcionais, a menos que sejam requeridos pela autoridade de certificação selecionada:

Senha do Desafio

Use esse campo para designar uma senha à solicitação de assinatura de certificado. Esse campo pode conter no máximo 30 caracteres.

Nome Não Estruturado

Use esse campo para informações adicionais, como um nome não estruturado que é designado ao IMM. Esse campo pode conter no máximo 60 caracteres.

5. Depois de concluir as informações, clique em **Gerar CSR**. As novas chaves de criptografia e o certificado são gerados. Esse processo pode levar alguns minutos.
6. Clique em **Download do CSR** e, em seguida, clique em **Salvar** para salvar o arquivo em sua estação de trabalho. O arquivo produzido quando você cria uma solicitação de assinatura de certificado está em formato DER. Se a autoridade de certificação esperar os dados em algum outro formato, como PEM, o arquivo poderá ser convertido usando uma ferramenta como OpenSSL (<http://www.openssl.org>). Se a autoridade de certificação pedir a você para copiar o conteúdo do arquivo de solicitação de assinatura de certificado em uma janela do navegador da web, geralmente é esperado o formato PEM. O comando para converter uma solicitação de assinatura de certificado do formato DER para PEM usando OpenSSL é semelhante ao exemplo a seguir:

```
openssl req -in csr.der -inform DER -out csr.pem -outform PEM
```
7. Envie a solicitação de assinatura de certificado para a autoridade de certificação. Quando a autoridade de certificação retornar o certificado assinado, poderá ser necessário converter o certificado para o formato DER. (Se você recebeu o certificado como texto em um email ou em uma página da web, provavelmente ele estará no formato PEM.) É possível alterar o formato usando uma ferramenta fornecida por sua autoridade de certificação ou utilizando uma ferramenta como a OpenSSL (<http://www.openssl.org>). O comando para converter um certificado do formato PEM para DER é semelhante ao exemplo a seguir:

```
openssl x509 -in cert.pem -inform PEM -out cert.der -outform DER
```

Acesse a etapa 8 depois que o certificado assinado retornar da autoridade de certificação.
8. Na área de janela de navegação, clique em **Segurança**. Role para a área **Gerenciamento de Certificado do Servidor SSL** ou a área **Gerenciamento de Certificado do IBM Systems Director sobre HTTPS**.
9. Clique em **Importar um Certificado Assinado**.
10. Clique em **Procurar**.
11. Clique no arquivo de certificado desejado e, em seguida, clique em **Abrir**. O nome do arquivo (incluindo o caminho completo) é exibido no campo ao lado do botão **Procurar**.
12. Clique em **Importar Certificado do Servidor** para iniciar o processo. Um indicador de progresso é exibido conforme o arquivo é transferido para armazenamento no IMM. Continue exibindo essa página até a conclusão da transferência.

Ativando SSL para o servidor da web seguro ou IBM Systems Director sobre HTTPS

Conclua as etapas a seguir para ativar o servidor da web seguro.

Nota: Para ativar o SSL, um certificado SSL válido deve ser instalado.

1. Na área de janela de navegação, clique em **Segurança**. A página que é exibida mostra que um certificado do servidor SSL válido está instalado. Se o status do certificado de servidor SSL não mostrar que um certificado SSL válido está instalado, acesse “Gerenciamento de certificado do servidor SSL” na página 83.
2. Role para a área **Configuração do Servidor SSL para servidor da web** ou para a área **Configuração do IBM Systems Director sobre HTTPS**, selecione **Ativado** no campo **Cliente SSL** e, em seguida, clique em **Salvar**. O valor selecionado entrará em vigor na próxima vez em que o IMM for reiniciado.

Gerenciamento de certificado de cliente SSL

O cliente SSL requer que um certificado válido e uma chave de criptografia privada correspondente sejam instalados antes da ativação do SSL. Dois métodos estão disponíveis para gerar a chave privada e o certificado requerido: usando um certificado autoassinado ou um certificado assinado por uma autoridade de certificação.

O procedimento para gerar a chave de criptografia privada e o certificado para o cliente SSL é o mesmo procedimento para o servidor SSL, exceto que você usa a área **Gerenciamento de Certificado de Cliente SSL** da página da web **Segurança** em vez da área **Gerenciamento de Certificado do Servidor SSL**. Se você deseja usar um certificado autoassinado para o cliente SSL, consulte “Gerando um certificado autoassinado” na página 83. Se você deseja usar um certificado assinado por autoridade de certificação para o cliente SSL, consulte “Gerando uma solicitação de assinatura de certificado” na página 85 para obter mais informações.

Gerenciamento de certificado confiável do cliente SSL

O cliente SSL seguro (cliente LDAP) usa certificados confiáveis para identificar positivamente o servidor LDAP. Um certificado confiável pode ser o certificado da autoridade de certificação que assinou o certificado do servidor LDAP ou pode ser o certificado real do servidor LDAP. Pelo menos um certificado deve ser importado para o IMM antes de o cliente SSL ser ativado. É possível importar até três certificados confiáveis.

Para importar um certificado confiável, conclua as etapas a seguir:

1. Na área de janela de navegação, selecione **Segurança**.
2. Na área **Configuração do Cliente SSL para Cliente LDAP**, certifique-se de que o cliente SSL esteja desativado. Se não estiver desativado, selecione **Desativado** no campo **Cliente SSL** e, em seguida, clique em **Salvar**.
3. Role para a área **Gerenciamento de Certificado Confiável do Client SSL**.
4. Clique em **Importar** ao lado de um dos campos **Certificado CA Confiável 1**.
5. Clique em **Procurar**.
6. Selecione o arquivo de certificado desejado e clique em **Abrir**. O nome do arquivo (incluindo o caminho completo) é exibido na caixa ao lado do botão **Procurar**.

7. Para iniciar o processo de importação, clique em **Importar Certificado**. Um indicador de progresso é exibido conforme o arquivo é transferido para armazenamento no IMM. Continue a exibir essa página até que a transferência esteja concluída.

O botão **Remover** está disponível agora para a opção Certificado CA Confiável

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

Você pode importar outros certificados confiáveis usando os botões **Importar** do Certificado CA Confiável 2 e Certificado CA Confiável 3.

Ativando SSL para o cliente LDAP

Use a área **Configuração do Cliente SSL para Cliente LDAP** da página Segurança para ativar ou desativar o SSL para o Cliente LDAP. Para ativar o SSL, um certificado de cliente SSL válido e pelo menos um certificado confiável deve ser instalado primeiro.

Para ativar o SSL para o cliente, conclua as etapas a seguir:

1. Na área de janela de navegação, clique em **Segurança**.
A página Segurança mostra um certificado cliente SSL instalado e o Certificado CA Confiável 1.
2. Na página Configuração do Cliente SSL para Cliente LDAP, selecione **Ativado** no campo **Cliente SSL**.

Nota:

- a. O valor selecionado (Ativado ou Desativado) entra em vigor imediatamente.
 - b. Para poder ativar o SSL, um certificado SSL válido deve estar em vigor.
 - c. Seu servidor LDAP deve suportar SSL3 ou TLS para ser compatível com a implementação de SSL que o cliente LDAP utiliza.
3. Clique em **Salvar**. O valor selecionado entra em vigor imediatamente.

Gerenciamento de Criptografia

Use a área **Gerenciamento de Criptografia** da página Segurança para configurar a força dos conjuntos de cifras para servidores SSL no IMM, incluindo o servidor HTTPS e o IBM System Director sobre HTTPS.

Os modos de gerenciamento de criptografia têm diferentes forças de segurança. O modo Compatível Básico é o modo padrão e é compatível com versões de firmware mais antigas e com navegadores e outros clientes de rede que não implementam os requisitos de segurança mais rígidos. O modo de Alta Segurança restringe o IMM a usar uma chave simétrica SSL não menor que 128 bits.

Para configurar o modo, conclua as etapas a seguir:

1. Na área de janela de navegação, clique em **Segurança**.
2. Localize a área **Gerenciamento de Criptografia** e selecione **Modo Compatível Básico** ou **Modo de Alta Segurança**.
3. Clique em **Salvar**, e o modo selecionado entrará em vigor depois que o IMM tiver sido reiniciado.

Configurando o servidor Shell Seguro

O recurso Shell Seguro (SSH) fornece acesso seguro aos recursos de interface da linha de comandos e redirecionamento serial (console de texto) do IMM.

Os usuários do Shell Seguro são autenticados com a troca de ID de usuário e senha. A senha e o ID de usuário são enviados após o canal de criptografia ser estabelecido. O par de ID de usuário e senha pode ser um dos 12 IDs de usuário e senhas armazenados localmente, ou podem estar armazenados em um servidor LDAP. A autenticação de chave pública não é suportada.

Gerando uma chave do servidor Shell Seguro

Uma chave do servidor Shell Seguro é usada para autenticar a identidade do servidor Shell Seguro para o cliente. O Shell Seguro deve ser desativado antes de você criar uma nova chave privada do servidor Shell Seguro. É necessário criar uma chave do servidor antes de ativar o servidor Shell Seguro.

Ao solicitar uma nova chave do servidor, uma chave Rivest, Shamir e Adelman e uma chave DSA são criadas para permitir o acesso ao IMM a partir de um cliente SSH versão 2. Por segurança, o backup da chave privada do servidor Shell Seguro não é feito durante uma operação de salvamento e restauração da configuração.

Para ativar uma nova chave do servidor Shell Seguro, conclua as etapas a seguir:

1. Na área de janela de navegação, clique em **Segurança**.
2. Role para a área **Servidor Shell Seguro (SSH)** e certifique-se de que o servidor Shell Seguro esteja desativado. Se ele não estiver desativado, selecione **Desativado** no campo **Servidor SSH** e, em seguida, clique em **Salvar**.
3. Role para a área **Gerenciamento de Chave do Servidor SSH**.
4. Clique em **Gerar Chave Privada do Servidor SSH**. Uma janela de progresso é aberta. Aguarde a conclusão da operação.

Ativando o Servidor Shell Seguro

Na página Segurança, é possível ativar ou desativar o servidor Shell Seguro. A seleção que você faz só tem efeito depois que o IMM é reiniciado. O valor exibido na tela (Ativado ou Desativado) é o último valor selecionado e é o valor que é usado quando o IMM é reiniciado.

Nota: Só será possível ativar o servidor Shell Seguro se uma chave privada válida do servidor Shell Seguro estiver instalada.

Para ativar o servidor Shell Seguro, conclua as etapas a seguir:

1. Na área de janela de navegação, clique em **Segurança**.
2. Role para a área **Servidor Shell Seguro (SSH)**.
3. Clique em **Ativado** no campo **Servidor SSH**.
4. Na área de janela de navegação, clique em **Reiniciar IMM** para reiniciar o IMM.

Usando o Servidor Shell Seguro

Se você estiver usando o cliente Shell seguro incluído no Red Hat Linux versão 7.3, para iniciar uma sessão de Shell Seguro para um IMM com o endereço de rede 192.168.70.132, digite um comando semelhante ao seguinte exemplo:

```
ssh -x -l userid 192.168.70.132
```

em que -x indica nenhum encaminhamento do X Window System e -l indica que a sessão deve utilizar o ID de usuário *userid*.

Restaurando e modificando a configuração do IMM

É possível restaurar uma configuração salva por completo, ou modificar campos-chave na configuração salva antes de restaurar a configuração para o IMM. A modificação do arquivo de configuração antes de restaurá-lo possibilita configurar diversos IMM com configurações semelhantes. É possível especificar rapidamente os parâmetros que exigem valores, como nomes e endereços IP, sem precisar inserir informações comuns compartilhadas.

Para restaurar ou modificar a configuração atual, conclua as etapas a seguir:

1. Efetue login no IMM no qual você deseja restaurar a configuração. Para obter mais informações, consulte Capítulo 2, “Abrindo e usando a interface da web do IMM”, na página 11.
2. Na área de janela de navegação, clique em **Arquivo de Configuração**.
3. Na área **Restaurar Configuração do IMM**, clique em **Procurar**.
4. Clique no arquivo de configuração desejado; em seguida, clique em **Abrir**. O arquivo (incluindo o caminho completo) aparece na caixa ao lado da opção **Procurar**.
5. Se você não deseja fazer mudanças no arquivo de configuração, clique em **Restaurar**. Uma nova janela é aberta com as informações de configuração do IMM. Certifique-se de que esta seja a configuração que você deseja restaurar. Se não for a configuração correta, clique em **Cancelar**.

Para fazer mudanças no arquivo de configuração antes de restaurar a configuração, clique em **Modificar e Restaurar** para abrir uma janela de resumo de configuração editável. Inicialmente, apenas os campos que permitem mudanças são exibidos. Para alterar entre essa visualização e a visualização de resumo de configuração completa, clique no botão **Alternar Visualização** na parte superior ou inferior da janela. Para modificar o conteúdo de um campo, clique na caixa de texto correspondente e digite os dados.

Nota: Ao clicar em **Restaurar** ou **Modificar e Restaurar**, uma janela de alerta poderá ser aberta se o arquivo de configuração que você está tentando restaurar foi criado por um tipo diferente de processador de serviços ou foi criado pelo mesmo tipo de processador de serviços com firmware mais antigo (e portanto com menos funcionalidade). Essa mensagem de alerta inclui uma lista de funções de gerenciamento de sistemas que você deve configurar após a conclusão da restauração. Algumas funções requerem configurações em mais de uma janela.

6. Para continuar restaurando esse arquivo para o IMM, clique em **Restaurar Configuração**. Um indicador de progresso é exibido à medida que o firmware no IMM é atualizado. Uma janela de confirmação é aberta para verificar se a atualização foi bem-sucedida.

Nota: As configurações de segurança na página Segurança não são restauradas pela operação de restauração. Para modificar configurações de segurança, consulte “Protegendo o servidor da web, IBM Systems Director e LDAP seguro” na página 82.

7. Depois de receber uma confirmação de que o processo de restauração está concluído, na área de janela de navegação, clique em **Reiniciar IMM**; em seguida, clique em **Reiniciar**.
8. Clique em **OK** para confirmar que você deseja reiniciar o IMM.
9. Clique em **OK** para fechar a janela atual do navegador.

10. Para efetuar login no IMM novamente, inicie o navegador e siga o processo normal de login.

Usando o arquivo de configuração

Selecione **Arquivo de Configuração** na área de janela de navegação para fazer backup e restaurar a configuração do IMM.

Importante: As definições da página Segurança não são salvas com a operação de backup e não podem ser restauradas com a operação de restauração.

Fazendo backup da sua configuração atual

É possível fazer download de uma cópia da sua atual configuração do IMM para o computador cliente que está executando a interface da web do IMM. Use essa cópia de backup para restaurar a configuração do IMM se ela for alterada acidentalmente ou danificada. Use-a como uma base que você pode modificar para configurar vários IMM com configurações semelhantes.

As informações de configuração que são salvas nesse procedimento não incluem as definições de configuração de firmware do servidor System x nem quaisquer definições da IPMI que não são comuns com as interfaces com o usuário não IMPI.

Para fazer backup de sua configuração atual, conclua as etapas a seguir:

1. Efetue login no IMM no qual você deseja fazer backup de sua configuração atual. Para obter mais informações, consulte Capítulo 2, “Abrindo e usando a interface da web do IMM”, na página 11.
2. Na área de janela de navegação, clique em **Arquivo de Configuração**.
3. Na área **Fazer Backup da Configuração do IMM**, clique em **Visualizar o resumo da configuração atual**.
4. Verifique as definições e, em seguida, clique em **Fechar**.
5. Para fazer backup dessa configuração, clique em **Backup**.
6. Digite um nome para o backup, selecione o local em que o arquivo será salvo e, em seguida, clique em **Salvar**.

No Mozilla Firefox, clique em **Salvar Arquivo**; em seguida, clique em **OK**.

No Microsoft Internet Explorer, clique em **Salvar este arquivo em disco**; em seguida, clique em **OK**.

Restaurando e modificando a configuração do IMM

É possível restaurar uma configuração salva por completo, ou modificar campos-chave na configuração salva antes de restaurar a configuração para o IMM. A modificação do arquivo de configuração antes de restaurá-lo possibilita configurar diversos IMM com configurações semelhantes. É possível especificar rapidamente os parâmetros que exigem valores, como nomes e endereços IP, sem precisar inserir informações comuns compartilhadas.

Para restaurar ou modificar a configuração atual, conclua as etapas a seguir:

1. Efetue login no IMM no qual você deseja restaurar a configuração. Para obter mais informações, consulte Capítulo 2, “Abrindo e usando a interface da web do IMM”, na página 11.
2. Na área de janela de navegação, clique em **Arquivo de Configuração**.
3. Na área **Restaurar Configuração do IMM**, clique em **Procurar**.

4. Clique no arquivo de configuração desejado; em seguida, clique em **Abrir**. O arquivo (incluindo o caminho completo) aparece na caixa ao lado da opção **Procurar**.

5. Se você não deseja fazer mudanças no arquivo de configuração, clique em **Restaurar**. Uma nova janela é aberta com as informações de configuração do IMM. Certifique-se de que esta seja a configuração que você deseja restaurar. Se não for a configuração correta, clique em **Cancelar**.

Para fazer mudanças no arquivo de configuração antes de restaurar a configuração, clique em **Modificar e Restaurar** para abrir uma janela de resumo de configuração editável. Inicialmente, apenas os campos que permitem mudanças são exibidos. Para alterar entre essa visualização e a visualização de resumo de configuração completa, clique no botão **Alternar Visualização** na parte superior ou inferior da janela. Para modificar o conteúdo de um campo, clique na caixa de texto correspondente e digite os dados.

Nota: Ao clicar em **Restaurar** ou **Modificar e Restaurar**, uma janela de alerta poderá ser aberta se o arquivo de configuração que você está tentando restaurar foi criado por um tipo diferente de processador de serviços ou foi criado pelo mesmo tipo de processador de serviços com firmware mais antigo (e portanto com menos funcionalidade). Essa mensagem de alerta inclui uma lista de funções de gerenciamento de sistemas que você deve configurar após a conclusão da restauração. Algumas funções requerem configurações em mais de uma janela.

6. Para continuar restaurando esse arquivo para o IMM, clique em **Restaurar Configuração**. Um indicador de progresso é exibido à medida que o firmware no IMM é atualizado. Uma janela de confirmação é aberta para verificar se a atualização foi bem-sucedida.

Nota: As configurações de segurança na página Segurança não são restauradas pela operação de restauração. Para modificar configurações de segurança, consulte “Protegendo o servidor da web, IBM Systems Director e LDAP seguro” na página 82.

7. Depois de receber uma confirmação de que o processo de restauração está concluído, na área de janela de navegação, clique em **Reiniciar IMM**; em seguida, clique em **Reiniciar**.
8. Clique em **OK** para confirmar que você deseja reiniciar o IMM.
9. Clique em **OK** para fechar a janela atual do navegador.
10. Para efetuar login no IMM novamente, inicie o navegador e siga o processo normal de login.

Restaurando padrões

Use o link **Restaurar Padrões** para restaurar a configuração padrão do IMM, se você tiver acesso de Supervisor.

Atenção: Quando você clicar em **Restaurar Padrões**, perderá todas as modificações feitas no IMM.

Para restaurar os padrões do IMM, conclua as etapas a seguir:

1. Efetue login no IMM. Para obter mais informações, consulte Capítulo 2, “Abrindo e usando a interface da web do IMM”, na página 11.

2. Na área de janela de navegação, clique em **Restaurar Padrões** para restaurar as configurações padrão do IMM. Se este for um servidor local, a conexão TCP/IP será interrompida e você deverá reconfigurar a interface de rede para restaurar a conectividade.
3. Efetue login novamente para usar a interface da web do IMM.
4. Reconfigure a interface de rede para restaurar a conectividade. Para obter informações sobre a interface de rede, consulte “Configurando as interfaces de rede” na página 38.

Reiniciando o IMM

Use o link **Reiniciar IMM** para reiniciar o IMM. Você só poderá executar essa função se tiver acesso de Supervisor. Qualquer conexão Ethernet será eliminada temporariamente. Você deve efetuar login novamente para usar a interface da web do IMM.

Para reiniciar o IMM, conclua as etapas a seguir:

1. Efetue login no IMM. Para obter mais informações, consulte Capítulo 2, “Abrindo e usando a interface da web do IMM”, na página 11.
2. Na área de janela de navegação, clique em **Reiniciar IMM** para reiniciar o IMM. As suas conexões de TCP/IP ou modem são interrompidas.
3. Efetue login novamente para usar a interface da web do IMM.

Partição escalável

O IMM permite que você configure e controle o sistema em um complexo escalável.

O IMM permite que você configure e controle o sistema em um complexo escalável. Se existir um erro com o servidor, o IMM retornará um código de evento para os logs de eventos (consulte “Visualizando os logs de eventos” na página 106).

1. Efetue login no IMM no qual você deseja restaurar a configuração. Para obter mais informações, consulte Capítulo 2, “Abrindo e usando a interface da web do IMM”, na página 11.
2. Na área de janela de navegação, clique em **Partição Escalável**; em seguida, clique em **Gerenciar Partições**.

Recurso de Consultor de Serviço

O recurso Consultor de Serviço detecta e coleta eventos de erro de hardware do sistema e encaminha automaticamente os dados ao Suporte IBM para determinação de problemas. O recurso Consultor de Serviço também pode coletar dados sobre os erros do sistema e encaminhar esses dados para o suporte IBM. Consulte a documentação de seu servidor para ver se ele suporta esse recurso. As instruções para configurar, testar e manter o Consultor de Serviço estão incluídas nos tópicos a seguir.

- Configurando o Consultor de Serviço
- Usando o Consultor de Serviço

Configurando o Consultor de Serviço

Para configurar o Consultor de Serviço, conclua as etapas a seguir.

1. Efetue login no IMM no qual você deseja ativar o Consultor de Serviço. Para obter mais informações, consulte Capítulo 2, “Abrindo e usando a interface da web do IMM”, na página 11.
2. Na área de janela de navegação, clique em **Consultor de Serviço**.
3. Se esta for a primeira vez que você usa essa opção, ou se o IMM foi reconfigurado para os valores padrão, você deverá ler e aceitar o contrato de licença.
 - a. Clique em **Visualizar Termos e Condições** para visualizar o contrato do Consultor de Serviço.
 - b. Clique em **Eu aceito o contrato** na página Termos e Condições para ativar o Consultor de Serviço.
4. Clique na guia **Configurações do Consultor de Serviço**.
É exibida uma página semelhante à da ilustração a seguir.

5. Insira as informações de contato para o administrador do servidor. Consulte a tabela a seguir para obter uma explicação dos campos **Informações de Contato**.

Tabela 15. Informações de Contato

Campo	Descrição
IBM Service Support Center	Especifique o código do país para o IBM Service Support Center nesse campo. Este é um código de país ISO de dois caracteres e se aplica apenas para aqueles com acesso ao IBM Service Support Center.
Nome da Empresa	Especifique o nome da organização ou da empresa da pessoa de contato nesse campo. Esse campo pode conter de 1 a 30 caracteres.
Nome do Contato	Especifique o nome da organização ou da empresa da pessoa de contato nesse campo. Esse campo pode conter de 1 a 30 caracteres.
Telefone	Especifique o número de telefone da pessoa de contato nesse campo. Esse campo pode conter de 5 a 30 caracteres.
Email	Especifique o endereço de email da pessoa de contato nesse campo. O comprimento máximo desse campo é de 30 caracteres.

Tabela 15. Informações de Contato (continuação)

Campo	Descrição
Endereço	Especifique o endereço em que o IMM está fisicamente localizado nesse campo. Esse campo pode conter de 1 a 30 caracteres.
Cidade	Especifique a cidade ou localidade onde o IMM está fisicamente localizado nesse campo.
Estado	Especifique o estado onde o IMM está fisicamente localizado nesse campo. Esse campo pode conter de 2 a 3 caracteres.
Código de endereçamento postal	Especifique o código de endereçamento postal do local para este servidor nesse campo. Esse campo pode conter de 1 a 9 caracteres, (somente caracteres alfanuméricos são válidos).

6. Crie um proxy HTTP se o IMM não tiver uma conexão de rede direta com o Suporte IBM. Conclua as etapas a seguir para configurar as informações de conectividade de saída.
 - a. No campo **Você precisa de um proxy**, clique em **Sim**. Consulte a ilustração anterior.

É exibida uma página semelhante à da ilustração a seguir.

- b. Insira o **Local do Proxy**, a **Porta do Proxy**, o **Nome do Usuário** e a **Senha**.
7. Clique em **Salvar Suporte IBM** para salvar suas mudanças.
8. Clique em **Ativar Suporte IBM** (que está localizado perto da parte superior da página) para permitir que o Consultor de Serviço entre em contato com o Suporte IBM quando um código de evento que permite manutenção for gerado.

Nota: Depois de ativar o Suporte IBM, um código de teste é enviado para o site do suporte IBM.

9. Clique na guia **Log de Atividades do Consultor de Serviço** para visualizar o status do código de teste.

É exibida uma página semelhante à da ilustração a seguir.

10. Se você deseja permitir que outro provedor de serviços receba os códigos de evento antes de você entrar em contato com o Suporte IBM, clique em **Ativar Relatório para Servidor FTP/TFTP**.

Atenção: Ao inserir um servidor FTP/TFTP, você está consentindo no compartilhamento de dados de serviço de hardware com o proprietário desse

servidor FTP/TFTP. No compartilhamento dessas informações, você garante que está em conformidade com todas as leis de importação/exportação.

Uma página semelhante à da ilustração a seguir é exibida.

FTP/TFTP Server of Service Data

Use this feature to send hardware serviceable events and data to the FTP/TFTP site you specify. If an approved service provider is providing your hardware warranty, you should specify the FTP/TFTP site provided by your service provider. Information contained in the service data will assist your service provider in correcting the hardware issue.

☒ Enable Report to FTP/TFTP Server

By entering an FTP/TFTP server, you are consenting to share hardware service data with the owner of that FTP/TFTP server. In sharing this information, you warrant that you are in compliance with all import/export laws.

Protocol: FTP

FTP/TFTP Server Fully Qualified Hostname or IP Address: Port: 0

User Name:

Password:

Usando o Consultor de Serviço

Depois que o Consultor de Serviço estiver configurado, você poderá visualizar o log de atividades ou gerar uma mensagem de teste.

Conclua as etapas a seguir para criar um relatório de problemas de hardware para seu servidor:

1. Efetue login no IMM no qual você deseja usar o Consultor de Serviço. Para obter mais informações, consulte Capítulo 2, “Abrindo e usando a interface da web do IMM”, na página 11.
2. Na área de janela de navegação, clique em **Consultor de Serviço**.
3. Clique na guia **Call Home Manual**.

É exibida uma página semelhante à da ilustração a seguir.

Service Advisor Activity Log Service Advisor Settings **Manual Call Home** Test Call Home

You can use this feature to make a call home for any known hardware issues that did not generate an automatic call home event to IBM Support or FTP/TFTP Server. Manually calling home an event sends the same data and will be processed in the same way as an automatic call home event.

Problem Description

Ambient temp is high

Manual Call Home

4. Conclua as etapas a seguir para efetuar call home manualmente de um evento.
 - a. Insira a descrição do problema no campo **Descrição do Problema**.
 - b. Clique no botão **Call Home Manual**.
5. Para gerar uma mensagem de teste, clique na guia **Call Home de Teste**; em seguida, selecione o botão **Call Home de Teste**.

Notas:

- O menu do call home de teste valida o caminho de comunicação entre IMM e o servidor IBM ou FTP/TFTP com as configurações atuais.
 - Se o teste não for bem-sucedido, verifique a configuração da rede.
 - Para relatório ao Suporte IBM, o Consultor de Serviço requer a configuração correta do endereço do servidor DNS no IMM.
 - Se a chamada for bem-sucedida, um Número de Serviço Designado ou número de chamado será designado. O chamado que é aberto no Suporte IBM será identificado como um chamado de teste. Nenhuma ação é requerida do Suporte IBM para um chamado de teste e a chamada será fechada.
6. Clique na guia **Log de Atividades do Consultor de Serviço** para visualizar o status do log de atividades.

É exibida uma página semelhante à da ilustração a seguir.

Service Advisor Activity Log

Service Advisor Settings

Manual Call Home

Test Call Home

Help

Refresh

Display For Both IBM Support and FTP/TFTP Server

Corrected	IBM Support		FTP/TFTP Server	Event ID	Event Severity	Date/Time	Message	
	Send	Assigned Num						
☐	NO	Pending	N/A	Pending	0x400000ca00000000	Info	08/07/2012: 18:58:41	Manual Call Home by USERID: Ambient temp is high.
☐	NO	Pending	N/A	Pending	0x400000c900000000	Info	08/07/2012: 18:31:56	Test Call Home Generated by USERID
☐	NO	Success	672P492FG3	Disabled	0x400000c900000000	Info	08/07/2012: 18:29:25	Test Call Home Generated by USERID
☐	NO	Disabled	N/A	Pending	0x400000c900000000	Info	08/07/2012: 17:47:14	Test Call Home Generated by USERID
End Of Log								

Save

You can use the [Call Home Exclusion List](#) to specify specific call home events not to be reported

Notas:

- O log de atividades mostra os últimos cinco eventos de Call Home, incluindo os eventos de Call Home de Teste e Call Home Manual.
- Os resultados no campo **Enviar** podem ser um dos seguintes:

Sucesso

A chamada foi recebida com êxito na IBM ou no FTP/TFTP. O campo **Número de Serviço Designado** inclui um número de chamado de problema.

Pendente

O evento Call Home está em andamento.

Com Falha

O evento Call Home falhou. No caso de uma falha de evento call home, entre em contato com o Suporte IBM para relatar o evento de serviço de hardware. Os eventos Call Home que falharam não serão tentados novamente.

- Depois de resolver um evento, clique na caixa de seleção **Corrigido** para esse evento para facilitar a localização de eventos não resolvidos.

Nota: Se a caixa de seleção **Corrigido** não estiver marcada para um evento, a próxima ocorrência do mesmo evento não será *called home* até cinco dias após a primeira ocorrência do evento.

- Clique em **Atualizar** para exibir as informações mais recentes.

Nota: O **Número de Serviço Designado** pode ser usado para fazer referência ao evento Call Home ao se comunicar com o Suporte IBM.

- Para remover um evento especificado do relatório para o Suporte IBM, execute as etapas a seguir:
 - Clique no link **Lista de Exclusão Call Home**. Uma página semelhante à da ilustração a seguir é exibida.

Call Home Exclusion List

This table below shows the list of event IDs that will not be reported by call home. You can add events to this table by entering an event ID in the text box and clicking the add button. Event IDs can be obtained from the [Event Log](#) and [Service Advisor Activity Log](#) and entered into the textbox using the copy-and-paste function.

A maximum of 20 events can be added to this exclusion list; currently 20 more events can be added.

Selected	Index	Event ID
No entries		

- b. Insira o ID do Evento hexadecimal no campo **ID do Evento**.
- c. Clique em **Incluir**.

Encerrando sessão

Para efetuar logoff do IMM ou de outro servidor remoto, clique em **Efetuar Logoff** na área de janela de navegação.

Capítulo 4. Monitorando o status do servidor

Use os links sob o título **Monitores** da área de janela de navegação para visualizar o status do servidor que você está acessando.

Nas páginas Status do Sistema, é possível:

- Monitorar o status de energia do servidor e visualizar o estado do sistema operacional
- Visualizar as leituras de temperatura, limites de voltagem e velocidades de ventilador do servidor
- Visualizar a captura de tela mais recente de falha do sistema operacional do servidor
- Visualizar a lista de usuários que efetuaram login no IMM

Na página Indicadores Luminosos Virtuais, é possível visualizar o nome, a cor e o status de qualquer LED que esteja aceso em um servidor.

Na página Log de Eventos, é possível:

- Visualizar determinados eventos que são registrados no log de eventos do IMM
- Visualizar a severidade dos eventos

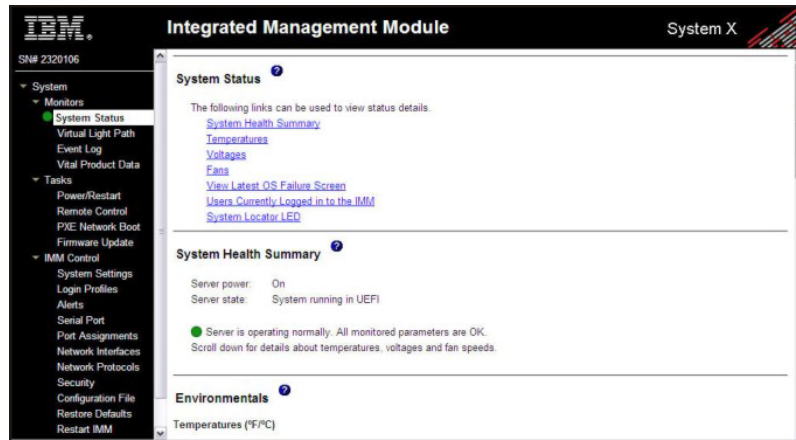
Na página Dados Vitais do Produto (VPD), é possível visualizar os dados vitais do produto.

Visualizando o status do sistema

Na página Status do Sistema, é possível monitorar leituras de temperatura, limites de voltagem e status do ventilador de seu servidor. É possível também visualizar a tela de falha do sistema operacional mais recente, os usuários que estão com login efetuado no IMM e o LED do localizador do sistema.

Para visualizar o funcionamento do sistema e as informações de ambiente do servidor, conclua as etapas a seguir:

1. Efetue login no IMM. Para obter mais informações, consulte Capítulo 2, “Abrindo e usando a interface da web do IMM”, na página 11.
2. Na área de janela de navegação, clique em **Status do Sistema** para visualizar uma atualização gerada dinamicamente do funcionamento geral do servidor. Uma página semelhante à da ilustração a seguir é exibida.



O status do servidor determina a mensagem que é mostrada na parte superior da página Resumo do Funcionamento do Sistema. Um dos seguintes símbolos é exibido:

- Um círculo verde sólido e a frase **Server is operating normally**
- Um círculo vermelho que contém um X ou um triângulo amarelo que contém um ponto de exclamação e a frase **One or more monitored parameters are abnormal**

Se os parâmetros monitorados estiverem operando fora dos intervalos normais, uma lista dos parâmetros anormais específicos será exibida na página Resumo do Funcionamento do Sistema.

3. Role para baixo até a área **Temperatura** na seção **Ambientais** da página, que inclui as informações de temperatura, voltagem e velocidade do ventilador.

O IMM controla as leituras de temperatura e os níveis de limite atuais dos componentes do sistema, como microprocessadores, placa-mãe e painel traseiro da unidade de disco rígido. Quando você clica em uma leitura de temperatura, uma nova janela é aberta.

Ambient Temp Thresholds (°C)			
Sensors	Non - Critical	Critical	Fatal
Upper Threshold	34.000000	37.000000	41.000000
Lower Threshold	N/A	N/A	N/A

A página Limites de Temperatura exibe os níveis de temperatura nos quais o IMM reage. Os valores de limite de temperatura estão predefinidos no servidor remoto e não podem ser alterados.

As temperaturas relatadas são medidas com relação aos seguintes intervalos de limite:

Não Crítico

Quando a temperatura atinge um valor especificado, um alerta de temperatura é enviado aos receptores de alertas remotos configurados. Você deve marcar a caixa de seleção **Alertas de Aviso** na área

Configurações de Alertas SNMP da página Alertas ou a caixa de seleção **Alertas de Aviso** na página Receptor de Alertas Remotos para que o alerta seja enviado.

Para obter mais informações sobre a seleção de opções de alerta, consulte “Configurando definições de alerta SNMP” na página 34 ou “Configurar receptores de alerta remoto” na página 32.

Crítico

Quando a temperatura atinge um valor especificado superior ao valor de aviso (o limite de encerramento temporário), um segundo alerta de temperatura é enviado para os receptores de alertas remotos configurados e o servidor inicia o processo de encerramento com um encerramento ordenado do sistema operacional. O servidor então se desliga. Você deve marcar a caixa de seleção **Alertas Críticos** na área **Configurações de Alertas SNMP** da página Alertas ou a caixa de seleção **Alertas Críticos** na página Receptor de Alertas Remotos para que o alerta seja enviado.

Para obter mais informações sobre a seleção de opções de alerta, consulte “Configurando definições de alerta SNMP” na página 34 ou “Configurar receptores de alerta remoto” na página 32.

Fatal

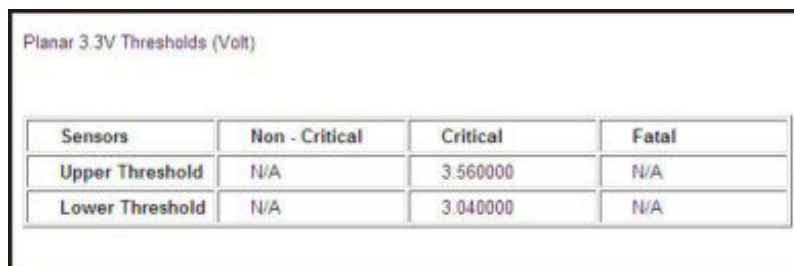
Quando a temperatura atinge um valor especificado superior ao valor de encerramento temporário (o limite de encerramento permanente), o servidor é encerrado imediatamente e envia um alerta para os receptores de alertas remotos configurados. Você deve marcar a caixa de seleção **Alertas Críticos** na área **Configurações de Alertas SNMP** da página Alertas ou a caixa de seleção **Alertas Críticos** na página Receptor de Alertas Remotos para que o alerta seja enviado.

Para obter mais informações sobre a seleção de opções de alerta, consulte “Configurando definições de alerta SNMP” na página 34 ou “Configurar receptores de alerta remoto” na página 32.

O IMM gera um evento não crítico ou crítico quando o limite é atingido e inicia ações de encerramento, se elas forem requeridas.

4. Role para baixo até a área **Voltagens**. O IMM enviará um alerta se alguma voltagem de fonte de alimentação monitorada ficar fora de seus intervalos operacionais especificados.

Se você clicar em uma leitura de voltagem, uma nova janela será aberta.



Sensors	Non - Critical	Critical	Fatal
Upper Threshold	N/A	3.560000	N/A
Lower Threshold	N/A	3.040000	N/A

A página Limites de Voltagem exibe os intervalos de voltagem nos quais o IMM reage. Os valores de limite de voltagem estão predefinidos no servidor remoto e não podem ser alterados.

A interface da web do IMM exibe as leituras de voltagem da placa-mãe e dos módulos do regulador de voltagem (VRM). O sistema define um intervalo de voltagem no qual as seguintes ações são executadas:

Não Crítico

Quando a voltagem fica abaixo ou excede um intervalo de voltagem especificado, um alerta de voltagem é enviado para os receptores de alertas remotos configurados. Você deve marcar a caixa de seleção **Alertas de Aviso** na área **Configurações de Alertas SNMP** da página **Alertas** para que o alerta seja enviado.

Para obter mais informações sobre a seleção de opções de alerta, consulte “Configurando definições de alerta SNMP” na página 34.

Crítico

Quando a voltagem fica abaixo ou excede um intervalo de voltagem especificado, um alerta de voltagem é enviado para os receptores de alertas remotos configurados e o servidor inicia o processo de encerramento com um encerramento ordenado do sistema operacional. O servidor então se desliga. Você deve marcar a caixa de seleção **Alertas Críticos** na área **Configurações de Alertas SNMP** da página **Alertas** para que o alerta seja enviado.

Para obter mais informações sobre a seleção de opções de alerta, consulte “Configurando definições de alerta SNMP” na página 34.

Fatal

Quando a voltagem fica abaixo ou excede um intervalo de voltagem especificado, o servidor é encerrado imediatamente e envia um alerta para os receptores de alertas remotos configurados. Você deve marcar a caixa de seleção **Alertas Críticos** na área **Configurações de Alertas SNMP** da página **Alertas** para que o alerta seja enviado.

Nota: O alerta de encerramento permanente será enviado apenas se um alerta de encerramento temporário ainda não foi enviado.

Para obter mais informações sobre a seleção de opções de alerta, consulte “Configurando definições de alerta SNMP” na página 34.

O IMM gera um evento não crítico ou crítico quando o limite é atingido e gera ações de encerramento, se elas forem requeridas.

Não crítico

Se o IMM indicar que esse limite foi atingido, um evento de aviso será gerado.

Crítico

Se o IMM indicar que esse limite foi atingido, um evento crítico será gerado.

5. Role para baixo até a área **Velocidades do Ventilador (% do máx.)**. A interface da web do IMM exibe a velocidade de operação dos ventiladores do servidor (expressa em uma porcentagem da velocidade máxima do ventilador). Se você clicar em uma leitura de ventilador, uma nova janela será aberta.

Fan 1A Tach Thresholds (RPM)			
Sensors	Non - Critical	Critical	Fatal
Upper Threshold	N/A	N/A	N/A
Lower Threshold	N/A	290.000000	N/A

Você recebe um alerta de ventilador quando as velocidades do ventilador caem para um nível inaceitável ou quando os ventiladores param. Você deve marcar

a caixa de seleção **Alertas Críticos** na área **Configurações de Alertas SNMP** da página **Alertas** para que o alerta seja enviado.

Para obter mais informações sobre a seleção de opções de alerta, consulte “Configurando definições de alerta SNMP” na página 34.

6. Role para baixo até a área **Visualizar Tela de Falha do S.O. Mais Recente**. Clique em **Visualizar Tela de Falha do S.O.** para acessar uma imagem da tela de falha do sistema operacional que foi capturada quando o servidor parou de funcionar.

Nota:

O recurso de captura de tela de falha do sistema operacional está disponível apenas com o IMM Premium. Para obter informações sobre o upgrade do IMM Standard para o IMM Premium, consulte “Fazendo Upgrade do IMM Standard para o IMM Premium” na página 5.

Se ocorrer um evento que faz com que o sistema operacional pare de ser executado, o watchdog do sistema operacional será acionado, o que faz com que o IMM capture os dados da tela de falha do sistema operacional e armazene-os. O IMM armazena apenas as informações mais recentes do evento de erro, sobrescrevendo os dados mais antigos da tela de falha do sistema operacional quando ocorre um novo evento de erro.

Para acessar remotamente uma imagem da tela de falha do sistema operacional do servidor, conclua as etapas a seguir:

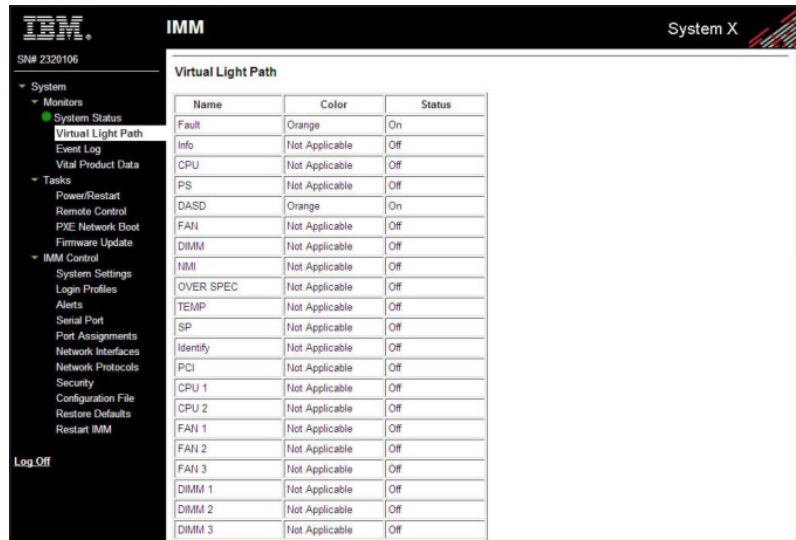
- a. Efetue login no IMM. Para obter mais informações, consulte Capítulo 2, “Abrindo e usando a interface da web do IMM”, na página 11.
 - b. Na área de janela de navegação, clique em **Funcionamento do Sistema** e role para baixo até a área **Visualizar Tela de Falha do S.O. Mais Recente**.
 - c. Clique em **Visualizar Tela de Falha do S.O.**. A imagem da tela de falha do sistema operacional é exibida na tela.
7. Role para baixo até a área **Usuários com Login Efetuado Atualmente**. A interface da web do IMM exibe o ID de login e o método de acesso de cada usuário que está com login efetuado no IMM.
 8. Role para baixo até a área **LED do Localizador do Sistema**. A interface da web do IMM exibe o status do LED localizador do sistema. Ela também fornece botões para alterar o estado do LED. Para obter o significado dos gráficos que são exibidos nessa área, consulte a ajuda online.

Visualizando Indicadores Luminosos Virtuais

A tela Indicadores Luminosos Virtuais exibe o nome, a cor e o status de qualquer LED que esteja aceso no servidor.

Para acessar e visualizar os Indicadores Luminosos Virtuais, conclua as etapas a seguir:

1. Efetue login no IMM. Para obter mais informações, consulte Capítulo 2, “Abrindo e usando a interface da web do IMM”, na página 11.
2. Na área de janela de navegação, clique em **Indicadores Luminosos Virtuais** para visualizar o histórico recente de eventos no servidor. Uma página semelhante à da ilustração a seguir é exibida.



3. Role para baixo para visualizar o conteúdo completo dos Indicadores Luminosos Virtuais.

Nota: Se um LED não estiver aceso no servidor, a coluna Cor da tabela Indicadores Luminosos Virtuais indicará que a Cor do LED é Não Aplicável.

Visualizando os logs de eventos

Nota: Para obter uma explicação de um determinado evento ou mensagem, consulte a documentação do servidor.

Códigos e mensagens de erro são exibidos nos tipos de logs de eventos a seguir:

- **Log de evento do sistema:** Esse log contém eventos de autoteste inicial e interrupção de gerenciamento do sistema (SMI) e todos os eventos que são gerados pelo BMC que está integrado no IMM. É possível visualizar o log de evento do sistema por meio do utilitário de configuração e por meio do programa Dynamic System Analysis (DSA) (como o log de eventos da IPMI).

O log de evento do sistema tem limite de tamanho. Quando ele estiver cheio, as novas entradas não sobrescreverão as entradas existentes; assim, você deve salvar periodicamente e, em seguida, limpar o log de evento do sistema usando o utilitário de configuração. Ao resolver problemas, poderá ser necessário salvar e, em seguida, limpar o log de evento do sistema para tornar os eventos mais recentes disponíveis para análise.

As mensagens são listadas no lado esquerdo da tela e os detalhes sobre a mensagem selecionada são exibidos no lado direito da tela. Para mover de uma entrada para outra, use as teclas de Seta para Cima (↑) e Seta para Baixo (↓).

O log de evento do sistema indica um evento de asserção quando um evento ocorreu. Ele indica um evento de desasserção quando o evento não está mais ocorrendo.

Alguns sensores do IMM fazem com que eventos de asserção sejam registrados quando seus setpoints são atingidos. Quando uma condição de setpoint não existe mais, um evento de desasserção correspondente é registrado. No entanto, nem todos os eventos são do tipo asserção.

- **Log de eventos do módulo de gerenciamento integrado (IMM):** Esse log contém um subconjunto filtrado de todos os eventos do IMM, autoteste inicial e

interrupção de gerenciamento de sistema (SMI). É possível visualizar o log de eventos do IMM por meio da interface da web do IMM e por meio do programa DSA (como o log de eventos do ASM).

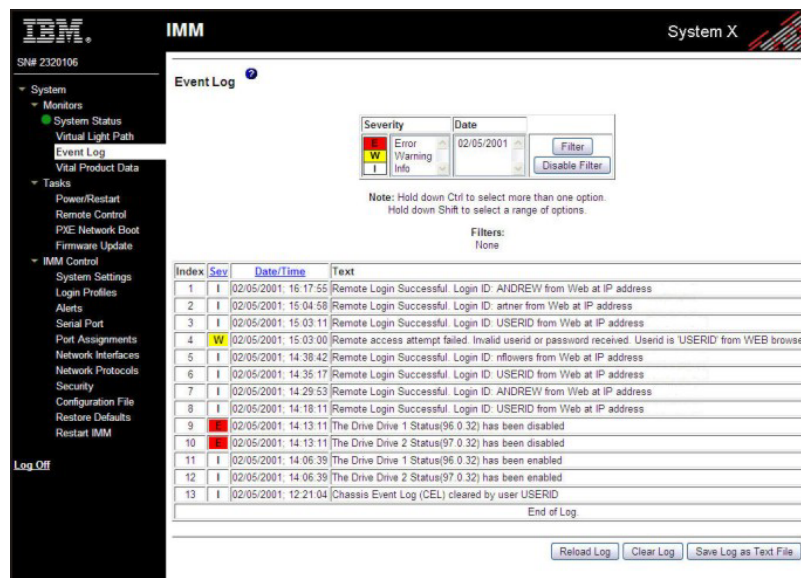
- **Log do DSA:** Esse log é gerado pelo programa DSA e é uma mesclagem ordenada cronologicamente do log de evento do sistema (como o log de eventos da IPMI), o log de eventos do chassi do IMM (como o log de eventos do ASM) e os logs de eventos do sistema operacional. É possível visualizar o log do DSA por meio do programa DSA.
- **Log de eventos do chassi:** O IMM gera mensagens de texto para os eventos de asserção e desasserção da IPMI e cria entradas para eles no log de eventos do chassi. O texto é gerado para esses eventos por meio das especificações da Distributed Management Task Force (DMTF), DSP0244 e DSP8007. Esse log também contém entradas para eventos que não são de asserções e desasserções de sensor da IPMI. Por exemplo, o log de eventos do chassi inclui entradas quando um usuário altera uma configuração de rede ou quando um usuário efetua login na interface da web. Esse log pode ser visualizado a partir da interface da web do IMM.

Visualizando o log de eventos do sistema a partir da interface da web

Nota: O log de eventos do sistema tem uma capacidade limitada. Quando esse limite é atingido, os eventos mais antigos são excluídos em uma ordem primeiro a entrar, primeiro a sair.

Para acessar e visualizar o log de eventos, conclua as etapas a seguir:

1. Efetue login no IMM. Para obter mais informações, consulte Capítulo 2, “Abrindo e usando a interface da web do IMM”, na página 11.
2. Na área de janela de navegação, clique em **Log de Eventos** para visualizar o histórico recente de eventos no servidor. Uma página semelhante à da ilustração a seguir é exibida.



3. Role para baixo para visualizar o conteúdo completo do log de eventos. Os eventos recebem os seguintes níveis de severidade:

Informativo

Esse nível de severidade é designado a um evento do qual você deve tomar nota.

Aviso Esse nível de severidade é designado a um evento que pode afetar o desempenho do servidor.

Erro Esse nível de severidade é designado a um evento que precisa de atenção imediata.

A interface da web do IMM diferencia os eventos de aviso com a letra W em um plano de fundo amarelo na coluna de severidade e eventos de erro com a letra E em um plano de fundo vermelho.

4. Clique em **Salvar Log como Arquivo de Texto** para salvar o conteúdo do log de eventos como um arquivo de texto. Clique em **Recarregar Log** para atualizar a exibição do log de eventos. Clique em **Limpar Log** para excluir o conteúdo do log de eventos.

Visualizando logs de eventos do utilitário de configuração

Para obter informações completas sobre como usar o utilitário de configuração, consulte a documentação fornecida com o servidor.

Para visualizar o log de eventos de POST ou o log de eventos do sistema, conclua as etapas a seguir:

1. Ligue o servidor.

Nota: Aproximadamente 2 minutos após o servidor ser conectado à energia de corrente alternada, o botão liga/desliga torna-se ativo.

2. Quando o prompt <F1> Configurar for exibido, pressione F1. Se você tiver configurado uma senha de ativação e uma senha de administrador, digite a senha do administrador para visualizar os logs de eventos.
3. Selecione **Logs de Eventos do Sistema** e use um dos seguintes procedimentos:
 - Para visualizar o log de eventos de POST, selecione **Event Viewer de POST**.
 - Para visualizar o log de eventos do sistema, selecione **Log de Eventos do Sistema**.

Visualizando logs de eventos sem reiniciar o servidor

Se o servidor não tiver sido interrompido, os métodos estarão disponíveis para a visualização de um ou mais logs de eventos sem precisar reiniciar o servidor.

Se você instalou o Portable ou Installable Dynamic System Analysis (DSA), é possível usá-lo para visualizar o log de eventos do sistema (como o log de eventos da IPMI), o log de eventos do IMM (como o log de eventos do ASM), o log de eventos do sistema operacional, ou o log do DSA mesclado. Também é possível usar o DSA Preboot para visualizar esses logs, apesar de você ter de reiniciar o servidor para usar o DSA Preboot. Para instalar o DSA Móvel, o DSA Instalável ou o DSA Preboot ou fazer o download da imagem do CD do DSA Preboot, acesse <http://www.ibm.com/systems/support/supportsite.wss/docdisplay?Indocid=SERV-DSA&brandind=5000008> ou conclua as etapas a seguir.

Nota: São feitas mudanças periodicamente no website da IBM. O procedimento real pode variar um pouco em relação ao que é descrito neste documento.

1. Acesse <http://www.ibm.com/systems/support/>.
2. Em **Suporte do produto**, clique em **System x**.

3. Em **Links populares**, clique em **Software e drivers de dispositivo**.
4. Em **Downloads relacionados**, clique em **Dynamic System Analysis (DSA)** para exibir a matriz de arquivos DSA para download.

Se o IPMItool estiver instalado no servidor, será possível usá-lo para visualizar o log de eventos do sistema. As versões mais recentes do sistema operacional Linux são fornecidas com uma versão atual do IPMItool. Para obter informações sobre o IPMItool, acesse <http://sourceforge.net/>.

Nota: São feitas mudanças periodicamente no website da IBM. O procedimento real pode variar um pouco em relação ao que é descrito neste documento.

1. Acesse <http://publib.boulder.ibm.com/infocenter/toolscctr/v1r0/index.jsp>.
2. Na área de janela de navegação, clique em **Centro de Ferramentas do IBM System x e BladeCenter**.
3. Expanda **Referência de ferramentas, Ferramentas de configuração, Ferramentas IPMI** e clique em **IPMItool**.

Para ter uma visão geral da IPMI, acesse <http://publib.boulder.ibm.com/infocenter/systems/index.jsp?topic=/liaai/ipmi/liaaiipmi.htm> ou conclua as etapas a seguir:

1. Acesse <http://publib.boulder.ibm.com/infocenter/systems/index.jsp>.
2. Na área de janela de navegação, clique em **Centro de Informações do IBM Systems**.
3. Expanda **Sistemas operacionais, Informações do Linux, Blueprints para Linux em sistemas IBM** e clique em **Usando a Intelligent Platform Management Interface (IPMI) em plataformas IBM Linux**.

É possível visualizar o log de eventos do IMM por meio do link **Log de Eventos** na interface da web do IMM.

A tabela a seguir descreve os métodos que podem ser usados para visualizar os logs de eventos, dependendo da condição do servidor. As suas primeiras condições geralmente não exigem que você reinicie o servidor.

Tabela 16. Métodos para visualizar logs de eventos

Condição	Ação
O servidor não foi interrompido e está conectado a uma rede.	Use qualquer um dos seguintes métodos: • Execute Portable ou Installable DSA para visualizar os logs de eventos ou criar um arquivo de saída que você pode enviar para o serviço e suporte da IBM. • Digite o endereço IP do IMM e acesse a página Log de Eventos. • Use o IPMItool para visualizar o log de eventos do sistema.
O servidor não foi interrompido e não está conectado a uma rede.	Use o IPMItool localmente para visualizar o log de eventos do sistema.

Tabela 16. Métodos para visualizar logs de eventos (continuação)

Condição	Ação
O servidor foi interrompido.	• Se o DSA Preboot estiver instalado, reinicie o servidor e pressione F2 para iniciar o DSA Preboot e visualizar os logs de eventos. • Se o DSA Preboot não estiver instalado, insira o CD do DSA Preboot e reinicie o servidor para iniciar o DSA Preboot e visualize os logs de eventos. • Como alternativa, é possível reiniciar o servidor e pressionar F1 para iniciar o utilitário de configuração e visualizar o log de eventos de POST ou o log de eventos do sistema. Para obter mais informações, consulte “Visualizando logs de eventos do utilitário de configuração” na página 108.

Visualizando dados vitais do produto

Quando o servidor é iniciado, o IMM coleta informações do servidor, informações do firmware do servidor e os dados vitais do produto (VPD) do componente do servidor e os armazena na memória não volátil. É possível acessar essas informações a qualquer momento de quase qualquer computador. A página Dados Vitais do Produto contém informações chave sobre o servidor gerenciado remoto que o IMM está monitorando.

Para visualizar os dados vitais do produto do componente do servidor, conclua as etapas a seguir:

1. Efetue login no IMM. Para obter mais informações, consulte Capítulo 2, “Abrindo e usando a interface da web do IMM”, na página 11.
2. Na área de janela de navegação, clique em **Dados Vitais do Produto** para visualizar o status dos componentes de hardware e software no servidor.
3. Role para baixo para visualizar as seguintes leituras de VPD:

VPD do nível de máquina

Os dados vitais do produto para o servidor aparecem nessa área. Para visualizar o VPD, o VPD do nível da máquina inclui um identificador exclusivo universal (UUID).

Nota: O VPD do nível da máquina, o VPD do nível de componente e o log de atividades do componente fornecem informações apenas quando o servidor está ligado.

Tabela 17. Dados vitais do produto do nível da máquina

Campo	Função
Tipo de máquina e modelo	Identifica o tipo e o número do modelo do servidor que o IMM está monitorando.
Número de série	Identifica o número de série do servidor que o IMM está monitorando.
UUID	Identifica o identificador exclusivo universal (UUID), um número hexadecimal de 32 dígitos, do servidor que o IMM está monitorando.

VPD do Nível de Componente

Os dados vitais do produto para os componentes do servidor gerenciado remoto são exibidas nesta área.

Tabela 18. Dados vitais do produto do nível de componente

Campo	Função
Nome da FRU	Identifica a unidade substituível em campo (FRU) para cada componente.
Número de série	Identifica o número de série de cada componente.
ID do Fabricante	Identifica o ID do fabricante de cada componente.

Log de Atividades do Componente

É possível visualizar um registro da atividade do componente nesta área.

Tabela 19. Log de atividades do componente

Campo	Função
Nome da FRU	Identifica a unidade substituível em campo (FRU) do componente.
Número de série	Identifica o número de série do componente.
ID do Fabricante	Identifica o fabricante do componente.
Ação	Identifica a ação a ser tomada para cada componente.
Registro de data e hora	Identifica a data e hora da ação do componente. A data é exibida no formato <i>mm/dd/aa</i> . A hora é exibida no formato <i>hh:mm:ss</i> .

VPD do IMM

É possível visualizar o VPD do firmware do IMM, do firmware do servidor System x e do firmware do Dynamic System Analysis para o servidor gerenciado remoto nesta área.

Tabela 20. Dados vitais do produto do firmware do IMM, UEFI e DSA

Campo	Função
Tipo de firmware	Indica o tipo de código de firmware.
Sequência de versão	Indica a versão do código de firmware.
Data de liberação	Indica quando o firmware foi liberado.

Capítulo 5. Executando tarefas do IMM

Use as funções sob o título **Tarefas** na área de janela de navegação para controlar diretamente as ações do IMM e o servidor. As tarefas que podem ser executadas dependem do servidor no qual o IMM está instalado.

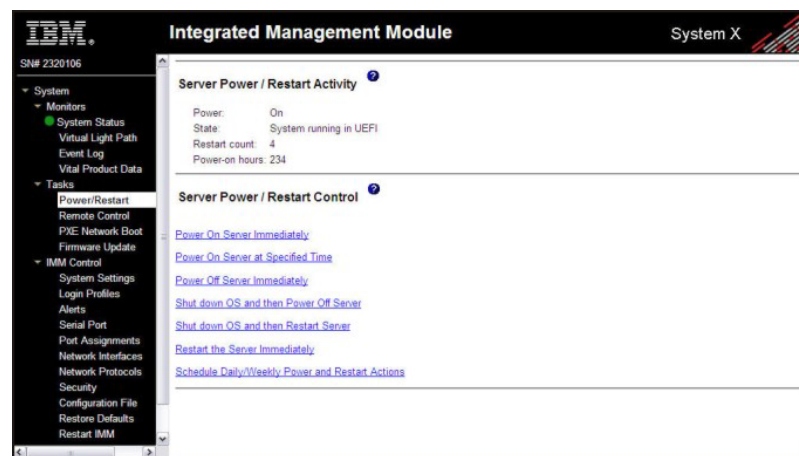
É possível executar as seguintes tarefas:

- 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
- Atualizar o firmware do IMM

Nota: Alguns recursos estão disponíveis apenas nos servidores que estão executando um sistema operacional Microsoft Windows suportado.

Visualizando a atividade de energia e reinicialização do servidor

A área **Atividade de Energia/Reinicialização do Servidor** exibe o status de energia do servidor quando a página da web foi gerada.



Energia

Esse campo mostra o status de energia do servidor quando a página da web atual foi gerada.

Estado

Esse campo mostra o estado do servidor quando a página da web atual foi gerada. Os seguintes estados são possíveis:

- Sistema desligado/Estado desconhecido
- Sistema ligado/iniciando UEFI
- Sistema interrompido na UEFI (Erro detectado)
- Sistema em execução na UEFI
- Inicializando S.O. ou S.O. não suportado (pode estar no sistema operacional se o sistema operacional não estiver configurado para suportar a interface dentro da banda para o IMM)

- S.O. inicializado

Contagem de reinicializações

Esse campo mostra o número de vezes que o servidor foi reiniciado.

Nota: O contador é zerado toda vez que o subsistema do IMM é limpo para os padrões de fábrica.

Horas ligado

Esse campo mostra o número total de horas em que o servidor ficou ligado.

Controlando o status de energia de um servidor

O IMM fornece controle total de energia sobre o servidor com as ações ligar, desligar e reiniciar. Além disso, as estatísticas de ligação e reinicialização são capturadas e exibidas para mostrar a disponibilidade do hardware do servidor. Para executar as ações na área **Controle de Energia/Reinicialização do Servidor**, você deve ter acesso de Supervisor ao IMM.

Para executar as ações de energia e reinicialização do servidor, conclua as etapas a seguir.

Nota: Selecione as opções a seguir apenas no caso de uma emergência, ou se você estiver fora e o servidor não estiver respondendo.

1. Efetue login no IMM. Para obter mais informações, consulte Capítulo 2, “Abrindo e usando a interface da web do IMM”, na página 11.
2. Na área de janela de navegação, clique em **Energia/Reinicialização**. Role para baixo até a área **Controle de Energia/Reinicialização do Servidor**.
3. Clique em uma das opções a seguir:

Ligue o servidor imediatamente

Ligue o servidor e inicie o sistema operacional.

Ligue o servidor no horário especificado

Ligue o servidor em um horário especificado e inicie o sistema operacional.

Desligue o servidor imediatamente

Desligue o servidor sem encerrar o sistema operacional.

Encerrar o S.O. e depois desligar o servidor

Encerre o sistema operacional e, em seguida, desligue o servidor.

Nota: Se o sistema operacional estiver no modo de proteção de tela ou bloqueado quando a solicitação "Encerrar o S.O. e depois desligar o servidor" for tentada, o IMM talvez não consiga iniciar um encerramento normal. O IMM executará uma reconfiguração brusca ou encerramento após o intervalo de atraso de desligamento expirar, enquanto o sistema operacional ainda pode estar ativo e em execução.

Encerrar o S.O. e depois reiniciar o servidor

Reinicie o sistema operacional.

Nota: Se o sistema operacional estiver no modo de proteção de tela ou bloqueado quando a solicitação "Encerrar o S.O. e depois reiniciar o servidor" for tentada, o IMM talvez não consiga iniciar um encerramento normal. O IMM executará uma reconfiguração brusca ou encerramento após o intervalo de atraso de desligamento expirar, enquanto o sistema operacional ainda pode estar ativo e em execução.

Reiniciar o servidor imediatamente

Desligue e, em seguida, ligue o servidor imediatamente, sem antes encerrar o sistema operacional.

Planejar ações diárias/semanais de energia e reinicialização

Encerre o sistema operacional, desligue o servidor em um horário diário ou semanal especificado (com ou sem reiniciar o servidor) e ligue o servidor em um horário diário ou semanal especificado.

Uma mensagem de confirmação será exibida se você selecionar uma dessas opções; e a operação poderá ser cancelada se tiver sido selecionada por engano.

Presença remota

Nota:

1. A função de presença remota do IMM só está disponível no IMM Premium. Para obter mais informações sobre o upgrade do IMM Standard para o IMM Premium, consulte “Fazendo Upgrade do IMM Standard para o IMM Premium” na página 5.
2. O recurso de controle remoto só está disponível por meio da interface da web do IMM. Você deve efetuar login no IMM com um ID de usuário que tenha acesso Supervisor para usar qualquer um dos recursos de controle remoto.

É possível usar a função de presença remota, ou recurso de controle remoto na interface da web do IMM, para visualizar e interagir com o console do servidor. É possível também designar ao servidor uma unidade de CD ou DVD, unidade de disquete, unidade flash USB ou imagem de disco que está em seu computador.

O recurso de controle remoto fornece as funções a seguir:

- Ver vídeos remotamente com resoluções gráficas de até 1280 x 1024, a 75 Hz, independentemente do estado do servidor
- Acessar remotamente o servidor, usando teclado e mouse 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 para a memória do IMM e mapeá-la para o servidor como uma unidade virtual

Atualizando o firmware do IMM e o applet Java ou ActiveX

Importante: O IMM usa um applet Java ou ActiveX para executar a função de presença remota. Quando o IMM 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 IMM, o applet Java que o servidor usa pode não estar no nível mais recente.

Para corrigir este problema, conclua as seguintes etapas:

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 IMM.

Para obter mais informações sobre atualização de firmware do IMM, consulte “Atualizando o Firmware” na página 126.

Ativando a função de presença remota

Nota: A função de presença remota do IMM só está disponível no IMM Premium. Para obter mais informações sobre o upgrade do IMM Standard para o IMM Premium, consulte “Fazendo Upgrade do IMM Standard para o IMM Premium” na página 5.

Para ativar o recurso de presença remota, conclua as etapas a seguir:

1. Desconecte a energia do servidor, retirando o cabo de energia.
2. Instale a chave de mídia virtual no slot dedicado na placa-mãe.
3. Reconecte a energia ao servidor.

Nota: Aproximadamente 2 minutos após o servidor ser conectado à energia de corrente alternada, o botão liga/desliga torna-se ativo.

4. Ligue o servidor.

Controle remoto

O recurso de controle remoto do IMM consiste em dois aplicativos Java em duas janelas separadas:

Visualizador de Vídeo

O 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. Você vê em seu monitor exatamente o que está no console do servidor e tem o controle do teclado e mouse do console.

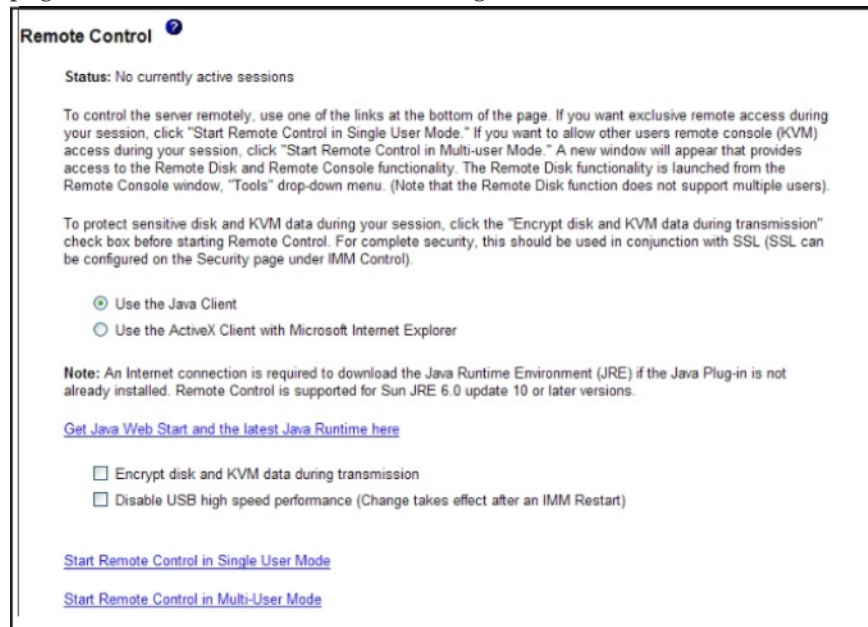
Sessão de Mídia Virtual

A janela Sessão de Mídia Virtual lista todas as unidades no cliente que podem ser mapeadas como unidades remotas. Ela 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.

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

1. Efetue login no IMM. Para obter mais informações, consulte Capítulo 2, “Abrindo e usando a interface da web do IMM”, na página 11.

2. Na área de janela de navegação, clique em **Controle Remoto**. É exibida uma página semelhante à da ilustração a seguir.



3. Escolha uma das opções a seguir:
- Clique em **Usar o Cliente Java** para usar o applet Java para executar a presença remota.
 - Clique em **Usar o ActiveX Client com o Microsoft Internet Explorer** para usar o Internet Explorer nos Sistemas Operacionais Windows se você deseja usar o applet ActiveX para executar a função de presença remota.

Nota: O ActiveX Remote Presence Client de 32 bits está disponível com o firmware versão 1.28 ou posterior do IMM. O ActiveX Client de 64 bits está disponível com o firmware versão 1.30 ou posterior do IMM.

4. Para controlar o servidor remotamente, use um dos links na parte inferior da página Controle Remoto. Se você deseja obter acesso remoto exclusivo durante sua sessão, clique em **Iniciar Controle Remoto no Modo de Usuário Único**. Para permitir a outros usuários o acesso ao console remoto (KVM) durante sua sessão, clique em **Iniciar Controle Remoto no Modo Multiusuário**. São abertas novas janelas que fornecem acesso à funcionalidade Disco Remoto e Console Remoto.

Se a caixa de seleção **Criptografar dados do disco e KVM durante a transmissão** foi marcada antes de abrir a janela Controle Remoto, os dados do disco serão criptografados com a criptografia ADES.

Feche a janela Visualizador de Vídeo e a janela Sessão de Mídia Virtual quando você tiver terminado de usar o recurso Controle Remoto.

Notas:

1. Não feche a janela Sessão de Mídia Virtual se um disco remoto estiver atualmente mapeado. Consulte “Disco remoto” na página 123 para obter instruções sobre como fechar e remover o mapeamento de um disco remoto.
2. Se você tiver problemas com mouse ou teclado ao usar o Controle Remoto, consulte a ajuda que está disponível na página Controle Remoto na interface da web.

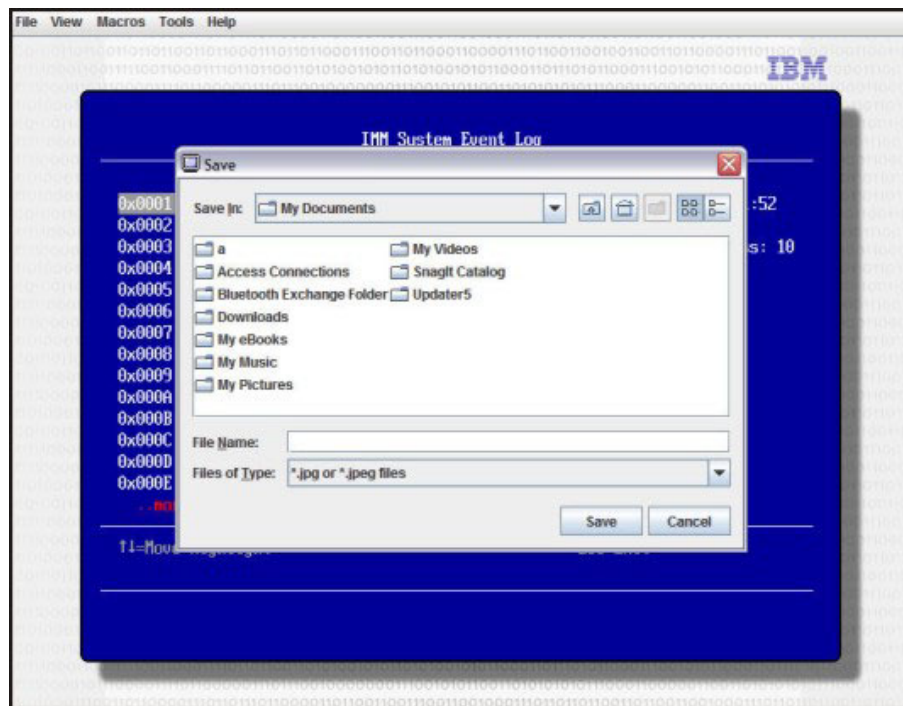
3. Se você usar o console remoto para alterar configurações do IMM no programa utilitário de configuração, o servidor poderá reiniciar o IMM. Você perderá o console remoto e a sessão de login. Depois de um curto atraso, é possível efetuar login no IMM novamente com uma nova sessão, iniciar o console remoto novamente e sair do programa utilitário de configuração.

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 for solicitado, nomeie o arquivo de imagem e salve-o no local escolhido no cliente local.

Nota: As imagens da captura de tela são salvas como tipos de arquivo JPG ou JPEG.



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:

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.

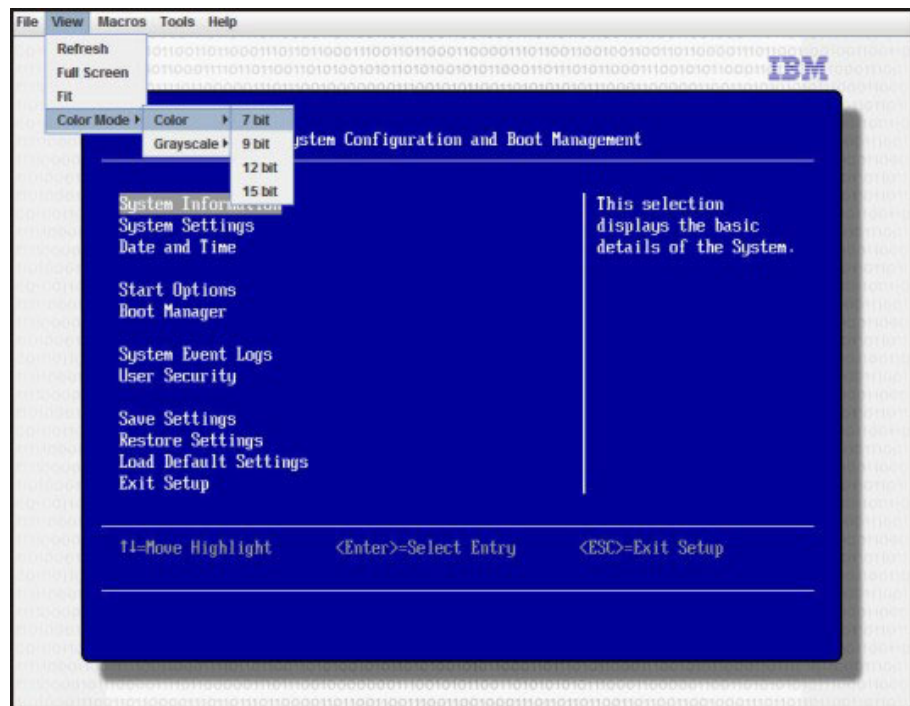
Modo de cor de vídeo do controle remoto

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: Em vez da régua de controle de largura de banda na interface Remote Supervisor Adapter II, o IMM tem um item de menu que permite o ajuste de intensidade de cor para reduzir os dados que são transmitidos em situações de largura de banda estreita.

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

1. Na janela Visualizador de Vídeo, clique em **Visualizar**.
2. Quando você move o ponteiro do mouse sobre **Modo de Cor** no menu, duas opções de modo de cor são exibidas:
 - Cor: 7, 9, 12 e 15 bits
 - Escala de tons: 16, 32, 64, 128 sombras

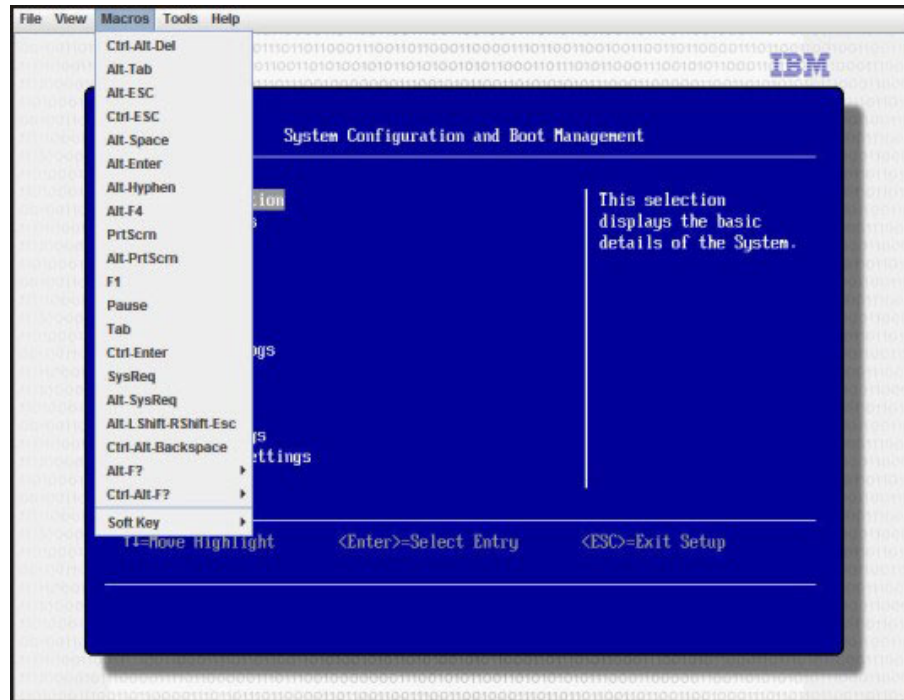


3. Selecione a configuração de cor ou escala de tons.

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 pelo usuário.



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 **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 pop-up e, em seguida, clique em **OK**.
5. Ao concluir a definição ou a 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 recurso de passagem do teclado desativa a manipulação da maioria das combinações de teclas especiais no cliente para que elas possam ser transmitidas 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 teclas 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 transmitir esses pressionamentos 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 exibida, clique na guia **Geral**.
4. Marque a caixa de seleção **Transmitir todos os pressionamentos de teclas para o destino** para ativar ou desativar o recurso.
5. Clique em **OK** para salvar a opção.

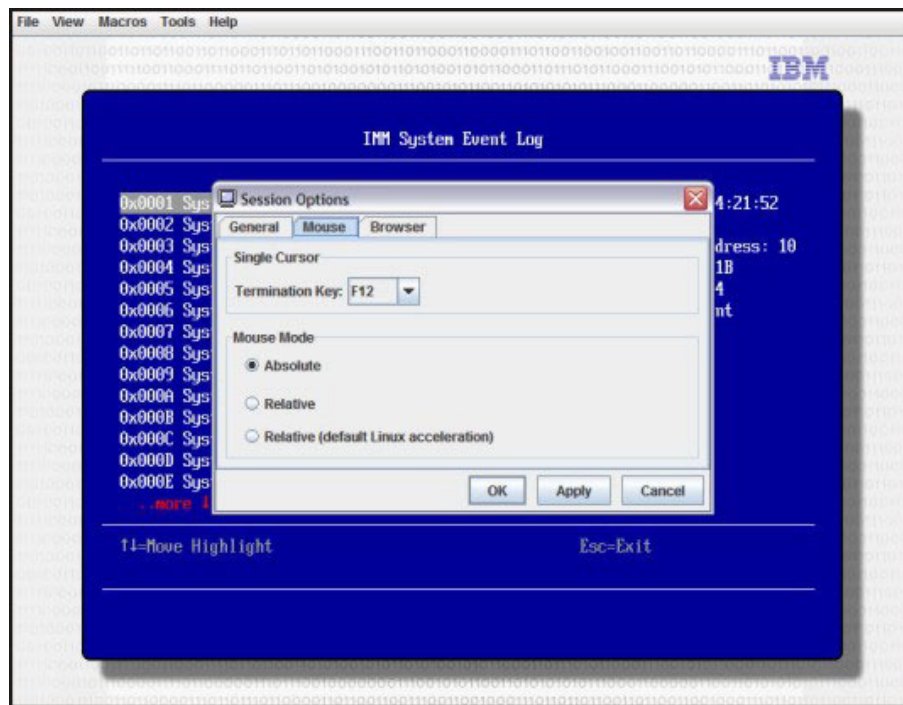
Suporte a mouse de controle remoto

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 exibida, clique na guia **Mouse**.



4. Selecione um dos seguintes modos do mouse:

Absoluto

O cliente envia mensagens do local do mouse para o servidor que são sempre relativas à origem (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, conclua as etapas a seguir:

1. Na janela Visualizador de Vídeo, clique em **Ferramentas**.
2. Selecione **Cursor Único**.

Quando o Visualizador de Vídeo está no modo de cursor único, não é possível usar o mouse para alternar para outra janela ou então clicar fora da janela do cliente KVM, porque não há cursor local. Para desativar o modo de cursor único, pressione a tecla de 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. Quando você move o ponteiro do mouse sobre **Energia** no menu, estas opções são exibidas:

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, conclua as etapas a seguir:

1. Na janela Visualizador de Vídeo, clique em **Ferramentas**.
2. Clique em **Stats**. 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 geralmente é 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 alternar para o uso de um cliente RDP em vez do cliente KVM. O servidor remoto deve estar configurado para receber conexões RDP.

Disco remoto

Na janela Sessão de Mídia Virtual, é possível designar ao servidor uma unidade de CD ou DVD, uma unidade de disquete ou 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 usar o recurso Controle Remoto para acessar o disco remoto. As unidades e imagens de disco são exibidas como unidades USB no servidor.

Notas:

1. Os seguintes sistemas operacionais de servidor têm suporte de USB, que é necessário para o recurso Disco Remoto:
 - Microsoft Windows Server 2008
 - Microsoft Windows Server 2003
 - Red Hat Linux versões 4.0 e 5.0
 - SUSE Linux versão 10.0
 - Novell NetWare 6.5
2. O servidor do cliente requer o Plug-in Java 1.5 ou posterior.
3. 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. Efetue login no IMM. Para obter mais informações, consulte Capítulo 2, “Abrindo e usando a interface da web do IMM”, na página 11.
 2. Na área de janela de navegação, clique em **Controle Remoto**.
 3. Na página Controle Remoto, clique em uma das opções de **Iniciar Controle Remoto**:
 - Se você deseja obter acesso remoto exclusivo durante sua sessão, clique em **Iniciar Controle Remoto no Modo de Usuário Único**.
 - Se você deseja permitir que outros usuários tenham acesso ao console remoto (KVM) durante sua sessão, clique em **Iniciar Controle Remoto no Modo Multiusuário**.
- A janela do Visualizador de Vídeo é aberta.
4. Para abrir uma janela Sessão de Mídia Virtual, clique em **Ferramentas > Ativar Mídia Virtual** na janela Visualizador de Vídeo.

Nota: Se a caixa de seleção **Criptografar dados do disco e KVM durante a transmissão** foi marcada antes de abrir a janela Controle Remoto, 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 com a versão de firmware 1.03 e posterior do IMM

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.

É possível selecionar um arquivo de imagem de disquete e salvar a imagem de disquete na memória do IMM. Isso permite que o disco permaneça montado no servidor para que você possa acessar o disco mais tarde, mesmo depois que a sessão da interface da web do IMM for encerrada. No máximo, uma imagem de unidade pode ser armazenada no cartão do IMM. O conteúdo da unidade ou imagem deve ser de 1.44 MB ou menos. Para fazer upload de um arquivo de imagem de disquete, conclua as etapas a seguir:

1. Clique em **RDOC**.
2. Quando a nova janela for aberta, clique em **Fazer Upload**.
3. Clique em **Procurar** para selecionar o arquivo de imagem que você deseja usar.
4. No campo **Nome**, digite um nome para a imagem e clique em **OK** para fazer upload do arquivo.

Nota: Para descarregar o arquivo de imagem da memória, selecione o nome na janela Configuração do RDOC e clique em **Excluir**.

Mapeando e removendo o mapeamento de unidades com a versão de firmware 1.02 e anterior do IMM

Para mapear uma unidade, marque a caixa de seleção **Mapeado** 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.

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 de uma unidade, desmarque a caixa de seleção **Mapeado** para a unidade. Antes de remover o mapeamento da unidade, você deve confirmar se deseja removê-lo.

É possível selecionar um arquivo de imagem de disquete e salvar a imagem de disquete na memória do IMM. Isso permite que o disco permaneça montado no servidor para que você possa acessar o disco mais tarde, mesmo depois que a sessão da interface da web do IMM for encerrada. No máximo, uma imagem de unidade pode ser armazenada no cartão do IMM. O conteúdo da unidade ou imagem deve ser de 1.44 MB ou menos. Para fazer upload de um arquivo de imagem de disquete, conclua as etapas a seguir:

1. Clique em **RDOC**.

2. Quando a nova janela for aberta, clique em **Fazer Upload**.
3. Clique em **Procurar** para selecionar o arquivo de imagem que você deseja usar.
4. No campo **Nome**, digite um nome para a imagem e clique em **OK** para fazer upload do arquivo.

Nota: 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 a janela Visualizador de Vídeo e a janela Sessão de Mídia Virtual quando você tiver terminado de usar o recurso Controle Remoto.

Configurando a inicialização da rede PXE

Para configurar seu servidor para tentar uma inicialização da rede Preboot Execution Environment (PXE) na próxima reinicialização de servidor, conclua as etapas a seguir:

1. Efetue login no IMM. Para obter mais informações, consulte Capítulo 2, “Abrindo e usando a interface da web do IMM”, na página 11.
2. Na área de janela de navegação, clique em **Inicialização da Rede PXE**.
3. Marque a caixa de seleção **Tentar a inicialização da rede PXE na próxima reinicialização do servidor**.
4. Clique em **Salvar**.

Atualizando o Firmware

Use a opção Atualizar Firmware na área de janela de navegação para atualizar o firmware do IMM, o firmware do servidor System x e o firmware do Dynamic System Analysis (DSA).

Para atualizar o firmware, conclua as etapas a seguir.

Nota: São feitas mudanças periodicamente no website da IBM. O procedimento real pode variar um pouco em relação ao que é descrito neste documento.

1. Faça download da atualização de firmware mais recente aplicável para o servidor no qual o IMM está instalado:
 - a. Acesse <http://www.ibm.com/systems/support/>.
 - b. Em **Suporte do Produto**, clique em **System x** ou **BladeCenter**.
 - c. Em **Links populares**, clique em **Software e drivers de dispositivo**.
 - d. Clique no link aplicável para seu servidor para exibir a matriz de arquivos para download.
 - e. Role para a área IMM, firmware do servidor ou DSA, selecione o link para a atualização de firmware e salve o arquivo de atualização.
2. Efetue login no IMM. Para obter mais informações, consulte Capítulo 2, “Abrindo e usando a interface da web do IMM”, na página 11.
3. Na área de janela de navegação, clique em **Atualização de Firmware**.
4. Clique em **Procurar**.
5. Navegue para o pacote de atualização que você deseja atualizar.

Nota:

- a. O firmware do servidor System x não poderá ser atualizado enquanto o servidor estiver desligado ou sendo iniciado.

- b. Para determinar o tipo de arquivo de firmware a ser usado, consulte o arquivo leia-me do pacote de atualização. Na maioria dos casos, o IMM pode usar o arquivo EXE ou BIN para executar a atualização.
6. Clique em **Abrir**. O arquivo (incluindo o caminho completo) é exibido na caixa ao lado de **Procurar**.
7. Para iniciar o processo de atualização, clique em **Atualizar**. Um indicador de progresso é aberto conforme o arquivo é transferido para armazenamento temporário no IMM. Uma janela de confirmação é aberta quando a transferência do arquivo é concluída.
8. Verifique se o arquivo que é mostrado na janela Confirmar Atualização de Firmware é o que você planeja atualizar. Se não for, clique em **Cancelar**.
9. Para concluir o processo de atualização, clique em **Continuar**. Um indicador de progresso é aberto conforme o firmware é atualizado. Uma janela de confirmação é aberta para verificar se a atualização foi bem-sucedida.
10. Se você estiver atualizando o firmware do IMM, clique em **Reiniciar IMM** na área de janela de navegação e, em seguida, clique em **Reiniciar**. O firmware do servidor System x e as atualizações de DSA não exigem que o IMM seja reiniciado. Essas atualizações entrarão em vigor na próxima vez que o servidor for iniciado.
11. Clique em **OK** para confirmar que você deseja reiniciar o IMM.
12. Clique em **OK** para fechar a janela atual do navegador.
13. Depois que o IMM for reiniciado, efetue login nele novamente para acessar a interface da web.

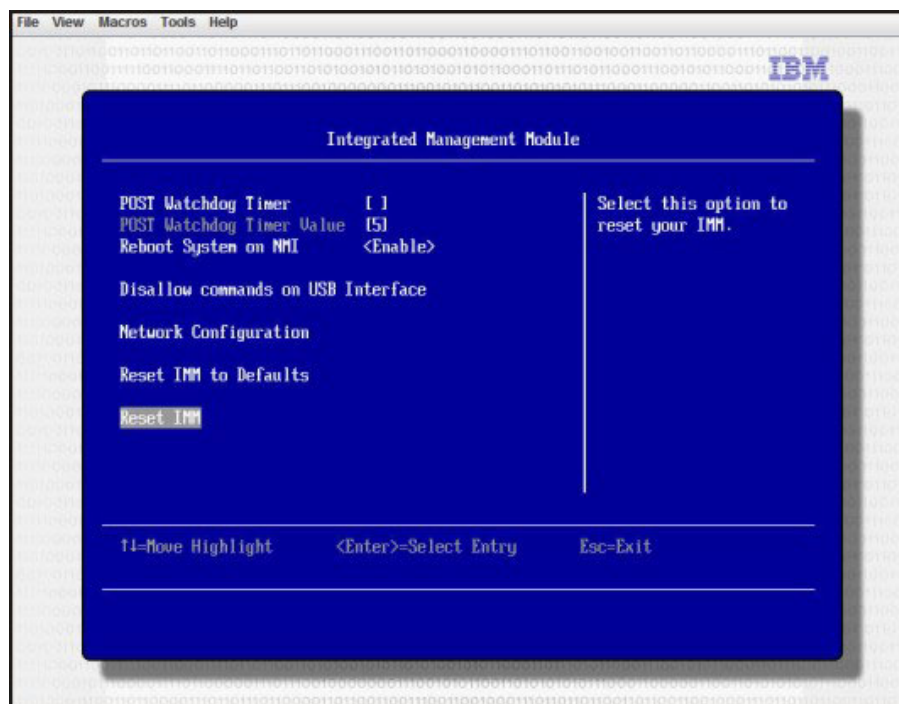
Reconfigurando o IMM com o utilitário de Configuração

Para reconfigurar o IMM por meio do utilitário de Configuração, conclua as etapas a seguir:

1. Ligue o servidor.

Nota: Aproximadamente 2 minutos após o servidor ser conectado à energia de corrente alternada, o botão liga/desliga se torna ativo.

2. Quando o prompt F1 Setup 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. Selecione **Reconfigurar IMM**.



Nota: Depois de reconfigurar o IMM, esta mensagem de confirmação será exibida imediatamente:

O comando de reconfiguração do IMM foi enviado com êxito!! Pressione ENTER para continuar.

O processo de reconfiguração do IMM não foi concluído ainda. É preciso aguardar por aproximadamente 4 minutos para que o IMM seja reconfigurado antes de tornar-se funcional novamente. Se você tentar acessar as informações de firmware do servidor enquanto o servidor está sendo reconfigurado, será exibido Desconhecido nos campos e a descrição será Erro ao recuperar informações do IMM.

Gerenciando ferramentas e utilitários com o IMM e IBM System x Server Firmware

Esta seção descreve as ferramentas e os utilitários que são suportados pelo IMM e IBM System x Server Firmware. As ferramentas IBM que você usa para gerenciar o IMM dentro da banda não requerem a instalação de drivers de dispositivo. No entanto, se você optar por usar determinadas ferramentas como o IPMITool dentro da banda, deverá instalar os drivers OpenIPMI.

Atualizações e downloads para ferramentas e utilitários de gerenciamento de sistemas IBM estão disponíveis no website da IBM. Para verificar atualizações para ferramentas e utilitários, conclua as etapas a seguir.

Nota: 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/systems/support/>.
2. Em **Suporte do produto**, clique em **System x**.

3. Em **Links Populares**, clique em **Utilitários**.

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 IMM.

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

Usando o OSA System Management Bridge

O OSA System Management Bridge (SMBridge) é uma ferramenta que pode ser usada para gerenciar servidores remotamente. É possível utilizá-la para administrar servidores usando os protocolos IPMI 1.5 e Serial over LAN (SOL).

Para obter mais informações sobre o SMBridge, acesse <http://www-947.ibm.com/systems/support/supportsite.wss/docdisplay?lnnodocid=MIGR-62198&brandind=5000008> ou conclua as etapas a seguir:

1. Acesse <http://www.ibm.com/systems/support/>.
2. Clique em **System x**.
3. Em **Suporte & Downloads**, clique em **Procurar**.
4. Digite **smbridge** no campo de procura e clique em **Procurar**.
5. Na lista de resultados, clique no link **Ajuda da Ferramenta SMBridge - Servidores**.

Usando o IBM Advanced Settings Utility

O IBM Advanced Settings Utility (ASU) versão 3.0.0 ou posterior é requerido para gerenciar o IMM. O ASU é uma ferramenta que você pode usar para modificar configurações de firmware a partir da interface da linha de comandos em diversas plataformas de sistema operacional. Ele também permite emitir comandos de configuração do IMM selecionados. É possível usar o ASU dentro e fora da banda para gerenciar e configurar o IMM.

Nota: Se a interface USB dentro da banda (LAN sobre USB) estiver desativada, o ASU exigirá a instalação de drivers de dispositivo IPMI.

Para obter mais informações sobre o ASU, consulte <http://www-947.ibm.com/systems/support/supportsite.wss/docdisplay?lnnodocid=MIGR-55021&brandind=5000008> ou conclua as etapas a seguir:

1. Acesse <http://www.ibm.com/systems/support/>.
2. Clique em **System x**, selecione o servidor no menu **Família de produtos** e clique em **Ir**.
3. No menu **Refinar resultados**, selecione **Utilitário de Configurações Avançadas** e clique em **Ir**.
4. Clique no link para a versão mais recente do ASU.

Usando os Utilitários de Atualização IBM

Um utilitário de atualização permite atualizar hardware e firmware do servidor e elimina a necessidade de instalar manualmente novo firmware ou atualizações de firmware a partir de um disquete físico ou outra mídia. É possível usar os

utilitários de atualização IBM para IMM, firmware do servidor e DSA, dentro ou fora da banda. Para localizar um utilitário de atualização, conclua as etapas a seguir:

1. Acesse <http://www.ibm.com/systems/support/>.
2. Em **Suporte do produto**, clique em **System x**.
3. Digite `flash utility` no campo de procura e clique em **Procurar**.
4. Clique no link para o utilitário de atualização aplicável.

Outros métodos para gerenciar o IMM

É possível usar as seguintes interfaces com o usuário para gerenciar e configurar o IMM:

- Interface da web do IMM
- SNMPv1
- SNMPv3
- CLI Telnet
- CLI SSH

Capítulo 6. LAN sobre USB

Diferentemente do BMC e do Remote Supervisor Adapter II, o IMM não requer drivers de dispositivo IPMI ou daemons USB para comunicação do IMM dentro da banda. Em vez disso, uma interface de LAN sobre USB permite comunicações dentro da banda com o IMM; o hardware IMM na placa-mãe apresenta uma NIC Ethernet interna do IMM para o sistema operacional.

Nota: A LAN sobre USB também é chamada de “interface dentro da banda USB” na interface da web do IMM.

O endereço IP do IMM para a interface LAN sobre USB é configurado como um endereço estático 169.254.95.118 com uma máscara de sub-rede 255.255.0.0. A única exceção é o IMM no Nó Secundário de um sistema com vários nós (por exemplo, x3850 X5 ou x3950 X5), em que o endereço IP no lado do IMM da interface LAN sobre USB é 169.254.96.118.

Potenciais conflitos com a interface LAN sobre USB

Em algumas situações, a interface LAN sobre USB do IMM pode entrar em conflito com determinadas configurações de rede e/ou aplicativos. Por exemplo, a MPI Aberta tenta usar todas as interfaces de rede disponíveis em um servidor. A MPI Aberta detecta a interface LAN sobre USB do IMM e tenta usá-la para comunicação com outros sistemas em um ambiente em cluster. A interface LAN sobre USB é uma interface interna, de modo que essa interface não funciona para comunicações externas com outros sistemas no cluster.

Resolvendo conflitos com a interface LAN sobre USB do IMM

Há diversas ações que resolvem conflitos de LAN sobre USB com configurações de rede e aplicativos:

- Para conflitos com Open MPI, configure o aplicativo para que ele não tente usar a interface.
- Desative a interface (execute `ifdown` no Linux).
- Remova o driver de dispositivo (execute `rmmmod` no Linux).
- Desative a interface USB dentro da banda no IMM por meio dos métodos a seguir.

Importante: Se você desativar a Interface USB dentro da banda, não será possível executar uma atualização dentro da banda do firmware do IMM usando os utilitários de atualização do Linux ou Windows. Se a Interface USB dentro da banda estiver desativada, use a opção Atualização de Firmware na interface da web do IMM para atualizar o firmware. Para obter mais informações, consulte “Atualizando o Firmware” na página 126.

Se você desativar a interface USB dentro da banda, desative também os tempos limites de watchdog para evitar que o servidor seja reiniciado inesperadamente. Para obter mais informações sobre como desativar os watchdogs, consulte “Configurando tempos limites do servidor” na página 21.

- Para desativar a interface LAN sobre USB a partir da interface da web do IMM, consulte “Desativando a interface USB dentro da banda” na página 24.

- Para desativar a interface LAN sobre USB a partir da interface da web do módulo de gerenciamento avançado, conclua as etapas a seguir:
 1. Efetue login na interface da web do módulo de gerenciamento avançado.
 2. Na área de janela de navegação, clique em **Configuração do Blade** sob o título **Tarefas do Blade**.
 3. Role para baixo até a interface LAN sobre USB do processador de serviços na página da web de Configuração do Blade. A seção lista todos os servidores blade no chassi que são capazes de ativar e desativar a interface LAN sobre USB.
 4. Marque as caixas de seleção ao lado dos servidores blade que você deseja ativar ou desativar.
 5. Clique em **Desativar** para desativar a interface LAN sobre USB nos servidores blade selecionados.

Configurando a interface LAN sobre USB manualmente

Para que o IMM use a interface LAN sobre USB, pode ser necessário concluir outras tarefas de configuração se a configuração automática falhar ou você preferir configurar a LAN sobre USB manualmente. O pacote de atualização de firmware ou o Advanced Settings Utility (ASU) tenta executar a configuração automaticamente. Para obter mais informações sobre a configuração da LAN sobre USB em sistemas operacionais diferentes, consulte o White Paper IBM *Transitioning to UEFI and IMM* no website da IBM.

Instalando drivers de dispositivo

Para que o IMM use a interface LAN sobre USB, você pode ter de instalar os drivers do sistema operacional. Se a configuração automática falhar ou você preferir configurar a LAN sobre USB manualmente, use um dos procedimentos a seguir. Para obter mais informações sobre a configuração da LAN sobre USB em sistemas operacionais diferentes, consulte o White Paper IBM *Transitioning to UEFI and IMM* no website da IBM.

Instalando o driver de dispositivo IPMI do Windows

O driver de dispositivo Microsoft IPMI não é instalado por padrão nos sistemas operacionais Microsoft Windows Server 2003 R2. Para instalar o driver de dispositivo Microsoft IPMI, conclua as etapas a seguir:

1. Na área de trabalho do Windows, clique em **Iniciar > Painel de Controle > Adicionar ou Remover Programas**.
2. Clique em **Adicionar/Remover Componentes do Windows**.
3. Na lista de componentes, selecione **Ferramentas de Gerenciamento e Monitoramento** e, em seguida, clique em **Detalhes**.
4. Selecione **Gerenciamento de Hardware**.
5. Clique em **Avançar**. O assistente de instalação é aberto e orienta a instalação.

Nota: O CD de instalação do Windows pode ser necessário.

Instalando o driver de dispositivo LAN sobre USB Windows

Quando você instala o Windows, um dispositivo RNDIS desconhecido é mostrado no Gerenciador de Dispositivo. Você deve instalar um arquivo INF do Windows que identifica esse dispositivo e é requerido pelo sistema operacional Windows para detectar e usar a funcionalidade LAN sobre USB. A versão assinada do INF

está incluída em todas as versões Windows dos pacotes de atualização do IMM, UEFI e DSA. O arquivo precisa ser instalado apenas uma vez. Para instalar o arquivo INF do Windows, conclua as etapas a seguir:

1. Obtenha uma versão Windows do IMM, do firmware do servidor ou do pacote de atualização do DSA (consulte “Atualizando o Firmware” na página 126 para obter mais informações).
2. Extraia os arquivos `ibm_rndis_server_os.inf` e `device.cat` do pacote de atualização do firmware e copie-os no subdiretório `\WINDOWS\inf`.
3. **Para Windows 2003:** Instale o arquivo `ibm_rndis_server_os.inf` clicando com o botão direito do mouse no arquivo e selecionando **Instalar**. Isso gera um arquivo PNF do mesmo nome em `\WINDOWS\inf`. **Para Windows 2008:** Acesse **Gerenciamento do Computador, Gerenciador de Dispositivo** e localize o dispositivo RNDIS. Selecione **Propriedades > Driver > Reinstalar driver**. Aponte o servidor para o diretório `\Windows\inf`, no qual ele pode localizar o arquivo `ibm_rndis_server_os.inf` e instalar o dispositivo.
4. Acesse **Gerenciamento do Computador, Gerenciador de Dispositivo**, clique com o botão direito do mouse em **Adaptadores de rede** e selecione **Verificar alterações de hardware**. Uma mensagem confirma que o dispositivo Ethernet foi localizado e instalado. O Assistente de Novo Hardware é iniciado automaticamente.
5. Quando aparecer a pergunta O Windows pode conectar-se ao Windows Update para procurar software?, clique em **Não desta vez**. Clique em **Avançar** para continuar.
6. Quando aparecer a pergunta O que você deseja que o assistente faça?, clique em **Instalar a partir de uma lista ou local específico (Avançado)**. Clique em **Avançar** para continuar.
7. Quando aparecer o aviso Escolha suas opções de pesquisa e instalação, clique em **Não pesquisar. Eu escolherei o driver a ser instalado**. Clique em **Avançar** para continuar.
8. Quando aparecer o aviso Selecione um tipo de hardware e, em seguida, clique em **Avançar**, clique em **Adaptadores de rede**. Clique em **Avançar** para continuar.
9. Quando aparecer o aviso Concluindo o Assistente de Novo Hardware Encontrado, clique em **Concluir**.

Nota: Uma nova conexão de área local é exibida e pode indicar Esta conexão tem conectividade limitada ou não tem conectividade. Ignore essa mensagem.

10. Volte para o Gerenciador de Dispositivo. Verifique se **Dispositivo de Rede IBM USB Remote NDIS** aparece em **Adaptadores de Rede**.
11. Abra um prompt de comandos, digite `ipconfig` e pressione Enter. A conexão de área local para o IBM USB RNDIS é exibida com um endereço IP no intervalo 169.254.xxx.xxx, com uma máscara de sub-rede configurada como 255.255.0.0.

Instalando o driver de dispositivo LAN sobre USB Linux

As versões atuais do Linux, como RHEL5 Atualização 2 e SLES10 Service Pack 2, suportam a interface LAN sobre USB por padrão. Essa interface é detectada e exibida durante a instalação desses sistemas operacionais. Ao configurar o dispositivo, use um endereço IP estático 169.254.95.130 com uma máscara de sub-rede 255.255.0.0.

Nota: Distribuições mais antigas do Linux podem não detectar a interface de LAN sobre USB e requerer configuração manual. Para obter informações sobre como configurar a LAN sobre USB em distribuições Linux específicas, consulte o White Paper da IBM, *Transitioning to UEFI and IMM*, no website da IBM.

A interface LAN sobre USB do IMM requer que os drivers de dispositivo `usbnet` e `cdc_ether` sejam carregados. Se os drivers de dispositivo não tiverem sido instalados, use o comando `modprobe` para instalá-los. Quando esses drivers de dispositivo estão instalados, a interface de rede USB do IMM é mostrada como um dispositivo de rede no sistema operacional. Para descobrir o nome que o sistema operacional designou à interface de rede USB do IMM, digite:

```
dmesg | grep -i cdc ether
```

Use o comando `ifconfig` para configurar a interface para ter um endereço IP no intervalo `169.254.xxx.xxx`. Por exemplo:

```
ifconfig IMM_device_name 169.254.1.102 netmask 255.255.0.0
```

Essa interface é configurada para ter um endereço IP no intervalo `169.254.xxx.xxx` toda vez que o sistema operacional for iniciado.

Capítulo 7. Interface da linha de comandos

Use a interface da linha de comandos do IMM (CLI) para acessar o IMM sem ter de utilizar 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 IMM para poder emitir qualquer comando da CLI.

Gerenciando a IPMI com o IMM

O IMM é fornecido com o ID do Usuário 2 configurado inicialmente como um nome de usuário USERID e uma senha PASSWORD (com um zero, não a letra O). Esse usuário tem acesso de Supervisor.

Importante: Altere essa senha padrão durante a configuração inicial para uma maior segurança.

O IMM também fornece os seguintes recursos de gerenciamento do servidor remoto IPMI:

Interfaces da linha de comandos

A interface da linha de comandos fornece acesso direto às funções de gerenciamento do servidor por meio do protocolo IPMI 2.0. É possível usar o SMBridge ou o IPMITool para emitir comandos para controlar a energia do servidor, visualizar informações do servidor e identificar o servidor. Com o SMBridge, você também pode salvar um ou mais comandos em um arquivo de texto e executar o arquivo como um script. Para obter mais informações sobre o IPMITool, consulte “Usando o IPMITool” na página 129. Para obter mais informações sobre o SMBridge, consulte “Usando o OSA System Management Bridge” na página 129.

Serial over LAN

Para gerenciar servidores a partir de um local remoto, use SMBridge ou IPMITool para estabelecer uma conexão Serial over LAN (SOL). Para obter mais informações sobre o IPMITool, consulte “Usando o IPMITool” na página 129. Para obter mais informações sobre o SMBridge, consulte “Usando o OSA System Management Bridge” na página 129.

Acessando a linha de comandos

Para acessar a linha de comandos, inicie uma sessão Telnet ou SSH para o endereço IP do IMM (consulte “Configurando o redirecionamento serial para Telnet ou SSH” na página 36 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 IMM.
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 IMM.

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. Em seguida, é feito seu logoff e a sessão é encerrada.

Sintaxe do comando

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 IMMA00096B9E003A
-r auto
-d auto
```

```
-m 1500
-b 00:09:6B:9E:00:3A
-l 00:00:00:00:00:00
system>
```

- Na interface de linha de comandos, 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 que estão descritos nas seções a seguir podem não estar disponíveis. Para ver uma lista dos comandos que são suportados, use a opção `help` ou `?`, conforme mostrado nos seguintes exemplos:

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

Comandos Utilitários

Os comandos de utilitário são os seguintes:

- `exit`
- `help`
- `history`

comando **exit**

Use o comando **exit** para efetuar logoff e encerrar a sessão da interface da linha de comandos.

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 IMMA00096B9E003A
-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:

- clearlog
- fans
- readlog
- syshealth
- temps
- volts
- vpd

Comando clearlog

Use o comando **clearlog** para limpar o log de eventos do IMM ou o IMM. 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 readlog

Use o comando **readlog** para exibir as entradas do log de eventos do IMM, 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 -f reconfigura o contador e exibe as 5 primeiras entradas no log de eventos, iniciando com a mais recente.

Sintaxe:

```
readlog [options]
option:
-f
```

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 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 IMM 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  9/320
DASD1 66/19  73/23  82/28  88/31  9/332
Amb   59/15  70/21  83/28  90/32  9/355
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), IMM, firmware do servidor (bios) e Dynamic System Analysis Preboot (dsa). As mesmas informações são exibidas como na interface da web.

Sintaxe:

```
vpd sys
vpd IMM
vpd biosvpd dsa
```

Exemplo:

```
system> vpd dsa
Type      Version      ReleaseDate
-----
dsa       D6YT19AUS      02/27/2009
system>
```

Comandos de controle de energia e reinicialização do servidor

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

- power
- reset

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 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

Há um comando de redirecionamento serial: console.

comando do console

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

Sintaxe:

```
console 1
```

Comandos de configuração

Os comandos de configuração são os seguintes:

- dhcpinfo
- dns
- gprofile
- ifconfig
- ldap

- ntp
- passwordcfg
- portcfg
- slp
- srcfg
- ssl
- tcpcmdmode
- timeouts
- usbeth
- users

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      : IMMA-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 a configuração de DNS do IMM.

Sintaxe:

dns

Nota: O exemplo a seguir mostra uma configuração de IMM 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
-dnsrc : dhcp
-p     : ipv6

system>
```

A tabela a seguir descreve a saída do exemplo.

Opção	Descrição
-state	Estado do DNS (enabled ou disabled)
-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)
-p	Servidores DNS preferenciais (ipv4 ou ipv6)

Comando gprofile

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

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 segurança baseado em função (autoridade)	Supervisor, operador, rbs <lista de funções>: ns uam rca rcrda rpr bac ce aac 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] [options]
options:
-clear state
-n group_name
-a nível de segurança:
    -ns rede e segurança
    -uam gerenciamento de conta do usuário
    -rca acesso ao console remoto
    -rcrda acesso ao console remoto e disco remoto
    -rpr acesso de energia/reinicialização do servidor remoto
    -bac configuração básica de adaptador
    -ce capacidade para limpar logs de eventos
    -aac configuração avançada de adaptador
-h
```

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.
-dn	Nome de domínio	Nome de domínio no formato válido

Opção	Descrição	Valores
-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 IMM. Esse valor é somente leitura e não é configurável.
-ipv6static	Estado do IPv6 estático	disabled, enabled
-i6	Endereço IP estático	Endereço IP estático para canal Ethernet 0 no formato IPv6
-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
-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
-auto	Configuração de negociação automática, que determina se as definições Taxa de dados e Rede duplex são configuráveis	true, false
-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).

Sintaxe:

```
ifconfig eth0 [options]
options:
-state interface_state
-c config_method
-i static_ip_address
-g gateway_address
-s subnet_mask
-n hostname
-r data_rate
-d duplex_mode
-m max_transmission_unit
-l locally_administered_MAC
```

Exemplo:

```
system> ifconfig eth0
-state enabled
-c dthens
```

```

-i 192.168.70.125
-g 0.0.0.0
-s 255.255.255.0
-n IMMA00096B9E003A
-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 IMM.
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 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
-aom	Modo somente autenticação	Ativado, desativado
-a	Método de autenticação do usuário	Somente local, somente LDAP, local primeiro depois LDAP, LDAP primeiro depois local
-b	Método de ligação	Conexão com Anônimo, conexão com ClientDN e senha e conexão com Credencial de Login
-c	Nome distinto do cliente	Sequência de até 63 caracteres para <i>client_dn</i>
-fn	Nome da floresta	Ambientes Active Directory, sequência de até 127 caracteres para <i>forest_name</i>
-d	Domínio de procura	Sequência de até 31 caracteres para <i>search_domain</i>
-f	Filtro de grupo	Sequência de até 63 caracteres para <i>group_filter</i>
-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 <i>client_pw</i> -pc <i>confirm_pw</i></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> , e o comando falhará se eles não corresponderem.
-r	Nome distinto (DN) de entrada raiz	Sequência de até 63 caracteres para <i>root_dn</i>
-rbs	Segurança Aprimorada Baseada em Função para usuários do Active Directory	Ativado, desativado

Opção	Descrição	Valores
s1ip	Nome do host/endereço IP do servidor 1	Sequência de até 63 caracteres ou um endereço IP para <i>host name/ip_addr</i>
s2ip	Nome do host/endereço IP do servidor 2	Sequência de até 63 caracteres ou um endereço IP para <i>host name/ip_addr</i>
s3ip	Nome do host/endereço IP do servidor 3	Sequência de até 63 caracteres ou um endereço IP para <i>host name/ip_addr</i>
-s4ip	Nome do host/endereço IP do servidor 4	Sequência de até 63 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 -rbs está ativada, esse campo especifica um nome de destino que pode ser associado a uma ou mais funções no Active Directory Server por meio do Snap-In de Segurança Baseado em Função.
-u	Atributo de procura UID	Sequência de até 23 caracteres para <i>search_attrib</i>
-v	Obter endereço do servidor LDAP por meio de DNS	Desativado, ativado
-h	Exibe o uso e as opções do comando	

Sintaxe:

ldap [*options*]

options:

```
-aom enabled|disabled|
-a loc|ldap|locId|ldloc
-b anon|client|login
-c client_dn
-d search_domain
-fn forest_name
-f group_filter
-g group_search_attr
-l string
-p client_pw
-pc confirm_pw
-r root_dn
-rbs enabled|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	Nome ou endereço IP do servidor Network Time Protocol	O nome do servidor NTP a ser usado para a sincronização de clock.
-f	A frequência (em minutos) com que o clock do IMM é sincronizado com o servidor Network Time Protocol	3 a 1440 minutos
-synch	Solicita uma sincronização imediata com o servidor Network Time Protocol	Nenhum valor é usado com esse parâmetro.

Sintaxe:

```

ntp [options]
options:
-en state
-i hostname
-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 portcfg

Use o comando **portcfg** para configurar a porta serial. 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.

Os parâmetros são configurados no hardware e não pode ser alterados:

- 8 bits de dados
- sem paridade
- 1 bit de parada

A tabela a seguir mostra os argumentos das opções.

Opção	Descrição	Valores
-b	Taxa de bauds	9600, 19200, 38400, 57600, 115200, 230400
-climode	Modo da CLI	nenhum, cliems, cliuser • nenhum: A interface da linha de comandos é desativada • cliems: A interface da linha de comandos é ativada com sequências de pressionamento de tecla compatíveis com EMS • cliuser: A interface da linha de comandos é ativada com sequências de pressionamento de tecla definidas pelo usuário

Sintaxe:

```
portcfg [options]
portcfg [options]
options:
-b baud_rate
-climode cli_mode
-cliauth cli_auth
```

Exemplo:

```
system> portcfg
-b      : 115200
-climode : 2 (CLI with user defined keystroke sequences)
system>
```

Comando portcontrol

Use o comando **portcontrol** para configurar o status da porta do serviço do IMM. Para alterar o status da porta, digite as opções, seguidas pelos valores. Para alterar o status de controle da porta, 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
-ipmi	Porta IPMI	on, off

Sintaxe:

```
portcontrol [options]
options:
-ipmi status
```

Exemplo:

```
system> portcontrol
-ipmi: on
```

Comando srcfg

Use o comando **srcfg** para configurar o redirecionamento serial. Digite **srcfg** para exibir a configuração atual. 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.

A tabela a seguir mostra os argumentos para a opção **-exitcliseq**.

Opção	Descrição	Valores
-exitcliseq	Sair de uma sequência de pressionamento de tecla da interface de linha de comandos	Sequência de pressionamento de tecla definida pelo usuário para sair da CLI. Para obter detalhes, consulte os valores para a opção -entercliseq nesta tabela.

Sintaxe:

```
srcfg [options]
options:
-exitcliseq exitcli_keyseq
```

Exemplo:

```
system> srcfg
-exitcliseq ^[Q
system>
```

Comando ssl

Use o comando **ssl** para exibir e configurar os parâmetros Secure Sockets Layer (SSL).

Nota: Para poder ativar um cliente SSL, um certificado de cliente deve ser instalado.

Opção	Descrição
-ce	Ativa ou desativa um cliente SSL
-se	Ativa ou desativa um servidor SSL
-h	Lista o uso e as opções

Sintaxe:

```
ssl [options]
options:
-ce on | off
-se on | off
-h
```

Parâmetros: Os seguintes parâmetros são apresentados na exibição de status da opção para o comando **ssl** e são a saída apenas a partir da interface da linha de comandos:

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 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
-o	Tempo limite do sistema operacional	minutos	desativado, 2.5, 3, 3.5, 4
-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

Sintaxe:

```
timeouts [options]
options:
-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. Para obter mais informações sobre a ativação ou desativação dessa interface, consulte “Desativando a interface USB dentro da banda” na página 24.

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 de usuário e seus níveis de autoridade e para criar novas contas de usuário e modificar as contas existentes.

Leia as diretrizes a seguir sobre o comando **users**:

- Os números de usuário devem ser de 1 a 12, inclusive.
- Os nomes de usuário devem ter menos de 16 caracteres e só podem conter números, letras, pontos e sublinhados.
- As senhas devem ter mais de 5 e menos de 16 caracteres e devem conter pelo menos um caractere alfabético e um não alfabético.
- O nível de autoridade pode ser um dos seguintes:
 - super (supervisor)
 - ro (somente leitura)
 - Qualquer combinação dos valores a seguir, separados por |:
 - am (Acesso de gerenciamento de 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])

Sintaxe:

```
users [options]  
options:  
-user number  
-n username  
-p password  
-a authority level
```

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. jacybyacknovic 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. jacobjackenovic 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 IMM

Os comandos de controle do IMM são os seguintes:

- clearcfg
- clock
- identify
- resetsp
- update

Comando clearcfg

Use o comando **clearcfg** para definir a configuração do IMM para seus padrões de fábrica. Você deve ter pelo menos autoridade de Configuração de Adaptador Avançada para emitir esse comando. Depois que a configuração do IMM tiver sido limpa, o IMM será reiniciado.

Comando clock

Use o comando **clock** para exibir a data e hora atuais de acordo com o clock do IMM 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 ou +10, 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), gtb (Grã-Bretanha), egt (Egito), fle (Finlândia).
- Para +10, as configurações de horário de verão são as seguintes: off, ea (Zona Oriental da Austrália), tas (Tasmânia), vlad (Vladivostok).
- 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
12/12/2003 13:15:23 GMT-5:00 dst on
system> clock -d 12/31/2004
ok
system> clock
12/31/2004 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 resetsp

Use o comando **resetsp** para reiniciar o IMM. Você deve ter pelo menos autoridade de Configuração de Adaptador Avançada para poder emitir esse comando.

comando update

Use o comando **update** para atualizar o firmware no IMM ou o IMM. Para usar esse comando, você deve ter pelo menos autoridade de Configuração de Adaptador Avançada. O arquivo de firmware (especificado por *filename*) é transferido primeiro do servidor TFTP (especificado por seu endereço IP) para o IMM ou IMM e, em seguida, atualizado. A opção -v especifica o modo detalhado.

Nota: Certifique-se de que o servidor TFTP esteja sendo executado no servidor a partir do qual o arquivo será transferido por download.

Opção	Descrição
-i	Endereço IP do servidor TFTP
-l	Nome do arquivo (a ser atualizado)
-v	Modo detalhado

Sintaxe:

```
update -i TFTP_server_IP_address -l filename
```

Exemplo: No modo detalhado, o progresso de atualização é exibido em tempo real na porcentagem de conclusão.

```
system>update -i 192.168.70.200 -l imm_yuoo20a.upd -v
Atualização de firmware está em andamento. Aguarde..
Fazendo download da imagem - 66%
```

```
system>update -i 192.168.70.200 -l imm_yuoo20a.upd -v
Atualização de firmware está em andamento. Aguarde..
Imagem Transferida por Download.
```

```
system>update -i 192.168.70.200 -l imm_yuoo20a.upd -v
Atualização de firmware está em andamento. Aguarde..
Imagem Transferida por Download.
Atualizando imagem - 45%
```

```
system>update -i 192.168.70.200 -l imm_yuoo20a.upd -v
Atualização de firmware está em andamento. Aguarde..
Imagem Transferida por Download.
Operação de atualização concluído.
system>
```

Se a atualização não estiver no modo detalhado, o progresso será exibido em caracteres # consecutivos.

```
system>update -i 192.168.70.200 -l dsa_d6yt28a_68608_2.upd
Atualização de firmware está em andamento. Por favor, aguarde..
Fazendo download da imagem: #####
Atualizando imagem: #####
Operação de atualização concluído.
```

Comandos do Consultor de Serviço

Os comandos do Consultor de Serviço são os seguintes:

- autoftp
- chconfig
- chlog
- chmanual
- events
- sdemail

Comando autoftp

Use o comando **autoftp** para exibir e configurar as definições do servidor FTP/TFTP para o Consultor de Serviço.

Nota: Os termos e condições do Consultor de Serviço devem ser aceitos antes de usar esse comando.

A tabela a seguir mostra os argumentos das opções.

Opção	Descrição	Valores
-m	Modo de relatório de problemas automatizado	<i>ftp, tftp, desativado</i>

Opção	Descrição	Valores
-i	endereço IP ou nome do host do servidor ftp/tftp para relatório de problemas automatizado	Endereço IP ou nome do host
-p	porta de transmissão ftp/tftp	Numérico entre 1 e 65535 para <i>port_number</i>
-u	Nome de usuário ftp delimitado por aspas para relatório de problemas	Sequência de até 63 caracteres para <i>user_name</i>
-pw	Senha ftp delimitada por aspas para relatório de problemas	Sequência de até 63 caracteres para <i>password</i>
Nota: Para o valor <i>ftp</i> , todas as opções (campos -i, -p, -u e -pw) devem ser configuradas. Para o valor <i>tftp</i> , apenas as opções -i e -p são necessárias.		

Sintaxe:

```
autoftp [options]
options:
-m ftp|tftp|disable
-i host name|ip_addr
-p port_number
-u user_name
-pw password
```

Comando chconfig

Use o comando **chconfig** para exibir e configurar as definições do Consultor de Serviço para o IMM.

A tabela a seguir mostra os argumentos das opções.

Opção	Descrição	Valores
-li	Visualize ou aceite o Termos e Condições do Consultor de Serviço. Os Termos e Condições do Consultor de Serviço devem ser aceitos por meio dessa opção antes de configurar outras opções.	visualizar, aceitar
-sa	Status do Consultor de Serviço do Suporte IBM	ativado, desativado
-sc	Código do país para o IBM Service Support Center	Código do país ISO de dois caracteres
-ca	Endereço delimitado por aspas do local da máquina	Sequência de até 30 caracteres para <i>address</i>
-cci	Cidade delimitada por aspas do local da máquina	Sequência de até 30 caracteres para <i>city</i>
-ce	Endereço de email da pessoa de contato no formato <i>userid@hostname</i>	Sequência de até 30 caracteres para <i>email_addr</i>
-cn	Nome da pessoa de contato delimitado por aspas	Sequência de até 30 caracteres para <i>contact_name</i>

Opção	Descrição	Valores
-co	Organização/nome da empresa da pessoa de contato delimitado por aspas	Sequência de até 30 caracteres para <i>company_name</i>
-cph	Número de telefone da pessoa de contato delimitado por aspas	Sequência entre 5 e 30 caracteres para <i>phone_number</i>
-cs	Estado do local da máquina	Sequência entre 2 e 3 caracteres para <i>state/province</i>
-cz	Código postal do local da máquina delimitado por aspas	Sequência de até 9 caracteres para <i>postal_code</i>
-loc	Nome completo do host ou endereço IP para o proxy HTTP	Sequência de até 63 caracteres ou um endereço IP para <i>host_name/ip_addr</i>
-po	Porta do proxy HTTP	Um número de porta entre 1 e 65535 para <i>port_number</i>
-ps	Status do proxy HTTP	ativado, desativado
-pw	Senha do proxy HTTP delimitada por aspas	Sequência de até 15 caracteres para <i>password</i>
-u	Nome de usuário do proxy HTTP delimitado por aspas	Sequência de até 30 caracteres para <i>user_name</i>
1. Os termos e condições do Consultor de Serviço devem ser aceitos por meio da opção -li antes de configurar outras opções. 2. Todos os campos de informações de contato, bem como os campos do IBM Service Support Center são obrigatórios para que o Suporte IBM do Consultor de Serviço possa ser ativado. Se um proxy for necessário, os campos do proxy HTTP deverão ser configurados.		

Sintaxe:

```
chconfig [options]
options:
-li view|accept
-sa service advisor state
-sc country_code
-ca address
-cci city
-ce email_addr
-cn contact_name
-co company_name
-cph phone_number
-cs state/province
-cz postal_code
-loc host_name/ip_addr
-po port_number
-ps status
-pw password
-u user_name
```

Comando chlog

Use o comando **chlog** para exibir os últimos cinco eventos de call home que foram gerados pelo sistema ou pelo usuário. A entrada call home mais recente é listada primeiro.

A tabela a seguir mostra os argumentos das opções.

Nota: Os termos e condições do Consultor de Serviço devem ser aceitos antes de usar esse comando.

Opção	Descrição	Valores
-event_index	Especifique uma entrada call home usando o Índice do Log de Atividades	Numérico entre 1 e 5
-ack	Reconhecer/não reconhecido, um evento call home foi corrigido	sim, não
-s	Apenas exibir o resultado do Suporte IBM	
-f	Apenas exibir o resultado do Servidor FTP/TFTP	

Sintaxe:

```
chlog [options]
options:
-event_index
-ack yes|no
-s
-f
```

Comando chmanual

Use o comando **chmanual** para gerar um evento Call Home manual ou um evento Call Home de Teste.

Nota: Os termos e condições do Consultor de Serviço devem ser aceitos antes de usar esse comando.

A tabela a seguir mostra os argumentos das opções.

Opção	Descrição	Valores
-test	Gerar um evento Call Home de teste	
-desc	Descrição do problema delimitada por aspas	Sequência de até 100 caracteres para <i>description</i>

Sintaxe:

```
chmanual [options]
options:
-test
-desc description
```

Comandos events

Use o comando **events** para visualizar e editar eventos de exclusão.

Nota: Os termos e condições do Consultor de Serviço devem ser aceitos antes de usar esse comando.

A tabela a seguir mostra os argumentos das opções.

Opção	Descrição	Valores
-che	Visualizar e editar eventos de exclusão	
-add	Incluir um evento de call home na lista de exclusão de call home	<i>event_id</i> no formato 0xxxxxxxxxxxxxxxxxxx
-rm	Remover um evento de call home da lista de exclusão de call home	<i>event_id</i> <i>all</i> no formato 0xxxxxxxxxxxxxxxxxxx, ou todos

Sintaxe:

```
events [options]
options: -che {-add} | {-rm}
-add event_id
-rm event_id|all
```

Comando **sdemail**

Use o comando **sdemail** para configurar as informações de serviço de email para os destinatários especificados.

A tabela a seguir mostra os argumentos das opções.

Opção	Descrição	Valores
-subj	Assunto do email delimitado por aspas	Sequência de até 119 caracteres para <i>email_subject</i>
-to	Endereço de email do destinatário. Essa opção pode consistir em vários endereços separados por uma vírgula.	Sequência de até 119 caracteres para <i>email_addrs</i>

Sintaxe:

```
sdemail [options]
options:
-subj email_subject
-to email_addrs
```

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 sobre quais produtos são suportados pela Linha de Suporte em seu país ou região, consulte <http://www.ibm.com/services/supline/products>.

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 **Business Partner Locator**. 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 21. Limites para partículas e gases

Contaminante	Limites
Partículas	- 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	- 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:

Gerência de Relações Comerciais e Industriais da IBM Brasil
Av. Pasteur, 138-146

Botafogo

- Rio de Janeiro, RJ
- 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 전자파적합기기로서 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类产品，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

- a conexão do IBM Systems Director, Configurando 80
- a criptografia de dados sensíveis, Configurando 80
- ActiveX 115
- Advanced Settings Utility (ASU) 1, 5, 129
- ajuda
 - da World Wide Web 162
 - enviando dados diagnósticos à IBM 162
 - origens de 161
- alertas 31
 - configurações SNMP 34
 - configurando destinatários 32
 - configurando tentativas remotas 33, 34
 - definições globais 33
 - selecionando para enviar
 - aviso 32
 - críticos 32
 - sistema 32
- alertas críticos 32
- alertas de aviso 32
- alertas de sistema 32
- alertas remotos
 - configurando definições 31
 - configurando destinatários 32
 - configurando tentativas 34
 - tipos
 - aviso 32
 - críticos 32
 - sistema 32
- applet
 - ActiveX 115
 - Java 115
- arquivo de configuração 92
- assistência, obtendo 161
- assistência ao produto, IBM Taiwan 163
- assistência ao produto IBM Taiwan 163
- ativando
 - criptografia de dados 82
- ativar criptografia de dados 82
- atraso de desligamento (tempo limite do servidor) 21
- atualizando o firmware 126
- autenticação baseada em função
 - active directory 70
 - ferramenta de snap-in de segurança 70
- autenticação do active directory
 - autorização local 63
- autenticação do usuário durante o login 30
- autorização local
 - autenticação do active directory 63
- aviso de Classe A da FCC 169
- aviso de Classe A da FCC nos Estados Unidos 169

- aviso de emissão eletrônica da Classe A 169
- aviso 165
 - emissão eletrônica 169
 - FCC, Classe A 169
- aviso e instruções 10
- aviso importantes 166

B

- baseboard management controller (BMC) 1
- Baseboard Management Controller (BMC) 5
- BIOS (sistema BIOS) 1
- bit de permissão
 - descrições 74
- BladeCenter 1, 9, 11, 36

C

- captura de tela azul 118
- captura de tela do sistema
 - operacional 5, 118
- centro de informações 162
- certificado autoassinado, gerando 83
- chaves de criptografia, gerando 85
- clock, sincronizando em uma rede 23
- clock de tempo real, sincronizando com o servidor NTP 23
- comando de redirecionamento serial 141
- comando portcontrol 150
- comandos, tipos de
 - configuração 141
 - consultor de serviço 156
 - controle do IMM 154
 - energia e reinicialização do servidor 141
 - monitor 138
 - redirecionamento serial 141
 - utilitário 137
- comandos de configuração 141
- comandos de controle do IMM 154
- comandos de monitor 138
- comandos de utilitário 137
- comandos do consultor de serviço 156
- conexão, Configurando o IBM Systems Director 80
- conexão de rede 11
 - endereço IP, estático padrão 11
 - endereço IP estático, padrão 11
 - endereço IP estático padrão 11
- conexão do Director, Configurando o IBM Systems 80
- conexão do IBM Systems Director, Configurando a 80
- conexão do Systems Director, configurando o IBM 80
- conexão Ethernet, configurando 38

- conexões, Configurando segurança SSL para LDAP 80
- conexões de rede 38, 41, 42
- conexões LDAP, Configurando segurança SSL para 80
- configuração do IMM
 - conexões de rede 38, 41
 - configurando o consultor de serviço 94
 - fazendo backup 92
- IMM
 - configurações de conexão de rede 38, 41, 42
- IPv6 42
- modificando e restaurando 91, 92
- Partição escalável 94
- usando o recurso de consultor de serviço 97
- configurações
 - alerta remoto 31
 - configurando login global 30
 - data e hora 22
 - Ethernet 38
 - informações do sistema 20
 - IPv4 41
 - IPv6 42
 - Secure Sockets Layer (SSL) 82
- configurações de login, global (interface da web) 30
- configurações globais de login (interface da web) 30
- configurando
 - alertas remotos 31, 32
 - conexão Ethernet 38
 - configurações globais de alerta remoto 33
 - configurações globais de login 30
 - designações de porta 36
 - DNS 45
 - interfaces de rede 38
 - LDAP 46
 - portas seriais 34
 - protocolos de rede 43
 - redirecionamento serial para SSH 36
 - redirecionamento serial para
 - Telnet 36
 - segurança 80
 - SMTP 46
 - SNMP 34, 43
 - SSH 89
 - Telnet 46
- Configurando a conexão do IBM Systems Director 80
- Configurando a criptografia de dados sensíveis 80
- Configurando gerenciamento de criptografia 80
- configurando o consultor de serviço 94
- Configurando o servidor da web seguro 80

- Configurando segurança SSL para conexões LDAP 80
- Configurando uma partição escalável 94
- configurar status da porta 150
- console do servidor 115, 116
- consultor de serviço
 - configuração 94
- contaminação, partículas e gases 167
- contaminação de gases 167
- contaminação por partículas 167
- controle de mouse
 - absoluto 121
 - relativa com aceleração padrão Linux 121
 - relativo 121
- controle de mouse absoluto 121
- controle de mouse relativo 121
- controle de mouse relativo para Linux (aceleração padrão Linux) 121
- controle remoto
 - applet ActiveX 115
 - applet Java 115
 - Applet Java 116
 - captura de tela 118
 - comandos de energia e reinicialização 123
 - controle de mouse absoluto 121
 - controle de mouse relativo 121
 - controle de mouse relativo para Linux (aceleração padrão Linux) 121
 - descrição 116
 - estatísticas de desempenho 123
 - funções 115
 - modo de cursor único 122
 - modo de passagem do teclado 121
 - saindo 126
 - Sessão de Mídia Virtual 116, 123
 - suporte de mouse 121
 - suporte de teclado 120
 - suporte de teclado internacional 120
 - Visualizador de Vídeo 116, 118, 119
- controle remoto de energia 123
- controle remoto de energia do servidor 114
- criando perfis de login 25
- criando uma página da web de suporte personalizada 163
- criptografia, ativar dados 82
- criptografia, Configurando os dados sensíveis 80
- criptografia de dados 82
- criptografia de dados, ativar 82
- criptografia de dados, Configurando sensíveis 80
- criptografia de dados sensíveis, Configurando a 80

D

- dados vitais do produto (VPD) 110
 - visualizando log de atividades do componente 110
 - visualizando VPD de nível de componente 110
 - visualizando VPD de nível de máquina 110
 - visualizando VPD do IMM 110

- dados vitais do produto do log de atividades do componente, visualizando 110
- data e hora, verificando 22
- declaração de Classe A da Alemanha 170
- declaração de Classe A da Austrália 169
- declaração de Classe A da Nova Zelândia 169
- declaração de conformidade com a Diretiva EMC da União Europeia 170
- declaração de emissão eletrônica de Classe A da China 172
- declaração de emissão eletrônica de Classe A da República Popular da China 172
- declaração regulamentar de telecomunicação 169
- desativando interface USB dentro da banda 24
 - a partir do IMM 131
 - do módulo de gerenciamento avançado 131
- descrição de certificado SSL 83
- designações de porta, configurando 36
- deslocamento GMT em configurações de tempo 22
- disco, remoto 3, 123
- disco remoto 3, 123, 124, 125
- DNS, configurando 45
- documentação
 - formato 168
 - usando 162
- documentação acessível 168
- driver de dispositivo IPMI do Windows 132
- driver LAN sobre USB Linux 133
- driver LAN sobre USB Windows 132
- DSA, enviando dados à IBM 162
- Dynamic System Analysis (DSA) 110

E

- efetuando login no IMM 14
- efetuando logoff da interface da web 99
- endereço IP
 - configurando 11
 - IPv4 11
 - IPv6 11
- endereço IP, estático padrão 11
- endereço IP estático, padrão 11
- endereço IP estático padrão 11
- energia e reinicialização do servidor
 - atividade 113
 - comandos 141
 - controle remoto 114
- enviando dados diagnósticos à IBM 162
- evento de asserção, log de evento do sistema 106
- evento de desasserção, log de evento do sistema 106
- exemplo de esquema do usuário, LDAP 47

F

- fazendo backup da configuração do IMM 92
- ferramentas 128
 - Advanced Settings Utility (ASU) 129
 - IPMItool 129
 - outras ferramentas de gerenciamento do IMM 130
 - SMBridge 129, 135
 - utilitários de Atualização 129
- firmware, atualizando 126
- funcionamento do sistema, monitorando
 - LED do localizador do sistema 101
 - limites de temperatura 101
 - limites de voltagem 101
 - página de resumo 101
 - velocidade do ventilador 101

G

- gerenciamento, Configurando
 - criptografia 80
- gerenciamento de certificado confiável do cliente SSL 88
- gerenciamento de certificado de cliente SSL 88
- gerenciamento de certificado do servidor SSL 83
 - certificado autoassinado 83
 - sobre HTTPS 88
 - solicitação de assinatura de certificado 85
- gerenciamento de criptografia 89
- gerenciamento de criptografia, Configurando 80
- gerenciando criptografia 89

H

- horário de verão, ajustando para 22

I

- IBM BladeCenter 1, 9, 11, 36
- IBM System x Server Firmware
 - atualizando o firmware 126
 - descrição 1
 - ferramentas e utilitários 128
 - utilitário de Configuração 11, 108, 127
 - VPD 110
- IDs de usuários
 - IMM 25
 - IPMI 25
- IMM
 - alertas 31
 - atualizando o firmware 126
 - comparação com BMC com RSA 5
 - conexão de rede 11
 - configuração 92
 - configurando 19
 - controle remoto 116
 - descrição 1
 - descrições de ações 15
 - designações de porta 36

IMM (*continuação*)

- funções 5
- gerenciando ferramentas e utilitários 128
- IDs de usuários 25
- IMM Premium 3
- IMM Premium, fazendo upgrade para 5
- IMM Standard 3
- IMM Standard, fazendo upgrade do 5
- Indicadores Luminosos Virtuais 105
- informações do sistema 20
- interface da web 11
- interfaces de rede 38
- LAN sobre USB 131
- logoff 99
- logs de eventos 106
- monitorar 101
- novas funções 1
- padrões 93
- perfis de login 25
- presença remota 115
- protocolos de rede 43
- recursos 3
- redirecionamento serial 36
- reiniciando 94
- tarefas 113
- IMM Premium, fazendo upgrade para 5
- IMM Standard, fazendo upgrade do 5
- Indicadores Luminosos 105
- Indicadores Luminosos Virtuais 15, 105
- informações do sistema, configurando 20
- inicialização da rede PXE 126
- inicialização remota 123
- instrução de emissão eletrônica de Classe A da Coreia 171
- instrução de emissão eletrônica de Classe A da Rússia 172
- instrução de emissão eletrônica de Classe A de Taiwan 172
- instrução de emissão eletrônica de Classe A do Canadá 169
- instrução de emissão eletrônica de Classe A do Japão 171
- interface da linha de comandos (CLI)
 - acessando 135
 - descrição 135
 - efetuando login 135
 - recursos e limitações 136
 - sintaxe de comando 136
- interface da web
 - efetuando login na interface da web 14
- interface da web, abrindo e usando 11
- interface USB dentro da banda, desativando 24, 131
- interfaces de rede
 - configurando a conexão Ethernet 38
- IPMI
 - gerenciamento de servidor remoto 135
 - IDs de usuários 25
- IPMITool 129, 135
- IPv6 11

J

- Java 5, 9, 115, 116, 123

L

- LAN sobre USB
 - configuração manual de 132
 - configurações 131
 - conflitos 131
 - descrição 131
 - driver de dispositivo IPMI do Windows 132
 - driver do Windows 132
 - driver Linux 133
- LDAP
 - configurando a ordem de autenticação 30
 - descrição 46
 - seguro 82
- LDAP, configurando
 - autenticação do active directory 63
 - autenticação legada 74
 - autorização legada 74
 - baseado em função do active Directory 70
 - configurando o cliente LDAP 63
 - exemplo de esquema do usuário 47
- Microsoft Windows Server 2003 Active Directory
 - incluindo usuários em grupos de usuários 58
 - níveis de autoridade 59
 - verificando configuração 62
- navegando no servidor LDAP 56
- Novell eDirectory
 - Configurando níveis de autoridade 51
 - incluindo usuários em grupos de usuários 50
 - níveis de autoridade 50
 - participação em grupos 49
- visualização de esquema do Novell eDirectory 48
- visualização do esquema do Windows Server 2003 Active Directory 58
- LDAP legado
 - autenticação 74
 - autorização 74
- LED do localizador do sistema 101
- log de evento do sistema 106
- logs de eventos
 - acesso remoto 22
- log de eventos da IPMI 106
- log de eventos do ASM 106
- log de eventos do chassi 106
- log de eventos do IMM 106
 - visualizando 107
- log de eventos do módulo de gerenciamento integrado 106
- log de eventos do servidor
 - níveis de severidade 107
- log do DSA 106
- logs, tipos de
 - log de evento do sistema 106
 - log de eventos do chassi 106
 - log de eventos do IMM 106

logs, tipos de (*continuação*)

- log do DSA 106
- logs de eventos
 - descrição 106
 - níveis de severidade 107
 - visualizando da interface da web 107
 - visualizando do utilitário de configuração 108

M

- mapeando unidades 124, 125
- marcas registradas 166
- método de autenticação para o usuário no login 30
- Microsoft Windows Server 2003 Active Directory 58
 - incluindo usuários em grupos de usuários 58
 - níveis de autoridade 59
 - verificando configuração 62
- modificando a configuração do IMM 91, 92
- modo de cor de vídeo no controle remoto 119
- modo de cursor único 122
- modo de passagem do teclado no controle remoto 121
- modos de visualização no controle remoto 118
- módulo de gerenciamento avançado 1, 9, 11, 131
- monitoramento de temperatura 101
- monitoramento de velocidade do ventilador 101
- monitoramento de voltagens 101

N

- Network Time Protocol (NTP) 23
- níveis de autoridade, definindo no perfil de login 25
- níveis de autoridade customizados no perfil de login 25
- notas, importantes 166
- números de porta, reservado 36
- números de telefone 163
- números de telefone do serviço e suporte a software 163
- números de telefone do serviço e suporte de hardware 163

O

- o servidor da web seguro, Configurando 80
- OSA System Management Bridge 129

P

- padrões, restaurando a configuração 93
- padrões de fábrica, restaurando 93
- padrões do IMM, restaurando 93
- página da web de suporte, customizada 163

- página da web de suporte
 - customizada 163
- para conexões LDAP, Configurando
 - segurança SSL 80
- perfis, login
 - configurando direitos de acesso 25
 - criando 25
 - excluindo 30
- perfis de login
 - configurando direitos de acesso 25
 - criando 25
 - excluindo 30
 - limitações de ID do usuário 25
 - níveis de autoridade
 - customizados 25
- portas seriais, configurando 34
- presença remota
 - ativando 116
 - descrição 115
- protocolo de segurança SSL 82
- protocolos
 - DNS 45
 - LDAP 46
 - SMTP 46
 - SNMP 43
 - SSL 82
 - Telnet 46
- protocolos de rede
 - configurando LDAP 46
 - configurando o DNS 45
 - configurando o SNMP 43
 - configurando o SSL 82
 - configurando SMTP 46
 - descrição 43
- publicações on-line
 - informações de atualização da
 - documentação 1
 - informações de atualização de
 - firmware 1
 - informações de código de erro 1
- PXE Boot Agent 15

R

- reconfigurar IMM 127
- recurso
 - consultor de serviço 97
- recurso de consultor de serviço
 - descrição 94
- recursos do IMM 3
- redirecionamento serial para SSH 36
- redirecionamento serial para Telnet 36
- reiniciando o IMM 94
- Remote Desktop Protocol (RDP),
 - ativação 123
- Remote Supervisor Adapter II 1, 3, 5
- requisitos
 - navegador da web 9
 - sistema operacional 9
- requisitos de navegador 9
- requisitos de navegador da web 9
- requisitos de sistema operacional 9
- restaurando a configuração do IMM 91, 92
- restaurando padrões do IMM 93
- resumo da configuração,
 - visualizando 15

S

- Secure Sockets Layer (SSL) 82
- segurança 80
- segurança para conexões LDAP,
 - Configurando SSL 80
- segurança SSL para conexões LDAP,
 - Configurando 80
- sequência de inicialização, alterando 15
- sequência de inicialização do servidor
 - host, alterando 15
- Serial over LAN 135
- serviço e suporte
 - antes de ligar 161
 - hardware 163
 - software 163
- servidor, Configurando o da web
 - seguro 80
- servidor da web, Configurando
 - seguro 80
- servidor da web, seguro 82
- servidor da web seguro, Configurando
 - o 80
- servidor da web seguro e LDAP seguro
 - ativando o SSL para o cliente
 - LDAP 89
 - ativando SSL para o servidor da web
 - seguro 88
 - descrição 82
 - descrição de certificado SSL 83
 - gerenciamento de certificado confiável
 - do cliente SSL 88
 - gerenciamento de certificado de
 - cliente SSL 88
 - gerenciamento de certificado do
 - servidor SSL 83
- servidor Shell Seguro
 - ativando 90
 - gerando chave privada 90
 - usando 90
- servidor Shell Seguro (SSH) 89
- servidores blade 1, 9, 11, 36
- servidores blade IBM 1, 9, 11, 36
- servidores remotos, monitorando
 - limites de temperatura 101
 - limites de voltagem 101
 - velocidade do ventilador 101
- Sessão de Mídia Virtual 116
 - disco remoto 123
 - mapear unidades 124, 125
 - remover mapeamento de
 - unidades 124, 125
 - saindo 126
- sincronizando clocks em uma rede 23
- SMBridge 129, 135
- SMTP, configurando 46
- SNMP 25, 31
 - configurações de alerta 34
 - configurando 43
- solicitação de assinatura de certificado,
 - gerando 85
- SSL, ativando
 - para o cliente LDAP 89
 - para servidor da web seguro 88
- status da porta, configurar 150
- status do sistema 101
- suporte de mouse de controle
 - remoto 121

- suporte de mouse no controle
 - remoto 121
- suporte de teclado internacional no
 - controle remoto 120
- suporte de teclado no controle
 - remoto 120

T

- Telnet 46
- tempos limites, consulte tempos limites
 - do servidor 21
- tempos limites do servidor
 - Atraso de desligamento 21
 - watchdog do carregador 21
 - watchdog do S.O. 21
- tempos limites do servidor,
 - configurando 21
- tentativas de alerta remoto global,
 - configuração 33

U

- usando o recurso de consultor de
 - serviço 97
- utilitários 128
- utilitários de Atualização 129

V

- visualização de esquema do Novell
 - eDirectory 48
- visualização de esquema do Novell
 - eDirectory, LDAP
 - Configurando níveis de
 - autoridade 51
 - incluindo usuários em grupos de
 - usuários 50
 - níveis de autoridade 50
 - participação em grupos 49
- Visualizador de Vídeo 116
 - captura de tela 118
 - comandos de energia e
 - reinicialização 123
 - controle de mouse absoluto 121
 - controle de mouse relativo 121
 - controle de mouse relativo para Linux
 - (aceleração padrão Linux) 121
 - estatísticas de desempenho 123
 - modo de cor de vídeo 119, 120
 - modo de cursor único 122
 - modo de passagem do teclado 121
 - modos de visualização 118
 - saindo 126
 - suporte de mouse 121
 - suporte de teclado internacional 120
- visualizando logs de eventos 108
- VPD de nível de componente 110
- VPD de nível de máquina 110

W

- watchdog (tempo limite do servidor)
 - carregador 21
 - sistema operacional (OS) 21

watchdog do carregador (tempo limite do
servidor) 21
watchdog do sistema operacional (OS)
(tempo limite do servidor) 21



Número da Peça: 00FH264

Impresso no Brasil

(1P) P/N: 00FH264

