Dell Security Management Server Virtual

Guia de Início Rápido e de Instalação v10.2.5

Notas, avisos e advertências

NOTA: Uma NOTA indica informações importantes que ajudam a melhorar a utilização do produto.

AVISO: Um AVISO indica potenciais danos do hardware ou a perda de dados e explica como evitar o problema.

ADVERTÊNCIA: Uma ADVERTÊNCIA indica potenciais danos no equipamento, lesões pessoais ou mesmo morte.

2019 - 06

Rev. A01

Índice

1

Guia de Início Rápido

Este Guia de início rápido destina-se a utilizadores mais avançados que pretendem iniciar e executar rapidamente o Dell Server. Como regra geral, a Dell recomenda instalar primeiro o Dell Server, instalando de seguida os clientes.

Para obter instruções mais detalhadas, consulte o Guia de Instalação do Security Management Server Virtual.

Para obter mais informações sobre os pré-requisitos do Dell Server, consulte Security Management Server Virtual, Pré-requisitos da Management Console e Pré-requisitos do Modo Proxy.

Para obter mais informações sobre como atualizar um Dell Server, consulte Atualizar Security Management Server Virtual.

A instalação

1 Procure no diretório onde estão armazenados os ficheiros do Dell Data Security e clique duas vezes para importar para o VMware o Security Management Server Virtual **v10.x.x Build x.ova**.

> **NOTA: O ficheiro OVA tem agora uma assinatura SHA256 e não poderá ser importado para o cliente de grandes dimensões do VMWare. Para obter mais informações, consulte https://kb.vmware.com/s/article/2151537.**

2 Ligue o Security Management Server Virtual

3 Siga as instruções no ecrã.

Configuração

Antes de ativar os utilizadores, recomendamos que conclua as seguintes tarefas de configuração no terminal do Security Management Server Virtual:

- Configurar definições SMTP
- Importar um certificado existente ou inscrever um novo certificado de servidor
- Atualizar o Security Management Server Virtual
- Instale um cliente FTP que suporte SFTP na porta 22, e Configurar utilizadores de transferência de ficheiros (FTP).

Se a sua organização tiver dispositivos com disposição externa, consulte Instalar e configurar o Modo Proxy.

Abrir a Management Console

Abra a Management Console neste endereço: https://server.domain.com:8443/webui/

As credenciais predefinidas são **superadmin/changeit**.

Para aceder a uma lista de browsers suportados, consulte Pré-requisitos da Management Console.

Tarefas administrativas

Se ainda não iniciou a Management Console, faça-o agora. As credenciais predefinidas são **superadmin/changeit**.

A Dell recomenda a atribuição de papéis de administrador logo que possível. Para concluir esta tarefa agora, consulte Atribuir o papel de administrador da Dell.

Clique em "?" no canto superior direito da Management Console para iniciar a *AdminHelp*. É apresentada a página *Como começar*. Clique em **Adicionar domínios**.

Foram definidas políticas de base para a sua organização que devem ser alteradas consoante as suas necessidades específicas, da seguinte forma (as licenças e elegibilidades guiam todas as ativações):

- A Policy Based Encryption será ativada com a encriptação de Chave comum
- Os computadores com unidades de encriptação automática serão encriptados
- A gestão do BitLocker não está ativada
- O Advanced Threat Prevention não está ativado
- O Threat Protection está desativado
- Os suportes multimédia externos não serão encriptados
- As portas não serão geridas pelo Controlo de portas
- Os dispositivos com a Full Disk Encryption instalada não serão encriptados
- O Data Guardian está desativado

Consulte o tópico da AdminHelp *Gerir Políticas* para aceder aos Grupos tecnológicos e às descrições das políticas.

As tarefas de Início Rápido estão concluídas.

2

Guia de instalação detalhada

Este Guia de instalação destina-se à instalação e configuração do Security Management Server Virtual. Como regra geral, a Dell recomenda instalar primeiro o Security Management Server Virtual, instalando de seguida os clientes.

Para obter mais informações sobre como atualizar um Security Management Server Virtual existente, consulte Atualizar Security Management Server Virtual.

Acerca do Security Management Server Virtual

A Management Console permite aos administradores monitorizar o estado dos endpoints, da aplicação de políticas e da proteção em toda a empresa. O modo Proxy fornece uma opção front-end (modo DMZ) para utilização com o Security Management Server Virtual.

O Security Management Server Virtual tem as seguintes funções:

- Gestão centralizada de até 3500 dispositivos
- Criação e gestão de políticas de segurança baseadas em funções
- Recuperação de dispositivos assistida por administrador
- Separação de deveres administrativos
- Distribuição automática de políticas de segurança
- Caminhos fidedignos para comunicação entre componentes
- Geração de chaves de encriptação exclusivas e caução de chave de segurança automática
- Relatórios e auditorias de conformidade centralizados
- Geração automática de certificados autoassinados

Contacte o Dell ProSupport

Contacte o número 877-459-7304, extensão 4310039 para obter suporte telefónico permanente (24 x 7) para o seu produto Dell.

Adicionalmente, o suporte online para os produtos Dell encontra-se disponível em dell.com/support. O suporte online inclui controladores, manuais, conselhos técnicos, FAQ e problemas emergentes.

Ajude-nos a garantir que o direcionamos rapidamente para o especialista técnico mais indicado para si tendo o seu Código de serviço ou Código de serviço expresso disponível quando nos contactar.

Para números de telefone fora dos Estados Unidos, consulte Números de telefone internacionais do Dell ProSupport.

Requisitos

Security Management Server Virtual

Hardware

O espaço em disco recomendado para o Security Management Server Virtual é 80 GB.

Ambiente virtual

O Security Management Server Virtual v10.2.5 foi validado com os seguintes ambientes virtuais.

A Dell atualmente suporta o alojamento do Dell Security Management Server ou do Dell Security Management Server Virtual numa Infraestrutura alojada na nuvem como um ambiente de serviço (IaaS), como, por exemplo, Amazon Web Services, Azure e vários outros fornecedores. O suporte para estes ambientes só será limitado para a funcionalidade do servidor de aplicação alojado no interior destas máquinas virtuais, a administração e segurança destas máquinas virtuais dependerão do administrador da solução IaaS.

Os requisitos adicionais da infraestrutura (Active Directory, bem como o SQL Server para o Dell Security Management Server) ainda são necessários para a funcionalidade adequada.

Ambientes virtuais

- VMware Workstation 12,5
  - Necessário CPU de 64 bits
  - Necessários 8 GB de RAM
  - 80 GB de espaço no disco rígido
  - Computador anfitrião com pelo menos dois núcleos
  - Consulte http://www.vmware.com/resources/compatibility/search.php?deviceCategory=software&testConfig=17 para obter uma lista completa dos sistemas operativos anfitriões compatíveis
  - O hardware deve cumprir os requisitos mínimos do VMware
  - Consulte https://kb.vmware.com/s/article/1003746 para obter mais informações

- VMware Workstation 14.0
  - Necessário CPU de 64 bits
  - Necessários 8 GB de RAM
  - 80 GB de espaço no disco rígido
  - Computador anfitrião com pelo menos dois núcleos
  - Consulte http://www.vmware.com/resources/compatibility/search.php?deviceCategory=software&testConfig=17 para obter uma lista completa dos sistemas operativos anfitriões compatíveis
  - O hardware deve cumprir os requisitos mínimos do VMware
  - Consulte https://kb.vmware.com/s/article/1003746 para obter mais informações

- VMware Workstation 14.1
  - Necessário CPU de 64 bits
  - Necessários 8 GB de RAM
  - 80 GB de espaço no disco rígido
  - Computador anfitrião com pelo menos dois núcleos
  - Consulte http://www.vmware.com/resources/compatibility/search.php?deviceCategory=software&testConfig=17 para obter uma lista completa dos sistemas operativos anfitriões compatíveis
  - O hardware deve cumprir os requisitos mínimos do VMware
  - Consulte https://kb.vmware.com/s/article/1003746 para obter mais informações

- VMware ESXi 6.5
  - Necessário CPU de 64 bits x86
  - Computador anfitrião com pelo menos dois núcleos
  - Mínimo de 8 GB de RAM necessário
  - 80 GB de espaço no disco rígido
  - Não é necessário um sistema operativo
  - Consulte http://www.vmware.com/resources/compatibility/search.php?deviceCategory=software&testConfig=17 para obter uma lista completa dos sistemas operativos anfitriões compatíveis
  - O hardware deve cumprir os requisitos mínimos do VMware
  - Consulte https://kb.vmware.com/s/article/1003746 para obter mais informações

Ambientes virtuais

- VMware ESXi 6.0
  - Necessário CPU de 64 bits x86
  - Computador anfitrião com pelo menos dois núcleos
  - Mínimo de 8 GB de RAM necessário
  - 80 GB de espaço no disco rígido
  - Não é necessário um sistema operativo
  - Consulte http://www.vmware.com/resources/compatibility/search.php?deviceCategory=software&testConfig=17 para obter uma lista completa dos sistemas operativos anfitriões compatíveis
  - O hardware deve cumprir os requisitos mínimos do VMware
  - Consulte https://kb.vmware.com/s/article/1003746 para obter mais informações
- VMware ESXi 5.5
  - Necessário CPU de 64 bits x86
  - Computador anfitrião com pelo menos dois núcleos
  - Mínimo de 8 GB de RAM necessário
  - 80 GB de espaço no disco rígido
  - Não é necessário um sistema operativo
  - Consulte http://www.vmware.com/resources/compatibility/search.php?deviceCategory=software&testConfig=17 para obter uma lista completa dos sistemas operativos anfitriões compatíveis
  - O hardware deve cumprir os requisitos mínimos do VMware
  - Consulte https://kb.vmware.com/s/article/1003746 para obter mais informações
- Servidor Hyper-V (instalação completa ou essencial)
  - Necessário CPU de 64 bits x86
  - Computador anfitrião com pelo menos dois núcleos
  - Mínimo de 8 GB de RAM necessário
  - 80 GB de espaço no disco rígido
  - Não é necessário um sistema operativo
  - O hardware deve cumprir os requisitos mínimos do Hyper-V
  - Deve ser executado como uma máquina virtual de 1.ª geração

NOTA: Para obter informações sobre como configurar o Hyper-V, siga as instruções para Sistemas operativos de ponto terminal: https://docs.microsoft.com/en-us/virtualization/hyper-v-on-windows/quick-start/enable-hyper-v ou para Sistemas operativos de servidor: https://docs.microsoft.com/en-us/windows-server/virtualization/hyper-v/get-started/install-the-hyper-v-role-on-windows-server.

Management Console

Browsers

NOTA:
O browser tem de aceitar cookies.

A tabela seguinte apresenta os browsers suportados.

Browsers

- Internet Explorer 11.x ou posterior

- Mozilla Firefox 41.x ou posterior
- Google Chrome 46.x ou posterior

Modo de proxy

Hardware

A tabela seguinte indica os requisitos *mínimos* de hardware.

Processador

CPU Dual-Core moderna (1,5 Ghz +)

RAM

Mínimo de 2 GB de RAM dedicada/4 GB de RAM dedicada recomendados

Espaço livre em disco

1,5 GB de espaço livre em disco (mais espaço de paginação virtual)

Placa de rede

Placa de interface de rede 10/100/1000

Diversos

IPv4, IPv6 ou uma combinação de IPv4 e IPv6 são suportados

Software

A tabela seguinte descreve pormenorizadamente o software que deve existir antes de instalar o servidor do modo proxy.

Pré-requisitos

- **Windows Installer 4.0 ou posterior**

  O Windows Installer 4.0 ou posterior deve estar instalado no servidor onde a instalação for executada.

- **Pacote Redistribuível do Microsoft Visual C++ 2010**

  Se não estiver instalado, o instalador irá fazê-lo por si.

- **Microsoft .NET Framework Versão 4.5.2**

  A Microsoft publicou atualizações de segurança para o .NET Framework Version 4.5.2

NOTA:
O Universal Account Control (UAC) tem de estar desativado se for instalado num diretório protegido. Depois de desativar o UAC, o servidor tem de ser reiniciado para que esta alteração seja implementada.

Localização do registo para os Servidores Windows: HKLM\SOFTWARE\Dell.

A tabela seguinte descreve pormenorizadamente os requisitos de software para o servidor de modo proxy.

Sistema operativo

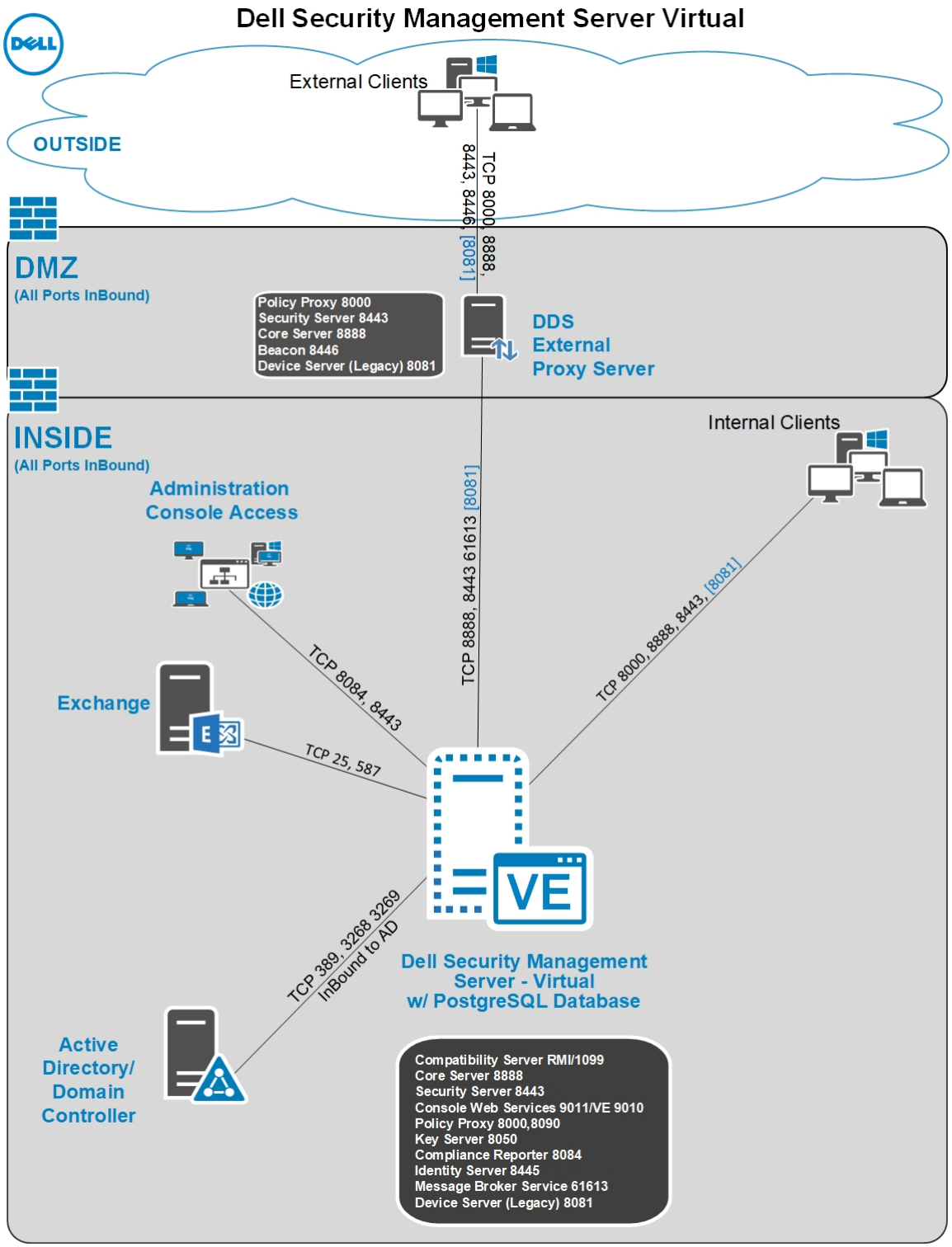
- **Windows Server 2019**
  - Standard Edition
  - Datacenter Edition
- **Windows Server 2016**
  - Standard Edition
  - Datacenter Edition
- **Windows Server 2012 R2**
  - Standard Edition
  - Datacenter Edition
- **Repositório LDAP**
  - Active Directory 2008 R2
  - Active Directory 2012 R2
  - Active Directory 2016

Arquitetura do Security Management Server Virtual

As soluções Dell Encryption, Endpoint Security Suite Enterprise e Data Guardian são produtos altamente dimensionáveis, com base no número de pontos terminais pretendidos para encriptação na sua organização.

Componentes da arquitetura

Abaixo encontra-se uma implementação básica para o Dell Security Management Server Virtual.



Transferir e instalar um ficheiro OVA

Durante a instalação inicial, o Security Management Server Virtual é fornecido como um ficheiro OVA (Open Virtual Application), uma aplicação utilizada para o fornecimento de software executado numa máquina virtual. O ficheiro OVA está disponível em www.dell.com/support, nas páginas de apoio técnico para os seguintes produtos Dell Data Security:

- Encriptação

- Endpoint Security Suite Enterprise
- Data Guardian

Para transferir o ficheiro OVA:

1 Navegue para a página *Controladores e transferências* do produto adequado listado acima.
2 Clique em **Controladores e transferências**.
3 Selecione a versão VMware ESXi adequada.
4 Transfira o pacote adequado.

Para instalar o ficheiro OVA:

Antes de começar, certifique-se de que todos os Requisitos de sistema e de ambiente virtual sejam atendidos.

1 No suporte multimédia de instalação da Dell, localize *Security Management Server Virtual v9.x.x Build x.ova* e faça duplo clique para importar para o VMware.

> **NOTA: Se estiver a utilizar o Hyper-V em vez do VMware, siga as instruções para o Windows 10 https://docs.microsoft.com/en-us/virtualization/hyper-v-on-windows/about/. Para sistemas operativos de funcionamento em servidor, siga as instruções https://docs.microsoft.com/en-us/windows-server/virtualization/hyper-v/get-started/install-the-hyper-v-role-on-windows-server. Se estiver a utilizar o ESXi em vez do VMware, siga as instruções: https://kb.vmware.com/s/article/2109708.**

2 Siga as instruções no ecrã.

> **NOTA: Se a importação falhar ao utilizar o VMWare, o ficheiro OVA terá de ser importado através do caminho sugerido do cliente Web. Para obter mais informações, consulte https://kb.vmware.com/s/article/2151537.**

3 Ligue o Security Management Server Virtual.
4 Selecione o idioma do contrato de licença e selecione **Apresentar EULA**.
5 Leia o contrato e selecione **Aceitar EULA**.
6 Se estiver disponível uma atualização, selecione **Aceitar**.
7 Selecione **Modo Ligado** ou **Modo Desligado**.

> **NOTA:**
> Se selecionar **Modo Desligado**, nunca pode ser alterado para o Modo ligado.
>
> O modo desligado isola o Dell Server da Internet e de uma LAN ou outra rede não segura. Todas as atualizações têm de ser efetuadas manualmente. Para obter mais informações sobre as políticas e o modo Desligado, consulte *AdminHelp*.

8 Em *Definir a palavra-passe delluser*, introduza a palavra-passe atual (predefinida), **delluser** e, em seguida, introduza uma palavra-passe exclusiva, volte a introduzir a palavra-passe exclusiva e selecione **Aplicar**.

As palavras-passe devem incluir o seguinte:

- Pelo menos 8 caracteres
- Pelo menos 1 letra maiúscula
- Pelo menos 1 número
- Pelo menos 1 carácter especial

> **NOTA: É possível manter a palavra-passe predefinida ao selecionar Cancelar, ou ao premir Escape no teclado.**

9 Selecione **fechar** para entrar na janela de configuração do nome do anfitrião.
10 Em *Configurar o nome de anfitrião*, utilize a tecla de retrocesso para remover o nome de anfitrião predefinido. Introduza um nome de anfitrião exclusivo e selecione **OK**.
11 Em *Configurar definições de rede*, escolha uma das opções abaixo e selecione **OK**.

- (Predefinida) Usar DHCP (IPv4)

- (Recomendada) No campo *Usar DHCP*, prima a barra de espaços para remover o X e introduzir manualmente estes endereços, conforme aplicável:

  IP estático

  Máscara de rede

  Gateway predefinido

  Servidor DNS 1

  Servidor DNS 2

  Servidor DNS 3

  É possível selecionar IPv6 ou IPv4 para uma configuração estática.

- **NOTA: Ao utilizar um IP estático, também tem de criar uma entrada de anfitrião no servidor DNS.**

12 No aviso de confirmação do fuso horário, selecione **OK**.

13 Quando for apresentada a mensagem que indica que a primeira configuração está concluída, selecione **OK**.

14 Configurar definições SMTP.

15 Importar um certificado existente ou inscrever um novo certificado de servidor.

16 Atualizar o Security Management Server Virtual.

17 Instale um cliente FTP que suporte SFTP na porta 22, e Configurar utilizadores de transferência de ficheiros (FTP).

As tarefas de instalação do Security Management Server Virtual estão concluídas.

Abrir a Management Console

Abra a Management Console neste endereço: https://server.domain.com:8443/webui/

As credenciais predefinidas são **superadmin/changeit**.

Para aceder a uma lista de browsers suportados, consulte Pré-requisitos da Management Console.

Instalar e configurar o Modo Proxy

O modo Proxy fornece uma opção de front-end (modo DMZ) para utilização com o , o Dell Server. Se pretender implementar componentes Dell no DMZ, certifique-se de que estão devidamente protegidos contra ataques.

NOTA: O serviço de Sinalizador é instalado como parte desta instalação para apoiar o sinalizador de chamada de retorno do Data Guardian, o qual insere um sinalizador de chamada de retorno em cada ficheiro protegido pelo Data Guardian ao permitir ou implementar os documentos protegidos do Office no ambiente. Isto permite a comunicação entre qualquer dispositivo em qualquer localização e o servidor de front-end. Certifique-se de que a segurança de rede necessária está configurada antes de usar o sinalizador de chamada de retorno.

Para efetuar esta instalação, irá necessitar do nome de anfitrião totalmente qualificado do servidor DMZ.

1 No suporte multimédia de instalação da Dell, aceda ao diretório Security Management Server. **Descomprima** (NÃO copie/cole nem arraste/largue) o Security Management Server-x64 para o diretório de raiz do servidor onde está a desinstalar o Security Management Server Virtual. ***As operações de copiar/colar ou arrastar/largar produzem erros e uma instalação malsucedida.***

2 Clique duas vezes no ficheiro **setup.exe**.

3 Selecione o idioma da instalação e, de seguida, clique em **OK**.

4 Se os pré-requisitos ainda não estiverem instalados, é apresentada uma mensagem a informar que pré-requisitos serão instalados. Clique em **Instalar**.

5 Clique em **Seguinte** na caixa de diálogo Bem-vindo.

6 Leia o contrato de licença, aceite os termos e clique em **Seguinte**.

7 Introduza a chave do produto de 32 caracteres e, em seguida, clique em **Seguinte**. A chave do produto encontra-se no ficheiro EnterpriseServerInstallKey.ini.

8 Selecione **Instalação de front-end** e clique em **Seguinte**.

9 Para instalar o servidor de front-end na localização predefinida C:\Program Files\Dell, clique em **Seguinte**. Caso contrário, clique em **Alterar** para selecionar outra localização e clique em **Seguinte**.

10 Tem à sua disposição vários tipos de certificados digitais que pode utilizar.

NOTA: É altamente recomendável que utilize um certificado digital de uma autoridade de certificação fidedigna.

Selecione a opção "a" ou "b" abaixo:

a Para utilizar um certificado existente comprado junto de uma autoridade de CA, selecione **Importar um certificado existente** e clique em **Seguinte**.

b Para criar um certificado autoassinado, selecione **Criar um certificado autoassinado e importá-lo para a key store e clique em Seguinte.**

Na caixa de diálogo *Criar certificado autoassinado*, introduza as seguintes informações:

Nome do computador completamente qualificado (exemplo: nomedocomputador.domínio.com)

Organização

Unidade organizacional (exemplo: Segurança)

Cidade

Distrito (nome completo)

País: abreviatura de duas letras do país

Clique em **Seguinte**.

NOTA: A validade do certificado é de 10 anos, por predefinição.

11 Na caixa de diálogo *Configuração do servidor de front-end*, introduza o nome de anfitrião totalmente qualificado ou o alias de DNS do servidor de back-end, selecione **Dell Security Management Server** e clique em **Seguinte**.

12 A partir da caixa de diálogo *Configuração da instalação do servidor de front-end*, pode visualizar ou editar os nomes dos anfitriões e as portas.

- Para aceitar as portas e os nomes dos anfitriões predefinidos, na caixa de diálogo *Configuração da instalação do servidor de front-end*, clique em **Seguinte**.
- Para ver ou editar os nomes dos anfitriões, na caixa de diálogo *Configuração do servidor de front-end*, clique em **Editar nomes dos anfitriões**. Edite os nomes dos anfitriões apenas se necessário. A Dell recomenda que utilize os nomes predefinidos.

NOTA:
Um nome de anfitrião não pode conter um caráter de sublinhado ("_").

Desmarque um proxy apenas se tiver a certeza de que não o pretende configurar para instalação. Se desmarcar um proxy nesta caixa de diálogo, este não é instalado.

Quando terminar, clique em **OK**.

- Para ver ou editar as portas, na caixa de diálogo *Configuração do servidor de front-end*, clique em **Editar portas externas** ou **Editar portas de ligação internas**. Edite as portas apenas se necessário. A Dell recomenda que utilize os nomes predefinidos.

Se desmarcar um proxy na caixa de diálogo *Editar nomes de anfitriões de front-end*, a respetiva porta não é apresentada nas caixas de diálogo Portas externas ou Portas internas.

Quando terminar, clique em **OK**.

13 Na caixa de diálogo *Preparado para instalar o programa*, clique em **Instalar**.

14 Quando a instalação estiver concluída, clique em **Concluir**.

Tarefas de configuração básica do terminal

É possível aceder às tarefas de configuração básicas a partir do menu principal.

Verificar o Painel do sistema

Para verificar o estado dos serviços do Dell Server, selecione **Painel do sistema** no menu principal.

O widget *Informações do Sistema* apresenta a versão atual, o nome do anfitrião, o endereço IP, bem como a utilização da CPU, da memória e do disco.

O widget *Histórico de versões* apresenta alterações de versão no esquema da base de dados. Os dados são fornecidos pela tabela "informações" e estão ordenados cronologicamente, com a versão mais recente no topo.

A tabela seguinte descreve cada serviço e a respetiva função no widget *Estado de funcionamento do serviço*.

Nome	Descrição
Message Broker	Bus do Enterprise Server
Identity Server	Trata dos pedidos de autenticação de domínio.
Compatibility Server	Um serviço para gerir a arquitetura empresarial.
Security Server	Oferece o mecanismo de controlo de comandos e de comunicação com o Active Directory.
Compliance Reporter	Oferece uma visão abrangente do ambiente, tendo em vista a elaboração de relatórios de auditoria e conformidade.
Core Server	Um serviço para gerir a arquitetura empresarial. Este serviço também processa toda a ativação, políticas e recolha de inventário de dispositivos com base em "Agente".
Core Server HA (Elevada Disponibilidade)	Um serviço de elevada disponibilidade que permite o aumento da segurança e do desempenho das ligações HTTPS durante a gestão da arquitetura empresarial.
Inventory Server	Processa a fila de inventário.
Forensic Server	Disponibiliza serviços web para API forense.
Policy Proxy	Oferece uma linha de comunicação com base na rede de forma a proporcionar atualizações de políticas de segurança e atualizações de inventário.

Os serviços são monitorizados e reiniciados automaticamente, se necessário.

NOTA: Se o processo de personalização de bases de dados falhar, os servidores passam para o estado de Falha de execução. Para verificar o registo de personalização de base de dados, selecione Ver registos no menu principal.

Alterar Nome do anfitrião

Esta tarefa pode ser realizada em qualquer momento. Não é necessário começar a utilizar Security Management Server Virtual.

1 No menu *Configuração básica*, selecione **Nome do anfitrião**.
2 Utilize a tecla de retrocesso para remover o nome do anfitrião existente, substitua-o por um novo nome do anfitrião e selecione **OK**.

Alterar definições de rede

Esta tarefa pode ser realizada em qualquer momento. Não é necessário começar a utilizar Security Management Server Virtual.

1 No menu de *Configuração básica*, selecione **Rede**.
2 No ecrã *Configurar definições de rede*, escolha uma das opções abaixo e selecione **OK**.
   - (Predefinida) Usar DHCP (IPv4).
   - (Recomendada) No campo *Utilizar DHCP*, prima a barra de espaços para remover o X e introduzir manualmente estes endereços, conforme aplicável:

     IP estático

     Máscara de rede

     Gateway predefinido

     Servidor DNS 1

     Servidor DNS 2

     Servidor DNS 3

     É possível selecionar IPv6 ou IPv4 para uma configuração estática.

     NOTA:
     Ao utilizar um IP estático, tem de criar uma entrada de anfitrião no servidor DNS.

Ativar o suporte do DMZ Server

Esta tarefa pode ser realizada em qualquer momento. Não é necessário começar a utilizar Security Management Server Virtual.

1 No menu de *Configuração básica*, selecione **Assistência do DMZ Server**.
2 Utilize a barra de espaços para introduzir um **X** no campo Ativar o suporte do servidor DMZ
3 Introduza o nome de domínio totalmente qualificado do servidor DMZ e selecione **OK**.

NOTA: Para utilizar um servidor DMZ, consulte as instruções de instalação de um servidor proxy acima: Instalar e configurar o Modo Proxy.

Alterar fuso horário

Esta tarefa pode ser realizada em qualquer momento. Não é necessário começar a utilizar Security Management Server Virtual.

1 No menu *Configuração básica*, selecione **Fuso horário**.
2 No ecrã *Fuso horário*, utilize as teclas de seta para realçar o seu fuso horário e selecione **Enter**.

Atualizar o Security Management Server Virtual

Para obter informações sobre uma atualização específica, consulte os *Conselhos técnicos do Security Management Server Virtual*, que se encontram em dell.com/support. Para ver a versão e data de instalação de uma atualização que já foi aplicada, verifique o *Painel do sistema*.

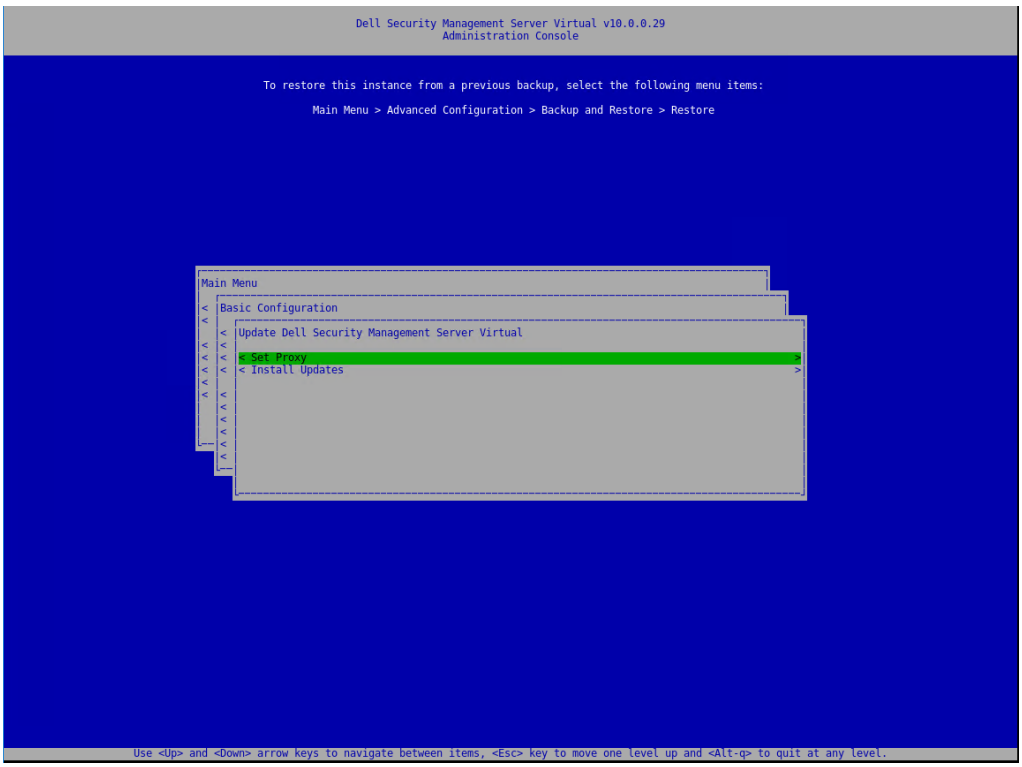
Para receber notificações por e-mail quando estiverem disponíveis atualizações para o Dell Server, consulte Configurar definições SMTP.

Se tiverem sido efetuadas alterações à política que não foram consolidadas na Management Console, submeta as alterações da política antes de atualizar o Dell Server:

1 Como administrador Dell, inicie sessão na Management Console.
2 No menu esquerdo, clique em **Gestão** > **Consolidar**.
3 Introduza uma descrição da alteração no campo Comentários.
4 Clique em **Consolidar políticas**.
5 Quando a consolidação estiver completa, termine sessão na Management Console.

Atualizar o Security Management Server Virtual (Modo Ligado)

1 A Dell recomenda a realização frequente de cópias de segurança. Antes de atualizar, certifique-se de que o processo de cópia de segurança está a funcionar corretamente. Consulte Cópia de segurança e Restauro.
2 No menu **Configuração básica**, selecione **Atualizar Dell Security Management Server Virtual**.



NOTA: O número da versão poderá ser diferente do apresentado na captura de ecrã anexada.

3 Selecione a ação pretendida:

- Configurar as definições de proxy - Selecione esta opção para configurar as definições de proxy para transferência de atualizações.

  No ecrã *Configurar definições de proxy*, pressione a barra de espaços para introduzir um **X** no campo *Utilizar proxy*. Introduza o HTTPS e o HTTP. Se for necessária a autenticação da firewall, pressione a barra de espaços para introduzir um **X** em Autenticação necessária. Introduza o nome de utilizador e a palavra-passe, e selecione **OK**.

  NOTA: Esta opção Definir proxy agora também atualiza as definições de proxy para as várias aplicações baseadas em java, para extrair licenças On-The-Box, bem como a comunicação ao Endpoint Security Suite Enterprise SaaS e à infraestrutura back-end Dell/Credant.

- Ao selecionar **Instalar Atualizações**, o Security Management Server Virtual consulta os repositórios Ubuntu predefinidos incorporados e o dist.ddspproduction.com, o repositório personalizado da Dell que contém as atualizações da aplicação.

  NOTA: A Dell consulta o dist.ddspproduction.com através da porta 443 e da porta 80 para todas as atualizações Ubuntu. Todas as atualizações disponíveis são transferidas. As configurações de proxy definidas na Configuração de Proxy são utilizadas para as ligações para transferências da porta 443 e da porta 80.

Atualizar o Security Management Server Virtual (Modo Desligado)

1 A Dell recomenda a realização frequente de cópias de segurança. Antes de atualizar, certifique-se de que o processo de cópia de segurança está a funcionar corretamente. Consulte Cópia de segurança e Restauro.

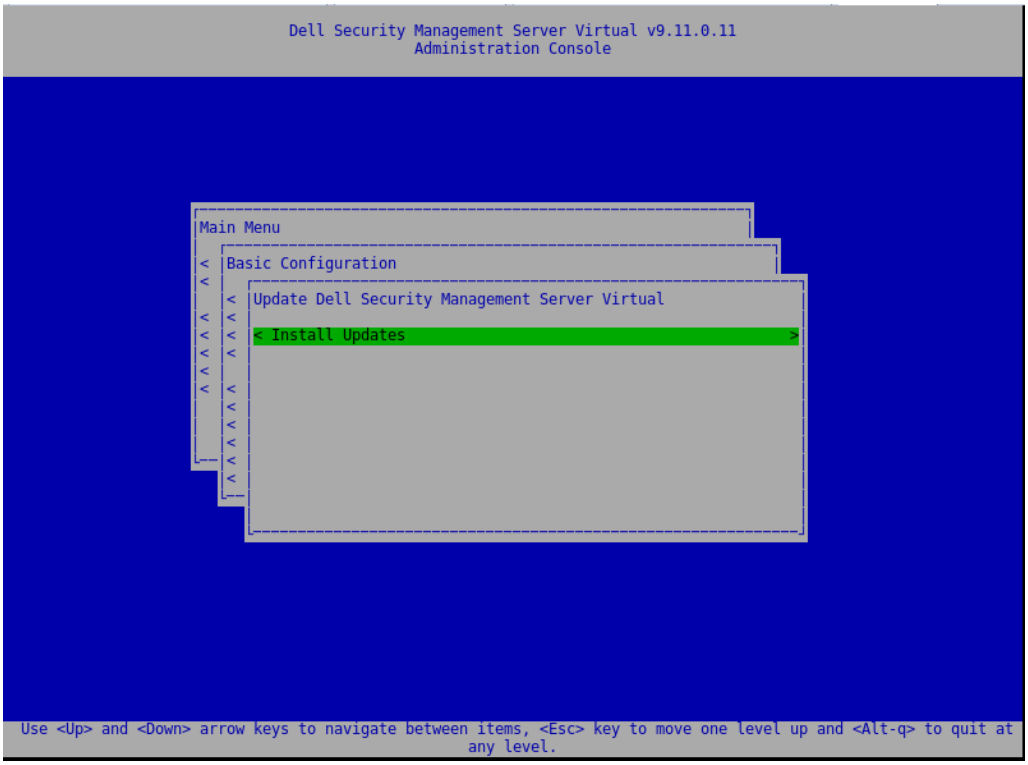
2 Obtenha o ficheiro .deb que contém as mais recentes atualizações do Dell Server no Dell ProSupport.

3 Guarde o ficheiro .deb na pasta /updates no servidor FTP seguro do Dell Server.

Certifique-se de que o cliente de FTP suporta SFTP na porta 22, e que um utilizador de FTP está configurado. Consulte Configurar utilizadores de transferência de ficheiros (FTP).

4 No menu **Configuração básica**, selecione **Atualizar Security Management Server Virtual**.

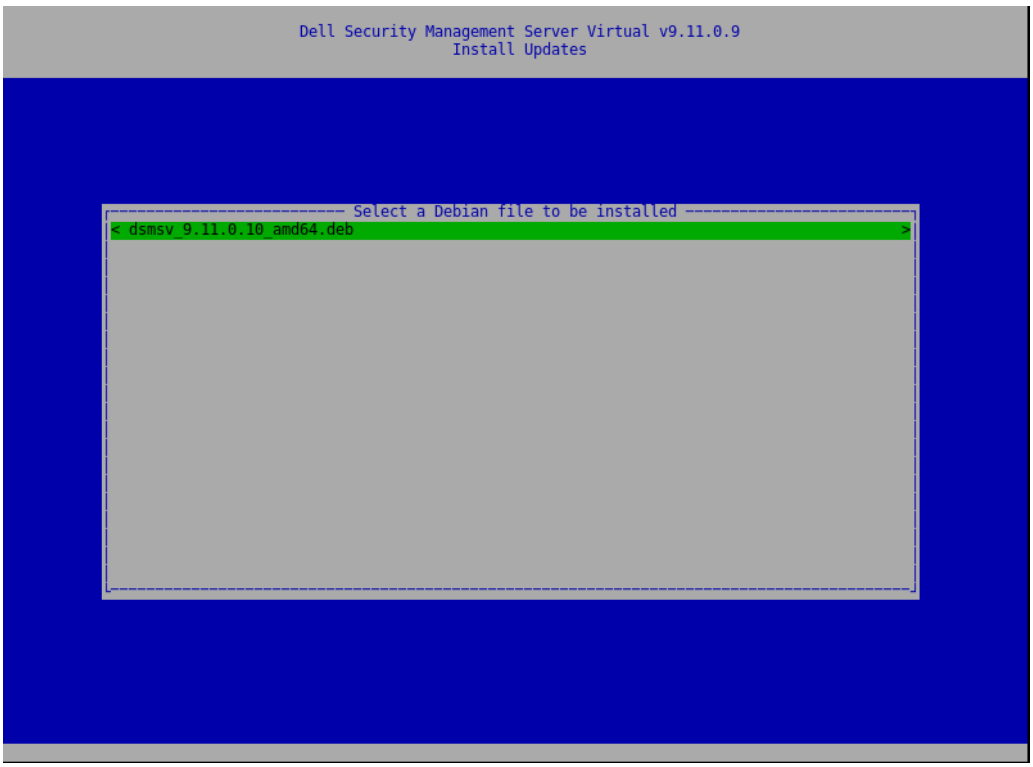
5 Selecione **Instalar atualizações** e prima a tecla **Enter**.



NOTA: O número da versão poderá ser diferente do apresentado na captura de ecrã anexada.

Se o ficheiro .deb não for apresentado, certifique-se de que o ficheiro .deb está armazenado no local certo.

6 Selecione o ficheiro de atualização .deb que pretende instalar e prima a tecla **Enter**.



NOTA: O número da versão poderá ser diferente do apresentado na captura de ecrã anexada.

Alterar palavras-passe de utilizadores

Esta tarefa pode ser realizada em qualquer momento. Não é necessário começar a utilizar Security Management Server Virtual.

Pode alterar as palavras-passe para os seguintes utilizadores:

- delluser (Administrador do terminal) - Este utilizador tem acesso ao terminal Dell Server e aos respetivos menus.
- dellconsole (acesso à shell) - Este utilizador tem acesso à shell Dell Server. O acesso à shell está disponível para que um administrador de rede verifique e resolva problemas de conetividade da rede.
- dellsupport (Administrador Dell ProSupport) - Este utilizador tem direitos "sudo" que devem ser utilizados com moderação. Por razões de segurança, a palavra-passe desta conta é controlada por si.

1 No menu *Configuração básica*, selecione **Alterar palavras-passe de utilizador**.
2 No ecrã *Alterar palavras-passe de utilizador,* selecione a palavra-passe a alterar e selecione **Enter**.
3 No ecrã *Definir palavra-passe*, introduza a palavra-passe atual, introduza a nova palavra-passe, reintroduza a nova palavra-passe e selecione **OK**.

   As palavras-passe devem incluir o seguinte:

   - Pelo menos 8 caracteres
   - Pelo menos 1 letra maiúscula
   - Pelo menos 1 número
   - Pelo menos 1 carácter especial

   NOTA:
   Para selecionar contas de utilizador diferentes, utilize a barra de espaço no teclado para visualizar a lista de seleção.

Configurar Utilizadores de Transferência de Ficheiros Segura (SFTP)

Esta tarefa pode ser realizada em qualquer momento. Não é necessário começar a utilizar Security Management Server Virtual.

1 No menu *Configuração básica*, selecione **SFTP**.
2 No ecrã *SFTP*, para adicionar um utilizador SFTP e definir uma palavra-passe, prima a tecla **Enter** ou a tecla para baixo em *Estado* do utilizador. Premir a barra de espaço permite-lhe atualizar ou eliminar um utilizador existente. Para desativar um utilizador SFTP, selecione **Eliminar** depois de selecionar utilizador e, em seguida, selecione **Sim** no ecrã de confirmação SFTP.
3 Introduza um nome de utilizador e palavra-passe para o utilizador SFTP.

   As palavras-passe devem incluir o seguinte:

   - Pelo menos 8 caracteres
   - Pelo menos 1 letra maiúscula
   - Pelo menos 1 número
   - Pelo menos 1 carácter especial
4 Quando terminar de introduzir utilizadores de SFTP, selecione **Aplicar**.

Ativar SSH

Esta tarefa pode ser realizada em qualquer momento. Não é necessário começar a utilizar Security Management Server Virtual.

Pode ativar o SSH para o início de sessão do administrador de suporte, o acesso à shell e a interface de linha de comandos do terminal.

1 No menu de *Configuração básica*, selecione **SSH**.
2 Realce o utilizador para o qual pretende ativar o SSH, pressione a barra de espaços para introduzir um **X** e selecione **OK**.

Iniciar ou parar serviços

Realize esta tarefa apenas se tal for necessário.

1 Para iniciar ou parar simultaneamente todos os serviços, a partir do menu *Configuração básica*, selecione **Iniciar aplicação** ou **Parar aplicação**.
2 No pedido de confirmação, selecione **Sim**.

> **NOTA:**
> As alterações ao estado do servidor podem demorar até dois minutos a serem concluídas.

Reiniciar o dispositivo

Realize esta tarefa apenas se tal for necessário.

1 No menu *Configuração básica*, selecione **Reiniciar dispositivo**.
2 No pedido de confirmação, selecione **Sim**.
3 Após o reinício, inicie sessão no Security Management Server Virtual.

Encerrar dispositivo

Realize esta tarefa apenas se tal for necessário.

1 No menu *Configuração Básica*, desloque para baixo e selecione **Encerrar dispositivo**.
2 No pedido de confirmação, selecione **Sim**.
3 Após o reinício, inicie sessão no Security Management Server Virtual.

Tarefas de configuração avançada do terminal

É possível aceder às tarefas de configuração avançadas a partir do menu principal.

Configurar rotação de registos

> **NOTA: As instruções abaixo definem a rotação de registos para aplicações no Dell Security Management Server Virtual que suportam rotação de registos.**

Esta tarefa pode ser realizada em qualquer momento. Não é necessário começar a utilizar Security Management Server Virtual.

A rotação de registos diária está ativada por predefinição. Para alterar a rotação de registos predefinida, no menu *Configuração avançada*, selecione **Configuração de rotação de registos**.

Para desativar a rotação de registos, utilize a barra de espaços para introduzir um **X** em *Sem rotação* e selecione **OK**.

Para ativar a rotação de registos, siga estes passos:

1 Para ativar rotação diária, semanal ou mensal, utilize a barra de espaço para introduzir um **X** no campo adequado. Para uma rotação semanal, utilize o menu pendente para selecionar o dia da semana adequado. Para uma rotação mensal, introduza o dia do mês adequado.
2 Introduza uma hora para a rotação em *Hora de rotação de registos*.
3 Selecione **OK**.

Cópia de Segurança e Restauro

As cópias de segurança podem ser configuradas ou realizadas em qualquer altura e não é necessário começar a utilizar o Security Management Server Virtual. A Dell recomenda a configuração de um processo de realização de cópias de segurança frequente. Para obter mais informações, consulte http://www.dell.com/support/article/us/en/19/sln304943/how-to-back-up-and-restore-dell-security-management-server-virtual-dell-data-protection-virtual-edition?lang=en

Quando armazenadas no Dell Server e o disco atinge uma capacidade de 90 por cento, não são armazenadas cópias de segurança novas. Se tiver configurado as notificações por e-mail, irá receber uma notificação por e-mail que indica que a alocação de espaço em disco é reduzida.

NOTA:
Para preservar espaço na partição do disco e prevenir a eliminação automática das cópias de segurança, remova as cópias de segurança desnecessárias do armazenamento.

As cópias de segurança são executadas diariamente, por predefinição. A Dell recomenda armazenar as cópias de segurança num servidor FTP seguro externo numa frequência que cumpra os requisitos da organização para cópias de segurança e uso apropriado de espaço de armazenamento.

Para configurar um agendamento de cópias de segurança, no menu *Configuração avançada*, selecione **Realizar cópia de segurança e restauro > Configuração** e siga estes passos:

1 Para ativar cópias de segurança diárias, semanais ou mensais, utilize a barra de espaços para introduzir um **X** no campo adequado. Para cópias de segurança semanais ou mensais, introduza o dia da semana ou o mês adequado como um numeral em que Segunda-feira = 1. Para desativar as cópias de segurança, utilize a barra de espaços para introduzir um **X** em *Sem cópias de segurança* e selecione **OK**.
2 Introduza uma hora para a execução da cópia de segurança em *Hora da cópia de segurança*.
3 Selecione **OK**.

Para realizar uma cópia de segurança manual, no menu *Configuração avançada* selecione **Realizar cópia de segurança e restauro - Realizar cópia de segurança agora**. Quando a confirmação da realização da cópia de segurança for apresentada, selecione **OK.**

NOTA:
Antes de começar uma operação de restauro, todos os serviços do Dell Server terão de estar em execução. Verificar estado do servidor. Se não estão em execução todos os serviços, reinicie os serviços. Para mais informações, consulte Iniciar ou parar serviços. Inicie o restauro ***apenas*** quando ***todos*** os serviços estiverem em execução.

Para restaurar a partir de uma cópia de segurança, no menu *Configuração avançada*, selecione **Realizar cópia de segurança e restauro > Restauro** e, em seguida, selecione o ficheiro de cópia de segurança a ser restaurado. No ecrã de confirmação, selecione **Sim**.

A cópia de segurança é restaurada após a reinicialização.

Armazenar cópias de segurança num servidor FTP seguro

Para armazenar cópias de segurança num servidor FTP, o cliente de FTP precisa de suportar SFTP na porta 22.

De acordo com os requisitos de cópias de segurança da organização, as cópias de segurança podem ser transferidas das seguintes formas:

- Manualmente
- Através de um script automatizado
- Através da solução de cópia de segurança aprovada da organização

Para transferir cópias de segurança utilizando a solução de cópia de segurança da organização, obtenha instruções detalhadas do seu vendedor da solução de cópia de segurança.

NOTA:
O Dell Server baseia-se no Linux Debian Ubuntu x64.

Inicie sessão no Dell Server como dellsupport e utilize o comando `sudo` para configurar a sua solução de cópia de segurança:

`sudo` <instruções do vendedor da solução de cópia de segurança>

Realize cópias de segurança das seguintes pastas:

/backup (necessário)

/certificates (altamente recomendado)

/support (opcional)

Quando o processo de sudo estiver concluído escreva **exit** e pressione **Enter** até que o comando de início de sessão seja apresentado.

Configurar definições SMTP

Para receber notificações por e-mail **ou** para utilizar o Data Guardian, siga os passos indicados nesta secção para configurar as definições SMTP. As notificações por e-mail informam os destinatários sobre os erros de estado do Dell Server, as atualizações de palavras-passe, a disponibilidade de atualizações do Dell Server e problemas relativos a licenças de cliente.

Reiniciar os serviços sempre que é realizada uma alteração nas definições constitui uma boa prática.

Para configurar definições SMTP, siga estes passos:

1. No menu *Configuração avançada*, selecione **Notificações por e-mail**.
2. No ecrã de Notificações por e-mail, para ativar os alertas por e-mail, pressione a barra de espaços para introduzir um **X** em *Ativar alertas por e-mail*.
3. Introduza o nome de domínio totalmente qualificado do Servidor de SMTP.
4. Introduza a porta SMTP.
5. Introduza o Utilizador de SMTP
6. Introduza a Palavra-passe de SMTP
7. Em *Enviar notificações de*, introduza a ID da conta de e-mail para enviar as notificações por e-mail.
8. Em *Enviar estado de servidor para*, introduza uma ID de conta de e-mail para enviar as notificações do estado do servidor. Os destinatários devem ser separados por vírgulas ou ponto e vírgula.
9. Em *Enviar alterações de palavra-passe para*, introduza uma ID de conta de e-mail para enviar as notificações de alterações de palavra-passe.
10. Em *Enviar atualizações de software para*, introduza uma ID de conta de e-mail para enviar as notificações de atualização de software.
11. Em *Lembrete de alerta de serviço*, para ativar os lembretes, pressione a barra de espaços para introduzir um **X** e, em seguida, defina o intervalo dos lembretes em minutos. Um Lembrete de alerta de serviço é acionado depois de decorrido o intervalo de lembretes, após o envio de uma notificação acerca de um problema de estado de funcionamento do sistema, e o anfitrião ou o serviço continuarem a permanecer no mesmo estado.
12. No campo *Relatório de resumo*, para ativar os relatórios de notificações, selecione o intervalo desejado (diário, semanal ou mensal) e, em seguida, pressione a barra de espaços para introduzir um **X**.

13 Selecione **OK**.

Importar um certificado existente ou inscrever um novo certificado de servidor

Pode importar um certificado existente ou criar um pedido de certificação através do Security Management Server Virtual.

Reiniciar os serviços sempre que é realizada uma alteração nas definições constitui uma boa prática.

Importar um certificado de servidor existente

1 Exporte o certificado existente e a cadeia de certificação da sua keystore.

> **NOTA: Guarde a palavra-passe de exportação pois deverá introduzi-la quando importar o certificado no Security Management Server Virtual.**

2 No servidor FTP do Dell Server, guarde o certificado em **/certificates**.

3 No menu *Configuração avançada*, selecione **Certificados de servidor**.

4 Selecione **Importar certificado existente.**

5 Selecione um ficheiro de certificado a ser instalado no Dell Server.

6 Quando for solicitado, introduza a palavra-passe de exportação de certificado e selecione **OK**.

7 Quando a importação estiver concluída, selecione **OK**.

> **NOTA: Para mais informações, consulte http://www.dell.com/support/article/us/en/19/sln302996/dell-data-protection-virtual-edition-dell-security-management-server-virtual-manual-csr-creation-and-certificate-import?lang=en**

Inscrever um certificado de servidor novo

1 No menu *Configuração avançada*, selecione **Certificados de servidor**.

2 Selecione **Novo certificado de servidor.**

3 Selecione **Criar pedido de certificado.**

4 Preencha os campos *Gerar pedido de certificado*:

- Nome do País: Código de país de duas letras.
- Estado/Região: Introduza o nome não abreviado do estado ou da região (por exemplo, Mondego).
- *Nome da localidade/cidade* Introduza o valor apropriado (por exemplo, Lisboa).
- Organização: introduza o valor apropriado (por exemplo, Dell).
- Unidade organizacional: Introduza o valor adequado (por exemplo, Segurança).
- *Nome comum*: introduza o nome de domínio completamente qualificado do Dell Server. Este nome completamente qualificado inclui o nome do anfitrião e o nome do domínio (exemplo: server.domain.com).
- ID de e-mail: Introduza o endereço de correio eletrónico para o qual o seu CSR será enviado.

5 Siga o seu processo organizacional para adquirir um certificado do servidor SSL de uma Autoridade de certificação. Envie os conteúdos do ficheiro CSR para assinatura.

6 Quando receber o certificado assinado, exporte-o como ficheiro .p7b e transfira a cadeia de certificação completa no formato .der.

7 Faça cópias de segurança do certificado e cadeia de certificação.

8 Carregue o ficheiro do certificado e respetiva cadeia de certificação completa para o servidor FTP do Dell Server.

9 No menu *Configuração avançada*, selecione **Certificados de servidor**.

10 Selecione **Novo certificado de servidor.**

11 Selecione `Completar inscrição de certificado`.

12 Selecione o ficheiro de certificado a ser instalado no Dell Server.

13 Se solicitado, introduza a Palavra-passe do certificado: **changeit**.

Para ativar a validação de confiança em clientes de Encriptação de funcionamento em Windows, consulte Ativar a verificação de cadeia de certificação do gestor.

Criar e instalar um certificado autoassinado

NOTA: Os certificados autoassinados gerados por predefinição são gerados durante 10 anos.

1 No menu *Configuração avançada* do Dell Server, selecione **Certificados do servidor**.

2 Selecione **Criar e instalar certificado autoassinado.**

3 Para confirmar que deseja substituir o certificado pré-instalado por um novo certificado, clique em **Sim**.

4 Introduza a Palavra-passe do certificado: **changeit**.

5 Após a instalação do novo certificado, selecione **OK** e aguarde até que os serviços sejam reiniciados.

Os serviços reiniciam-se automaticamente.

Ativar o acesso à base de dados

Esta tarefa pode ser realizada em qualquer momento. Não é necessário começar a utilizar Security Management Server Virtual.

NOTA: A Dell recomenda que ative o acesso à base de dados apenas se for necessário e que o desative quando não for necessário.

1 No menu *Configuração avançada*, selecione **Acesso à base de dados**.

2 Utilize a barra de espaços para introduzir um **X** no campo *Ativar acesso à base de dados* e selecione **OK**. Se a palavra-passe da base de dados ainda não tiver sido configurada, é apresentado um pedido de palavra-passe da base de dados.

3 Introduza a palavra-passe da base de dados.

4 Introduza novamente a palavra-passe da base de dados.

Os componentes da aplicação Dell Data Security param automaticamente.

Definir ou alterar o idioma do terminal

Reiniciar os serviços sempre que é realizada uma alteração nas definições constitui uma boa prática.

1 No Menu principal, selecione **Definir idioma**.

2 Utilize as teclas de seta para selecionar o idioma da sua preferência.

Ver registos

Para verificar os seguintes registos, selecione **Ver registos** no menu principal.

- Registos do sistema
  - Registo Syslog
  - Registo de correio
  - Registo Auth (SSH)
  - Registo Postgres
  - Registo de monitorização

- Registos de servidor
  - Message Broker
  - Identity Server
  - Compatibility Server
  - Security Server
  - Compliance Reporter
  - Core Server
  - Core Server HA
  - Inventory Server
  - Forensic Server
  - Policy Proxy
- Consola de administração
  - pybackup.log
  - pyconsole.log
  - pydatabase.log
  - update.log
- Registo do personalizador de bases de dados

NOTA: Para navegar através deste ecrã, utilize o seguinte:

- Para ir para o fim do registo, mantenha premida a tecla alt direita e, em seguida, prima a tecla "/" no teclado
- Para sair do registo, mantenha premido a tecla ctrl esquerda e prima "x" no teclado.
- as teclas de seta permitem a navegação.
- as teclas página para cima e página para baixo percorrem as páginas para cima e para baixo, uma de cada vez.
- a barra de espaços avança nos registos página a página.

Abrir a interface de linha de comandos

Para abrir a interface de linha de comandos, selecione **Iniciar a shell** no menu principal.

Para sair da interface de linha de comandos, escreva **exit** e pressione **Enter**.

Gerar um Registo de Instantâneo do Sistema

Para gerar um Registo de instantâneo do sistema para o Dell ProSupport, selecione **Ferramentas de suporte** no menu principal.

1 No menu *Ferramentas de suporte*, selecione **Gerar registo de instantâneo do sistema**.
2 Na indicação de que o ficheiro foi criado, selecione **OK**.

3

Manutenção

Remova as cópias de segurança desnecessárias do Security Management Server Virtual.

Apenas as dez cópias de segurança mais recentes são retidas. Se o espaço disponível na partição de disco for igual ou inferior a dez por cento, não serão armazenadas mais cópias de segurança. Se isto acontecer, receberá uma notificação por correio electrónico indicando que a alocação de espaço em disco é reduzida.

4

Resolução de problemas

Se ocorrer um erro, e tiver notificações por correio eletrónico configuradas, receberá uma notificação por correio eletrónico. Com base nas informações da notificação por correio eletrónico, siga estes passos:

1 Verifique os ficheiros de registo aplicáveis.
2 Reinicie serviços, conforme necessário. Reiniciar os serviços sempre que é realizada uma alteração nas definições constitui uma boa prática.
3 Gerar um registo instantâneo do sistema.
4 Contacte o Dell ProSupport. Para mais informações, consulte Contacte o Dell ProSupport.

5

Configuração de Pós-instalação

Após a instalação, alguns componentes do seu ambiente podem necessitar de ser configurados com base na solução Dell Data Security utilizada pela sua organização.

Depois de instalar o Security Management Server Virtual, devem ser alteradas as seguintes predefinições:

- Altere a palavra-passe do servidor de back-end na seguinte localização:

  `C:\Program Files\Dell\Enterprise Edition\Message Broker\conf\application.properties`

- Altere a palavra-passe para cada servidor de front-end no seu ambiente na seguinte localização:

  `C:\Program Files\DELL\Enterprise Edition\Beac\conf\application.properties`

A palavra-passe é apresentada da seguinte forma: `proxy-server.password=ENC(<texthere>)`

Para alterar a palavra-passe:

1 Selecione: `ENC(<texthere>)`

2 Altere o texto selecionado para: `CLR(<newpasswordhere>)`

Depois de reiniciar o serviço, a linha modificada é alterada para `ENC` de `CLR` e a palavra-passe é encriptada.

NOTA: é possível modificar o nome de utilizador do servidor proxy. No entanto, este deve corresponder ao ficheiro de propriedades da aplicação Message Broker e a todos os servidores de front-end ativos.

Configuração do Data Guardian

Para configurar o Dell Server para suportar o Data Guardian, na Management Console defina as uma ou ambas as políticas como **Ligadas**: *Documentos do Office protegidos* e *Encriptação na nuvem*.

Para obter instruções sobre como instalar o cliente Data Guardian, consulte o *Guia do administrador do Data Guardian* ou o *Guia do utilizador do Data Guardian*. Recomenda-se que os Administradores ativem o SMTP para permitir que o Dell Data Guardian envie e-mails para os utilizadores externos e para facilitar a gestão de chaves para os criadores.

Validar a verificação de cadeia de certificação do gestor

Se for utilizado um certificado autoassinado no Security Management Server Virtual para SED ou BitLocker Manager, a validação de certificação SSL/TLS deve manter-se ***desativada*** no computador cliente. Antes de ativar a validação de confiança SSL/TLS no computador cliente, os requisitos seguintes devem ser cumpridos:

- Deve ser importado um certificado assinado por uma autoridade raiz (por exemplo, EnTrust ou Verisign) para o Dell Server. Consulte Importar um certificado existente ou inscrever um novo certificado de servidor.
- A cadeia de confiança completa do certificado deve ser armazenada na keystore da Microsoft no computador cliente.

Para desativar a validação de confiança SSL/TLS no computador cliente, altere o valor da seguinte entrada de registo para 1:

[HKLM\System\CurrentControlSet\Services\DellMgmtAgent\Parameters]

DisableSSLCertTrust=REG_DWORD (32-bit):1

6

Tarefas do administrador da Management Console

Atribuir o papel de administrador da Dell

1 Inicie sessão na Management Console como administrador do Security Management Server Virtual: https://server.domain.com:8443/webui/. As credenciais predefinidas são **superadmin/changeit**.

2 No painel esquerdo, clique em **Populações** > **Domínios**.

3 Clique num domínio para adicionar um utilizador.

4 Na página Detalhe do domínio, clique no separador **Membros**.

5 Clique em **Adicionar utilizador**.

6 Introduza um filtro para pesquisar o nome de utilizador por Nome comum, Nome principal universal ou sAMAccountName. O carácter universal é *.

Tem de ser definido no servidor de diretório da empresa um Nome comum, Nome principal universal ou sAMAccountName para cada utilizador. Se um utilizador for membro de um Domínio ou Grupo mas não aparecer na lista de Membros do Domínio ou Grupo em Management Console, certifique-se de que os três nomes estão definidos de forma adequada para o utilizador no servidor de diretório da empresa.

A consulta irá procurar automaticamente por nome comum, UPN e nome sAMAccount, por esta ordem, até ser encontrada uma correspondência.

7 Selecione os utilizadores na *Lista de utilizadores do diretório* para adicionar ao domínio. Utilize <Shift><click> ou <Ctrl><click> para selecionar múltiplos utilizadores.

8 Clique em **Adicionar**.

9 Na barra de menus, clique no separador **Detalhes e ações** do utilizador especificado.

10 Desloque-se na barra de menus e selecione o separador **Administração**.

11 Selecione os papéis do administrador a adicionar a este utilizador.

12 Clique em **Guardar**.

Iniciar uma sessão com o Papel de administrador da Dell

1 Termine sessão na Management Console.

2 Inicie sessão na Management Console e inicie sessão com as credenciais de utilizador do domínio.

Clique em "?" no canto superior direito da Management Console para iniciar a *AdminHelp*. É apresentada a página *Como começar*. Clique em **Adicionar domínios**.

Foram definidas políticas de base para a sua organização mas estas devem ser modificadas consoante as suas necessidades específicas, da seguinte forma (as licenças e elegibilidades guiam todas as ativações):

- A Policy Based Encryption será ativada com a encriptação de Chave comum
- Os computadores com unidades de encriptação automática serão encriptados
- A gestão do BitLocker não está ativada
- O Advanced Threat Prevention não está ativado
- O Threat Protection está desativado
- Os suportes multimédia externos não serão encriptados

- As portas não serão geridas pelo Controlo de portas
- Os dispositivos com a Full Disk Encryption instalada não serão encriptados
- O Data Guardian está desativado

Consulte o tópico *Gerir políticas* em AdminHelp para obter descrições da política.

Consolidar políticas

Consolide políticas quando a instalação estiver concluída.

Para consolidar políticas após a instalação ou, posteriormente, após as modificações de políticas serem guardadas, siga estes passos:

1 No painel da esquerda, clique em **Gestão** > **Consolidar**.
2 Em *Comentário*, introduza uma descrição da alteração.
3 Clique em **Consolidar políticas**.

7

Portas

A tabela seguinte descreve cada componente e a sua função.

Nome	Porta predefinida	Descrição
ACL Service	TCP/ 8006	Gere várias permissões e o acesso de grupo para vários produtos Dell Security.
Compliance Reporter	HTTP(S)/ 8084	Oferece uma visão abrangente do ambiente, tendo em vista a elaboração de relatórios de auditoria e conformidade.
Management Console	HTTPS/ 8443	Consola de administração e centro de controlo para implementação na empresa inteira.
Core Server	HTTPS/ 8887 (fechada)	Gere o fluxo das políticas, as licenças e o registo para PBA (Preboot Authentication), SED Management, BitLocker Manager, Threat Protection e Advanced Threat Prevention. Processa dados de inventário para utilização pelo Compliance Reporter e pela Management Console. Reúne e armazena os dados de autenticação. Controla o acesso baseado em funções.
Core Server HA (Elevada Disponibilidade)	HTTPS/ 8888	Um serviço de elevada disponibilidade que permite o aumento da segurança e do desempenho das ligações HTTPS com a Management Console, Preboot Authentication, SED Management, FDE, BitLocker Manager, Threat Protection e Advanced Threat Prevention.
Security Server	HTTPS/ 8443	Comunica com o Policy Proxy; gere obtenções de chaves forenses, ativações de clientes, produtos Data Guardian e comunicação SED-PBA.
Compatibility Server	TCP/ 1099 (fechada)	Um serviço para gerir a arquitetura empresarial. Reúne e armazena os dados de inventário iniciais durante a ativação e os dados de políticas durante as migrações. Processa os dados com base nos grupos de utilizadores.
Message Broker Service	TCP/ 61616 (fechada) e STOMP/ 61613 (fechada ou, se configurado para DMZ, 61613 está aberta)	Trata da comunicação entre serviços do Dell Server. Prepara as informações de políticas criadas pelo Compatibility Server para colocação em fila de Policy Proxy.
Identity Server	8445 (fechada)	Trata dos pedidos de autenticação de domínio, incluindo a autenticação de SED Management.

Nome	Porta predefinida	Descrição
Forensic Server	HTTPS/ 8448	Permite que os administradores com privilégios adequados obtenham chaves encriptadas da Management Console para utilizar no desbloqueio de dados ou nas tarefas de desencriptação. Necessário para API forense.
Inventory Server	8887	Processa a fila de inventário.
Policy Proxy	TCP/ 8000	Oferece uma linha de comunicação com base na rede de forma a proporcionar atualizações de políticas de segurança e atualizações de inventário. Necessário para Encryption Enterprise (Windows e Mac)
PostGres	TCP/ 5432	Base de dados local utilizada para dados de eventos.
LDAP	389/636, 3268/3269 RPC - 135, 49125+	Porta 389 - Esta porta é utilizada para o pedido de informações a partir do controlador de domínio local. Os pedidos de LDAP enviados à porta 389 podem ser utilizados para procurar objetos apenas dentro do domínio raiz do catálogo global. No entanto, a aplicação requerente pode obter todos os atributos para esses objetos. Por exemplo, um pedido na porta 389 poderia ser utilizado para obter um departamento de utilizador. Porta 3268 - Esta porta é utilizada para consultas especificamente direcionadas para o catálogo global. Os pedidos de LDAP enviados à porta 3268 podem ser utilizados para procurar objetos na floresta inteira. No entanto, apenas os atributos marcados para replicação para o catálogo global podem ser devolvidos. Por exemplo, um departamento de utilizador não poderia ser devolvido utilizando a porta 3268 uma vez que este atributo não é replicado para o catálogo global.
Client Authentication	HTTPS/ 8449	Permite aos servidores de cliente autenticarem com o Dell Server. Necessário para Server Encryption
Beacon de chamada de retorno	HTTP/TCP 8446	Num servidor front-end, isto permite que um sinalizador de chamada de retorno seja inserido em cada ficheiro protegido do Office ao executar o modo protegido do Office do Data Guardian.