Guia de instalação

McAfee Enterprise Security Manager 9.5.0

COPYRIGHT

ATRIBUIÇÕES DE MARCAS COMERCIAIS

INFORMAÇÕES SOBRE LICENÇA

Contrato de licença

Conteúdo

Prefácio

Este guia fornece todas as informações necessárias para que você possa trabalhar com seu produto McAfee.

Conteúdo

Sobre este guia

Estas informações descrevem o público-alvo do guia, as convenções tipográficas e os ícones usados neste guia, além de como o guia é organizado.

Público-alvo

McAfee é cuidadosamente pesquisada e escrita tendo em vista o seu público-alvo.

A informação contida neste guia destina-se principalmente a:

- **Administradores**: Pessoas responsáveis pela implementação e imposição do programa de segurança da empresa.
- **Usuários**: Pessoas que utilizam o computador onde o software está instalado e que têm acesso a todos ou alguns dos seus recursos.

Convenções

Este guia usa as seguintes convenções tipográficas e ícones.

Título do livro, *termo*, *ênfase*	Título de um livro, capítulo ou tópico; um novo termo; ênfase.
Negrito	Texto bastante enfatizado.
`Digitação do usuário, código, mensagem`	Comandos e outros textos digitados pelo usuário; um fragmento de código; uma mensagem exibida.
Texto da interface	Palavras da interface do produto, como opções, menus, botões e caixas de diálogo.
Azul de hipertexto	Um link para um tópico ou para um site externo.
	**Observação:** Informações adicionais, como um método alternativo de acessar uma opção.
	**Dica:** Sugestões e recomendações.

Importante/cuidado: Informações importantes para proteger o sistema do seu computador, sua instalação de software, rede, negócios ou seus dados.

Aviso: Informações críticas para prevenir lesões corporais durante a utilização de um produto de hardware.

Localizar a documentação do produto

Após o lançamento de um produto, as informações adicionais sobre ele são introduzidas no Centro de conhecimento online da McAfee.

Tarefa

1 Acesse a guia **Knowledge Center** do ServicePortal da McAfee em http://support.mcafee.com.

2 No painel **Base de conhecimento**, clique em uma fonte de conteúdos:

- **Documentação do produto** para encontrar a documentação do usuário
- **Artigos técnicos** para encontrar artigos da Base de conhecimento

3 Selecione **Não limpar meus filtros**.

4 Insira um produto, selecione uma versão, e clique em **Pesquisar** para exibir uma lista de documentos.

1 Introdução

Este guia descreve como instalar e configurar estes dispositivos:

- McAfee® Nitro Intrusion Prevention System (IPS)
- McAfee® Enterprise Security Manager (McAfee ESM)
- McAfee Event Receiver
- McAfee ESM/Event Receiver (ESMREC)
- McAfee Database Event Monitor (DEM)
- McAfee Application Data Monitor (ADM)
- McAfee Enterprise Log Manager (ELM)
- McAfee Advanced Correlation Editor (ACE)
- McAfee Direct Attached Storage (DAS)
- McAfee Receiver/ELM (ELMERC)
- McAfee ESM/Receiver/ELM (ESMELM)

Ele se divide em duas seções principais:

- Instalação de um dispositivo McAfee ESM, que informa as etapas a seguir para inspecionar, montar, conectar e iniciar o dispositivo.
- Instalação de um dispositivo McAfee ESM, que descreve como configurar a interface de rede de cada tipo de dispositivo, configurar para o IPv6, efetuar logon no console do McAfee ESM e codificar o dispositivo.

1 Introdução

2 Instalação de dispositivos McAfee ESM

É preciso instalar os dispositivos McAfee antes de usá-los, a fim de proteger a rede de intrusões ou para coletar dados da rede. Estas instruções de instalação aplicam-se a todos os modelos atuais dos dispositivos McAfee ESM.

Conteúdo

Preparação para instalar dispositivos McAfee ESM

Antes de instalar os dispositivos, verifique se o seu sistema atende aos requisitos mínimos e se o equipamento não foi danificado durante o envio. Selecione o local para instalar o equipamento.

Requisitos de hardware e software

Seu sistema precisa atender aos requisitos mínimos de hardware e software.

Requisitos do sistema

- Processador: classe P4 (não Celeron) ou superior (Mobile/Xeon/Core2,Corei3/5/7) ou classe AMD AM2 ou superior (Turion64/Athlon64/Opteron64,A4/6/8)
- RAM: 1,5 GB
- Sistema operacional Windows: Windows 2000, Windows XP, Windows 2003 Server, Windows Vista, Windows 2008 Server, Windows Server 2012, Windows 7, Windows 8, Windows 8.1
- Navegador: Internet Explorer 7.x ou versões posteriores, Mozilla FireFox 3.0.0.0 ou versões posteriores, Google Chrome 12.0.742.91 ou versões posteriores
- Flash Player: versão 11.2.x.x ou posterior

Os recursos do ESM usam janelas pop-up quando fazem upload ou download dos arquivos. Desative o bloqueador de pop-ups do endereço IP ou nome de host do seu ESM.

Requisitos da máquina virtual

- Processador — 8 núcleos de 64 bits, Dual Core2/Nehalem ou superior ou AMD Dual Athlon64/Dual Opteron64 ou superior
- RAM — Depende do modelo (4 GB ou mais)
- Espaço em disco: Depende do modelo (250 GB ou mais)

- ESXi 5.0 ou posterior
- Configuração ampla ou reduzida — Você deve decidir quais requisitos de disco rígido são necessários para o seu servidor. Os requisitos mínimos são de 250 GB, a menos que a VM comprada tenha mais. Consulte as especificações de seu produto de VM.

O ENMELM VM usa muitos recursos que requerem CPU e RAM. Se o ambiente do ESXi compartilhar os requisitos de CPU/RAM com outras VMs, o desempenho do ENMELM VM será afetado. Não deixe de incluir o que é necessário em termos de CPU e RAM nos requisitos.

Inspeção de embalagem e dispositivo

Antes de instalar o equipamento, verifique se não existem sinais de danos ou violação.

Tarefa

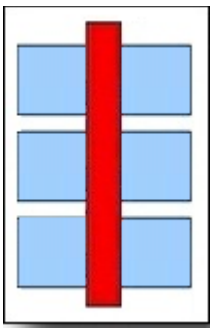
1 Assim que receber seu dispositivo, inspecione a embalagem e o próprio dispositivo para garantir que não haja sinais de danos ou tratamento indevido.

> No caso de uma instalação FIPS, verifique se a fita da embalagem apresenta sinais de violação. Se houver algum indício de violação, entre em contato imediatamente o Suporte da McAfee para obter instruções e não instale o produto.

2 Verifique se todos os itens listados no recibo estão incluídos no pacote.

3 Ao fazer uma instalação FIPS, encontre o selo antiviolação no pacote de acessórios do contêiner de envio. Aplique o selo para que ele bloqueie completamente as portas USB, impedindo seu uso sem deixar evidência de violação (consulte o Diagrama 1).

Diagrama 1: Posicionamento do selo antiviolação.



Entre em contato imediatamente o Suporte da McAfee se não estiver inteiramente satisfeito com a inspeção.

Identificação de um local para instalação

É preciso analisar a rede existente e identificar uma rede e um local físico para o dispositivo. A seleção correta do local afeta o bom uso dos dispositivos.

Ao selecione um local para os seus dispositivos:

- Instale o seu dispositivo ESM em um local na rede em que ele possa gerenciar dispositivos e ser acessado por qualquer sistema que estiver acessando o ESM. Se não for possível uma comunicação direta entre dispositivos gerenciados pelo ESM ou sistemas com o ESM em execução, configure sua rede para permitir o roteamento do tráfego da rede entre eles.
- Coloque o dispositivo Nitro IPS entre o lado confiável e o lado não confiável da rede. O lado confiável será o lado que você deseja proteger e o não confiável, aquele que será deixado intencionalmente sem proteção. Por exemplo, você pode posicionar o Nitro IPS entre o firewall (lado não confiável) e o switch (lado confiável). As configurações de rede variam muito, portanto, o local selecionado depende das suas necessidades específicas de segurança e do ambiente de rede.

  Este equipamento destina-se à instalação em local de acesso restrito.

- Os dispositivos Receptor e DEM devem estar acessíveis aos dispositivos que eles monitoram. Se não for possível uma comunicação direta, configure sua rede para permitir o roteamento correto do tráfego da rede entre eles.

Conectar e iniciar os dispositivos

Após inspecionar o dispositivo e identificar o local de instalação preferencial, siga as etapas indicadas nesta seção para instalá-lo.

Tarefa

1 Monte o dispositivo.

Para proteger o dispositivo e o cabeamento contra dano acidental ou desconexão, monte o dispositivo em um rack (consulte *Apêndice F – Instalar o conjunto de trilhos AXXVRAIL*).

a Prepare um espaço para o dispositivo no local de montagem.

b Monte o dispositivo com segurança no local selecionado.

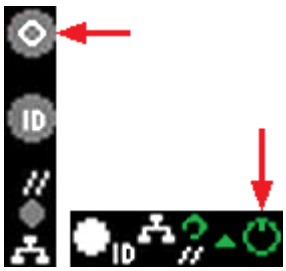
2 Conecte a fonte de alimentação ao dispositivo. Instale e estabilize o equipamento corretamente, de acordo com este manual de instruções e os códigos locais, estaduais e nacionais.

É altamente recomendável conectar todos os dispositivos ESM a uma UPS (fonte de alimentação ininterrupta). Um sistema com cabos de energia redundantes e módulos de energia operando em condições normais equilibra o compartilhamento de carga por meio de seu design paralelo, o que resulta em um sistema de energia confiável. Por ser um dispositivo em linha, o Nitro IPS precisa estar conectado a uma UPS.

3 Inicie o dispositivo.

a Conecte o cabo com a energia desligada e verifique se existe passagem de tráfego.

b Ligue o dispositivo.



4 Selecione o cabo da rede.

5 Conecte os cabos às portas confiáveis e não confiáveis. Se estiver conectando cabos de fibra, remova a proteção do cabo e do conector da rede somente quando estiver pronto para conectar os cabos.

6 Verifique a conectividade do dispositivo executando ping no lado confiável da rede em um endereço IP válido no lado não confiável.

Consulte também

Identificação dos tipos de conector e equipamento na página 12
Identificação dos cabos de rede na página 12
Identificação das portas de rede na página 13

Identificação dos tipos de conector e equipamento

É possível conectar o dispositivo IPS do Nitro à rede usando conectores de cobre ou fibra, dependendo do modelo do dispositivo.

Tabela 2-1 Tipo de conexão por dispositivo

Modelo IPS do Nitro	Tipo de conector
TX	RJ-45 (cobre)
SX	LC-Multimode (fibra)
LX	LC-Singlemode (fibra)

Conecte seus dispositivos ESM, Receptor e DEM à rede usando conectores de cobre e identifique os cabos de cobre ou fibra analisando os conectores. O cabo de cobre CAT5 tem conectores RJ-45 (1), ao passo que o cabo de fibra LC utiliza conectores de fibra (2).

É recomendável usar o CAT5 ou superior para a conexão de cobre. Para a conexão por gigabits, é recomendável usar CAT5e.

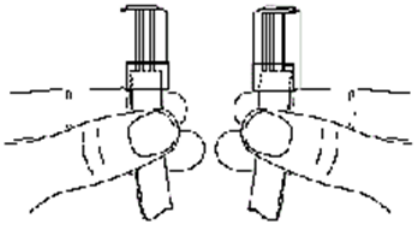
Tipo de equipamento

Existem dois tipos de equipamentos que podem ser conectados aos dispositivos ESM: DCE (Data Circuit-Terminating Equipment) e DTE (Data Terminal Equipment). Firewall e roteadores são DTE e switches são DCE. Os dispositivos ESM são DTE.

Identificação dos cabos de rede

Se seu dispositivo utiliza uma conexão de fibra, é preciso selecionar os cabos de fibra e conectá-los às portas. Se seu dispositivo utilizar uma conexão de cobre, use um cabo de cobre direto ou cruzado.

Para conectar uma porta RJ-45 do dispositivo ESM ao DCE, use um cabo direto. Para conectar a um DTE, use um cabo cruzado. Para diferenciar um cabo direto de um cruzado, segure as duas extremidades do cabo como ilustrado:



Em um cabo direto, os fios coloridos estão na mesma sequência em ambas as extremidades. Em um cabo cruzado, o primeiro (à esquerda) fio colorido em uma extremidade é da mesma cor do terceiro fio na outra extremidade.

Identificação das portas de rede

Após identificar os cabos necessários para a rede, identifique as portas no dispositivo McAfee aos quais esses cabos serão conectados.

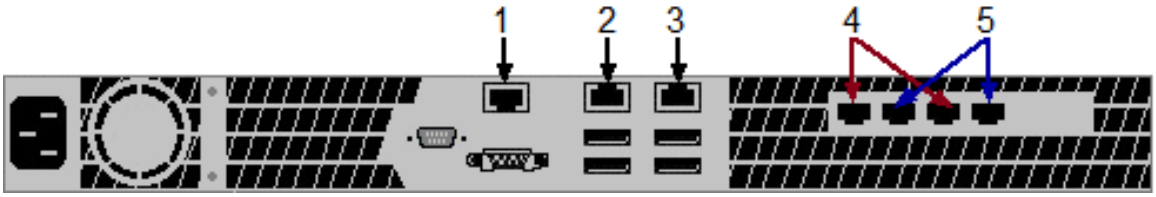
Sempre desligue as fontes de laser antes de inspecionar os conectores de fibra, os componentes ópticos ou conectores dos receptores. É possível emitir radiação a laser por fibra óptica via cabos ou conectores de fibra. Não olhe diretamente para o equipamento de fibra óptica. Sempre mantenha um protetor sobre os conectores de fibra desconectados.

Os dispositivos contêm portas de gerenciamento para que possam ser gerenciados no McAfee ESM. Além disso, os dispositivos IPS do Nitro e ADM contêm portas confiáveis e não confiáveis para conectar o dispositivo ao lado confiável e ao lado não confiável da rede.

Para identificar as portas de gerenciamento e as portas confiáveis e não confiáveis em todos os dispositivos, consulte a tabela abaixo.

Tipo de dispositivo	Número do modelo	Figura
ACE	ACE-2600 ou 3450	2-8
ADM	APM-1250, 1260	2-1
	APM-3450, 3460	2-3
DEM	DSM-2600 ou 3450	2-3
	DSM-4600	2-4
ELM	ELM-4600, 5600 ou 6000	2-8
ELM/Receptor	ELMERC-2600, 3450 ou 4600	2-8
ESM/ELM	ENMELM- 4600, 5600 ou 6000	2-8
ESM ou ESM/Receptor combinados	ETM-5600, 6000, X4 ou X6	2-8
	DAS-10, 25, 50 ou 100	2-9
IPS	NTP-1250	2-2
	NTP-2600, 3450-4BTX	2-3
	NTP-2600, 3450-8BTX	2-4
	NTP-2600, 3450-4BSX	2-5

Tipo de dispositivo	Número do modelo	Figura
	NTP-3450-2BSX	2-6
McAfee Reporter	ERU-5600	2-8
Receptor	ERC-1250, 1260	2-2
	ERC-2600, 3450 ou 4600	2-7
Receiver de HA	1U HA - ERC-1250-HA, 1260-HA	2-10, 2-11
	2U HA - ERC-2600 ou 4600-HA	2-12, 2-13



1 IPMI

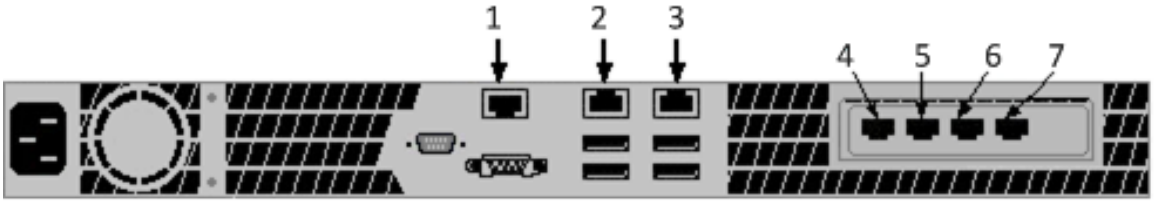
2 Ger. 2

3 Ger. 1

4 Confiável

5 Não confiável

Figura 2-1 NTP-1250



1 IPMI

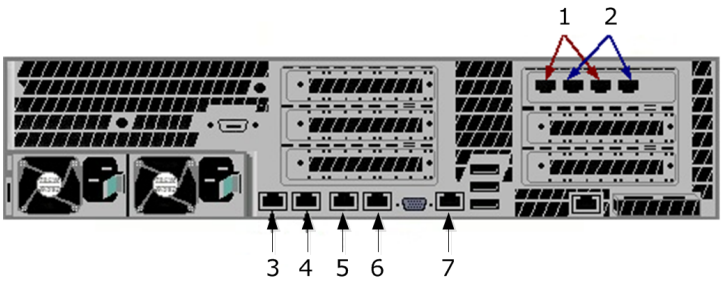
2 Ger. 2

3 Ger. 1

Em dispositivos APM-1250 e 1260, as portas de 4 a 7 são portas de coleta (sniffer), e não portas de gerenciamento.

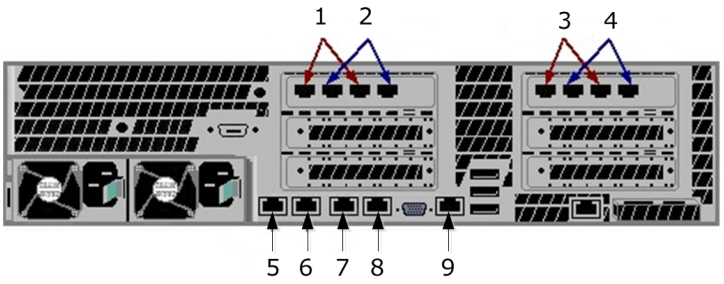
Em dispositivos ERC-1250, as portas de 4 a 7 são portas de gerenciamento adicionais.

Figura 2-2 ERC-1250, APM-1250, 1260



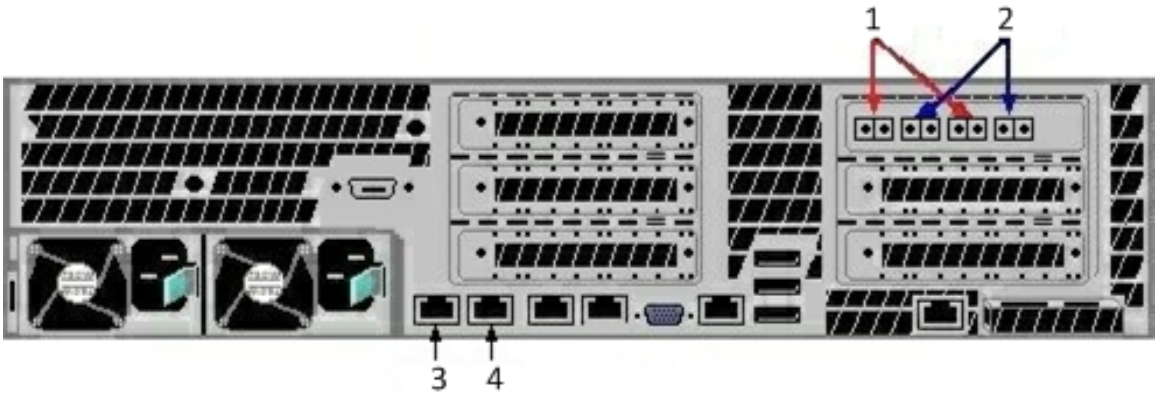
1 Confiável
2 Não confiável
3 Ger. 1
4 Ger. 2
5 Não usada
6 Não usada
7 Não usada

Figura 2-3 NTP-2600/3450-4BTX, 3460



1 Confiável
2 Não confiável
3 Confiável
4 Não confiável
5 Ger. 1
6 Ger. 2
7 Não usada
8 Não usada
9 Não usada

Figura 2-4 NTP-2600/3450-8BTX, DSM-4600

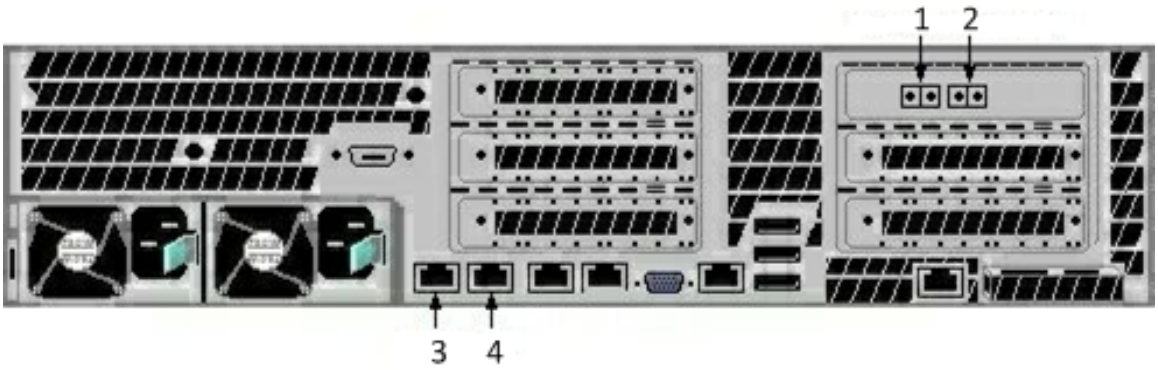


1 Confiável
2 Não confiável

3 Ger. 1

4 Ger. 2

Figura 2-5 NTP-2600/3450-4BSX



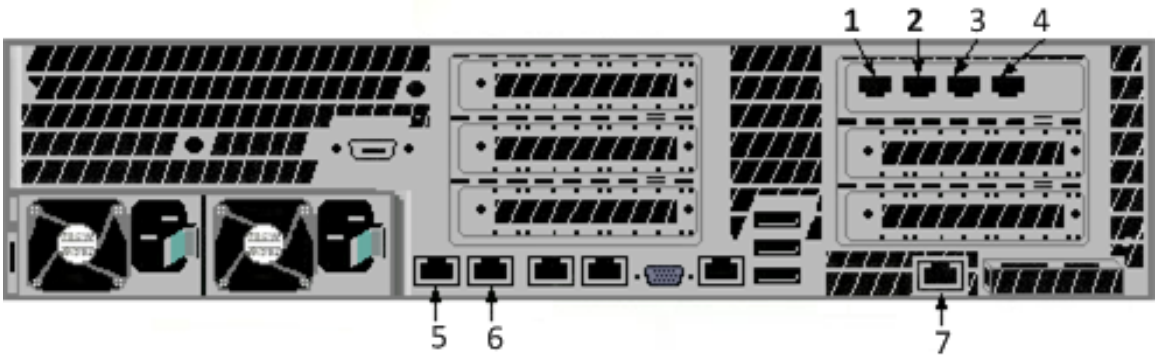
1 Confiável

2 Não confiável

3 Ger. 1

4 Ger. 2

Figura 2-6 NTP-3450-2BSX



1 NIC da IPMI

2 HB

5 Ger.

6 Dados

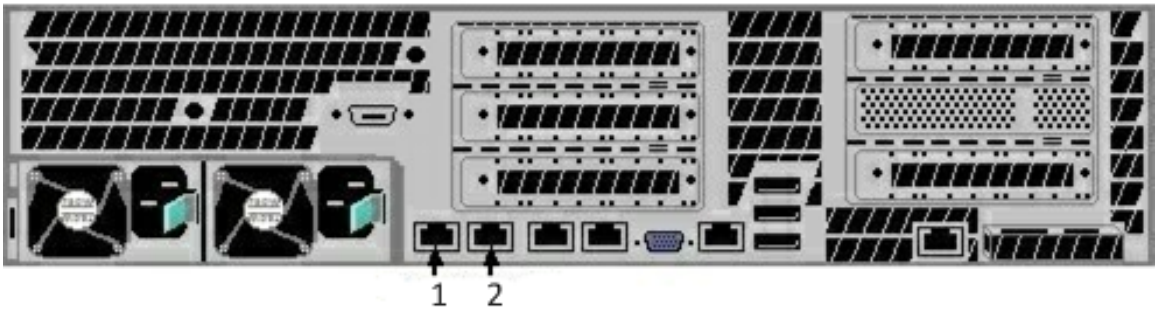
3 Ger. 2

4 Ger. 3

7 IPMI

Em dispositivos DSM-2600/3450 e APM-3450/3460, as portas de 4 a 7 são portas de coleta (sniffer), e não portas de gerenciamento.

Figura 2-7 ERC-2600/3450/4600, DSM-2600/3450 e APM-3450/3460



1 Ger. 1

2 Ger. 2

Figura 2-8 ETM-5600/6000/X4/X6, ELMERC-2600/3450/4600, ELM-4600/5600/6000, ACE-2600/3450, ENMELM-4600/5600/6000, ERU-5600

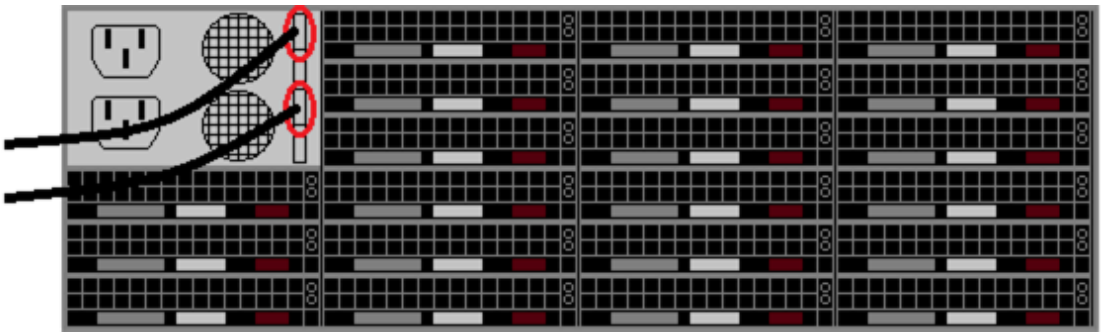
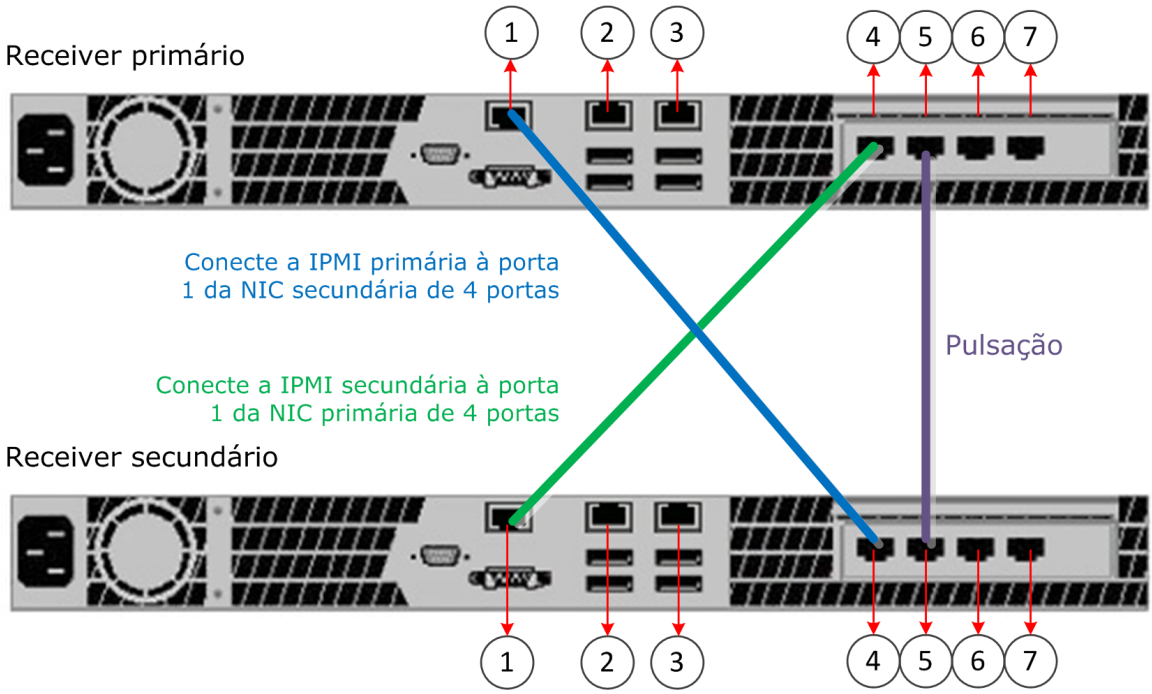
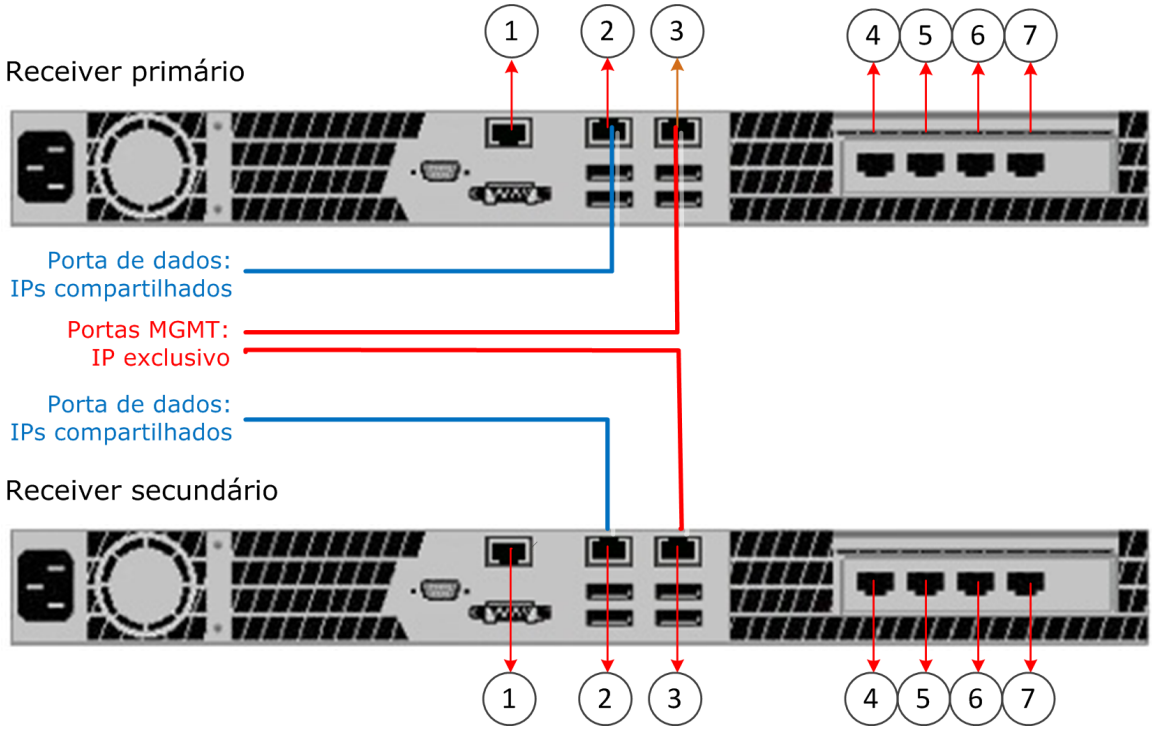


Figura 2-9 Cabos de dados DAS



1	IPMI primária	4	IPMI secundária
2	Ger. 2	5	Pulsação (HB)
3	Ger. 1	6	Ger. 3

Figura 2-10 Etapa 1: Estabelecer conexão entre Receivers de HA 1U



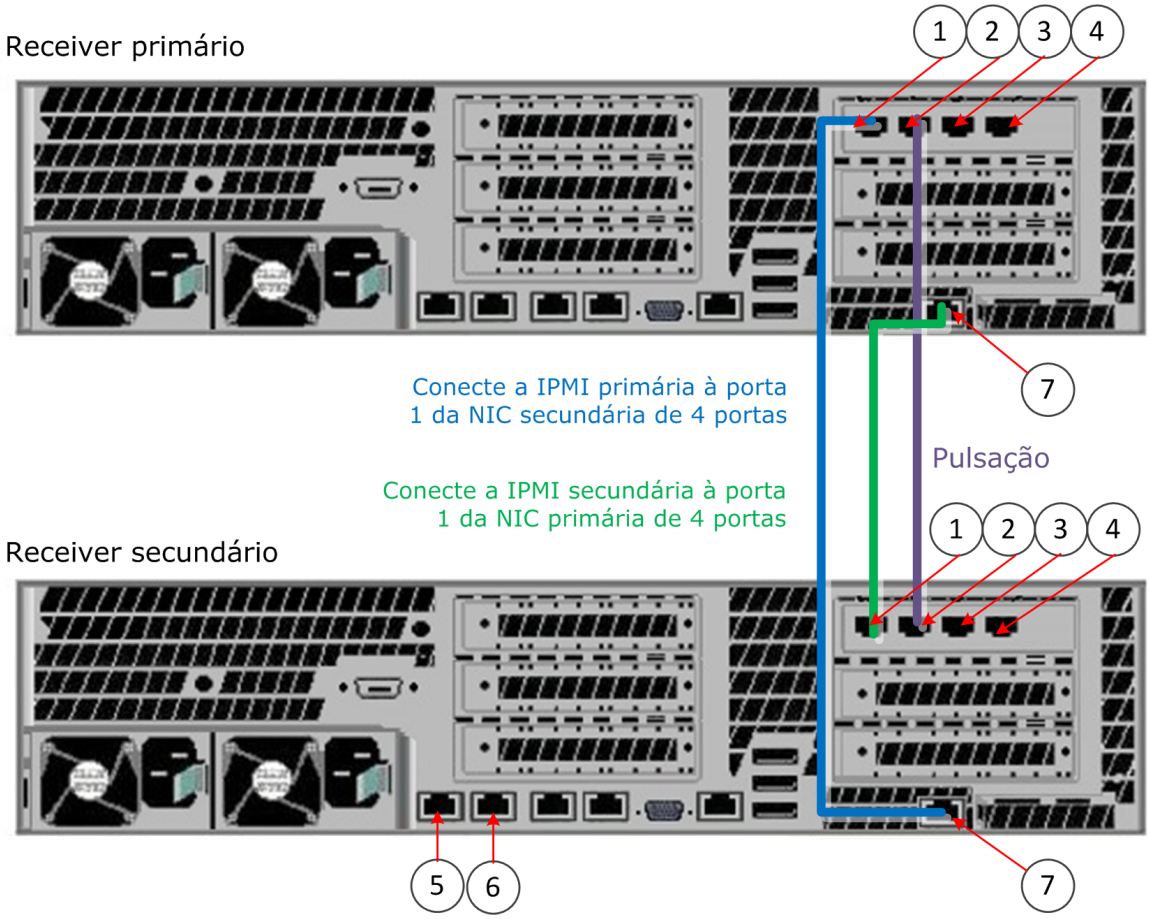
1	IPMI	5	MGMT4 (eth3)
2	MGMT2 (eth1)	6	MGMT5 (eth4)

3 MGMT1 (eth0)

4 MGMT3 (eth2)

7 MGMT6 (eth5)

Figura 2-11 Etapa 2: Conectar Receivers de HA 1U ao switch/roteador da rede



1 IPMI

2 MGMT2 (eth1)

5 MGMT4 (eth3)

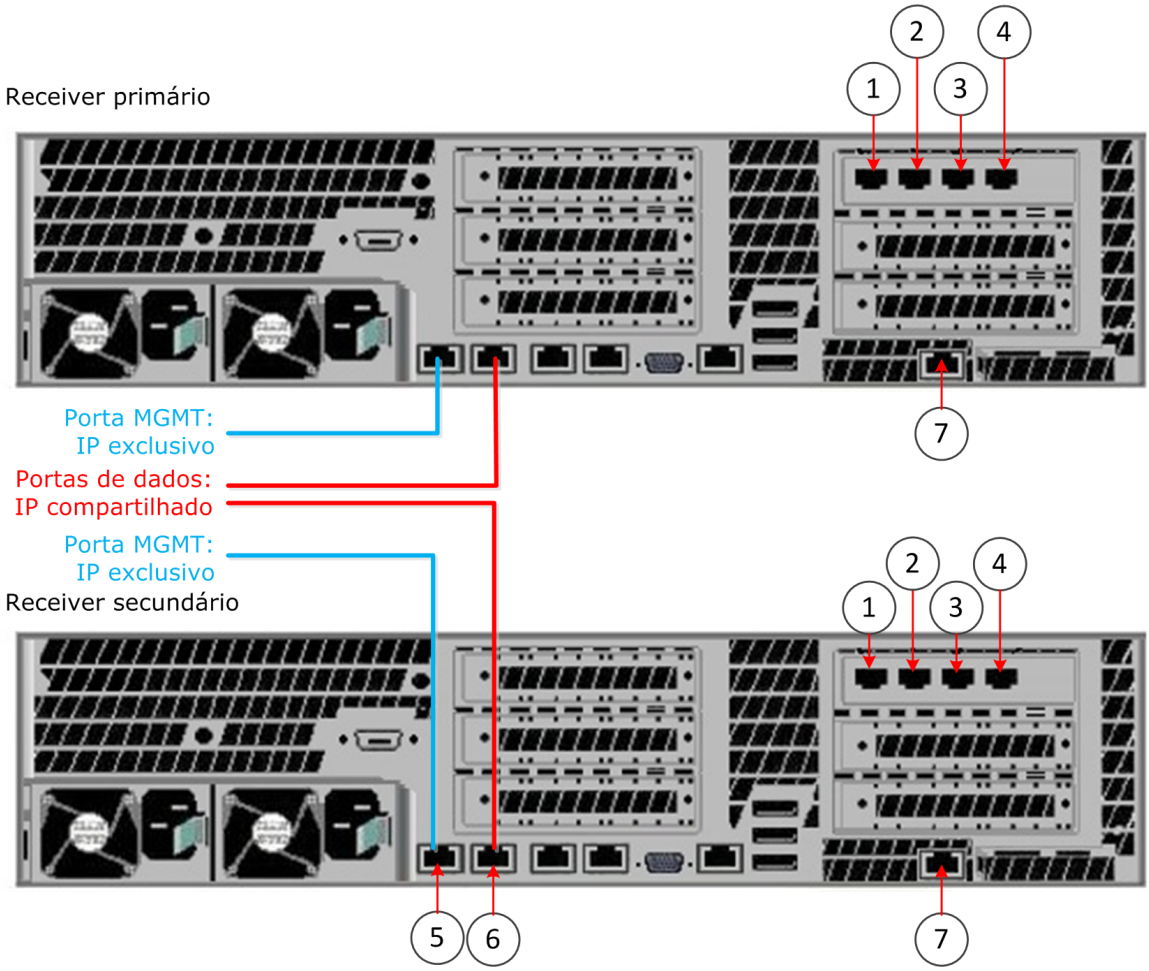
6 MGMT5 (eth4)

3 MGMT1 (eth0)

4 MGMT3 (eth2)

7 MGMT6 (eth5)

Figura 2-12 Etapa 1: Estabelecer conexão entre Receivers de HA 2U



1 IPMI

2 MGMT2 (eth1)

3 MGMT1 (eth0)

4 MGMT3 (eth2)

5 MGMT4 (eth3)

6 MGMT5 (eth4)

7 MGMT6 (eth5)

Figura 2-13 Etapa 2: Conectar Receivers de HA 2U ao switch/roteador da rede

Consulte também

Identificação de um local para instalação na página 10

3 Configuração de dispositivos do McAfee ESM

A configuração dos dispositivos é essencial para seu bom funcionamento. Para configurá-los, configure o IPv6 e a interface de rede de cada tipo de dispositivo e entre no McAfee ESM.

Conteúdo

Configurar a interface de rede no IPS do Nitro

Siga estas etapas para configurar informações de IP.

Antes de iniciar

Ative o Nitro IPS e verifique se o processo de inicialização foi concluído. Conecte um monitor e um teclado ao dispositivo.

Tarefa

1. Pressione **Alt + F1** para ir até a página LCD e pressione **Esc** duas vezes.
2. Role para baixo até **MGT IP Conf** (Conf. de IP de ger.) e pressione **Enter**.
3. Selecione **Mgt 1** (Ger. 1) e pressione **Enter**.
4. No menu **Active** (Ativo), selecione **IP Address** (Endereço IP) e pressione **Enter**.
5. Defina o valor e pressione **Enter**.
6. Role para baixo até **Netmask** (Máscara de rede) e defina o valor.
7. Role para baixo até **Done** (Concluído) e pressione **Enter**.
8. Role para baixo até **Gateway** (Gateway) e pressione **Enter**.
9. Defina o endereço do gateway, role para baixo até **Concluído** e pressione **Enter**.

10 Role para baixo até **Número da porta**, defina o valor e pressione **Enter**.

Anote o novo número da porta e insira-o quando codificar o dispositivo. Se o sistema operar no modo FIPS, não altere o número da porta de comunicação.

11 Role para baixo até **Save Changes** (Salvar alterações) e pressione **Enter**.

Configurar a interface de rede no Receptor, ELM e ACE

Siga estas etapas para configurar a interface de rede em um dispositivo Receptor, ELM ou ACE.

Antes de iniciar

Conecte um monitor e um teclado ao dispositivo.

Tarefa

1 Pressione **Alt + F1** para ter acesso à página LCD, pressione **Esc** duas vezes, role para baixo até **MGT IP Conf** e pressione **Enter**.

2 Selecione **Mgt 1** (Ger. 1) e pressione **Enter**, selecione **IP Address** (Endereço IP) e pressione **Enter**.

3 Defina o valor e pressione **Enter**.

4 Role para baixo até **Netmask** (Máscara de rede) e defina o valor.

5 Role para baixo até **Done** (Concluído) e pressione **Enter**.

6 Role para baixo até **Gateway** (Gateway) e pressione **Enter**.

7 Defina o endereço do gateway, role para baixo até **Concluído** e pressione **Enter**.

8 Role para baixo até **DNS 1**, pressione **Enter** e defina o valor.

9 Role para baixo até **Done** (Concluído) e pressione **Enter**.

10 Se estiver no modo FIPS, role para baixo até **Número da porta**, altere o valor, se necessário, e pressione **Enter**.

Anote o novo número da porta. Insira-o ao codificar o dispositivo. Não altere a porta de comunicação TCP.

11 Role para baixo até **Save Changes** (Salvar alterações) e pressione **Enter**.

Configurar a interface de rede no DEM e ADM

Siga estas etapas para configurar a interface de rede em um dispositivo DEM ou ADM.

Antes de iniciar

Conecte um monitor e um teclado ao dispositivo.

Tarefa

1 Pressione **Alt + F1** para ir até a página LCD e pressione **Esc** duas vezes.

2 Role para baixo até **MGT IP Conf** (Conf. de IP de ger.) e pressione **Enter**.

3 Selecione **Mgt 1** (Ger. 1) e pressione **Enter**.

4 No menu **Active** (Ativo), selecione **IP Address** (Endereço IP) e pressione **Enter**.

5 Defina o valor e pressione **Enter**.

6 Role para baixo até **Netmask** (Máscara de rede) e defina o valor.

7 Role para baixo até **Done** (Concluído) e pressione **Enter**.

8 Role para baixo até **Gateway** (Gateway) e pressione **Enter**.

9 Defina o endereço do gateway, role para baixo até **Concluído** e pressione **Enter**.

10 Se estiver no modo FIPS, role para baixo até **Número da porta**, altere o valor, se necessário, e pressione **Enter**.

Anote o novo número da porta e insira-o quando codificar o dispositivo. Não altere a porta de comunicação TCP.

11 Role para baixo até **Save Changes** (Salvar alterações) e pressione **Enter**.

Configurar a interface de rede no ESM

Siga estas etapas para configurar a interface de rede em um ESM.

Antes de iniciar

Ative o ESM e verifique se o processo de reinicialização foi concluído para, em seguida, conectar um monitor e um teclado ao dispositivo.

Tarefa

1 Pressione **Alt + F1** para ter acesso à página LCD, pressione **Esc** duas vezes, role para baixo até **Conf de MGT IP** e pressione **Enter**.

2 Selecione **Mgt 1** (Ger. 1) e pressione **Enter**, selecione **IP Address** (Endereço IP) e pressione **Enter**.

3 Defina o valor e pressione **Enter**.

4 Role para baixo até **Netmask** (Máscara de rede) e defina o valor.

5 Role para baixo até **Done** (Concluído) e pressione **Enter**.

6 Role para baixo até **Gateway** (Gateway) e pressione **Enter**.

7 Defina o endereço do gateway, role para baixo até **Done** (Concluído) e pressione **Enter**.

8 Role para baixo até **DNS 1**, pressione **Enter** e defina o valor.

9 Role para baixo até **Done** (Concluído) e pressione **Enter**.

10 Role para baixo até **Save Changes** (Salvar alterações) e pressione **Enter**.

Configurar para usar o IPv6

Se quiser usar o IPv6 em qualquer dispositivo e sua rede for compatível com a configuração automática sem estado do IPv6, configure o sistema para gerenciar IPv6.

Antes de iniciar

Conecte um monitor e um teclado ao dispositivo.

Para configurar manualmente um endereço para o ESM, consulte a seção *Configurações de rede* do *Guia de produto do McAfee Enterprise Security Manager*. Para configurar manualmente um endereço para cada tipo de dispositivo, consulte a seção *Interfaces* do dispositivo específico.

Tarefa

1. Pressione **Alt + F1** para ir até a página **LCD** e pressione **Esc** duas vezes.
2. Role para baixo até **IPv6 Config** (Config do IPv6) e pressione **Enter**.
3. Selecione **Mgt 1** (Ger. 1) e pressione **Enter**.
4. Role para baixo até **Save** (Salvar) e pressione **Enter**.
5. Para localizar o endereço IPv6 configurado automaticamente:
   a. Inicie o dispositivo e aguarde o carregamento do menu.
   b. Role para baixo até **MGT IP Conf** (Conf. de IP de ger.) e pressione **Enter**.
   c. Role para baixo até **IPv6 Global** e pressione **Enter**.
   d. Confirme o endereço IPv6 e pressione **Enter** para retornar ao menu.
   e. Role para baixo até **Done** (Concluído) e pressione **Enter**.
   f. Role para baixo até **Cancel Changes** (Cancelar alterações) e pressione **Enter**.

Efetuar logon no console do McAfee ESM

Depois de ter instalado e configurado o ESM e os dispositivos, você poderá efetuar logon no console para começar a definir as configurações do sistema e dos dispositivos.

Antes de iniciar

Verifique a necessidade de operar o sistema no modo FIPS (consulte a etapa 5).

Tarefa

1. Abra um navegador da Web no computador cliente e vá até o endereço IP que você definiu ao configurar a interface de rede.
2. Clique em **Entrar**, selecione o idioma para o console e digite a senha e o nome do usuário padrão.
   - Nome do usuário padrão: `NGCP`
   - Senha padrão: `security.4u`
3. Clique em **Login**, leia o **Contrato de licença do usuário final** e clique em **Aceitar**.
4. Quando solicitado, altere o nome do usuário e a senha e clique em **OK**.

5 Selecione se deseja ativar o modo FIPS.

Se houver necessidade de trabalhar no modo FIPS, ative-o ao entrar pela primeira vez para que todas as comunicações futuras com dispositivos McAfee sejam no modo FIPS. Não ative o modo FIPS se não for solicitado. Para obter mais informações sobre o FIPS, consulte *Apêndice A*.

6 Siga as instruções exibidas para obter o nome do usuário e a senha, que são necessários para o acesso às atualizações de regras.

7 Defina a configuração inicial do ESM:

a Selecione o idioma que será usado para os registros do sistema.

b Selecione o fuso horário do ESM e o formato de data a serem usados nesta conta e clique em **Avançar**.

c Defina as configurações nas cinco páginas do assistente **Configuração inicial do ESM**, clicando no ícone **Ajuda** em cada página para obter instruções.

8 Clique em **OK**.

Você está pronto para codificar e configurar os dispositivos. Consulte o *Guia de produto do McAfee Enterprise Security Manager*.

A Sobre o modo FIPS

O FIPS (Federal Information Processing Standard) consiste em padrões públicos desenvolvidos pelo governo federal dos Estados Unidos. Caso seja necessário atender a essas normas, você deverá operar o sistema no modo FIPS.

O modo FIPS deve ser selecionado na primeira vez que você efetuar logon no sistema e não poderá ser alterado posteriormente.

Conteúdo

Informações sobre o modo FIPS

Em virtude das normas FIPS, alguns recursos do ESM não estão disponíveis, alguns recursos disponíveis estão fora de conformidade e outros estão disponíveis somente durante o modo FIPS. Esses recursos são observados em todo o documento e estão listados aqui.

Status do recurso	Descrição
Recursos removidos	• Receivers de alta disponibilidade. • Terminal GUI. • Capacidade de se comunicar com o dispositivo usando o protocolo SSH. • No console do dispositivo, o shell principal é substituído por um menu de gerenciamento de dispositivo.
Recursos disponíveis somente no modo FIPS	• Há quatro funções de usuário que não se sobrepõem: **Usuário**, **Usuário avançado**, **Auditoria de admin** e **Admin de chave e certificado**. • Todas as páginas de **Propriedades** têm uma opção de **Autoteste** que permite verificar se o sistema está funcionando corretamente no modo FIPS. • Se houver falha de FIPS, será adicionado um sinalizador de status à árvore de navegação de sistemas para refletir a falha. • Todas as páginas de **Propriedades** têm a opção **Exibir** que, quando é clicada, abre a página **Token de identidade FIPS**. Ela exibe um valor que precisa ser comparado ao valor mostrado naquelas seções do documento, para garantir que o FIPS não foi comprometido. • Em **Propriedades do sistema** | **Usuários e Grupos** | **Privilégios** | **Editar grupo**, a página inclui o privilégio **Autoteste de criptografia do FIPS** que concede aos membros do grupo a autorização para executar autotestes do FIPS. • Quando você clica em **Importar chave** ou **Exportar chave** em **Propriedades de IPS** | **Gerenciamento de chaves**, é exibido um prompt para selecionar o tipo de chave que você deseja importar ou exportar. • Em **Assistente para Adicionar dispositivo**, o protocolo TCP é sempre definido como Porta 22. A porta SSH pode ser alterada.

Selecione o modo FIPS

Ao efetuar logon pela primeira vez no sistema, você precisa indicar se deseja que o sistema opere no modo FIPS. Depois que essa seleção for feita, não será possível alterá-la.

Tarefa

Para obter definições de opções, clique em **?** na interface.

1 A primeira vez que você entra no ESM:

   a No campo **Nome do usuário**, digite `NGCP`.

   b No campo **Senha**, digite `security.4u`.

   Você será solicitado a alterar sua senha.

2 Insira e confirme a nova senha.

3 Na página **Ativar FIPS**, clique em **Sim**.

O aviso **Ativar FIPS** exibe informações de solicitação de confirmação se você deseja que o sistema opere no modo FIPS permanentemente.

4 Clique em **Sim** para confirmar sua seleção.

Verificar integridade FIPS

Se você estiver operando no modo FIPS, o FIPS 140-2 exige que o teste de integridade do software seja executado regularmente. Esse teste deve ser executado no sistema e em cada dispositivo.

Tarefa

Para obter definições de opções, clique em **?** na interface.

1 Na árvore de navegação do sistema, selecione **Propriedades do sistema** e verifique se a opção **Informações do sistema** está selecionada.

2 Execute uma das ações a seguir.

No campo...	Faça isto...
Status do FIPS	Exiba os resultados dos autotestes de FIPS mais recentes executados no ESM.
Teste ou **Autoteste de FIPS**	Execute os autotestes de FIPS, que testam a integridade dos algoritmos usados no cripto-executável. Os resultados podem ser exibidos no **Registro de mensagens**. Se o autoteste de FIPS falhar, o FIPS for comprometido ou ocorrer falha no dispositivo. Entre em contato com o Suporte da McAfee.
Exibir ou **Identidade FIPS**	Abra a página **Token de identidade FIPS** para executar o teste de integridade do software de inicialização. Compare o valor abaixo com a chave pública que aparece nesta página: -----BEGIN PUBLIC KEY----- MIICIjANBgkqhkiG9w0BAQEFAAOCAg8AMIICCgKCAgEAt8FWOP2mvVjvTTxkhGqk LdgA+sx0jBv+zYnCkGYOHHzNAdum9yuMn69GNbYXm7I5OcKv2+nz6axBruCZ5XX1 jCGWnmsj8YZJoNp/FLUy1jYE7lXI5/NRm2uhjhzjdOjgFv10SkgxVfL/aBJjqZFJ KKbHMzYEBwdyseQUc56u3mKaBtP4rydfRmEtytkuOsZgQuPHKYhaQJlnbV5LfrLa o6HQSlzHYHlcF/Yog+QHJ6ClSRA1lk8MPyFG9RHdKnwcq3sY8QjQMbIZ5SDobbK0 GPOOucG8vWDWdxSiabJLBdklVsmB0zwdH6lOCkkGTidayMk12hDh+2BA6el7YQBV 8EJaJ5wvz8aQKwDfiinlb9vmC+sk+Rwo/E7uRn3El4+RxouHi9J3f92I9qXZeJCV iYV2XahhyxSpq8ro/j0BMTiab3dIjjogxMxCI9QjEpm3J/ZyUpWtNKaHq8BgSE1e daiJob7O/kvef1T/ZOb3O90bSK3vtn+3Si3K3cpaY/qBm9var6xVNyGhHztRJv0F 0nSJlyddWuXL1U+hMTO2YE33T3s4Uf4jiomTVSDTJ087hLT5l/hCz6A33Hzl7gk8 Q89SNsmL/p0RAJzJ3+mGyoUAd1D2u6sYq6NkGCn640a5A2zAOQdX/M8R8S+NKjgi nLg3n+/+25KsCB3KDY3AkYECAwEAAQ== -----END PUBLIC KEY----- Se este valor não corresponder ao da chave pública, o FIPS está comprometido. Entre em contato com o Suporte da McAfee.

Adicionar um dispositivo codificado ao modo FIPS

Há dois métodos no modo FIPS para adicionar um dispositivo que já tenha sido codificado a um ESM. Essa terminologia e as extensões de arquivo são úteis durante esses processos.

Terminologia

- **Chave de dispositivo** — Contém os direitos de gerenciamento que um ESM tem para um dispositivo e não é usada para criptografia.
- **Chave pública** — A chave de comunicação SSH pública do ESM, que é armazenada na tabela de chaves autorizadas de um dispositivo.
- **Chave privada** — A chave de comunicação SSH privada do ESM, que é usada pelo executável de SSH em um ESM para estabelecer a conexão SSH com um dispositivo.
- **ESM primário** — O ESM que foi originalmente usado para registrar o dispositivo.
- **ESM secundário** — O ESM adicional que se comunica com o dispositivo.

Extensões de arquivo para arquivos de exportação diferentes

- **.exk** — Contém a chave do dispositivo.
- **.puk** — Contém a chave pública.
- **.prk** — Contém a chave privada e a chave do dispositivo.

Backup e restauração das informações de um dispositivo no modo FIPS

Esse método é usado para fazer backup e restaurar informações de comunicação de um dispositivo no ESM.

Seu uso principal é em caso de falha que exija a substituição do ESM. Se as informações de comunicação não forem exportadas antes da falha, a comunicação com o dispositivo não poderá ser restabelecida. Esse método exporta e importa o arquivo .prk.

A chave privada do ESM primário é usada pelo ESM secundário para estabelecer comunicação com o dispositivo inicialmente. Quando a comunicação é estabelecida, o ESM secundário copia sua chave pública para a tabela de chaves autorizadas do dispositivo. Em seguida, o ESM apaga a chave privada do ESM primário e inicia a comunicação com seu próprio par de chaves públicas ou privadas.

Ação	Etapas
Exportar o arquivo .prk do ESM primário	1 Na árvore de navegação do ESM primário, selecione o dispositivo com as informações de comunicação que deseja fazer backup e clique no ícone de **Propriedades**. 2 Selecione **Gerenciamento de chaves** e clique em **Exportar chave**. 3 Selecione **Backup da chave SSH privada** e clique em **Avançar**. 4 Digite e confirme uma senha e defina a data de expiração. Após a data de expiração, a pessoa que importa a chave não conseguirá comunicar-se com o dispositivo até que outra chave seja exportada com uma data de expiração futura. Se você selecionar **Nunca expira**, a chave nunca expirará se for importada para outro ESM. 5 Clique em **OK**, selecione o local onde deseja salvar o arquivo .prk criado pelo ESM e saia do ESM primário.
Adicionar um dispositivo ao ESM secundário e importar o arquivo .prk	1 Na árvore de navegação do sistema do dispositivo secundário, selecione o nó de nível do sistema ou grupo ao qual deseja adicionar o dispositivo. 2 Na barra de ferramentas de ações, clique em **Adicionar dispositivo**. 3 Selecione o tipo de dispositivo que você deseja adicionar e clique em **Avançar**. 4 Insira um nome para o dispositivo que seja exclusivo no grupo e clique em **Avançar**. 5 Insira o endereço IP de destino do dispositivo, insira a porta de comunicação do FIPS e clique em **Avançar**. 6 Clique em **Importar chave**, navegue até o arquivo .prk exportado anteriormente e clique em **Fazer upload**. Digite a senha especificada quando essa senha foi exportada inicialmente. 7 Faça logoff do ESM secundário.

Ativar a comunicação com vários dispositivos ESM no modo FIPS

Você pode permitir que vários ESMs se comuniquem com o mesmo dispositivo exportando e importando arquivos .puk e .exk.

Esse método usa dois processos de exportação e importação. Primeiro, o ESM primário é usado para importar o arquivo .puk exportado do dispositivo ESM secundário e enviar a chave pública contida no ESM secundário para o dispositivo, permitindo que os dois dispositivos ESM se comuniquem com o dispositivo. Segundo, o arquivo .exk do dispositivo é exportado do ESM primário e importado para o ESM secundário, concedendo ao ESM secundário a capacidade de se comunicar com o dispositivo.

Ação	Etapas
Exportar o arquivo .puk do ESM secundário	1 Na página **Propriedades do sistema** do ESM secundário, selecione **Gerenciamento de ESM**. 2 Clique em **Exportar SSH** e selecione o local onde o arquivo .puk deverá ser salvo. 3 Clique em **Salvar** e saia.
Importar o arquivo .puk para o ESM primário	1 Na árvore de navegação do sistema do ESM primário, selecione o dispositivo que deseja configurar. 2 Clique no ícone **Propriedades** e selecione **Gerenciamento de chaves**. 3 Clique em **Gerenciar chaves SSH**. 4 Clique em **Importar**, selecione o arquivo .puk e clique em **Fazer upload**. 5 Clique em **OK** e faça logoff do ESM primário.
Exportar o arquivo .exk do dispositivo do ESM primário	1 Na árvore de navegação do sistema do ESM primário, selecione o dispositivo que deseja configurar. 2 Clique no ícone **Propriedades** e selecione **Gerenciamento de chaves**. 3 Clique em **Exportar chave**, selecione a chave do dispositivo de backup e clique em **Avançar**. 4 Digite e confirme uma senha e defina a data de expiração. Após a data de expiração, a pessoa que importa a chave não conseguirá comunicar-se com o dispositivo até que outra chave seja exportada com uma data de expiração futura. Se você selecionar **Nunca expira**, a chave nunca expirará se for importada para outro ESM. 5 Selecione os privilégios do arquivo .exk e clique em **OK**. 6 Selecione o local onde esse arquivo deverá ser salvo e faça logoff do ESM primário.
Importar o arquivo .exk para o ESM secundário	1 Na árvore de navegação de sistemas do dispositivo secundário, selecione o nó no nível de sistema ou de grupo ao qual você deseja adicionar o dispositivo. 2 Na barra de ferramentas de ações, clique em **Adicionar dispositivo**. 3 Selecione o tipo de dispositivo que deseja adicionar e clique em **Avançar**. 4 Insira um nome para o dispositivo que seja exclusivo a esse grupo e clique em **Avançar**. 5 Clique em **Importar chave** e procure o arquivo .exk. 6 Clique em **Fazer upload** e insira a senha que foi especificada quando essa chave foi inicialmente exportada. 7 Faça logoff do ESM secundário.

Solução de problemas do modo FIPS

Podem surgir problemas durante a operação do ESM no modo FIPS.

Problema	Descrição e resolução
Não é possível comunicar-se com o ESM	• Verifique o LCD na parte frontal do dispositivo. Se ele informar **Falha de FIPS**, entre em contato com o Suporte da McAfee. • Verifique se há uma condição de erro na interface HTTP exibindo a página da Web de autoteste de FIPS do ESM em um navegador. Se um único dígito **0** for exibido, indicando que o dispositivo falhou em um autoteste de FIPS, reinicialize o dispositivo ESM e tente corrigir o problema. Se a condição de falha persistir, entre em contato com o Suporte para obter mais instruções. - Se um único dígito **1** for exibido, o problema de comunicação não está relacionado à falha de FIPS. Entre em contato com o suporte para obter mais etapas de solução de problemas.
Não é possível comunicar-se com o dispositivo	• Se houver um sinalizador de status ao lado do nó do dispositivo na árvore de navegação do sistema, coloque o cursor sobre ele. Se ele informar **Falha de FIPS**, entre em contato com o Suporte da McAfee no portal de suporte. • Siga a descrição sob o problema *Não é possível comunicar-se com o ESM*.
Erro **O arquivo é inválido** ao adicionar um dispositivo	Não é possível exportar uma chave de um dispositivo não FIPS e importá-la para um dispositivo que estiver operando no modo FIPS. Além disso, não é possível exportar uma chave de um dispositivo FIPS e importá-la para um dispositivo não FIPS. Esse erro aparece na tentativa dos dois cenários.

B Requisitos do VM ESXi

A VM deve atender aos requisitos mínimos a seguir.

- Processador: 8 núcleos ou mais, dependendo do modelo, 64 bits, Dual Core2/Nehalem ou superior ou AMD Dual Athlon64/Dual Opteron64 ou posterior
- RAM: Depende do modelo (4 GB ou mais)
- Disco: Depende do modelo (250 GB ou mais)
- ESXI: 5.0 ou posterior

Você pode selecionar os requisitos de disco rígido necessários para o servidor. Mas o requisito de VM depende do modelo do dispositivo (250 GB ou mais). Caso não haja pelo menos 250 GB disponíveis, será exibida uma mensagem de erro quando a VM for distribuída.

A VM usa muitos recursos que requerem o uso de CPU e RAM. Se o ambiente do ESXi compartilhar os requisitos de CPU ou RAM com outras VMs, o desempenho da VM será afetado. Planeje as necessidades de CPU e RAM de acordo com os requisitos aqui descritos.

A McAfee recomenda definir a opção de configuração como **Ampla**.

Conteúdo

Modelos de VM

Essa tabela lista os modelos de VM disponíveis, quantos eventos cada modelo pode processar por segundo (EPS), o armazenamento mecânico recomendado, a capacidade de armazenamento do SSD (unidade de estado sólido) e os requisitos da plataforma que executa a VM.

Número do modelo	Capacidade de EPS	Armazenamento mecânico	SSD	Requisitos da plataforma
ELU4 ELU12	1.000 5.000	Ambiente de VM recomendado de 250 GB VM recomendada Ambiente de no mínimo 500 GB	Nenhum No mínimo 240 GB	VMware ESX/ESXi Server v. 5.x+, 8 núcleos de processador (Processador Intel® Xeon® E5 ou E7), 4 GB de memória VMware ESX/ESXi Server v. 5.x+, 12 núcleos de processador (Processador Intel® Xeon® E5 ou E7), 64 GB de memória
ENU4 ENU12 ENU32	1.500* 40.000* 85.000*	Ambiente de VM recomendado de 250 GB Ambiente de VM recomendado de no mínimo 500 GB Ambiente de VM recomendado de no mínimo 2 TB	Nenhum No mínimo 480 GB No mínimo 3 TB	VMware ESX/ESXi Server v. 5.x+, 8 núcleos de processador (Processador Intel® Xeon® E5 ou E7), 4 GB de memória VMware ESX/ESXi Server v. 5.x+, 12 núcleos de processador (Processador Intel® Xeon® E5 ou E7), 64 GB de memória VMware ESX/ESXi Server v. 5.x+, 32 núcleos de processador (Processador Intel® Xeon® E5 ou E7), 96 GB de memória
ELM4 ELM12 ELM32	1.500* 30.000* 70.000*	Ambiente de VM recomendado de 250 GB Ambiente de VM recomendado de no mínimo 500 GB Ambiente de VM recomendado de no mínimo 2 TB	Nenhum No mínimo 480 GB No mínimo 3 TB	VMware ESX/ESXi Server v. 5.x+, 8 núcleos de processador (Processador Intel® Xeon® E5 ou E7), 4 GB de memória VMware ESX/ESXi Server v. 5.x+, 12 núcleos de processador (Processador Intel® Xeon® E5 ou E7), 64 GB de memória VMware ESX/ESXi Server v. 5.x+, 32 núcleos de processador (Processador Intel® Xeon® E5 ou E7), 96 GB de memória

Número do modelo	Capacidade de EPS	Armazenamento mecânico	SSD	Requisitos da plataforma
EV2 EV5 EV10	500 5.000 15.000	Ambiente de VM recomendado de 250 GB Ambiente de VM recomendado de no mínimo 500 GB Ambiente de VM recomendado de no mínimo 2 TB	Nenhum No mínimo 480 GB No mínimo 3 TB	VMware ESX/ESXi Server v. 5.x+, 8 núcleos de processador (Processador Intel® Xeon® E5 ou E7), 4 GB de memória VMware ESX/ESXi Server v. 5.x+, 12 núcleos de processador (Processador Intel® Xeon® E5 ou E7), 64 GB de memória VMware ESX/ESXi Server v. 5.x+, 32 núcleos de processador (Processador Intel® Xeon® E5 ou E7), 96 GB de memória
ELMERCVM4 ELMERCVM12	1.500 5.000	Ambiente de VM recomendado de 250 GB Ambiente de VM recomendado de no mínimo 500 GB	Nenhum No mínimo 240 GB	VMware ESX/ESXi Server v. 5.x+, 8 núcleos de processador (Processador Intel® Xeon® E5 ou E7), 4 GB de memória VMware ESX/ESXi Server v. 5.x+, 12 núcleos de processador (Processador Intel® Xeon® E5 ou E7), 64 GB de memória
ACV12 ACV32	< 30.000* < 80.000*	Ambiente de VM recomendado de 250 GB Ambiente de VM recomendado de no mínimo 500 GB	No mínimo 480 GB No mínimo 3 TB	VMware ESX/ESXi Server v. 5.x+, 12 núcleos de processador (Processador Intel® Xeon® E5 ou E7), 64 GB de memória VMware ESX/ESXi Server v. 5.x+, 32 núcleos de processador (Processador Intel® Xeon® E5 ou E7), 96 GB de memória
APM4 APM12	250 Mbps 500 Mbps	Ambiente de VM recomendado de 250 GB Ambiente de VM recomendado de no mínimo 500 GB	Nenhum No mínimo 480 GB	VMware ESX/ESXi Server v. 5.x+, 8 núcleos de processador (Processador Intel® Xeon® E5 ou E7), 4 GB de memória VMware ESX/ESXi Server v. 5.x+, 12 núcleos de processador (Processador Intel® Xeon® E5 ou E7), 64 GB de memória

Dividir a unidade de armazenamento

Se o modelo for de mais de 250 GB, e você precisar usar a configuração **256 MB a 2 MB**, será necessário dividir a unidade de armazenamento da máquina virtual.

Tarefa

1 Selecione o servidor ESX, clique na guia **Configuração** e em **Armazenamento** na seção **Hardware**.

A VM usa muitos recursos que requerem o uso de CPU e RAM. Se o ambiente do ESXi compartilhar os requisitos de CPU/RAM com outras VMs, o desempenho da VM será afetado. Planeje as necessidades de CPU e RAM de acordo com os requisitos.

2 Clique em **Adicionar armazenamento** e selecione **Disco/LUN**.

3 Selecione um disco disponível e a opção correta do seu espaço em disco disponível. **Usar "espaço livre"** para uma unidade existente ou **Usar todas as partições disponíveis** para uma unidade disponível.

Você pode selecionar os requisitos de disco rígido para o servidor, mas o requisito para a VM é de 500 GB. Caso não haja 500 GB disponíveis, será exibida uma mensagem de erro quando a VM for distribuída. A McAfee recomenda definir a configuração como **Ampla**.

4 Nomeie a unidade de armazenamento e selecione **512 GB, tamanho de bloco: 2 MB** na lista suspensa **Tamanho máximo de arquivo** para garantir que haja 500 GB de espaço disponível na unidade.

Instalar a máquina virtual

Depois que você instalar e codificar uma VM, o funcionamento será igual ao do ESM.

Antes de iniciar

Verifique se o equipamento atende aos requisitos mínimos.

Tarefa

1 Acesse a raiz da unidade de CD (para instalação com CD) ou faça download dos arquivos fornecidos pelo Suporte da McAfee no computador local.

2 No **vSphere Client**, clique no endereço IP do servidor na árvore de dispositivos.

3 Clique em **File** (Arquivo) e selecione **Deploy OVF Template** (Distribuir modelo OVF).

4 Designe o nome, a pasta para instalação da VM, a definição da configuração de disco e a opção **VM Networking** (Rede VM).

5 Distribua os arquivos no servidor ESXi, selecione a VM e verifique estas definições na configuração **Edit Virtual Machine** (Editar máquina virtual).

6 Selecione as configurações de rede corretas para os switches/adaptadores de sua rede ESXi e clique em **Reproduzir** para inicializar a VM.

7 Usando o menu VM, defina o IP de MGT1, a máscara de rede, o gateway e os endereços DNS, e pressione **Esc** para ativar o menu.

8 Configure a interface de rede na VM, salve as alterações antes de sair da janela **Menu** e codifique o dispositivo.

Configurar a máquina virtual

Depois de instalar a VM, configure a interface de rede.

Tarefa

1 Clique em **Esc**, role para baixo até **Conf. de IP de ger.** no LCD e clique em **Enter** duas vezes.

2 Defina o endereço IP usando as setas para alterar o valor do dígito atual e alternar entre os dígitos, e clique em **Enter**.

3 Role até **Netmask** (Máscara de rede) e defina-a usando as setas.

4 Role até **Concluído** e clique em **Enter**. Role até **Gateway** e clique em **Enter**.

5 Defina o endereço do gateway usando as setas, role para baixo até **Concluído** e clique em **Enter**.

6 Role para baixo até **DNS1**, clique em **Enter** e selecione o endereço do servidor DNS usando as setas.

7 Role para baixo até **Concluído** e pressione **Enter**.

8 Para alterar a porta de comunicação quando o sistema estiver no modo FIPS (consulte *Sobre o modo FIPS*), pressione a seta para baixo duas vezes e clique em **Enter**.

Não altere a porta de comunicação TCP.

9 Altere o número da porta e pressione **Enter**.

Anote o novo número da porta. Insira-o ao codificar o dispositivo.

10 Role até **Salvar alterações** e clique em **Enter**.

Codificar o dispositivo VM

Codifique o dispositivo para estabelecer um vínculo entre ele e o ESM.

Antes de iniciar

Conecte o dispositivo fisicamente à rede (consulte *Instalação de dispositivos McAfee ESM*).

Tarefa

Para obter definições de opções, clique em **?** na interface.

1 Na árvore de navegação do sistema, clique no sistema ou grupo e no ícone **Adicionar dispositivo** no painel de ações.

2 Insira as informações solicitadas em cada página do **Assistente Adicionar dispositivo** (consulte *Adicionar dispositivos ao console do ESM* no *Guia de produto do McAfee Enterprise Security Manager*).

C

Instalação dos adaptadores qLogic 2460 ou 2562 SAN

O qLogic QLE2460 é um adaptador Fibre Channel PCIe x4 único, com velocidade de 4 GB. O QLE2562 é um adaptador Fiber Channel PCIe x8 único, com velocidade de 8 GB. Eles podem se conectar diretamente ao dispositivo SAN ou por meio de um switch SAN.

Antes de iniciar

- Verifique se o dispositivo SAN ou o switch SAN usados para a conexão se comunicam automaticamente.
- Verifique se o administrador de SAN aloca e cria espaço no SAN, atribuindo-o ao canal em que o adaptador qLogic está conectado. Use o nome WWPN do adaptador. O WWPN se localiza na placa do adaptador, na embalagem antiestática e na caixa.

Tarefa

1 Desligue o dispositivo em que estiver instalando o adaptador SAN.

2 Insira o adaptador, retorne o dispositivo ao rack e conecte os cabos.

No caso de um dispositivo 3U, insira o adaptador no slot mais próximo à tampa protetora da memória.

A mensagem de inicialização de BIOS do adaptador informa que o adaptador foi instalado e está em funcionamento. Se essa mensagem não for exibida ou se o cartão não emitir uma luz vermelha, amarela ou verde, ele não foi reconhecido. Se for esse o caso, verifique se o cartão está posicionado corretamente ou insira-o em outro slot PCI.

3 Inicie o dispositivo.

O ambiente operacional o detectará e carregará o driver QLAXXX. A mensagem de **Mounting Storage Facilities** (Montagem de recursos de armazenamento) exibe **OK**, e a inicialização continua.

4 Usando o console do ESM, codifique o dispositivo.

Quando o dispositivo estiver codificado, a página **Propriedades** incluirá a opção **Volumes SAN**.

D Instalação do DAS

O DAS é um dispositivo complementar ao ESM ou ELM das séries 4xxx/5xxx/6xxx.

A unidade DAS é enviada com um chassi e um cartão LSI 9280-8e RAID para:

- ETM-5205
- ETM-5510
- ETM-5600
- ETM-5750
- ETM-6000
- ETM-X3
- ETM-X4
- ETM-X5
- ETM-X6
- ESMREC-5205
- ESMREC-5510
- ENMELM-4600
- ENMELM-5205
- ENMELM-5510
- ENMELM-5600
- ENMELM-6000
- ELM-4600
- ELM-5205
- ELM-5510
- ELM-5600
- ELM-5750
- ELM-6000

Tarefa

1. Desligue o ESM seguindo o procedimento normal de encerramento.
2. Efetue pull no dispositivo do rack e abra a tampa superior. Talvez seja necessário remover um pequeno parafuso na parte frontal ou traseira da tampa).
3. Instale o cartão LSI 9280-8e RAID no slot 4 do ESM.
   - Nos dispositivos de face laranja, se o cartão Areca ou 3Ware RAID estiver no slot 4, mova o cartão RAID para o slot 6. Se o dispositivo McAfee ESM tiver um cartão Areca ou 3Ware RAID e também um cartão SSD instalados, instale o cartão LSI 9280-8e RAID no slot 5.
   - Nos dispositivos com face preta, instale o cartão em um slot aberto.
4. Substitua a parte superior no McAfee ESM e reinsira no rack.
5. Insira os conectores de cabo nos slots 1 e 2 dos slots externos do cartão LSI 9280-8e RAID. O cabo é encaixado.
6. Verifique se todas as unidades estão inseridas no DAS, acople-as aos trilhos internos do dispositivo DAS e insira o dispositivo no rack.
7. Insira os cabos de dados no primeiro e no terceiro slot na parte traseira do dispositivo DAS. Os cabos se encaixarão no lugar.

8 Insira os cabos elétricos e ligue o dispositivo DAS.

9

Uma luz de teste acenderá para todas as unidades. A unidade que apresentar a luz vermelha é a unidade "sobressalente" do DAS.

10 Ligue o dispositivo McAfee ESM e procure o utilitário BIOS do cartão LSI 9280-8e RAID.

O dispositivo DAS é previamente formatado e não requer a configuração de um conjunto RAID no dispositivo. Se a mensagem **RAID ausente** for exibida, ligue para o Suporte da McAfee para criar o RAID.

11 Entre e execute um comando `df -h` para verificar se você possui uma unidade /das1_hd.

Em **Propriedades do sistema** do console do ESM, o campo **Hardware** da guia **Informações do sistema** reflete o tamanho ampliado do disco rígido denominado /data_hd.

E

Instalação de dispositivos em um rack

É recomendável a instalação em um rack, para proteger os dispositivos e os cabos de danos acidentais ou desconexões.

Conteúdo

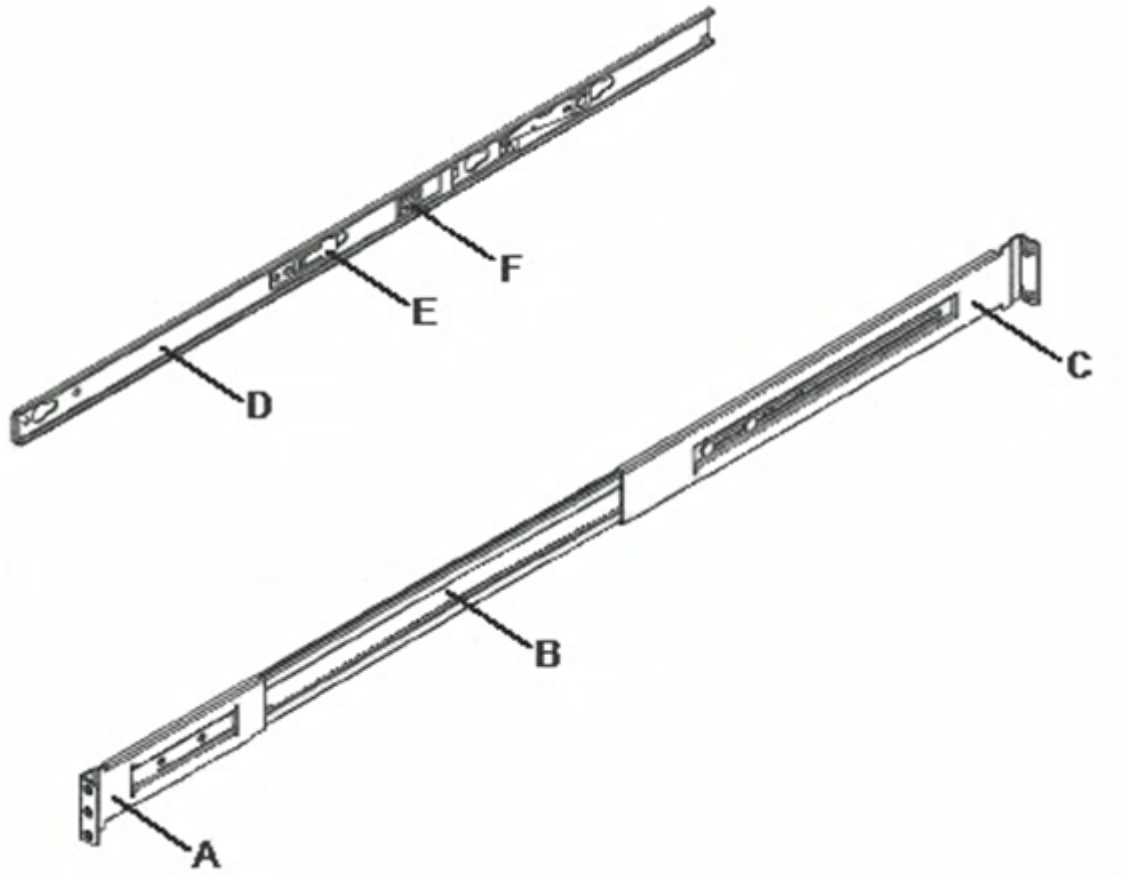
Instalar o conjunto de trilhos AXXVRAIL

Um conjunto de trilhos AXXVRAIL é enviado junto com cada dispositivo para instalação em rack.

Tarefa

1 Instale os trilhos no rack.

a Puxe o botão de destravamento (F) para remover a parte interna (D) das partes corrediças.



Componentes

A: suporte frontal

B: parte externa

C: suporte traseiro

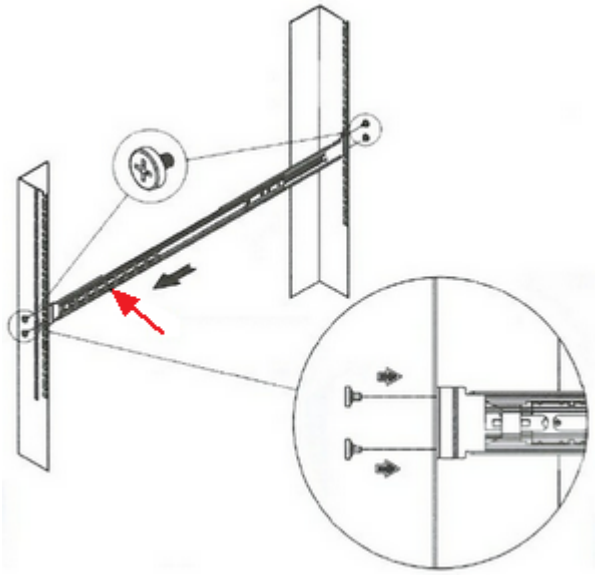
D: parte interna

E: trava de segurança

F: botão de destravamento

b Alinhe os suportes na posição vertical desejada no rack e insira os parafusos.

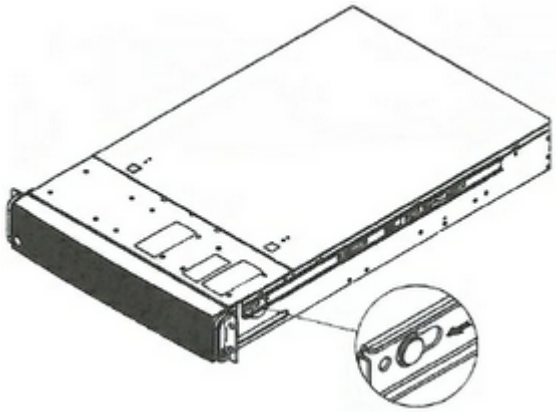
c Mova a esfera retentora para a frente das partes corrediças.



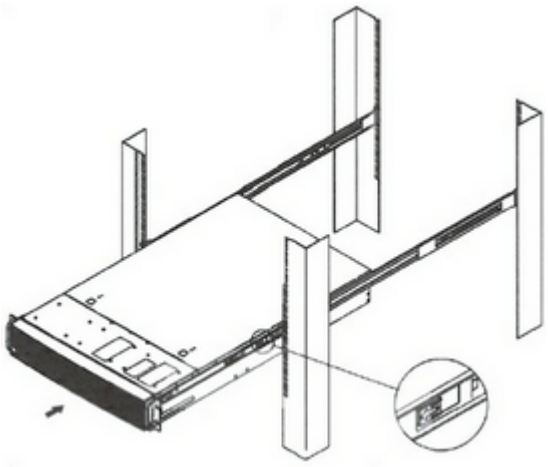
2 Instale o chassi.

a Alinhe os orifícios da parte interior aos bloqueadores do chassi.

b Mova a parte interior na direção indicada na imagem a seguir.



c Instale o chassi nas partes corrediças, puxando o botão de destravamento na parte interior para liberar e permitir o fechamento do chassi.



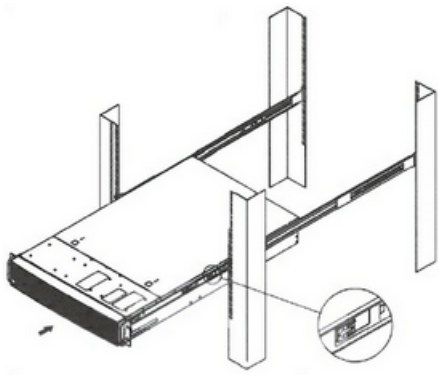
Remover o chassi

É possível remover o chassi dos trilhos.

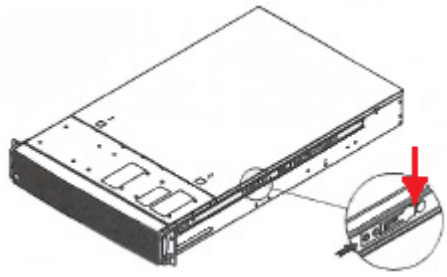
Tarefa

1 Estenda as partes corrediças até que elas travem.

2 Puxe o botão de destravamento para liberar a trava e desconectar a parte interna das partes corrediças.



3 Pressione a trava de segurança para liberar a parte interna do chassi.



F

Avisos regulamentares

Estas informações regulamentares se aplicam às diferentes plataformas que podem ser usadas.

Tabela F-1 Plataformas baseadas em SuperMicro

	McAfee 1U	McAfee 2U ou 3U
Emissões eletromagnéticas	Classe B do FCC, classe B do EN 55022, EN 61000-3-2/-3-3 Classe B do CISPR 22	Classe B do FCC, classe B do EN 55022, EN 61000-3-2/-3-3 Classe B do CISPR 22
Imunidade eletromagnética	EN 55024/CISPR 24, (EN 61000-4-2, EN 61000-4-3, EN 61000-4--4, EN 61000-4-5, EN 61000-4-6, EN 61000-4-8, EN 61000-4-11) 55024	EN 55024/CISPR 24, (EN 61000-4-2, EN 61000-4-3, EN 61000-4--4, EN 61000-4-5, EN 61000-4-6, EN 61000-4-8, EN 61000-4-11) 55024
Segurança	Em conformidade com EN 60950/IEC 60950, Lista UL (EUA) Lista CUL (Canadá) Certificação TUV (Alemanha) Marcação CE (Europa)	Em conformidade com EN 60950/IEC 60950, Lista UL (EUA) Lista CUL (Canadá) Certificação TUV (Alemanha) Marcação CE (Europa)

Tabela F-2 Plataformas baseadas em DAS

	DAS-50, DAS-100
Voltagem de entrada	100/240 VCA
Frequência de entrada	50/60 Hz
Fonte de alimentação	1400 W X3
Consumo de energia	472 W@120 VCA 461 W@240 VCA
Amperagem (máx.)	9,4 A
Altitude (máx.)	-45 a 9.500 pés
Temperatura (máx.)	10 ºC a 35 ºC (operacional) -40 ºC a 70 ºC (não operacional)
Altitude	-45 a 9500 pés (operacional) -45 a 25.000 pés (não operacional)

Tabela F-2 Plataformas baseadas em DAS *(continuação)*

	DAS-50, DAS-100
BTU	BTU/HR 1609
Umidade	Operacional: 10% a 85% (sem condensação) não operacional: 10% a 90%

Tabela F-3 Plataforma Intel 1U

Parâmetro	Limites
Temperatura operacional	+10 °C a +35 °C com a taxa máxima de alteração sem ultrapassar 10 °C por hora
Temperatura não operacional	-40 °C a +70 °C
Umidade não operacional	90%, sem condensação a 35 °C
Ruído acústico	Potência sonora: 7,0 BA em estado ocioso a uma temperatura ambiente normal de escritório. (23 +/- 2 graus C)
Choque, operacional	Meia senoide, 2 g pico, 11 ms
Choque, desembalado	Trapezoidal, 25 g, alteração de velocidade 3,45 m/s (≧ 18 kg a > 37 kg)
Choque, embalado	Queda livre não paletizada de uma altura de 60 cm (≧18 kg a > 37 kg)
Choque, operacional	Meia senoide, 2 g pico, 11 ms
Vibração, desembalado	5 Hz a 500 Hz, 2,20 g RMS aleatório
ESD	+/-12kV para descarga de ar e 8K para contato
Requisito do sistema de resfriamento em BTUs/h	1.660 BTUs/hora

Tabela F-4 Plataforma Intel 2U

Parâmetro		Limites
Temperatura	Operacional	• ASHRAE Classe A2 — Operação contínua. 10 °C a 35 °C (50 °F a 95 °F) com a taxa máxima de alteração que não ultrapasse 10 °C por hora. • ASHRAE Classe A3: inclui operação até 40 °C por até 900 horas por ano • ASHRAE Classe A4: inclui operação até 45 °C por até 90 horas por ano
	Envio	-40 °C a 70 °C (-40 °F a 158 °F)
Altitude (operacional)		Operação compatível de até 3.050 m com diminuição de potência na classe ASHRAE
Umidade (envio)		50% a 90%, sem condensação, com lâmpada úmida no máximo até 28 °C (em temperaturas entre 25 °C e 35 °C)
Choque	Operacional	Meia senoide, 2 g, 11 ms
	Desembalado	Trapezoidal, 25 g, alteração da velocidade baseada no peso com embalagem

Tabela F-4 Plataforma Intel 2U *(continuação)*

Parâmetro		Limites
	Embalado	Peso do produto: ≥ 40 a < 80 Altura de queda livre não paletizada = 45,72 cm Altura de queda livre paletizada (produto único) = ND
Vibração		5 Hz a 500 Hz 2,20 g RMS aleatório
	Embalado	5 Hz a 500 Hz 1,09 g RMS aleatório
AC-DC	Voltagem	90 Hz a 132 V e 180 V a 264 V
	Frequência	47 Hz a 63 Hz
	Interrupção de fonte	Sem perda de dados para interrupção de energia de 12 ms
	Sobretensão não operacional e operacional	Unidirecional

Índice

N

P

R

S

T