Dell Data Protection

Guia de migração e instalação do Enterprise Server v9.7

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.

Guia de migração e instalação do Enterprise Server

2017 - 04

Rev. A01

Índice

1

Introdução ao Dell Enterprise Server

Acerca do Dell Enterprise Server

O Enterprise Server é a porção de administração de segurança da solução Dell. A Remote Management Console permite aos administradores monitorizar o estado dos endpoints, da aplicação de políticas e da proteção em toda a empresa.

O Enterprise Server tem as seguintes funções:

- Gestão centralizada de 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

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 Data Protection.

Adicionalmente, o suporte online para os produtos Dell Data Protection 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 disponível quando nos contactar.

Para número de telefone fora dos Estados Unidos, consulte Dell ProSupport International Phone Numbers (Números de telefone internacionais do Dell ProSupport).

Requisitos e Arquitetura do Dell Enterprise Server

Esta secção especifica os requisitos de hardware e software e recomendações de projeto para implementações do Dell Data Protection.

Requisitos do Dell Enterprise Server

Os componentes do Dell Enterprise Server têm requisitos de hardware e software complementares ao software fornecido no suporte multimédia de instalação da Dell. Certifique-se de que o ambiente de instalação cumpre os requisitos antes de continuar as tarefas de instalação ou atualização/migração.

Antes de iniciar a instalação, certifique-se que são realizadas todas as atualizações e aplicações de patches em todos os servidores utilizados na instalação.

Pré-requisitos do Dell Enterprise Server

A tabela seguinte descreve pormenorizadamente o software que deve existir antes de instalar o Dell Enterprise Server. As ligações e instruções para instalar estes pré-requisitos são apresentadas em Configuração de Pré-instalação.

Todos os itens de software terão de ser instalados antes de iniciar a instalação, salvo se for indicado que o programa de instalação procede à instalação deste itens. Caso contrário, a instalação fracassará.

Hardware do Dell Enterprise Server

Pré-requisitos

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

  Se não estiver instalado, o instalador irá fazê-lo por si.
- **Pacote Redistribuível do Visual C++ 2013**

  Se não estiver instalado, o instalador irá fazê-lo por si.
- **Pacote Redistribuível do Visual C++ 2015**

  Se não estiver instalado, o instalador irá fazê-lo por si.
- **.NET Framework Versão 3.5 SP1**
- **.NET Framework Versão 4.5**

  A Microsoft publicou atualizações de segurança para o .NET Framework Version 4,5.
- **SQL Native Client 2012**

  Se utilizar o SQL Server 2012 ou o SQL Server 2016.

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

A tabela seguinte descreve pormenorizadamente os requisitos *mínimos* de hardware para o Dell Enterprise Server. Consulte Arquitetura do Dell Enterprise Server para obter informações adicionais sobre o dimensionamento com base no tamanho da sua implementação.

Requisitos de Hardware

Processador

CPU Dual-Core moderna mínima (2 GHz+), incluindo Core Duo, Core 2 Duo, Core i3, Core i5, Core i7, Xeon, Itanium ou equivalente a AMD

CPU Quad-Core moderna (2 GHz+) para configuração de servidor único

RAM

Mínimo de 8 GB, consoante a configuração

16 GB para configuração de servidor único

Espaço livre em disco

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

20 GB ou mais de espaço livre em disco (mais espaço de paginação virtual) para configuração de servidor único

Placa de rede

Placa de interface de rede 10/100/1000

Diversos

TCP/IPv4 instalado e ativado

Software do Dell Enterprise Server

A tabela seguinte descreve pormenorizadamente os requisitos de software para o Dell Enterprise Server e servidor proxy.

NOTA: O UAC terá de ser desativado antes da instalação. O servidor tem de ser reiniciado para que esta alteração seja implementada. No Windows Server 2012 R2 e no Windows Server 2016, o programa de instalação desativa o UAC.

NOTA: Localização dos registos do Dell Policy Proxy (se instalado): HKLM\SOFTWARE\Wow6432Node\Dell

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

Dell Enterprise Server - Servidor de back-end e Servidor Dell de front-end

- **Windows Server 2008 R2 SP0-SP1 de 64 bits**
  - Standard Edition
  - Enterprise Edition
- **Windows Server 2008 SP2 de 64 bits**
  - Standard Edition
  - Enterprise Edition
- **Windows Server 2012 R2**
  - Standard Edition
  - Datacenter Edition
- **Windows Server 2016**
  - Standard Edition

- Datacenter Edition

Servidores Exchange ActiveSync

Se pretender utilizar a Mobile Edition, são suportados os seguintes servidores Exchange ActiveSync. Este componente está instalado no seu Exchange Server de front-end.

- Exchange ActiveSync 12.0 – um componente do Exchange Server 2007
- Exchange ActiveSync 12.1 – um componente do Exchange Server 2007 SP1
- Exchange ActiveSync 14.0 – um componente do Exchange Server 2010
- Exchange ActiveSync 14.1 – um componente do Exchange Server 2010 SP1

Microsoft Message Queuing (MSMQ) tem de estar instalado/configurado no Exchange Server.

Repositório LDAP

- Active Directory 2008
- Active Directory 2008 R2
- Active Directory 2012

Ambientes virtuais recomendados para os componentes do Dell Enterprise Server

O Dell Enterprise Server pode opcionalmente ser instalado num ambiente virtual. Apenas são recomendados os seguintes ambientes.

O Dell Enterprise Server v9.7 foi validado com Hyper-V Server (instalação completa ou essencial), e como uma Função no Windows Server 2012 R2 ou Windows Server 2016.

- Servidor Hyper-V (instalação completa ou essencial)
  - Necessário CPU de 64 bits x86
  - Computador anfitrião com pelo menos dois núcleos
  - Recomendado um mínimo de 8 GB de RAM
  - Não é necessário um sistema operativo
  - O hardware deve cumprir os requisitos mínimos do Hyper-V
  - RAM mínima de 4 GB para recurso de imagem dedicado
  - Deve ser executado como uma máquina virtual de 1.ª geração
  - Consulte https://technet.microsoft.com/en-us/library/hh923062.aspx para obter mais informações

O Dell Enterprise Server v9.7 foi validado com o VMware ESXi 5.5 e VMware ESXi 6.0. Certifique-se de que todos os patches e atualizações são aplicados de imediato ao VMware ESXi de modo a resolver potenciais vulnerabilidades.

NOTA: Se estiver a executar o VMware ESXi e o Windows Server 2012 R2 ou o Windows Server 2016, recomenda-se a utilização de adaptadores Ethernet VMXNET3.

- VMware ESXi 5.5
  - Necessário CPU de 64 bits x86
  - Computador anfitrião com pelo menos dois núcleos
  - Recomendado um mínimo de 8 GB de RAM
  - Não é necessário um sistema operativo
  - Consulte http://www.vmware.com/resources/compatibility/search.php para obter uma lista completa dos sistemas operativos anfitriões compatíveis
  - O hardware deve cumprir os requisitos mínimos do VMware
  - RAM mínima de 4 GB para recurso de imagem dedicado
  - Consulte http://pubs.vmware.com/vsphere-55/index.jsp para obter mais informações
- VMware ESXi 6.0
  - Necessário CPU de 64 bits x86

- Computador anfitrião com pelo menos dois núcleos
- Recomendado um mínimo de 8 GB de RAM
- Não é necessário um sistema operativo
- Consulte http://www.vmware.com/resources/compatibility/search.php para obter uma lista completa dos sistemas operativos anfitriões compatíveis
- O hardware deve cumprir os requisitos mínimos do VMware
- RAM mínima de 4 GB para recurso de imagem dedicado
- Consulte http://pubs.vmware.com/vsphere-60/index.jsp para obter mais informações

NOTA: A base de dados do SQL Server que aloja o Dell Enterprise Server deve ser executada num computador independente.

Base de dados

- **SQL Server 2008 e SQL Server 2008 R2 -** Standard Edition/Enterprise Edition
- **SQL Server 2008 SP4 (com KB3045311) -** Standard Edition/Enterprise Edition
- **SQL Server 2012 -** Standard Edition/Business Intelligence/Enterprise Edition
- **SQL Server 2014 -** Standard Edition/Business Intelligence/Enterprise Edition
- **SQL Server 2016 -** Standard Edition/Enterprise Edition

NOTA: Express Editions não são suportadas para ambientes de produção. Express Editions podem ser utilizadas apenas em POC e avaliações.

Dell Data Protection Remote Management Console e Compliance Reporter

- Internet Explorer 11.x ou posterior
- Mozilla Firefox 41.x ou posterior
- Google Chrome 46.x ou posterior

NOTA: O browser tem de aceitar cookies.

Suporte de idiomas do Dell Enterprise Server

A Remote Management Console está em conformidade com a norma MUI (Multilingual User Interface - Interface de utilizador multilíngue) e suporta os seguintes idiomas:

Suporte de idiomas	
EN - Inglês	JA - Japonês
ES - Espanhol	KO - Coreano
FR - Francês	PT-BR - Português, Brasil
IT - Italiano	PT-PT - Português, Portugal (Ibérico)
DE - Alemão	

Arquitetura do Dell Enterprise Server

As soluções Dell Encryption, Endpoint Security Suite, Endpoint Security Suite Enterprise e Data Guardian são produtos altamente dimensionáveis, dimensionados de acordo com o tamanho da sua organização e do número de pontos finais pretendidos para encriptação. Esta secção oferece um conjunto de diretrizes para dimensionar a arquitetura desde 5000 até 60 000 endpoints.

NOTA: Se a organização tiver mais de 50 000 endpoints, contacte o Dell ProSupport para obter assistência.

NOTA:

Cada componente listado em cada secção inclui as especificações mínimas de hardware, que são necessárias para garantir um desempenho ótimo na maioria dos ambientes. A não atribuição dos recursos adequados a algum destes componentes pode causar a degradação do desempenho ou problemas de funcionamento da aplicação.

Até 5000 endpoints

Esta arquitetura acomoda a maioria das empresas de pequenas a médias dimensões, variando entre 1 e 5000 endpoints. Todos os componentes do Dell Enterprise Server podem ser instalados num único servidor. Opcionalmente, pode ser colocado um servidor de front-end no DMZ para publicar políticas e/ou ativar endpoints através da Internet.

Componentes da arquitetura

Dell Enterprise Server

Windows Server 2008 R2 SP0-SP1 de 64 bits/Windows Server 2008 SP2 de 64 bits - Standard Edition ou Enterprise Edition

Windows Server 2012 R2 - Standard Edition ou Datacenter Edition

Windows Server 2016 - Standard Edition ou Datacenter Edition

Configuração de servidor único

16 GB; 20 GB ou mais de espaço livre em disco (mais espaço de paginação virtual); CPU Quad-Core moderna (2 GHz+)

Configuração do servidor quando utilizado com um servidor front-end

Mínimo de 8 GB, consoante a configuração; +/-1,5 GB de espaço livre em disco (mais espaço de paginação virtual); CPU Dual-Core moderna mínima (2 GHz+), incluindo Core Duo, Core 2 Duo, Core i3, Core i5, Core i7, Xeon, Itanium ou equivalente a AMD

Servidor Dell de front-end externo

Windows Server 2008 R2 SP0-SP1 de 64 bits/Windows Server 2008 SP2 de 64 bits - Standard Edition ou Enterprise Edition

Windows Server 2012 R2 - Standard Edition ou Datacenter Edition

Windows Server 2016 - Standard Edition ou Datacenter Edition

Mínimo de 8 GB, consoante a configuração; +/-1,5 GB de espaço livre em disco (mais espaço de paginação virtual); CPU Dual-Core moderna mínima (2 GHz+), incluindo Core Duo, Core 2 Duo, Core i3, Core i5, Core i7, Xeon, Itanium ou equivalente a AMD

SQL Server

SQL Server 2008, SQL Server 2008 R2 e SQL Server 2008 SP4 (com KB3045311) Standard Edition/Enterprise Edition

SQL Server 2012 Standard Edition/Business Intelligence/Enterprise Edition

SQL Server 2014 Standard Edition/Business Intelligence/Enterprise Edition

SQL Server 2016 Standard Edition/Enterprise Edition

5000 - 20 000 endpoints

Esta arquitetura acomoda ambientes com 5000 a 20 000 endpoints. É adicionado um servidor de front-end para distribuir a carga adicional e preparado para trabalhar com aproximadamente 15 000 a 20 000 endpoints. Opcionalmente, pode ser colocado um servidor de front-end no DMZ para publicar políticas e/ou ativar endpoints através da Internet.

Componentes da arquitetura

Dell Enterprise Server

Mínimo de 8 GB, consoante a configuração; +/-1,5 GB de espaço livre em disco (mais espaço de paginação virtual); CPU Dual-Core moderna mínima (2 GHz+), incluindo Core Duo, Core 2 Duo, Core i3, Core i5, Core i7, Xeon, Itanium ou equivalente a AMD

Servidor Dell de front-end interno (1) e Servidor Dell de front-end externo (1)

Windows Server 2008 R2 SP0-SP1 de 64 bits/Windows Server 2008 SP2 de 64 bits - Standard Edition ou Enterprise Edition

Windows Server 2012 R2 - Standard Edition ou Datacenter Edition

Windows Server 2016 - Standard Edition ou Datacenter Edition

Mínimo de 8 GB, consoante a configuração; +/-1,5 GB de espaço livre em disco (mais espaço de paginação virtual); CPU Dual-Core moderna mínima (2 GHz+), incluindo Core Duo, Core 2 Duo, Core i3, Core i5, Core i7, Xeon, Itanium ou equivalente a AMD

SQL Server

SQL Server 2008, SQL Server 2008 R2 e SQL Server 2008 SP4 (com KB3045311) Standard Edition/Enterprise Edition

SQL Server 2012 Standard Edition/Business Intelligence/Enterprise Edition

SQL Server 2014 Standard Edition/Business Intelligence/Enterprise Edition

SQL Server 2016 Standard Edition/Enterprise Edition

20 000 - 40 000 endpoints

Esta arquitetura acomoda ambientes com 20 000 a 40 000 endpoints. É adicionado um servidor de front-end para distribuir a carga adicional. Cada servidor de front-end está preparado para trabalhar com aproximadamente 15 000 - 20 000 endpoints. Opcionalmente, pode ser colocado um servidor de front-end no DMZ para ativar endpoints e/ou publicar políticas em endpoints através da Internet.

Componentes da arquitetura

Dell Enterprise Server

Windows Server 2008 R2 SP0-SP1 de 64 bits/Windows Server 2008 SP2 de 64 bits - Standard Edition ou Enterprise Edition

Windows Server 2012 R2 - Standard Edition ou Datacenter Edition

Windows Server 2016 - Standard Edition ou Datacenter Edition

Mínimo de 8 GB, consoante a configuração; +/-1,5 GB de espaço livre em disco (mais espaço de paginação virtual); CPU Dual-Core moderna mínima (2 GHz+), incluindo Core Duo, Core 2 Duo, Core i3, Core i5, Core i7, Xeon, Itanium ou equivalente a AMD

Servidores Dell de front-end internos (2) e Servidor Dell de front-end externo (1)

Windows Server 2008 R2 SP0-SP1 de 64 bits/Windows Server 2008 SP2 de 64 bits - Standard Edition ou Enterprise Edition

Windows Server 2012 R2 - Standard Edition ou Datacenter Edition

Windows Server 2016 - Standard Edition ou Datacenter Edition

Mínimo de 8 GB, consoante a configuração; +/-1,5 GB de espaço livre em disco (mais espaço de paginação virtual); CPU Dual-Core moderna mínima (2 GHz+), incluindo Core Duo, Core 2 Duo, Core i3, Core i5, Core i7, Xeon, Itanium ou equivalente a AMD

SQL Server

SQL Server 2008, SQL Server 2008 R2 e SQL Server 2008 SP4 (com KB3045311) Standard Edition/Enterprise Edition

SQL Server 2012 Standard Edition/Business Intelligence/Enterprise Edition

SQL Server 2014 Standard Edition/Business Intelligence/Enterprise Edition

SQL Server 2016 Standard Edition/Enterprise Edition

40 000 - 60 000 endpoints

Esta arquitetura acomoda ambientes com 40 000 a 60 000 endpoints. É adicionado um servidor de front-end para distribuir a carga adicional. Cada servidor de front-end está preparado para trabalhar com aproximadamente 15 000 - 20 000 endpoints. Opcionalmente, pode ser colocado um servidor de front-end no DMZ para ativar endpoints e/ou publicar políticas em endpoints através da Internet.

NOTA:
Se a organização tiver mais de 50 000 endpoints, contacte o Dell ProSupport para obter assistência.

Componentes da arquitetura

Dell Enterprise Server

Windows Server 2008 R2 SP0-SP1 de 64 bits/Windows Server 2008 SP2 de 64 bits - Standard Edition ou Enterprise Edition

Windows Server 2012 R2 - Standard Edition ou Datacenter Edition

Windows Server 2016 - Standard Edition ou Datacenter Edition

Mínimo de 8 GB, consoante a configuração; +/-1,5 GB de espaço livre em disco (mais espaço de paginação virtual); CPU Dual-Core moderna mínima (2 GHz+), incluindo Core Duo, Core 2 Duo, Core i3, Core i5, Core i7, Xeon, Itanium ou equivalente a AMD

Servidores Dell de front-end internos (2) e Servidor Dell de front-end externo (1)

Windows Server 2008 R2 SP0-SP1 de 64 bits/Windows Server 2008 SP2 de 64 bits - Standard Edition ou Enterprise Edition

Windows Server 2012 R2 - Standard Edition ou Datacenter Edition

Windows Server 2016 - Standard Edition ou Datacenter Edition

Mínimo de 8 GB, consoante a configuração; +/-1,5 GB de espaço livre em disco (mais espaço de paginação virtual); CPU Dual-Core moderna mínima (2 GHz+), incluindo Core Duo, Core 2 Duo, Core i3, Core i5, Core i7, Xeon, Itanium ou equivalente a AMD

SQL Server

SQL Server 2008, SQL Server 2008 R2 e SQL Server 2008 SP4 (com KB3045311) Standard Edition/Enterprise Edition

SQL Server 2012 Standard Edition/Business Intelligence/Enterprise Edition

SQL Server 2014 Standard Edition/Business Intelligence/Enterprise Edition

SQL Server 2016 Standard Edition/Enterprise Edition

Considerações sobre elevada disponibilidade

Esta é uma arquitetura de elevada disponibilidade suportando até 60 000 endpoints. Numa configuração ativa/passiva há dois Dell Enterprise Servers configurados. Para uma ativação pós-falha do segundo Dell Enterprise Server, interrompa os serviços no nó primário e aponte o alias DNS (CNAME) para o segundo nó. Inicie os serviços no segundo nó e arranque a Remote Management Console para se certificar de que a aplicação está a funcionar corretamente. Os serviços no segundo nó (passivo) devem ser configurados como "Manuais" para evitar que os mesmos sejam iniciados acidentalmente durante a manutenção regular e a aplicação de patches.

A organização pode ainda optar por ter um servidor de base de dados SQL Cluster. Nesta configuração, o Dell Enterprise Server deve ser configurado para utilizar o IP ou nome do anfitrião do cluster.

NOTA:
A replicação da base de dados não é suportada.

O tráfego do cliente é distribuído por três servidores de front-end internos. Opcionalmente, podem ainda ser colocados vários servidores de front-end no DMZ para ativar endpoints e/ou publicar políticas em endpoints através da Internet.

Virtualização

O Dell Enterprise Server pode opcionalmente ser instalado num ambiente virtual. Apenas são recomendados os seguintes ambientes.

O Dell Enterprise Server v9.7 foi validado com Hyper-V Server (instalação completa ou essencial), e como uma Função no Windows Server 2012 R2 ou Windows Server 2016.

- Servidor Hyper-V (instalação completa ou essencial)
  - Necessário CPU de 64 bits x86
  - Computador anfitrião com pelo menos dois núcleos
  - Recomendado um mínimo de 8 GB de RAM
  - Não é necessário um sistema operativo
  - O hardware deve cumprir os requisitos mínimos do Hyper-V
  - RAM mínima de 4 GB para recurso de imagem dedicado
  - Deve ser executado como uma máquina virtual de 1.ª geração
  - Consulte https://technet.microsoft.com/en-us/library/hh923062.aspx para obter mais informações

O Dell Enterprise Server v9.7 foi validado com o VMware ESXi 5.5 e VMware ESXi 6.0. Certifique-se de que todos os patches e atualizações são aplicados de imediato ao VMware ESXi de modo a resolver potenciais vulnerabilidades.

NOTA: Se estiver a executar o VMware ESXi e o Windows Server 2012 R2 ou o Windows Server 2016, recomenda-se a utilização de adaptadores Ethernet VMXNET3.

- VMware ESXi 5.5
  - Necessário CPU de 64 bits x86
  - Computador anfitrião com pelo menos dois núcleos
  - Recomendado um mínimo de 8 GB de RAM
  - Não é necessário um sistema operativo
  - Consulte http://www.vmware.com/resources/compatibility/search.php para obter uma lista completa dos sistemas operativos anfitriões compatíveis
  - O hardware deve cumprir os requisitos mínimos do VMware
  - RAM mínima de 4 GB para recurso de imagem dedicado
  - Consulte http://pubs.vmware.com/vsphere-55/index.jsp para obter mais informações
- VMware ESXi 6.0
  - Necessário CPU de 64 bits x86
  - Computador anfitrião com pelo menos dois núcleos
  - Recomendado um mínimo de 8 GB de RAM
  - Não é necessário um sistema operativo
  - Consulte http://www.vmware.com/resources/compatibility/search.php para obter uma lista completa dos sistemas operativos anfitriões compatíveis
  - O hardware deve cumprir os requisitos mínimos do VMware
  - RAM mínima de 4 GB para recurso de imagem dedicado
  - Consulte http://pubs.vmware.com/vsphere-60/index.jsp para obter mais informações

NOTA: A base de dados do SQL Server que aloja o Dell Enterprise Server deve ser executada num computador independente.

SQL Server

Em ambientes de maiores dimensões é altamente recomendável que o servidor da Base de dados SQL seja executado num sistema redundante, como um SQL Cluster, para assegurar a disponibilidade e continuidade dos dados. É ainda recomendável que realize cópias de segurança completas todos os dias com registo transacional ativado para garantir que quaisquer chaves recentemente geradas através da ativação de utilizador/dispositivo são recuperáveis.

As tarefas de manutenção da base de dados devem incluir a reconstrução de todos os índices das bases de dados e a recolha de dados estatísticos.

3

Configuração de Pré-instalação

Antes de começar, leia o documento*Enterprise Server Technical Advisories* (Avisos técnicos do Enterprise Server) para ficar a conhecer soluções alternativas existentes ou problemas conhecidos relacionados com o Dell Enterprise Server.

A configuração de pré-instalação dos servidores onde pretende instalar o Dell Enterprise Server é muito importante. Preste especial atenção a esta secção para garantir a instalação correta do Dell Enterprise Server.

Configuração

1 Se ativada, desative a Configuração de segurança avançada do Internet Explorer (ESC). Adicione o URL do servidor aos sites fidedignos nas opções de segurança do browser. Reinicie o servidor.

2 Abra as portas seguintes para cada componente:

Internas:

Comunicação por Active Directory: TCP/389

Comunicação por correio eletrónico (opcional): 25

Para front-end (se necessário):

Comunicação entre Dell Policy Proxy externo e Dell Message Broker: TCP/61616 e STOMP/61613

Comunicação para o Dell Security Server de back-end: HTTPS/8443

Comunicação para o Dell Core Server de back-end: HTTPS/8888 e 9000

Comunicação para portas RMI - 1099

Comunicação para o Dell Device Server de back-end: HTTP(S)/8443 - Se a sua versão do Dell Enterprise Server for a v7.7 ou posterior. Se tiver uma versão anterior à v7.7 do Dell Enterprise Server, HTTP(S)/8081.

Servidor de sinalizador: HTTP/8446 (se utilizar o Data Guardian)

Externas (se necessário):

Base de dados SQL: TCP/1433

Remote Management Console: HTTPS/8443

LDAP: TCP/389/636 (controlador de domínio local), TCP/3268/3269 (catálogo global), TCP/135/49125+ (RPC)

Dell Compatibility Server: TCP/1099

Dell Compliance Reporter: HTTP(S)/8084 (configurado automaticamente na instalação)

Dell Identity Server: HTTPS/8445

Dell Core Server: HTTPS/8888 e 9000 (8888 configurado automaticamente na instalação)

Dell Device Server: HTTP(S)/8443 (Dell Enterprise Server v7.7 ou posterior) ou HTTP(S)/8081 (anterior à v7.7 do Dell Enterprise Server)

Dell Key Server: TCP/8050

Dell Policy Proxy: TCP/8000

Dell Security Server: HTTPS/8443

Autenticação do cliente: HTTPS/8449 (se utilizar Server Encryption)

Comunicação do cliente, se utilizar Advanced Threat Prevention: HTTPS/TCP/443

NOTA:
Se os seus clientes Enterprise Edition forem elegíveis de fábrica ou se adquirir licenças de fábrica, defina o GPO no controlador do domínio para ativar elegibilidades (poderá não ser o servidor que executa a Enterprise Edition). Certifique-se de que a porta de saída 443 está disponível para comunicar com o Servidor. Se a porta 443 estiver bloqueada por qualquer motivo, a funcionalidade de elegibilidade não funcionará. Para obter mais informações, consulte o Enterprise Edition Advanced Installation Guide (Guia do administrador da Enterprise Edition).

Criar base de dados Dell

3 Se ainda não tiver uma base de dados SQL configurada para o Dell Enterprise Server, o instalador criará a base de dados durante a instalação. Se preferir configurar uma base de dados antes de instalar o Dell Enterprise Server, siga as instruções abaixo para criar uma base de dados do SQL e utilizador do SQL no SQL Management Studio. ***Estas instruções são opcionais, pois o programa de instalação irá criar uma base de dados, caso uma ainda não exista.***

Ao instalar o Dell Enterprise Server, siga as instruções em Instalar servidor de back-end com a base de dados existente.

O Dell Enterprise Server suporta autenticação SQL e Windows. O método de autenticação predefinido é a autenticação SQL.

Após criar a base de dados, crie um utilizador de base de dados Dell com direitos de db_owner. O db_owner pode atribuir permissões, fazer cópias de segurança e restaurar a base de dados, criar e eliminar objetos e gerir contas de utilizador e funções sem qualquer limitação. Além disso, certifique-se de que este utilizador tem permissões/privilégios para executar procedimentos armazenados.

Quando utilizar uma instância não predefinida do SQL Server, após a instalação do Dell Enterprise Server, precisa especificar a porta dinâmica da instância no separador Base de dados do Server Configuration Tool. Para mais informações, consulte a Server Configuration Tool. Como alternativa, ative o serviço SQL Server Browser e certifique-se de que a porta UDP 1434 está aberta. Para obter mais informações, consulte https://msdn.microsoft.com/en-us/library/hh510203(v=sql.120).aspx.

Se a base de dados do SQL ou instância do SQL está configurada com um agrupamento não predefinido, o agrupamento precisa ser sensível a maiúsculas e minúsculas. Para ver a lista de agrupamentos e de sensibilidade a maiúsculas e minúsculas, consulte https://msdn.microsoft.com/en-us/library/ms144250(v=sql.105).aspx.

Para criar a base de dados SQL e o utilizador SQL no SQL Management Studio, escolha um:

Criar uma nova base de dados do Windows SQL Server utilizando a Autenticação do Windows:

a Clique em **Iniciar** > **Todos os programas** > **Microsoft SQL Server** > **Management Studio**.

b Clique com o botão direito do rato na pasta Bases de dados e, em seguida, clique em Nova base de dados. É apresentada a caixa de diálogo Propriedades da base de dados.

c Introduza o nome da base de dados e clique em **OK**.

d Expanda a pasta *Segurança* e clique com o botão direito do rato em **Inícios de sessão**.

e Clique em **Novo início de sessão** para criar um proprietário para a nova base de dados.

f Introduza um nome de utilizador no campo *Nome*.

g Selecione a opção *Autenticação do Windows*.

h Selecione **Mapeamento de utilizadores** e, em seguida, selecione a nova base de dados.

i Selecione a função da base de dados (db_owner) e clique em **OK**.

OU

Criar uma nova base de dados do SQL Server utilizando a Autenticação de SQL Server:

a Clique em **Iniciar** > **Todos os programas** > **Microsoft SQL Server** > **Management Studio**.

b Clique com o botão direito do rato na pasta *Bases de dados* e, em seguida, clique em **Nova base de dados**. É apresentada a caixa de diálogo *Propriedades da base de dados*.

c Introduza o nome da base de dados e clique em **OK**.

d Expanda a pasta *Segurança* e clique com o botão direito do rato em **Inícios de sessão**.

e Clique em **Novo início de sessão** para criar um proprietário para a nova base de dados.

f Introduza um nome de utilizador no campo *Nome*.

g Selecione a opção de autenticação *Autenticação de SQL Server*. Introduza e confirme a palavra-passe.

h Desmarque a opção **Impor a validade da palavra-passe**.

i Selecione **Mapeamento de utilizadores** e, em seguida, selecione a nova base de dados.

j Selecione a função da base de dados (db_owner) e clique em **OK**.

Instalar os pacotes redistribuíveis do Visual C++ 2010/2013/2015

4 *Se ainda não estiverem instalados*, instale os pacotes redistribuíveis do Microsoft Visual C++ 2010, 2013 e 2015. Se assim o desejar, pode permitir que o instalador do Dell Enterprise Server instale estes componentes.

Windows Server 2008 e Windows Server 2008 R2 - http://www.microsoft.com/download/en/details.aspx?displaylang=en&id=5555

Instalar o .NET Framework 4.5

5 *Se ainda não estiver instalado*, instale o .NET Framework 4.5.

Windows Server 2008 e Windows Server 2008 R2 - https://www.microsoft.com/en-us/download/details.aspx?id=42643

Instalar o SQL Native Client 2012

6 *Se estiver a utilizar o SQL Server 2012 ou o SQL Server 2016*, instale o SQL Native Client 2012. Se assim o desejar, pode permitir que o instalador do Dell Enterprise Server instale este componente.

http://www.microsoft.com/en-us/download/details.aspx?id=35580

Configurar o Microsoft CA (MSCEP)

Esta etapa apenas tem de ser concluída no servidor que executa MSCEP se pretender utilizar o iOS com a Mobile Edition.

7 Configure o MSCEP.

O Windows Server 2008 R2 tem de ser a Enterprise Edition. ***A Standard Edition não permitirá que a função MSCEP seja instalada***.

a Abra o Server Manager. No menu da esquerda, selecione **Funções de servidor** e marque a caixa de verificação **Serviços de certificados do Active Directory**. Clique em **Seguinte**. O Assistente para adicionar funções orienta-o nos passos seguintes.

Em *AAD CS > Serviços de função*, assinale as caixas de verificação dos serviços de função **Autoridade de certificação** e **Inscrição na Web da autoridade de certificação**. Selecione **Adicionar serviços de função requeridos para servidor Web IIS**, se solicitado. Clique em **Seguinte**.

Em *AD CS > Tipo de configuração* , selecione **Standalone**. Clique em **Seguinte**.

Em *AD CS > Tipo de configuração*, selecione **AC subordinada**. Clique em **Seguinte**.

Em *AD CS > Chave privada*, selecione **Criar uma nova chave privada**. Clique em **Seguinte**.

Em *AD CS > Chave privada > Encriptação*, mantenha as predefinições de **RSA#Microsoft Software Key Storage Provider**, **2048** e **SHA1**. Clique em **Seguinte**.

Em *AD CS > Chave privada > Nome de AC*, mantenha todos os valores predefinidos. Clique em **Seguinte**.

Em *AD CS > Chave privada > Requisição de certificado*, selecione **Enviar uma requisição de certificado para um elemento principal: AC**. Selecione **Procurar por: Nome AC**. Navegue até à **AC principal** e selecione-o. Clique em **Seguinte**.

Em *AD CS > Base de dados de certificados*, mantenha todos os valores predefinidos. Clique em **Seguinte**.

Em *Servidor Web (IIS)*, clique em **Seguinte**.

Em *Servidor Web (IIS) > Serviços de função*, mantenha os valores predefinidos. Clique em **Seguinte**.

Em *Confirmação*, clique em **Instalar**.

Em *Resultados*, reveja os resultados e clique em **Fechar**.

Em *Gestor de servidor > Funções*, selecione **Adicionar serviços de função** em *Serviços de certificados do Active Directory*.

Quando a janela *Selecionar serviços de função* for apresentada, assinale a caixa de verificação **Serviço de inscrição de dispositivos de rede**. Clique em **Seguinte**.

Adicione a conta de utilizador que o *Serviço de inscrição de dispositivos de rede* deve utilizar ao autorizar requisições de certificados para o grupo de utilizadores de IIS_IUSRS do servidor local. O formato é Domain\UserName. Clique em **OK**.

Nas janelas Especificar conta de utilizador, selecione o utilizador que acaba de ser adicionado ao grupo IIS_IUSRS. Clique em **Seguinte**.

Na janela *Especificar informações de autoridade de registo*, mantenha os valores predefinidos de *Informações necessárias* e *Adicionar informações opcionais*, conforme pretendido. Clique em **Seguinte**.

Na janela *Configurar encriptação para autoridade de registo*, mantenha os valores predefinidos. Clique em **Seguinte**.

Na janela *Confirmar seleções de instalação*, clique em **Instalar**.

Na janela *Resultados da instalação*, reveja os resultados e clique em **Fechar**.

Feche o Gestor de servidor.

b Modifique a chave de registo, conforme indicado a seguir:

HKLM\SOFTWARE\Microsoft\Cryptography\MSCEP\EnforcePassword

“EnforcePassword"=dword:00000000

c Abra o Gestor de IIS. Navegue até **\<ServerName > \Sites\Default Web Site\CertSrv\mscep_admin**.

Abra *Autenticação* e ative a **Autenticação anónima**.

d Clique em **Iniciar** > **Executar**. Escreva *certsrv.msc* e clique em **Enter**.

Quando a janela *certsrv* for apresentada, clique com o botão direito do rato no nome do servidor, selecione **Propriedades** e clique no separador **Módulo de política**.

Clique em **Propriedades** e selecione **Seguir as definições do modelo de certificado, se aplicável**. **Caso contrário, emitir automaticamente o certificado.** Clique em **OK**.

e Feche o Gestor de IIS.

f Reinicie o servidor. Para verificar, abra o Internet Explorer e, na barra de endereço, introduza

http://server.domain.com/certsrv/mscep_admin/.

Fim da configuração do MSCEP Windows Server 2008 R2.

Windows Server 2012 R2 ou Windows Server 2016:

a Siga as instruções de Configuração no artigo, "Network Device Enrollment Service (NDES) in Active Directory Certificate Services (AD CS)" (Serviço de inscrição de dispositivos de rede em Serviços de certificados do Active Directory).

b Modifique a chave de registo, conforme indicado a seguir:

HKLM\SOFTWARE\Microsoft\Cryptography\MSCEP\EnforcePassword

"EnforcePassword"=dword:00000000

c Abra o Gestor de IIS. Navegue até **\<ServerName\Sites\Default Web Site\CertSrv\mscep_admin**.

Abra *Autenticação* e ative a **Autenticação anónima**.

d Clique em **Iniciar** > **Executar**. Escreva *certsrv.msc* e clique em **Enter**.

Quando a janela *certsrv* for apresentada, clique com o botão direito do rato no nome do servidor, selecione **Propriedades** e clique no separador **Módulo de política**.

Clique em **Propriedades** e selecione **Seguir as definições do modelo de certificado, se aplicável**. **Caso contrário, emitir automaticamente o certificado.** Clique em **OK**.

e Feche o Gestor de IIS.

f Reinicie o servidor. Para verificar, abra o Internet Explorer e, na barra de endereço, introduza

http://server.domain.com/certsrv/mscep_admin/.

Fim da configuração do MSCEP Windows Server 2012 R2/Windows Server 2016.

Instalar/configurar o Microsoft Message Queuing (MSMQ)

Esta etapa apenas tem de ser realizada se pretender utilizar o iOS com a Mobile Edition. Este é um pré-requisito para que o Gestor de Dispositivos do EAS e o Gestor de caixas de correio do EAS consigam comunicar.

8 No Windows Server 2008 ou Windows Server 2008 R2 (no servidor que aloja o ambiente Exchange): http://msdn.microsoft.com/en-us/library/aa967729.aspx

OU

No Windows Server 2012 R2:

a Abra o Server Manager.

b Navegue até **Gerir** > **Adicionar funções e funcionalidades.**.

c No ecrã "Antes de começar", clique em **Seguinte**.

d Selecione **Instalação baseada em funções ou funcionalidades** e clique em **Seguinte**.

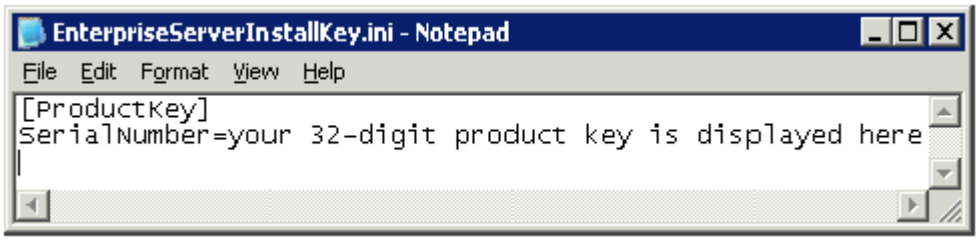
e Selecione o servidor onde pretende instalar a funcionalidade e clique em **Seguinte**.

f Não selecione quaisquer funções de servidor. Clique em **Seguinte**.

g Em Funcionalidades, selecione **Message Queuing** e clique em **Instalar**.

Opcional

9 **Para uma nova instalação** - copie a chave do produto (o nome do ficheiro é *EnterpriseServerInstallKey.ini*) para **C:\Windows** para preencher automaticamente a chave do produto de 32 caracteres no instalador do Dell Enterprise Server.



A configuração de pré-instalação do servidor está concluída. Continue para Instalar ou Atualizar/Migrar.

4

Instalar ou Atualizar/Migrar

O capítulo fornece instruções para o seguinte:

- Nova instalação - Para instalar um novo Dell Enterprise Server.
- Atualização/Migração - Para atualizar a partir de um Dell Enterprise Server funcional, v8.0 ou posterior.
- Desinstalar o Dell Enterprise Server - Para remover a instalação atual, se necessário.

  Se for necessário que a sua instalação inclua mais do que um servidor principal (back-end), contacte o seu representante do Dell ProSupport.

Antes de iniciar a Instalação ou a Atualização/Migração

Antes de começar, certifique-se de que concluiu os passos da Configuração de Pré-instalação aplicáveis.

Leia o documento *Enterprise Server Technical Advisories* (Avisos técnicos do Enterprise Server) para ficar a conhecer quaisquer soluções alternativas existentes ou problemas conhecidos relacionados com a instalação do Enterprise Server.

Se o Controlo de conta do utilizador (UAC) está ativado, tem de desativá-lo. No Windows Server 2012 R2, o programa de instalação desativa o UAC. O servidor tem de ser reiniciado para que esta alteração seja implementada.

Durante a instalação, são necessárias as credenciais de autenticação do Windows ou SQL para configurar a base de dados. Se selecionar Autenticação do Windows, serão utilizadas as credenciais do utilizador com sessão iniciada. O utilizador deve ter direitos de administrador do sistema e direitos para criar e gerir a base de dados SQL (criar base de dados, adicionar utilizador e atribuir permissões). No caso da autenticação de SQL, a conta utilizada deve ter estes mesmos direitos. Estas credenciais apenas são utilizadas durante a instalação. O produto instalado não utiliza estas credenciais.

Também durante a instalação, as credenciais de autenticação do tempo de execução do serviço devem ser especificadas para que os serviços Dell as possam utilizar para aceder ao SQL Server. A conta de utilizador deve ter o esquema predefinido de permissões do SQL Server: dbo e Associação de Funções da Base de Dados: dbo_owner, público.

Se não tem a certeza sobre os privilégios ou conectividade à base de dados, peça ao seu administrador da base de dados para os confirmar antes de iniciar a instalação.

A Dell recomenda que sejam seguidas as melhores práticas de utilização da base de dados para a base de dados da Dell e que o software Dell esteja incluído no plano de recuperação de desastres da sua organização.

Se pretender implementar componentes Dell no DMZ, certifique-se de que estão devidamente protegidos contra ataques.

Para produção, a Dell recomenda vivamente que instale o SQL Server num servidor dedicado.

Instalar o servidor de back-end antes de instalar e configurar um servidor de front-end constitui uma boa prática.

Os ficheiros de registo do instalador estão localizados neste diretório: **C:\ProgramData\Dell\Dell Data Protection\Installer Logs**

Nova instalação

Escolha uma de duas opções para a instalação do servidor de back-end:

- Instalar servidor de back-end e nova base de dados - Para instalar um novo Dell Enterprise Server e uma nova base de dados.
- Instalar servidor de back-end com a base de dados existente - Para instalar um novo Dell Enterprise Server e ligar-se a uma base de dados do SQL criada durante a Configuração de Pré-instalação ou a uma base de dados do SQL (v9.x ou posterior), quando a versão de esquema corresponde à versão do Dell Enterprise Server a ser instalada. Uma base de dados v8.x ou posterior deve ser migrada para o esquema mais recente com a versão mais recente da ferramenta Server Configuration Tool. Para instruções sobre a migração da base de dados com a Server Configuration Tool, consulte Migrar a base de dados. Para obter a Server Configuration Tool mais recente ou para migrar uma base de dados anterior à v8.0, entre em contacto com o Dell ProSupport para obter assistência.

NOTA:
Se possui um Dell Enterprise Server funcional, v8.x ou posterior, consulte as instruções em **Atualizar/migrar servidores de back-end**.

Se instalar o servidor de front-end, realize esta instalação depois da instalação do servidor de back-end:

- Instalar um servidor de front-end - Para instalar um servidor de front-end para comunicar com um servidor de back-end.

Instalar servidor de back-end e nova base de dados

1 No suporte multimédia de instalação da Dell, aceda ao diretório "Dell Enterprise Server". **Descomprima** (NÃO copie/cole nem arraste/largue) o Dell Enterprise Server-x64 para o diretório de raiz do servidor onde vai instalar o Enterprise Server. ***As operações de copiar/colar ou arrastar/largar produzirão erros e uma instalação malsucedida.***

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

3 Na caixa de diálogo do *Assistente InstallShield*, selecione o idioma de instalação e depois 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 Na caixa de diálogo *Boas-vindas*, clique em **Seguinte**.

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

7 Se concluiu opcionalmente o passo 9 na Configuração de Pré-instalação, clique em **Seguinte**. Caso contrário, introduza a chave do produto de 32 caracteres e clique em **Seguinte**. A chave do produto encontra-se no ficheiro "*EnterpriseServerInstallKey.ini*".

8 Selecione **Instalação de back end** e clique em **Seguinte**.

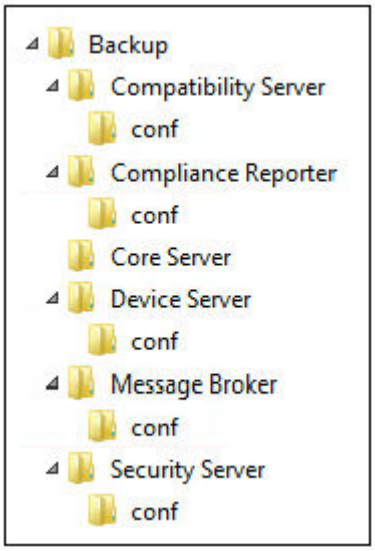
9 Para instalar o Dell Enterprise Server na localização predefinida **C:\Program Files\Dell**, clique em **Seguinte**. Caso contrário, clique em **Alterar** para selecionar uma localização diferente e clique em **Seguinte**.

10 Para selecionar uma localização para guardar os ficheiros de configuração da cópia de segurança, clique em **Alterar** e navegue até à pasta pretendida, em seguida, clique em **Seguinte**.

A Dell recomenda que selecione uma localização de rede remota ou uma unidade externa para a cópia de segurança.

Após a instalação, deve ser manualmente criada uma cópia de segurança com quaisquer alterações efetuadas nos ficheiros de configuração, incluindo alterações feitas com a Server Configuration Tool, nestas pastas. Os ficheiros de configuração são uma parte importante das informações totais utilizadas para restaurar manualmente o servidor.

NOTA: A estrutura de pastas criada pelo instalador durante esta etapa de instalação (exemplo apresentado abaixo) deve manter-se inalterada.



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

Clique em **Procurar** para introduzir o caminho do certificado.

Introduza a palavra-passe associada a este certificado. O ficheiro keystore precisa ser .p12 ou pfx. Para mais instruções consulte Exporting a Certificate to .PFX Using the Certificate Management Console (Exportar um Certificado para .Pfx Utilizando a Consola de Gestão de Certificados).

Clique em **Seguinte**.

> **NOTA:**
> Para utilizar esta definição, o certificado da AC exportado e que pretende importar precisa ter a cadeia de certificação completa. Se não tiver a certeza, volte a exportar o certificado da AC e certifique-se de que as opções seguintes estão selecionadas no "Certificate Export Wizard" (Assistente para Exportar Certificados):
>
> - Personal Information Exchange - PKCS#12 (.PFX)
> - Incluir todos os certificados no caminho de certificação, se possível
> - Exportar todas as propriedades expandidas

OU

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 um ano, por predefinição.

12 Para o Server Encryption (SE), tem à sua disposição vários tipos de certificados digitais que pode utilizar. 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**.

Clique em **Procurar** para introduzir o caminho do certificado.

Introduza a palavra-passe associada a este certificado. O ficheiro keystore precisa ser .p12 ou pfx. Para mais instruções consulte Exporting a Certificate to .PFX Using the Certificate Management Console (Exportar um Certificado para .Pfx Utilizando a Consola de Gestão de Certificados).

Clique em **Seguinte**.

> **NOTA:**
> Para utilizar esta definição, o certificado da AC exportado e que pretende importar precisa ter a cadeia de certificação completa. Se não tiver a certeza, volte a exportar o certificado da AC e certifique-se de que as opções seguintes estão selecionadas no "Certificate Export Wizard" (Assistente para Exportar Certificados):
>
> - Personal Information Exchange - PKCS#12 (.PFX)
> - Incluir todos os certificados no caminho de certificação, se possível
> - Exportar todas as propriedades expandidas

OU

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 um ano, por predefinição.

13 A partir da caixa de diálogo *Configuração da instalação do servidor de back-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 back-end*, clique em **Seguinte**.

- Se estiver a utilizar um servidor de front-end, selecione **Trabalha com o front-end para comunicar com clientes internamente na sua rede ou externamente no DMZ** e introduza o nome do anfitrião do Security Server de front-end (por exemplo: servidor.domínio.com).
- Para ver ou editar nomes de anfitriões, clique em **Editar nomes de 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 ("_").

  Quando terminar, clique em **OK**.
- Para ver ou editar portas, clique em **Editar Portas**. Edite as portas apenas se necessário. A Dell recomenda que utilize os nomes predefinidos. Quando terminar, clique em **OK**.

14 Para criar uma nova base de dados, siga estes passos:

a Clique em **Procurar** para selecionar o servidor onde pretende instalar a base de dados.

b Selecione o método de autenticação que o instalador deve utilizar para configurar a base de dados do Dell Data Protection. Após a instalação, o produto instalado não utiliza as credenciais aqui especificadas.

- **Credenciais de autenticação Windows do utilizador atual**

  Se escolher a Autenticação do Windows, as mesmas credenciais que foram utilizadas para iniciar sessão no Windows serão utilizadas para autenticação (os campos Nome de utilizador e Palavra-passe não serão editáveis). Certifique-se de que a conta tem direitos de administrador de sistema e a capacidade de gerir o SQL Server.

  OU

- **Autenticação do SQL Server a utilizar as credenciais abaixo apresentadas**

  Se utilizar a autenticação do SQL, a conta SQL utilizada precisa ter direitos de administrador do sistema no SQL Server.

  O instalador precisa efetuar a autenticação no SQL Server com estas permissões: criar base de dados, adicionar utilizador, atribuir permissões.

c Identifique o catálogo da base de dados:

Introduza o nome do novo catálogo da base de dados. Na caixa de diálogo seguinte é-lhe solicitado que crie um novo catálogo.

d Clique em **Seguinte**.

e Para confirmar que pretende que o instalador crie uma base de dados, clique em **Sim**. Para voltar ao ecrã anterior e fazer alterações, clique em **Não**.

15 Selecione o método de autenticação que o produto deve utilizar. Esta etapa associa uma conta ao produto.

- **Autenticação do Windows**

  Selecione **Autenticação do Windows utilizando as credenciais, abaixo** introduza as credenciais do produto a utilizar e clique em **Seguinte**.

  Certifique-se de que a conta tem direitos de administrador de sistema e a capacidade de gerir o SQL Server. A conta de utilizador precisa possuir o esquema predefinido de permissões do SQL Server: dbo e Associação de Funções da Base de Dados: dbo_owner, público.

  Estas credenciais são também utilizadas por serviços Dell, uma vez que são compatíveis com o Dell Enterprise Server.

  OU

- **Autenticação do SQL Server**

  Selecione **Autenticação do SQL Server utilizando as credenciais abaixo**, introduza as credenciais do SQL Server para os serviços Dell utilizarem enquanto trabalham no Dell Enterprise Server e clique em **Seguinte**.

  A conta de utilizador precisa possuir o esquema predefinido de permissões do SQL Server: dbo e Associação de Funções da Base de Dados: dbo_owner, público.

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

É apresentada uma caixa de diálogo de progresso durante todo o processo de instalação.

17 Quando a instalação estiver concluída, clique em **Concluir**.
As tarefas de instalação do servidor de back-end estão concluídas.

Os serviços Dell são reiniciados no final da instalação. Não é necessário reiniciar o servidor.

Instalar servidor de back-end com a base de dados existente

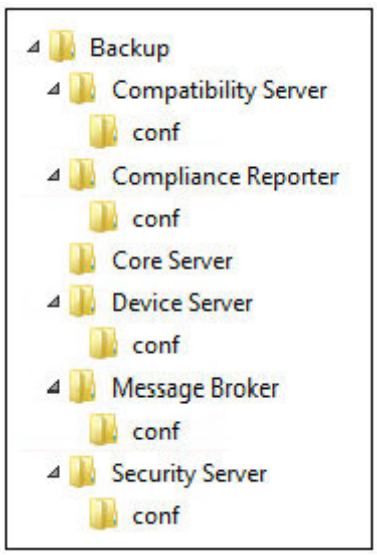
NOTA:
Se possui um Dell Enterprise Server v8.x ou posterior funcional, consulte as instruções em Atualizar/migrar servidores de back-end.

Pode instalar um novo Dell Enterprise Server e ligar-se a uma base de dados do SQL criada durante a Configuração de pré-instalação ou a uma base de dados do SQL (v9.x ou posterior), quando a versão de esquema corresponde à versão do Dell Enterprise Server a ser instalada.

Uma base de dados v8.x ou posterior deve ser migrada para o esquema mais recente com a versão mais recente da ferramenta Server Configuration Tool. Para instruções sobre a migração da base de dados com a Server Configuration Tool, consulte Migrar a base de dados. Para obter a Server Configuration Tool mais recente ou **para migrar uma base de dados anterior à v8.0**, entre em contacto com o Dell ProSupport para obter assistência**.**

A conta de utilizador a partir da qual a instalação é realizada deve ter privilégios de proprietário de base de dados para a base de dados do SQL. Se não tem a certeza sobre os privilégios ou conetividade à base de dados, peça ao seu administrador da base de dados para os confirmar antes de iniciar a instalação.

Se a base de dados existente tiver sido anteriormente instalada com o Dell Enterprise Server, antes de iniciar a instalação, certifique-se de que efetua uma cópia de segurança da base de dados existente, dos ficheiros de configuração e da secretKeyStore e de que estes estão acessíveis a partir do servidor no qual está a instalar o Dell Enterprise Server. Se necessário, aceda a estes ficheiros para configurar o Dell Enterprise Server e a base de dados existente. A estrutura de pastas criada pelo instalador durante a instalação (exemplo apresentado abaixo) não pode ser alterada.



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

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

3 Na caixa de diálogo do *Assistente InstallShield*, selecione o idioma de instalação e depois 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 Na caixa de diálogo *Boas-vindas*, clique em **Seguinte**.

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

7 Se concluiu opcionalmente o passo 9 na Configuração de Pré-instalação, clique em **Seguinte**. Caso contrário, introduza a chave do produto de 32 caracteres e clique em **Seguinte**. A chave do produto encontra-se no ficheiro "*EnterpriseServerInstallKey.ini*".

8 Selecione **Instalação de back-end** e **Instalação de recuperação**, em seguida clique em **Seguinte**.

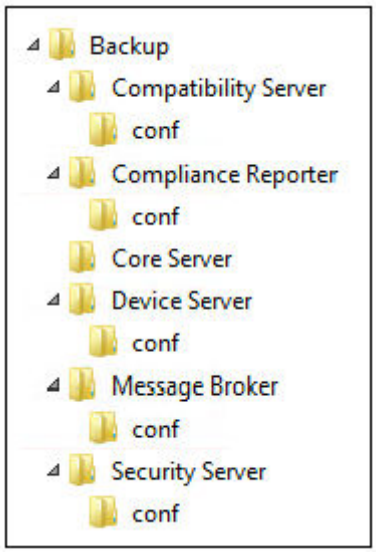
9 Para instalar o Dell Enterprise Server na localização predefinida **C:\Program Files\Dell**, clique em **Seguinte**. Caso contrário, clique em **Alterar** para selecionar uma localização diferente e clique em **Seguinte**.

10 Para selecionar uma localização para guardar os ficheiros de configuração da cópia de segurança, clique em **Alterar** e navegue até à pasta pretendida, em seguida, clique em **Seguinte**.

A Dell recomenda que selecione uma localização de rede remota ou uma unidade externa para a cópia de segurança.

Após a instalação, deve ser manualmente criada uma cópia de segurança com quaisquer alterações efetuadas nos ficheiros de configuração, incluindo alterações feitas com a Server Configuration Tool, nestas pastas. Os ficheiros de configuração são uma parte importante das informações totais utilizadas para restaurar manualmente o servidor.

NOTA: A estrutura de pastas criada pelo instalador durante a instalação (exemplo apresentado abaixo) não pode ser alterada.



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

Clique em **Procurar** para introduzir o caminho do certificado.

Introduza a palavra-passe associada a este certificado. O ficheiro keystore precisa ser .p12 ou pfx. Para mais instruções consulte Exporting a Certificate to .PFX Using the Certificate Management Console (Exportar um Certificado para .Pfx Utilizando a Consola de Gestão de Certificados).

Clique em **Seguinte**.

NOTA:

Para utilizar esta definição, o certificado da AC exportado e que pretende importar precisa ter a cadeia de certificação completa. Se não tiver a certeza, volte a exportar o certificado da AC e certifique-se de que as opções seguintes estão selecionadas no "Certificate Export Wizard" (Assistente para Exportar Certificados):

- Personal Information Exchange - PKCS#12 (.PFX)
- Incluir todos os certificados no caminho de certificação, se possível
- Exportar todas as propriedades expandidas

OU

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 um ano, por predefinição.

12 Para o Server Encryption (SE), tem à sua disposição vários tipos de certificados digitais que pode utilizar. 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**.

Clique em **Procurar** para introduzir o caminho do certificado.

Introduza a palavra-passe associada a este certificado. O ficheiro keystore precisa ser .p12 ou pfx. Para mais instruções consulte Exporting a Certificate to .PFX Using the Certificate Management Console (Exportar um Certificado para .Pfx Utilizando a Consola de Gestão de Certificados).

Clique em **Seguinte**.

NOTA:

Para utilizar esta definição, o certificado da AC exportado e que pretende importar precisa ter a cadeia de certificação completa. Se não tiver a certeza, volte a exportar o certificado da AC e certifique-se de que as opções seguintes estão selecionadas no "Certificate Export Wizard" (Assistente para Exportar Certificados):

- Personal Information Exchange - PKCS#12 (.PFX)
- Incluir todos os certificados no caminho de certificação, se possível
- Exportar todas as propriedades expandidas

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 um ano, por predefinição.**

13 A partir da caixa de diálogo *Configuração da instalação do servidor de back-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 back-end*, clique em **Seguinte**.
- Se estiver a utilizar um servidor de front-end, selecione **Trabalha com o front-end para comunicar com clientes internamente na sua rede ou externamente no DMZ** e introduza o nome do anfitrião do Security Server de front-end (por exemplo: servidor.domínio.com).
- Para ver ou editar nomes de anfitriões, clique em **Editar nomes de 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 ("_").**

  Quando terminar, clique em **OK**.
- Para ver ou editar portas, clique em **Editar Portas**. Edite as portas apenas se necessário. A Dell recomenda que utilize os nomes predefinidos. Quando terminar, clique em **OK**.

14 Especifique o método de autenticação que o instalador deve utilizar.

a Clique em **Procurar** para selecionar o servidor onde se encontra a base de dados.

b Selecione o tipo de autenticação.

- **Credenciais de autenticação Windows do utilizador atual**

  Se escolher a Autenticação do Windows, as mesmas credenciais que foram utilizadas para iniciar sessão no Windows serão utilizadas para autenticação (os campos Nome de utilizador e Palavra-passe não serão editáveis). Certifique-se de que a conta tem direitos de administrador de sistema e a capacidade de gerir o SQL Server.

  OU

- **Autenticação do SQL Server a utilizar as credenciais abaixo apresentadas**

  Se utilizar a autenticação do SQL, a conta SQL utilizada precisa ter direitos de administrador do sistema no SQL Server.

  O instalador precisa efetuar a autenticação no SQL Server com estas permissões: criar base de dados, adicionar utilizador, atribuir permissões.

c Clique em **Procurar** para selecionar o nome do catálogo de base de dados existente.

d Clique em **Seguinte**.

15 Selecione o método de autenticação que o produto deve utilizar. Esta é a conta que o produto utiliza para trabalhar com a base de dados e os serviços Dell.

- **Para usar a autenticação do Windows**

Selecione **Autenticação do Windows utilizando as credenciais, abaixo**, introduza as credenciais da conta que o produto pode utilizar e clique em **Seguinte**.

Certifique-se de que a conta tem direitos de administrador de sistema e a capacidade de gerir o SQL Server. A conta de utilizador precisa possuir o esquema predefinido de permissões do SQL Server: dbo e Associação de Funções da Base de Dados: dbo_owner, público.

OU

- **Para utilizar a autenticação do SQL Server**

  Selecione **Autenticação do SQL Server utilizando as credenciais, abaixo**, introduza as credenciais do SQL Server e clique em **Seguinte**.

  A conta de utilizador precisa possuir o esquema predefinido de permissões do SQL Server: dbo e Associação de Funções da Base de Dados: dbo_owner, público.

  Se o instalador detetar um problema na base de dados, é apresentada uma caixa de diálogo com a mensagem Erro na base de dados existente. As opções da caixa de diálogo dependem das circunstâncias:

  - O esquema da base de dados é de uma versão anterior. (Consulte o passo a.)
  - A base de dados já tem um esquema de base de dados que corresponde à versão que está atualmente a ser instalada. (Consulte o passo b.)

a Se o esquema da base de dados for de uma versão anterior, selecione **Sair do instalador para terminar esta instalação**. Em seguida, deve efetuar uma cópia de segurança da base de dados.

As opções seguintes apenas DEVEM ser utilizadas com a ajuda do Dell ProSupport:

- A opção **Migrar esta base de dados para o esquema atual** é utilizada para recuperar uma base de dados boa de uma implementação do servidor com falhas. Esta opção utiliza os ficheiros de recuperação da pasta \Backup para se ligar novamente à base de dados e, em seguida, executa a migração da base de dados para o esquema atual. Esta opção *apenas* deve ser utilizada após tentar reinstalar a versão correta do Enterprise Server pela primeira vez e, em seguida, executar o instalador mais recente para atualizar a versão.
- A opção **Avançar sem migrar a base de dados** instala os ficheiros do Enterprise Server sem configurar completamente a base de dados. A configuração da base de dados deve ser concluída mais tarde, manualmente, utilizando a Server Configuration Tool e requer alterações manuais adicionais.

b Se o esquema da base de dados já tiver o esquema da versão atual, mas não estiver ligado a um Dell Enterprise Server de back-end, é considerado uma *Recuperação*. É apresentada esta caixa de diálogo:

- Selecione **Modo de instalação de recuperação** para continuar a instalação com a base de dados selecionada.
- Selecione **Selecionar uma nova base de dados** para escolher uma base de dados diferente.
- Selecione **Sair do instalador para concluir esta instalação**.

c Clique em **Seguinte**.

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

É apresentada uma caixa de diálogo de progresso durante todo o processo de instalação.

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

As tarefas de instalação do servidor de back-end estão concluídas.

Os serviços Dell são reiniciados no final da instalação. Não é necessário reiniciar o servidor.

Instalar servidor de front-end

A Instalação do servidor de front-end fornece uma opção de front-end (Modo DMZ) para utilização com o Dell Enterprise 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, que insere um sinalizador de chamada de retorno em cada ficheiro protegido pelo Data Guardian quando em Modo de Office Protegido. Isto permite a comunicação entre qualquer dispositivo em qualquer localização e o servidor de front-end da Dell. Certifique-se de que a segurança de rede necessária está configurada antes de usar o sinalizador de chamada de retorno. A política Ativar Sinalizador de Chamada de Retorno está ativada por predefinição.

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 "Dell Enterprise Server". **Descomprima** (NÃO copie/cole nem arraste/largue) o Dell Enterprise Server-x64 para o diretório de raiz do servidor onde vai instalar o Enterprise Server. ***As operações de copiar/colar ou arrastar/largar produzirão erros e uma instalação malsucedida.***

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

3 Na caixa de diálogo do *Assistente InstallShield*, selecione o idioma de instalação e depois 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 Na caixa de diálogo *Boas-vindas*, clique em **Seguinte**.

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

7 Introduza a chave do produto.

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

9 Para instalar o Front End Server na localização predefinida C:\Program Files\Dell clique em **Seguinte**. Caso contrário, clique em **Alterar** para selecionar uma localização diferente e clique em **Seguinte**.

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

Clique em **Procurar** para introduzir o caminho do certificado.

Introduza a palavra-passe associada a este certificado. O ficheiro keystore precisa ser .p12 ou pfx. Para mais instruções consulte Exporting a Certificate to .PFX Using the Certificate Management Console (Exportar um Certificado para .Pfx Utilizando a Consola de Gestão de Certificados).

Clique em **Seguinte**.

NOTA:

Para utilizar esta definição, o certificado da AC exportado e que pretende importar precisa ter a cadeia de certificação completa. Se não tiver a certeza, volte a exportar o certificado da AC e certifique-se de que as opções seguintes estão selecionadas no "Certificate Export Wizard" (Assistente para Exportar Certificados):

- Personal Information Exchange - PKCS#12 (.PFX)
- Incluir todos os certificados no caminho de certificação, se possível
- Exportar todas as propriedades expandidas

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 um ano, 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 **Enterprise Edition** 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 quer configurar para instalação. Se desmarcar um proxy nesta caixa de diálogo, o proxy não será 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**.
É apresentada uma caixa de diálogo de progresso durante todo o processo de instalação.

14 Quando a instalação estiver concluída, clique em **Concluir**.
As tarefas de instalação do servidor de front-end estão completas.

Atualização/Migração

Pode atualizar o Dell Enterprise Server v8.0 e posteriores para o Dell Enterprise Server v9.x. Se a versão do Server for anterior à 8.0, primeiro tem de o atualizar para a v8.0 e, de seguida, atualizar para a v9.x.

Antes de iniciar uma Atualização/Migração

Antes de iniciar, certifique-se de que a Configuração de Pré-instalação está concluída. Isto é particularmente importante se estiver a implementar a Mobile Edition.

Leia o documento *Enterprise Server Technical Advisories* (Avisos técnicos do Enterprise Server) para ficar a conhecer quaisquer soluções alternativas existentes ou problemas conhecidos relacionados com a instalação do Enterprise Server.

A conta de utilizador a partir da qual a instalação é realizada deve ter privilégios de proprietário de base de dados para a base de dados do SQL. Se não tem a certeza sobre os privilégios ou conectividade à base de dados, peça ao seu administrador da base de dados para os confirmar antes de iniciar a instalação.

A Dell recomenda que sejam seguidas as melhores práticas de utilização da base de dados para a base de dados da Dell e que o software Dell esteja incluído no plano de recuperação de desastres da sua organização.

Se pretender implementar componentes Dell no DMZ, certifique-se de que estão devidamente protegidos contra ataques.

Para produção, a Dell recomenda que instale o SQL Server num servidor dedicado.

Para beneficiar das funcionalidades completas das políticas, recomendamos que atualize o Dell Enterprise Server e os Cientes para as versões mais recentes.

O Dell Enterprise Server v9.x suporta:

- Enterprise Edition:
  - Clientes Windows v7.x/8.x
  - Clientes Mac v7.x/8.x
  - Clientes SED v8.x
  - Autenticação v8.x
  - BitLocker Manager v7.2x+ e v8.x
  - Data Guardian v1.x
- Endpoint Security Suite v1.x
- Endpoint Security Suite Enterprise v1.x
- Mobile Edition v7.x/v8.x
- Atualização/Migração do Dell Enterprise Server, versão v8.x ou posterior. (Ao migrar do Dell Enterprise Server anterior à versão v8.x, contacte o Dell ProSupport para obter assistência.)

Ao atualizar/migrar o seu Dell Enterprise Server para uma versão que inclua novas políticas, consolide a política atualizada após a atualização/migração, de modo a garantir a implementação das suas preferências de políticas, para as novas políticas, em vez dos valores predefinidos.

Regra geral, o procedimento de atualização recomendado consiste em atualizar/migrar o Dell Enterprise Server e os seus componentes e, depois, instalar/atualizar o cliente.

Aplicar alterações de políticas

1 Como Administrador Dell, inicie sessão na Remote Management Console.

2 No painel da esquerda, 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 Remote Management Console.

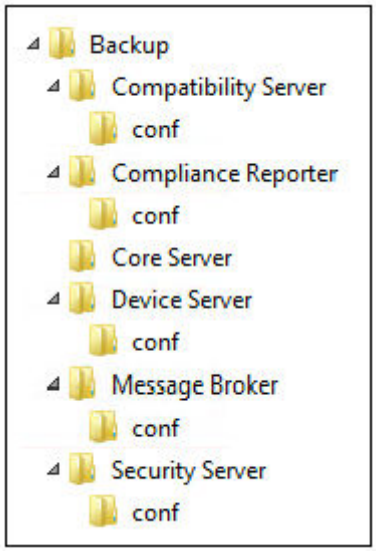
Certifique-se de que os serviços Dell estão a ser executados

6 No menu *Iniciar* do Windows, clique em **Iniciar** > **Executar**. Escreva *services.msc* e clique em **OK**. Quando a janela *Serviços* abrir, navegue até cada serviço Dell e clique em **Iniciar o serviço**.

Fazer uma cópia de segurança da instalação existente

7 Faça uma cópia de segurança da totalidade da instalação existente e guarde-a num local alternativo. A cópia de segurança deve incluir a base de dados SQL, a secretKeyStore e os ficheiros de configuração. Serão necessários vários ficheiros da sua instalação existente quando o processo de atualização/migração estiver concluído.

NOTA:
A estrutura de pastas criada pelo instalador durante a instalação (exemplo abaixo apresentado) não pode ser alterada



Atualizar/migrar servidores de back-end

1 No suporte multimédia de instalação da Dell, aceda ao diretório "Dell Enterprise Server". **Descomprima** (NÃO copie/cole nem arraste/largue) o Dell Enterprise Server-x64 para o diretório de raiz do servidor onde vai instalar o Enterprise Server. ***As operações de copiar/colar ou arrastar/largar produzirão erros e uma instalação malsucedida.***

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

3 Na caixa de diálogo do *Assistente InstallShield*, selecione o idioma de instalação e depois clique em **OK**.

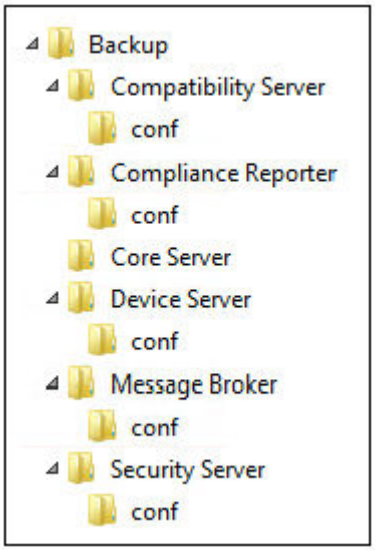
4 Na caixa de diálogo *Boas-vindas*, clique em **Seguinte**.

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

6 Para selecionar uma localização para guardar os ficheiros de configuração da cópia de segurança, clique em **Alterar** e navegue até à pasta pretendida, depois clique em **Seguinte**.

A Dell recomenda que selecione uma localização de rede remota ou uma unidade externa para a cópia de segurança.

A estrutura de pastas criada pelo instalador durante a instalação (exemplo apresentado abaixo) não pode ser alterada.



7 Quando o instalador localizar corretamente a base de dados existente, a caixa de diálogo é preenchida por si.

Para se ligar à base de dados existente, especifique o método de autenticação a utilizar. Após a instalação, o produto instalado não utiliza as credenciais aqui especificadas.

a Selecione o tipo de autenticação da base de dados:

- **Credenciais de autenticação Windows do utilizador atual**

  Se escolher a Autenticação do Windows, as mesmas credenciais que foram utilizadas para iniciar sessão no Windows serão utilizadas para autenticação (os campos Nome de utilizador e Palavra-passe não serão editáveis).

  Certifique-se de que a conta tem direitos de administrador de sistema e a capacidade de gerir o SQL Server. A conta de utilizador precisa possuir o esquema predefinido de permissões do SQL Server: dbo e Associação de Funções da Base de Dados: dbo_owner, público.

  OU

- **Autenticação do SQL Server a utilizar as credenciais abaixo apresentadas**

  Se utilizar a autenticação do SQL, a conta SQL utilizada precisa ter direitos de administrador do sistema no SQL Server.

  O instalador precisa efetuar a autenticação no SQL Server com estas permissões: criar base de dados, adicionar utilizador, atribuir permissões.

b Clique em **Seguinte**.

8 Se a caixa de diálogo Informações da conta de tempo de execução do serviço não for pré-preenchida, especifique o método de autenticação que o produto irá utilizar após a instalação.

a Selecione o tipo de autenticação.

b Introduza o nome de utilizador e a palavra-passe da conta do serviço de domínio que os serviços Dell irão utilizar para aceder ao SQL Server e clique em **Seguinte**.

A conta de utilizador precisa estar no formato DOMAIN\Username e possuir o esquema predefinido de permissões do SQL Server: dbo e Associação de Funções da Base de Dados dbo_owner, público.

9 Se não for feita uma cópia de segurança da base de dados, ***tem*** de fazer a cópia de segurança antes de prosseguir com a instalação. ***A atualização da base de dados não pode ser revertida.*** Apenas depois de efetuar a cópia de segurança da base de dados, selecione **Sim**, **foi efetuada a cópia de segurança da base de dados** e clique em **Seguinte**.

10 Clique em **Instalar** para começar a instalação.

É apresentada uma caixa de diálogo de progresso durante todo o processo de atualização.

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

Os serviços Dell são reiniciados no final da migração. Não é necessário reiniciar o servidor.

O instalador realiza as etapas 12-13 por si. A verificação destes valores para garantir que as alterações foram efetuadas corretamente é uma das melhores práticas.

12 Na cópia de segurança da sua instalação copie e cole: <Compatibility Server install dir>\conf\secretKeyStore para a nova instalação: <Compatibility Server install dir>\conf\secretKeyStore

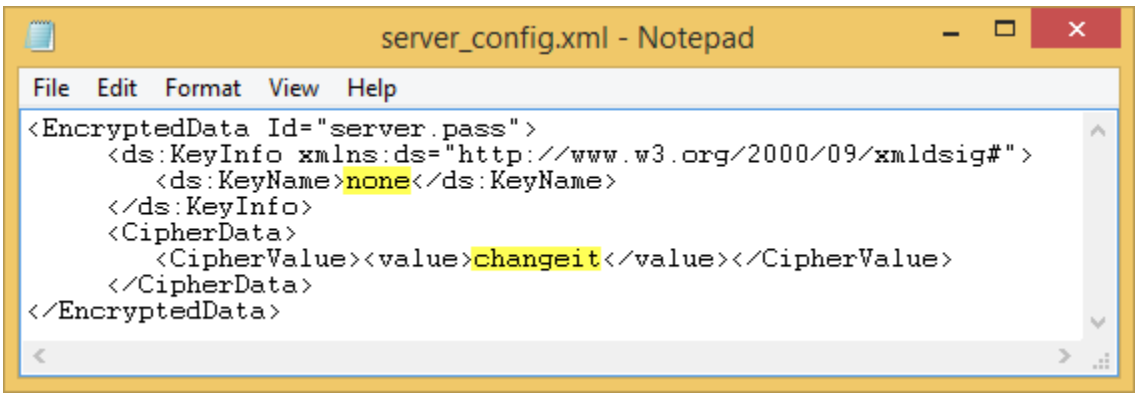
13 Na nova instalação, abra <Compatibility Server install dir>\conf\server_config.xml e substitua o valor **server.pass** pelo valor da cópia de segurança <Compatibility Server install dir>\conf\server_config.xml, conforme se segue:

Instruções para server.pass:

Se souber a palavra-passe, consulte o ficheiro de exemplo server_config.xml e faça as alterações seguintes:

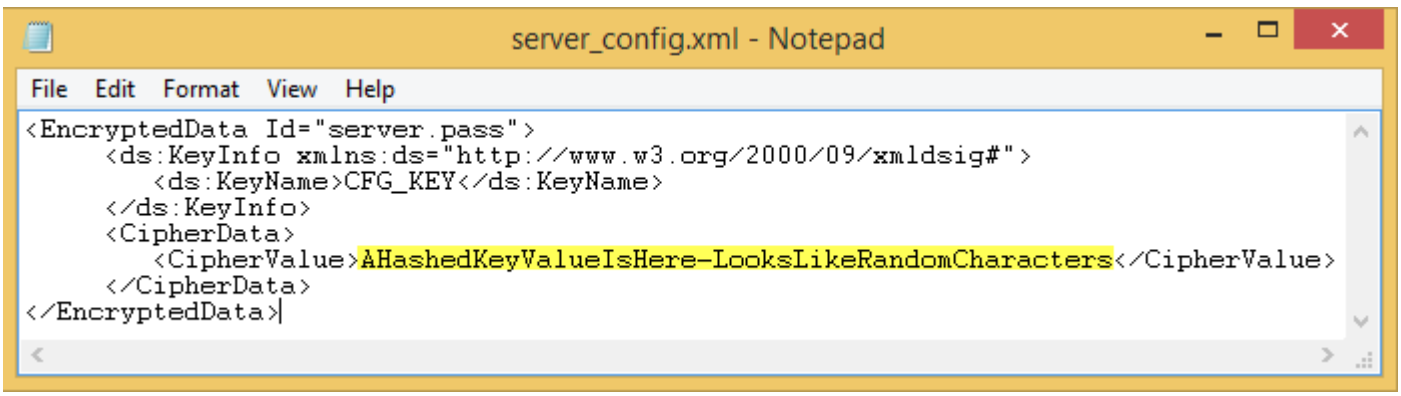
- Edite o *KeyName* de **CFG_KEY** para **nenhum**.
- Introduza a palavra-passe em texto simples e inclua-a entre *<value> </value>*, o que neste exemplo é **<value>changeit</value>**
- Quando o Dell Enterprise Server é iniciado, a palavra-passe em texto simples é convertida numa palavra-passe com *hash* e este valor com *hash* substitui o texto simples.

Palavra-passe conhecida



Se não souber a palavra-passe, corte e cole a secção semelhante à secção apresentada na Figura 4-2 do ficheiro de cópia de segurança <Compatibility Server install dir>\conf\server_config.xml para a secção correspondente do novo ficheiro *server_config.xml*.

Palavra-passe desconhecida



Guarde e feche o ficheiro.

NOTA:

Não tente mudar a palavra-passe do **Dell** Enterprise Server editando o valor server.pass em server_config.xml em nenhuma circunstância. Se alterar este valor, perde acesso à base de dados.

As tarefas de migração do servidor de back-end estão concluídas.

Atualizar/migrar servidores de front-end

NOTA: A partir da v9.5, o Serviço de Sinalizador é instalado como parte desta atualização, utilizando o nome do anfitrião predefinido e a porta 8446. O Serviço de Sinalizador apoia o sinalizador de chamada de retorno do Data Guardian, que insere um sinalizador de chamada de retorno em cada ficheiro protegido pelo Data Guardian quando em Modo de Office Protegido. Isto permite a comunicação entre qualquer dispositivo em qualquer localização e o servidor de front-end da Dell. A política Ativar Sinalizador de Chamada de Retorno está ativada por predefinição. Certifique-se de que a segurança de rede necessária está configurada antes de usar o sinalizador de chamada de retorno.

1 No suporte multimédia de instalação da Dell, aceda ao diretório "Dell Enterprise Server". **Descomprima** (NÃO copie/cole nem arraste/largue) o Dell Enterprise Server-x64 para o diretório de raiz do servidor onde vai instalar o Enterprise Server. ***As operações de copiar/colar ou arrastar/largar produzirão erros e uma instalação malsucedida.***

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

3 Na caixa de diálogo do *Assistente InstallShield*, selecione o idioma de instalação e depois 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 Na caixa de diálogo *Boas-vindas*, clique em **Seguinte**.

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

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

É apresentada uma caixa de diálogo de progresso durante todo o processo de instalação.

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

9 Configure o servidor de back-end para comunicar com o servidor de front-end.

a No servidor back-end, aceda a <Security Server install dir>\conf\ e abra o ficheiro application.properties.

b Localize o publicdns.server.host e defina o nome para um nome de anfitrião resolvível externamente.

c Localize a publicdns.server.port e defina a porta (a predefinição é 8443).

Os serviços Dell são reiniciados no final da instalação. Não é necessário reiniciar o servidor enquanto as tarefas de configuração pós-instalação não forem concluídas.

Instalação no modo desligado

O modo desligado isola o Entreprise Server da Internet e de uma LAN ou outra rede não segura. Após a instalação do Enterprise Server em Modo Desligado, este permanece em modo desligado e não pode ser alterado para o Modo Ligado.

O Enterprise Server é instalado no Modo Desligado na linha de comandos.

A tabela seguinte lista os comutadores disponíveis.

Opção	Significado
/v	Passa variáveis para o .msi dentro do *.exe
/s	Modo silencioso

A tabela seguinte lista as opções de visualização disponíveis.

Opção	Significado
/q	Sem caixa de diálogo de Progresso, reinicia-se após a conclusão do processo
/qb	Caixa de diálogo de progresso com botão **Cancelar**
/qn	Sem interface de utilizador

A tabela seguinte descreve os parâmetros disponíveis para a instalação. Estes parâmetros podem ser especificados na linha de comandos ou utilizados a partir de um ficheiro, através da propriedade:

```
INSTALL_VALUES_FILE=\"<file_path>\" "
```

Parâmetros

AGREE_TO_LICENSE=Yes - este valor deve ser "Yes."

PRODUCT_SN=xxxxx - opcional se tiver a informação de licença na localização normal; caso contrário, introduza-a aqui.

INSTALLDIR=<path> - opcional.

BACKUPDIR=<path> - onde os ficheiros de recuperação serão armazenados.

NOTA: A estrutura de pastas criada pelo instalador durante esta etapa de instalação (exemplo apresentado abaixo) deve manter-se inalterada.

AIRGAP=1 - este valor tem de ser "1" para instalar o Enterprise Server em Modo Desligado.

SSL_TYPE=n - sendo n igual a 1 para importar um certificado existente adquirido de uma autoridade certificadora e 2 para criar um certificado autoassinado. O valor SSL_TYPE determina as propriedades de SSL obrigatórias.

É necessário o seguinte com SSL_TYPE=1:

SSL_CERT_PASSWORD=xxxxx

SSL_CERT_PATH=xxxxx

É necessário o seguinte com SSL_TYPE=2:

SSL_CITYNAME

SSL_DOMAINNAME

SSL_ORGNAME

SSL_UNITNAME

SSL_COUNTRY - opcional, predefinição = "US"

SSL_STATENAME

SSOS_TYPE=n - sendo n igual a 1 para importar um certificado existente adquirido de uma autoridade certificadora e 2 para criar um certificado autoassinado. O valor SSOS_TYPE determina as propriedades SSOS obrigatórias.

É necessário o seguinte com SSOS_TYPE=1:

SSOS_CERT_PASSWORD=xxxxx

SSOS_CERT_PATH=xxxxx

É necessário o seguinte com SSOS_TYPE=2:

SSOS_CITYNAME

SSOS_DOMAINNAME

SSOS_ORGNAME

SSOS_UNITNAME

SSOS_COUNTRY - opcional, predefinição = "US"

SSOS_STATENAME

Parâmetros

DISPLAY_SQLSERVER - este valor será processado para obter a informação de servidor, ocorrência e porta.

Exemplo:

DISPLAY_SQLSERVER=SQL_server\Server_instance, port

IS_AUTO_CREATE_SQLSERVER=FALSE - opcional. O valor predefinido é FALSE, o que significa que a base de dados não é criada. A base de dados deve já existir no servidor.

Para criar uma nova base de dados, defina este valor como TRUE.

IS_SQLSERVER_AUTHENTICATION=0 - opcional. O valor predefinido é 0, que especifica que as credenciais de autenticação do Windows do utilizador com sessão iniciada atual são utilizadas para autenticar o SQL Server. Para utilizar autenticação SQL, defina este valor como 1.

NOTA: O instalador necessita efetuar a autenticação no servidor SQL com estas permissões: criar base de dados, adicionar utilizador, atribuir permissões. As credenciais são credenciais de tempo de instalação e não credenciais de tempo de execução.

Se for utilizada a autenticação SQL, é necessário o seguinte:

IS_SQLSERVER_USERNAME

IS_SQLSERVER_PASSWORD

EE_SQLSERVER_AUTHENTICATION - obrigatória. Especifique o método de autenticação que o produto deve utilizar. Esta etapa associa uma conta ao produto. Estas credenciais são também utilizadas por serviços Dell, uma vez que são compatíveis com o Enterprise Server. Para utilizar autenticação do Windows, defina este valor como 0. Para utilizar autenticação SQL, defina o valor como 1.

NOTA: Certifique-se de que a conta tem direitos de administrador de sistema e a capacidade de gerir o SQL Server. A conta de utilizador deve ter o esquema predefinido de permissões do SQL Server: dbo e Associação de Funções da Base de Dados: dbo_owner, público.

SQL_EE_USERNAME - obrigatório. Com autenticação Windows, utilize este formato: DOMÍNIO\username. Com autenticação SQL, especifique o nome de utilizador.

SQL_EE_PASSWORD - obrigatório. Especifique a palavra-passe associada ao nome de utilizador Windows ou SQL.

Se for utilizada a autenticação SQL (EE_SQLSERVER_AUTHENTICATION=1), é necessário o seguinte:

RUNAS_KEYSERVER_USER - defina o Key Server para "executar como" nome de utilizador Windows com o seguinte formato: Domain \user. Deve tratar-se de uma conta de utilizador Windows.

RUNAS_KEYSERVER_PSWD - defina o Key Server para "executar como" a palavra-passe associada à conta de utilizador Windows.

SQL_ADD_LOGIN=T - opcional. A predefinição é zero (estes dados de início de sessão não são adicionados). Quando o valor está definido como T, se SQL_EE_USERNAME não for o início de sessão ou o utilizador da base de dados, o programa de instalação tenta adicionar as credenciais de autenticação SQL do utilizador e definir os privilégios para permitir que as credenciais sejam utilizadas pelo produto.

Seguem-se os parâmetros de nome do anfitrião. Edite os nomes dos anfitriões apenas se necessário. A Dell recomenda que utilize os nomes predefinidos. O formato deve ser `server.domain.com`.

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

CORESERVERHOST - opcional. Nome do anfitrião do Core Server.

RMIHOST - opcional. Nome do anfitrião do Compatibility Server.

REPORTERHOST - opcional. Nome do anfitrião do Compliance Reporter.

Parâmetros
DEVICEHOST - opcional. Nome do anfitrião do Device Server.
KEYSERVERHOST - opcional. Nome do anfitrião do Key Server.
TIGAHOST - opcional. Nome do anfitrião do Security Server.
SMTP_HOST - opcional. Nome do anfitrião SMTP.
ACTIVEMQHOST - opcional. Nome do anfitrião do Message Broker.
Seguem-se os parâmetros de porta. Edite as portas apenas se necessário. A Dell recomenda que utilize as predefinições
SERVERPORT_CLIENTAUTH - opcional.
REPORTERPORT - opcional.
DEVICEPORT - opcional.
KEYSERVERPORT - opcional.
GKPORT - opcional.
TIGAPORT - opcional.
SMTP_PORT - opcional.
ACTIVEMQ_TCP - opcional.
ACTIVEMQ_STOMP - opcional.

Instalar o Enterprise Server em modo desligado

O exemplo seguinte instala o Enterprise Server no modo silencioso, com uma caixa de diálogo de progresso, utilizando os parâmetros de instalação listados no ficheiro `C:\mysetups\eeoptions.txt\" "`

```
Setup.exe /s /v"/qb INSTALL_VALUES_FILE=\"C:\mysetups\eeoptions.txt\" "
```

Desinstalar o Dell Enterprise Server

1. No suporte multimédia de instalação da Dell, aceda ao diretório "Dell Enterprise Server". **Descomprima** (NÃO copie/cole nem arraste/largue) o Dell Enterprise Server-x64 para o diretório de raiz do servidor onde está a desinstalar o Enterprise Server. ***As operações de copiar/colar ou arrastar/largar produzirão erros e uma instalação malsucedida.***
2. Clique duas vezes no ficheiro **setup.exe**.
3. Na caixa de diálogo *Boas-vindas*, clique em **Seguinte**.
4. Na caixa de diálogo *Remover o programa*, clique em **Remover**.
   É apresentada uma caixa de diálogo de progresso durante todo o processo de desinstalação.
5. Quando a desinstalação estiver concluída, clique em **Concluir**.

5

Configuração de Pós-instalação

Leia o documento *Enterprise Server Technical Advisories* (Avisos técnicos do Enterprise Server) para ficar a conhecer as soluções alternativas existentes ou problemas conhecidos relacionados com a configuração do Dell Enterprise Server.

Quer esteja a instalar o Dell Enterprise Server pela primeira vez ou a atualizar uma instalação existente, alguns componentes do seu ambiente têm de ser configurados.

Instalação e configuração do EAS Management

Esta secção tem de ser concluída se pretender utilizar a Mobile Edition. Caso contrário, ignore esta secção e avance para Configuração do Dell Security Server no modo DMZ.

Pré-requisitos

- A conta para iniciar sessão no Serviço do Gestor de caixas de correio do EAS deve ser uma conta para criar/modificar a política de Exchange ActiveSync, atribuir políticas a caixas de correio de utilizadores e informações sobre a consulta de dispositivos ActiveSync.
- O utilitário de configuração EAS deve ser executado com permissões de administrador para modificar ficheiros e reiniciar serviços.
- É necessária uma ligação de rede ao Dell Policy Proxy.
- Tenha o FQDN do Dell Policy Proxy à sua disposição.
- Tenha o número da porta do Dell Policy Proxy à sua disposição.
- Microsoft Message Queuing (MSMQ) já deve estar instalado/configurado no servidor que aloja o ambiente Exchange. Caso contrário, consulte Install/Configure Microsoft Message Queuing (MSMQ) (Instalar/configurar o Microsoft Message Queuing (MSMQ).

Durante o processo de implementação

Se pretender utilizar o Exchange ActiveSync para gerir dispositivos móveis através do Mobile Edition, o seu ambiente Exchange Server deve estar configurado.

Instalar o Gestor de dispositivos do EAS

1. No suporte multimédia de instalação da Dell, aceda à pasta do EAS Management. Na pasta Gestor de dispositivos do EAS, copie o ficheiro setup.exe para o(s) seu(s) *Servidor(es) de acesso de cliente do Exchange*.
2. Clique duas vezes no ficheiro **setup.exe** para dar início à instalação. Se o seu ambiente incluir mais que um *Servidor de acesso de cliente do Exchange*, execute este instalador para cada um deles.
3. Selecione o idioma da instalação e, em seguida, clique em **OK**.
4. Clique em **Next** (Seguinte) quando for apresentado o ecrã *Welcome* (Boas-vindas).
5. Leia o acordo de licença, aceite os termos e clique em **Seguinte**.
6. Clique em **Next** (Seguinte) para instalar o Gestor de Dispositivos do EAS na localização predefinida **C:\Inetpub\wwwroot\Dell\EAS Device Manager\.**
7. Clique em **Install** (Instalar) no ecrã *Ready to Begin Installation* (Pronto para iniciar a instalação).

   Uma janela de estado apresenta o progresso da instalação.
8. Se desejar, selecione a caixa para apresentar o registo do instalador do Windows e clique em **Finish** (Concluir).

Instalar o Gestor de caixas de correio do EAS

1 No suporte multimédia de instalação da Dell, aceda à pasta do EAS Management. Na pasta "EAS Mailbox Manager" (Gestor de caixas de correio do EAS), copie o ficheiro setup.exe para o(s) seu(s) *Servidor(es) de caixa de correio do Exchange*.

2 Clique duas vezes no ficheiro **setup.exe** para dar início à instalação. Se o seu ambiente incluir mais que um *Servidor de caixa de correio do Exchange*, execute este instalador para cada um deles.

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

4 Clique em **Next** (Seguinte) quando for apresentado o ecrã *Welcome* (Boas-vindas).

5 Leia o acordo de licença, aceite os termos e clique em **Seguinte**.

6 Clique em **Next** (Seguinte) para instalar o Gestor de caixas de correio do EAS na localização predefinida **C:\Program Files\Dell\EAS Mailbox Manager\.**

7 No ecrã Informações de início de sessão, introduza as credenciais da conta do utilizador que irá iniciar sessão para utilizar este serviço.

Nome de utilizador: DOMAIN\Username

Palavra-passe: a palavra-passe associada a este nome de utilizador

Clique em **Seguinte**.

8 Clique em **Install** (Instalar) no ecrã *Ready to Begin Installation* (Pronto para iniciar a instalação).

Uma janela de estado apresenta o progresso da instalação.

9 Se desejar, selecione a caixa para apresentar o registo do instalador do Windows e clique em **Finish** (Concluir).

Utilizar o utilitário de configuração EAS

1 No mesmo computador, aceda a **Start** > **Dell** > **EAS Configuration Utility** > **EAS Configuration** (Iniciar >Utilitário de configuração EAS da Dell > Configuração EAS) para executar o utilitário de configuração EAS.

2 Clique em **Setup** (Configuração) para configurar as Definições do EAS Management.

3 Introduza a informação seguinte:

FQDN do Dell Policy Proxy

Porta do Dell Policy Proxy (a porta predefinida é a 8090)

Intervalo de consulta do Dell Policy Proxy (a predefinição é de 1 minuto)

Selecione a caixa para executar o Gestor de dispositivos EAS em modo apenas de relatório (recomendado durante a implementação)

> **NOTA:**
> Este modo permite que dispositivos/utilizadores desconhecidos tenham acesso ao Exchange ActiveSync mas permitindo ainda que receba relatórios de tráfego. Logo que a implementação esteja concluída e a funcionar, pode alterar esta definição para aumentar a segurança.

Clique em **OK**.

4 É apresentada uma mensagem de êxito. Clique em **Yes** (Sim) para reiniciar os serviços do gestor de caixa de correio IIS e EAS.

5 Clique em **Quit** (Sair) quando terminar.

Configurar definições do EAS Management

Logo que a implementação esteja concluída e a funcionar e esteja pronto para aumentar a segurança, siga os passos abaixo indicados.

1 Aceda a **Start** > **Dell** > **EAS Configuration Utility** > **EAS Configuration** (Iniciar > Utilitário de configuração EAS da Dell > Configuração EAS para executar o utilitário de configuração EAS).
2 Clique em **Setup** (Configuração) para configurar as Definições do EAS Management.
3 Introduza a informação seguinte:

FQDN do Dell Policy Proxy

Porta do Dell Policy Proxy (a porta predefinida é a 8090)

Intervalo de consulta do Dell Policy Proxy (a predefinição é de 1 minuto)

Desmarque a caixa para executar o Gestor de dispositivos EAS em modo apenas de relatório

Clique em **OK**.

4 É apresentada uma mensagem de êxito. Clique em **Yes** (Sim) para reiniciar os serviços do gestor de caixa de correio IIS e EAS.
5 Clique em **Quit** (Sair) quando terminar.

Configuração do DellSecurity Server no modo DMZ

Se o Dell Security Server for implementado num DMZ e numa rede privada, e se apenas o servidor DMZ tiver um certificado de domínio de uma autoridade de certificação (AC) fidedigna, é necessário realizar alguns passos manualmente para adicionar o certificado fidedigno à keystore Java da rede privada do Dell Security Server.

Se for utilizado um certificado fidedigno, ignore esta secção e avance para APNs Enrollment (Inscrição no APNs).

NOTA: Recomendamos vivamente que utilize certificados de domínio de autoridades de certificação fidedignas tanto para servidores de rede privada como DMZ.

Utilize a aplicação Keytool para importar o certificado de domínio DMZ

IMPORTANTE:
Faça uma cópia de segurança dos cacerts do **Dell**Security Server existentes antes de prosseguir com as instruções da aplicação Keytool. Se ocorrer um erro de configuração, pode reverter para o ficheiro guardado.

Suposições

- O Dell Security Server foi instalado com um certificado não fidedigno.
- O Dell Security Server no modo DMZ foi instalado utilizando um certificado assinado (Entrust, Verisign, etc.)
- Está disponível um ficheiro de certificado .pfx. Se tiver de converter o seu certificado para .pfx, consulte “Exporting a Certificate to .PFX Using the Certificate Management Console” (Exportar um certificado para .PFX utilizando a consola de gestão de certificados).

Processo

1 Adicione a aplicação Keytool ao caminho do sistema.

```
set path=%path%;<Dell Java Install Dir>\bin
```

2 Utilize a aplicação Keytool para apresentar uma lista dos conteúdos de certificados de domínios fidedignos que pretende importar. Tome nota do nome do alias apresentado.

```
keytool -list -v -keystore "
```

3 Utilize a aplicação Keytool para importar os conteúdos do certificado assinado para o ficheiro cacerts do Dell Security Server:

```
keytool -importkeystore -v -srckeystore "
```

Para -srcalias, terá de reunir estas informações dos conteúdos exportados do certificado assinado.

Para -destalias, pode ser qualquer localização que escolher.

4 Faça uma cópia de segurança e substitua o ficheiro cacerts atual no diretório <Security Server install dir>\conf\ pelo ficheiro cacerts recentemente criado no Dell Security Server.

Modificar o ficheiro application.properties

Modifique o ficheiro application.properties para especificar o alias do certificado de assinatura.

1 Vá para <Security Server install dir>\conf\application.properties
2 Modifique a informação seguinte:
keystore.alias.signing=<Mude este valor para o valor do passo 3 acima, para `-destalias`>
3 Reinicie o serviço Dell Security Server.

Inscrição no APNs

Se pretender utilizar a Mobile Edition para o Mobile Device Security com dispositivos iOS, tem de usar o assistente de Inscrição no APNs para:

- Criar um CSR
- Criar um certificado Push da Apple
- Carregar um certificado Push

Se não pretender utilizar a Mobile Edition para Mobile Device Security com dispositivos iOS, ignore esta secção e avance para a Ferramenta de Configuração do Servidor.

O serviço de notificações Push da Apple (APNs — Push Notification service) permite a comunicação segura com dispositivos iOS sem fios. O APNs é utilizado para enviar notificações para um dispositivo iOS para que verifique o estado do Dell Enterprise Server. O APNs apenas envia a notificação para o dispositivo, não envia dados.

Processo

1 Abra um browser e aceda a https://<FQDN-of-security-server>:8443/csrweb.
2 Na caixa de diálogo de início de sessão do assistente de inscrição no APNs, introduza as suas credenciais de administrador Dell e clique em **Iniciar sessão**.
3 É apresentada uma caixa de diálogo que descreve os passos que vai realizar. Clique em **Seguinte**.

Passo I: Criar CSR

4 Introduza a informação seguinte:

Correio eletrónico: o endereço de e-mail pode ser qualquer UPN, mas recomendamos que utilize uma conta para o administrador que vai fazer a manutenção do certificado do APNs.

Nome comum: introduza o nome comum associado a este endereço de correio eletrónico.

Clique em **Gerar CSR**.

5 Depois de gerar o CSR, guarde o ficheiro num local de fácil acesso.

6 Clique em **Seguinte**.

Passo II: Criar certificado Push da Apple

7 Clique na ligação para o **Portal de certificados Push da Apple**. Inicie sessão com a sua ID e palavra-passe da Apple.

8 Leia os termos de utilização, indique a sua conformidade e clique em **Aceitar**.

9 Clique em **Procurar** e, em seguida, em **Carregar** para carregar o certificado que acaba de criar.

10 Na página *Certificados para servidores de terceiros*, clique em **Transferir**. Guarde o ficheiro num local de fácil acesso.

11 Volte ao assistente de inscrição no APNs e clique em **Seguinte**.

Passo III: Carregar um certificado Push

12 Introduza as seguintes informações (utilize as mesmas credenciais que utilizou em Passo I: Criar CSR.

Correio eletrónico:

Nome comum:

Ficheiro de certificado Push: Clique em **Procurar** para localizar o ficheiro guardado no passo 7. Clique em **Carregar**.

13 É apresentada uma mensagem de êxito. Clique em **Concluir**.

A inscrição do certificado no APNs com o Dell Enterprise Server está concluída.

Server Configuration Tool

Se for necessário configurar o seu ambiente depois de ter completado a instalação, utilize a Dell Server Configuration Tool para fazer essas alterações.

A Dell Server Configuration Tool permite-lhe:

- Adicionar certificados novos ou atualizados
- Importar Certificado do Dell Manager
- Importar Certificado de Identidade
- Configurar as definições de Certificado do Servidor SSL ou Mobile Edition
- Configurar definições de SMTP para Data Guardian ou serviços de email
- Alterar o nome da base de dados, a localização ou as credenciais
- Migrar a base de dados

O Core Server e o Compatibility Server não podem ser executados em simultâneo com a Dell Server Configuration Tool. Interrompa o serviço Dell Core Server e o serviço Dell Compatibility Server em *Serviços* (**Iniciar > Executar**. Escreva ***services.msc***) antes de iniciar a Dell Server Configuration Tool.

Para iniciar a Dell Server Configuration Tool vá a **Iniciar** > **Programas** > **Dell** > **Enterprise Edition** > **Server Configuration Tool** > **Executar Server Configuration Tool**.

A Dell Server Configuration Tool guarda os registos em **C:\Program Files\Dell\Enterprise Edition\Configuration Tool\Logs.**

Adicionar certificados novos ou atualizados

Pode escolher que tipo de certificados pretende utilizar - autoassinados ou assinados:

- Os certificados **autoassinados** são assinados pelo próprio criador. Os certificados autoassinados são adequados para pilotos, POCs, etc. Para um ambiente de produção, a Dell recomenda a utilização de certificados assinados por uma AC pública ou assinados por domínio.
- Os certificados **assinados** (assinados por uma AC pública ou assinados por domínio) são assinados por uma AC pública ou por um domínio. No caso de certificados assinados por uma autoridade de certificação (AC) pública, o certificado da autoridade assinante

normalmente já existe no arquivo de certificados da Microsoft e, como tal, a cadeia de certificação será automaticamente estabelecida. No caso dos certificados de uma AC de domínio, se a estação de trabalho tiver sido anexada ao domínio, o certificado da AC assinante de domínio terá sido adicionado ao arquivo de certificados da Microsoft da estação de trabalho, criando também uma cadeia de certificação.

Os componentes afetados pela configuração de certificados são:

- Serviços Java (por exemplo, Dell Device Server e assim por diante)
- Aplicações .NET (Dell Core Server)
- Validação de smart cards utilizados para a Autenticação de pré-arranque (Dell Security Server)
- Importação de chaves de encriptação privadas para serem utilizadas na assinatura de pacotes de política a enviar ao Dell Manager. O Dell Manager efetua a validação SSL para clientes Enterprise Edition geridos remotamente com unidades de encriptação automática ou com o BitLocker Manager.
- Estações de trabalho cliente:
    - Estações de trabalho que executam o BitLocker Manager
    - Estações de trabalho que executam o Enterprise Edition (clientes Windows)
    - Estações de trabalho que executam o Endpoint Security Suite
    - Estações de trabalho que executam o Endpoint Security Suite Enterprise

Informação acerca do tipo de certificados a utilizar:

A autenticação de pré-arranque utilizando smart cards requer a validação SSL com o Dell Security Server. O Dell Manager efetua a validação SSL ao ligar-se ao Dell Core Server. Para este tipo de ligações, a AC assinante terá de estar na keystore (seja na keystore da Java ou na keystore da Microsoft, dependendo do componente do servidor Dell em causa). Se forem selecionados certificados autoassinados, estão disponíveis as seguintes opções:

- Validação de smart cards utilizados para a autenticação de pré-arranque:
    - Importe o certificado de assinatura da "Agência raiz" e a cadeia de certificação completa na keystore Java do Dell Security Server. Para mais informações, consulte: criar um certificado autoassinado e gerar um pedido de assinatura de certificado. Tem de ser importada a cadeia de certificação completa.

Dell Manager:

- Insira o certificado de assinatura da "Agência raiz", a partir do certificado autoassinado que foi gerado, em "Autoridades de Certificação de Raiz Fidedigna" (para o "computador local") da estação de trabalho na keystore da Microsoft.
- Modificar o comportamento da validação SSL do lado do servidor. Para desativar a validação de confiança SSL do lado do servidor, marque **Desativar verificação da cadeia de certificação** no separador Definições.

Existem dois métodos para criar um certificado — o *Expresso* e o *Avançado*.

Escolha **um** método:

- Expresso - Escolha este método para gerar um certificado autoassinado para todos os componentes. Este é o método mais fácil, mas os certificados autoassinados são adequados apenas para pilotos, POC, etc. Para um ambiente de produção, a Dell recomenda a utilização de certificados assinados por uma autoridade de certificação (AC) pública ou assinados por domínio.
- Avançado - Escolha este método para configurar cada componente separadamente.

Expresso

1 A partir do menu superior, selecione **Ações** > **Configurar certificados**.

2 Quando o assistente de configuração for iniciado, selecione **Expresso** e clique em **Seguinte**. Serão utilizadas as informações do certificado autoassinado que foi criado aquando da instalação do Enterprise Server, se disponíveis.

3 A partir do menu superior, selecione **Configuração** > **Guardar**. Se pedido, confirme a gravação.

A configuração do certificado foi concluída. O resto da presente secção descreve pormenorizadamente o método avançado de criação de um certificado.

Avançado

Existem duas formas de criar um certificado - *Gerar um certificado autoassinado* e *Utilizar as definições atuais*. Escolha **uma** das formas:

- Caminhio1 - Gerar certificado autoassinado
- Caminho 2 - Utilizar definições atuais

Caminhio1 - Gerar certificado autoassinado

1 A partir do menu superior, selecione **Ações** > **Configurar certificados**.

2 Quando o assistente de configuração for iniciado, selecione **Avançado** e clique em **Seguinte**.

3 Selecione **Gerar certificado autoassinado** e clique em **Seguinte**. Serão utilizadas as informações do certificado autoassinado que foi criado aquando da instalação do Enterprise Server, se disponíveis.

4 A partir do menu superior, selecione **Configuração** > **Guardar**. Se pedido, confirme a gravação.

A configuração do certificado foi concluída. O resto da presente secção descreve pormenorizadamente o outro método de criação de um certificado.

Caminho 2 - Utilizar definições atuais

1 A partir do menu superior, selecione **Ações** > **Configurar certificados**.

2 Quando o assistente de configuração for iniciado, selecione **Avançado** e clique em **Seguinte**.

3 Selecione **Utilizar as definições atuais** e clique em **Seguinte**.

4 Na janela *Certificado SSL do Compatibility Server*, selecione **Gerar certificado autoassinado** e clique em **Seguinte**. Serão utilizadas as informações do certificado autoassinado que foi criado aquando da instalação do Enterprise Server, se disponíveis.

Clique em **Seguinte**.

5 Na janela *Certificado SSL do Core Server*, selecione uma das seguintes opções:

- *Selecionar certificado* - Selecione esta opção para utilizar um certificado existente. Clique em **Seguinte**.

  Navegue até à localização do certificado existente, introduza a palavra-passe associada ao certificado existente e clique em **Seguinte**.

  Clique em **Concluir** quando tiver terminado.
- *Gerar certificado autoassinado* – Serão utilizadas as informações do certificado autoassinado que foi criado aquando da instalação do Enterprise Server, se disponíveis. Se selecionar esta opção, a janela Certificado de segurança da mensagem não é apresentada (a janela é apresentada se selecionar a opção *Utilizar definições atuais* e é utilizado o certificado criado para o Dell Compatibility Server.

  Verifique se o nome do computador completamente qualificado está correto. Clique em **Seguinte**.

  É apresentada uma mensagem de aviso indicando que já existe um certificado com o mesmo nome. Quando lhe for perguntado se o pretende utilizar, clique em **Sim**.

  Clique em **Concluir** quando tiver terminado.
- *Utilizar definições atuais* - Selecione esta opção para alterar uma definição num certificado a qualquer altura após a configuração inicial do Dell Enterprise Server. Se selecionar esta opção, o seu certificado já configurado é guardado no devido lugar. Ao selecionar esta opção, avança até à janela Certificado de segurança da mensagem.

  Na janela Certificado de segurança da mensagem, selecione **uma** das seguintes opções:

  - *Selecionar certificado* - Selecione esta opção para utilizar um certificado existente. Clique em **Seguinte**.

    Navegue até à localização do certificado existente, introduza a palavra-passe associada ao certificado existente e clique em **Seguinte**.

Clique em **Concluir** quando tiver terminado.

- *Gerar certificado autoassinado* – Serão utilizadas as informações do certificado autoassinado que foi criado aquando da instalação do Enterprise Server, se disponíveis.

  Clique em **Seguinte**.

  Clique em **Concluir** quando tiver terminado.

A configuração do certificado foi concluída.

Quando terminar as alterações:

1 A partir do menu superior, selecione **Configuração** > **Guardar**. Se pedido, confirme a gravação.

2 Feche a Dell Server Configuration Tool.

3 Clique em **Iniciar** > **Executar**. Escreva *services.msc* e clique em **OK**. Quando a janela *Serviços* abrir, navegue até cada serviço Dell e clique em **Iniciar o serviço**.

Importar Certificado do Dell Manager

Se a sua implementação incluir clientes Enterprise Edition geridos remotamente com unidades de encriptação automática ou o BitLocker Manager, deve importar o seu certificado recentemente criado (ou existente). O certificado do Dell Manager é utilizado como um meio de proteger a chave privada utilizada para assinar os pacotes de política a enviar aos clientes geridos à distância do Enterprise Edition e BitLocker Manager.BitLocker Manager. Este certificado pode ser independente de qualquer um dos outros certificados. Adicionalmente, se a chave estiver comprometida, esta pode ser substituída por uma chave nova, e o Dell Manager irá pedir uma nova chave pública se não conseguir desencriptar os conjuntos de política.

1 Abra a Consola de Gestão da Microsoft (MMC - Microsoft Management Console).

2 Clique em **File** > **Add/Remove Snap-in** (Ficheiro > Adicionar/Remover Snap-in).

3 Clique em **Add** (Adicionar).

4 Na janela *Add Standalone Snap-in* (Adicionar Snap-in autónomo), selecione **Certificates** (Certificados) e clique em **Add** (Adicionar).

5 Selecione **Computer Account** (Conta de computador) e clique em **Next** (Seguinte).

6 Na janela *Select Computer* (Selecionar computador), selecione **Local computer (the computer this console is running on)** (Computador local (o computador onde esta consola é executada)) e clique em **Finish** (Concluir).

7 Clique em **Fechar**.

8 Clique em **OK**.

9 Na pasta *Console Root* (Raiz da consola), expanda *Certificates (Local Computer)* (Certificados (computador local)).

10 Aceda à pasta *Personal* (Pessoal) e localize o certificado pretendido.

11 Realce o certificado pretendido, clique com o botão direito do rato em **All Tasks** > **Export** (Todas as tarefas > Exportar).

12 Quando o assistente para exportar certificados abrir, clique em **Next** (Seguinte).

13 Selecione **Yes, export the private key** (Sim, exportar a chave privada) e clique em **Next** (Seguinte).

14 Selecione **Personal Information Exchange - PKCS #12 (.PFX)** e depois selecione as subopções **Include all certificates in the certification path if possible** (Incluir todos os certificados no caminho de certificação, se possível) e **Export all extended properties** (Exportar todas as propriedades expandidas). Clique em **Seguinte**.

15 Introduza e confirme uma palavra-passe. Esta pode ser qualquer palavra-passe da sua escolha. Escolha uma palavra-passe que seja fácil de recordar, mas difícil de outros adivinharem. Clique em **Seguinte**.

16 Clique em **Browse** (Procurar) para navegar para o local onde gostaria de guardar o ficheiro.

17 No campo `File Name` (Nome do ficheiro), introduza um nome para guardar o ficheiro como. Clique em **Guardar**.

18 Clique em **Seguinte**.

19 Clique em **Concluir**.

20 É apresentada uma mensagem indicando que a exportação foi realizada com êxito. Feche a MMC.

21 Volte para a Dell Server Configuration Tool.

22 A partir do menu superior, selecione **Actions** > **Import Manager Certificate** (Ações > Importar certificado do gestor).

23 Navegue até à localização onde o ficheiro exportado foi guardado. Selecione o ficheiro e clique em **Open** (Abrir).

24 Introduza a palavra-passe associada a este ficheiro e clique em **OK**.

A importação do certificado do Dell Manager está agora concluída.

Quando terminar as alterações:

1 A partir do menu superior, selecione **Configuration** > **Save** (Configuração > Guardar). Se pedido, confirme a gravação.

2 Feche a Dell Server Configuration Tool.

3 Clique em **Start** > **Run** (Iniciar > Executar). Escreva *services.msc* e clique em **OK**. Quando a janela *Services* (Serviços) abrir, navegue até cada serviço Dell e clique em **Start the service** (Iniciar o serviço).

Importar Certificado de Identidade

Se a sua implementação incluir o Server Encryption, terá de importar o certificado recentemente criado (ou existente). O certificado de identidade protege a chave privada que é utilizada para assinar os pacotes de políticas enviados aos servidores cliente. Este certificado pode ser independente de qualquer um dos outros certificados.

1 A partir do menu superior, selecione **Actions** > **Import Identity Certificate** (Ações > Importar certificado de identificação).

2 Procure para selecionar um certificado e clique em **Next** (Seguinte).

3 No pedido de Palavra-passe de certificado, introduza a palavra-passe associada com o certificado existente.

4 Na Caixa de diálogo de conta do Windows, escolha uma opção:

   a Para alterar as credenciais associadas com o certificado de identidade, selecione **Use different Windows account credentials with the identity certificate** (Utilizar credenciais de conta do Windows diferentes com o certificado de identidade).

   b Para continuar e utilizar as credenciais da conta presentemente ativa, clique em **Next** (Seguinte).

5 A partir do menu superior, selecione **Configuration** > **Save** (Configuração > Guardar). Se pedido, confirme a gravação.

Configurar as definições de Certificado do Servidor SSL ou Mobile Edition

Em Server Configuration Tool, clique no separador **Definições**.

Dell Manager:

Para desativar a validação de confiança SSL do lado do servidor do Dell Manager, assinale a opção **Desativar verificação de cadeia de certificação**.

SCEP:

Se estiver a utilizar a Mobile Edition, introduza o URL do servidor anfitrião do SCEP.

Quando terminar as alterações:

1 A partir do menu superior, selecione **Configuração** > **Guardar**. Se pedido, confirme a gravação.

2 Feche a Dell Server Configuration Tool.

3 Clique em **Iniciar** > **Executar**. Escreva *services.msc* e clique em **OK**. Quando a janela *Serviços* abrir, navegue até cada serviço Dell e clique em **Iniciar o serviço**.

Configurar definições de SMTP para Data Guardian ou serviços de email

Em Server Configuration Tool, clique no separador **SMTP**.

Este separador configura as definições SMTP para o Data Guardian. Se as definições SMTP tiverem de ser configuradas para outra finalidade fora do Data Guardian, consulte o tópico "Ativar servidor SMTP para notificações por correio eletrónico de licença" de "AdminHelp".

Introduza a informação seguinte:

1 No campo Nome do anfitrião:, introduza o FQDN do seu servidor SMTP, por exemplo smtpservername.domain.com.

2 No campo Nome de utilizador:, introduza o nome de utilizador que iniciará sessão no servidor de correio eletrónico. O formato pode ser DOMÍNIO\jsilva, jsilva ou o que for estabelecido pela sua organização.

3 No campo Palavra-passe:, introduza a palavra-palavra-passe associada a este nome de utilizador.

4 No campo Do endereço:, introduza o endereço de correio eletrónico de onde será enviada a mensagem. Este pode ser o mesmo da conta do nome de utilizador (jsilva@domínio.com), mas também pode ser de outra conta a que o nome de utilizador especificado tenha acesso para enviar mensagens de correio eletrónico (RegistonaNuvem@domínio.com).

5 No campo Porta:, introduza o número da porta (normalmente 25).

6 No menu Autenticação:, selecione Verdadeiro ou Falso.

Quando terminar as alterações:

1 A partir do menu superior, selecione **Configuração** > **Guardar**. Se pedido, confirme a gravação.

2 Feche a Dell Server Configuration Tool.

3 Clique em **Iniciar** > **Executar**. Escreva *services.msc* e clique em **OK**. Quando a janela *Serviços* abrir, navegue até cada serviço Dell e clique em **Iniciar o serviço**.

Alterar o nome da base de dados, a localização ou as credenciais

Em Server Configuration Tool, clique no separador **Database** (Base de dados).

1 No campo: `Server Name:` (Nome do Servidor) introduza o nome de domínio totalmente qualificado (no caso de existir um nome de instância, inclua-o) do servidor anfitrião da base de dados. Por exemplo, SQLTest.domain.com\DellDB.

A Dell recomenda a utilização de um nome de domínio totalmente qualificado, embora possa ser utilizado um endereço IP.

2 No campo `Server Port` (Porta do Servidor): introduza o número da porta.

Quando utilizar uma instância não predefinida do SQL Server, precisa especificar a porta dinâmica da instância no campo*Port:* (Porta). Como alternativa, ative o serviço SQL Server Browser e certifique-se de que a porta UDP 1434 está aberta. Para obter mais informações, consulte https://msdn.microsoft.com/en-us/library/hh510203(v=sql.120).aspx.

3 No campo `Database` (Base de dados): introduza o nome da base de dados.

4 No campo *Authentication:* (Autenticação) selecione **Windows Authentication** (Autenticação do Windows) ou **SQL Server Authentication** (Autenticação de SQL Server). Se escolher a Autenticação do Windows, as mesmas credenciais que foram utilizadas para iniciar sessão no Windows serão utilizadas para autenticação (os campos Nome de utilizador e Palavra-passe não serão editáveis).

5 No campo *User Name* (Nome de utilizador): introduza o nome de utilizador associado a esta base de dados.

6 No campo *Password* (Palavra-passe): introduza a palavra-passe associada ao nome de utilizador facultado no campo "UserName "(Nome de utilizador).

7 A partir do menu superior, selecione **Configuration** > **Save** (Configuração > Guardar). Se pedido, confirme a gravação.

8 Para testar a configuração da base de dados, no menu superior, selecione **Actions** > **Test Database Configuration** (Ações > Testar Configuração da Base de Dados). O Assistente de configuração é iniciado.

9 Na janela *Configuration Test* (Teste de Configuração), leia a informação e depois clique em **Next** (Seguinte).

10 No caso de escolher Autenticação do Windows no separador *Database* (Base de dados), poderá, opcionalmente, introduzir credenciais alternativas para utilizar as mesmas credenciais que serão usadas para executar o Dell Enterprise Server. Clique em **Seguinte**.

11 Na janela de *Test Configuration* (Testar Configuração), serão exibidos os resultados das definições de Testar Ligação, Teste de Compatibilidade e Teste Migrado de Base de Dados.

12 Clique em **Concluir**.

NOTA:
Se a base de dados do SQL ou instância do SQL está configurada com um agrupamento não predefinido, o agrupamento precisa ser sensível a maiúsculas e minúsculas. Para ver a lista de agrupamentos e de sensibilidade a maiúsculas e minúsculas, consulte https://msdn.microsoft.com/en-us/library/ms144250(v=sql.105).aspx.

Quando terminar as alterações:

1 A partir do menu superior, selecione **Configuration** > **Save** (Configuração > Guardar). Se pedido, confirme a gravação.

2 Feche a Dell Server Configuration Tool.

3 Clique em **Start** > **Run** (Iniciar > Executar). Escreva *services.msc* e clique em **OK**. Quando a janela *Services* (Serviços) abrir, navegue até cada serviço Dell e clique em **Start the service** (Iniciar o serviço).

Migrar a base de dados

Pode migrar uma base de dados v8.x para o esquema mais recente com a versão mais recente da Server Configuration Tool. Para obter a Server Configuration Tool mais recente ou para migrar uma base de dados anterior à v8.0, entre em contacto com o Dell ProSupport para obter assistência.

Em Server Configuration Tool, clique no separador **Database** (Base de dados).

1 Caso ainda não tenha realizado a cópia de segurança da sua atual base de dados Dell, **faça-o agora**.

2 No menu superior, selecione **Actions** > **Migrate Database** (Ações > Migrar Base de Dados). O Assistente de configuração é iniciado.

3 Será exibida uma mensagem de aviso na janela *Migrate Enterprise Database* (Migrar Base de Dados Enterprise). Confirme que realizou a cópia de segurança da totalidade da base de dados ou confirme que não é necessário realizar uma cópia de segurança da sua base de dados corrente. Clique em **Seguinte**.

   Na janela *Migrating Database* (a Migrar Base de Dados) serão exibidas mensagens informativas sobre o estado da migração.

   Ao terminar, verifique se ocorreram erros.

   NOTA: Uma mensagem de erro identificada por , indica que houve uma falha numa tarefa da base de dados e que é necessário tomar uma ação corretiva antes de poder migrar corretamente a base de dados. Clique em Finish (Concluir), corrija os erros da base de dados e repita o procedimento descrito nesta secção.

4 Clique em **Concluir**.

Uma vez concluída a migração:

1 A partir do menu superior, selecione **Configuration** > **Save** (Configuração > Guardar). Se pedido, confirme a gravação.

2 Feche a Dell Server Configuration Tool.

3 Clique em **Start** > **Run** (Iniciar > Executar). Escreva *services.msc* e clique em **OK**. Quando a janela *Services* (Serviços) abrir, navegue até cada serviço Dell e clique em **Start the service** (Iniciar o serviço).

Tarefas administrativas

Atribuir papel de Administrador Dell

1 Como Administrador Dell, inicie sessão na Remote Management Console neste endereço: https://server.domain.com:8443/webui/ As credenciais predefinidas são **superadmin/changeit**.
2 No painel esquerdo, clique em **Populations** > **Domains** (Populações > Domínios.)
3 Clique num domínio ao qual pretenda adicionar um utilizador.
4 Na página Detalhe do domínio, clique no separador **Members** (Membros).
5 Clique em **Add user** (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, 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 *Directory User List* (Lista de utilizadores do diretório) para adicionar ao domínio. Utilize <Shift><click> ou <Ctrl><click> para selecionar múltiplos utilizadores.
8 Clique em **Add** (Adicionar).
9 Na barra de menus, clique no separador **Details & Actions** (Detalhes e ações) do utilizador especificado.
10 Desloque-se na barra de menus e selecione o separador **Admin** (Administração).
11 Selecione os papéis do administrador a adicionar a este utilizador.
12 Clique em **Guardar**.

Iniciar sessão com o Papel de Administrador Dell

1 Termine sessão na Remote Management Console do Enterprise Server.
2 Inicie sessão na Remote Management Console do Enterprise Server com as credenciais de utilizador do domínio.

Carregar licença de acesso de cliente

Deverá ter recebido as licenças de acesso de cliente separadamente dos ficheiros de instalação, com a compra inicial ou mais tarde se tiver adicionado mais licenças de acesso de cliente.

1 No painel da esquerda, clique em **Management** (Gestão).
2 Clique em **License Management** (Gestão de licenças).
3 Clique em **Choose File** (Escolher ficheiro) para localizar e selecionar o ficheiro de licença de cliente.

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 **Management** > **Commit** (Gestão > Consolidar).
2 Introduza uma descrição da alteração no campo Comentários.
3 Clique em **Commit Policies** (Consolidar políticas).

Configurar o Dell Compliance Reporter

1 No painel da esquerda, clique em **Compliance Reporter**.
2 Quando o Dell Compliance Reporter iniciar, inicie sessão com as credenciais predefinidas de *superadmin/changeit*.
3 São suportados dois métodos de autenticação. Para configurar, selecione:

- Configurar autenticação do SQL com o Compliance Reporter
- Configurar autenticação do Windows com o Compliance Reporter

Configurar autenticação do SQL com o Compliance Reporter

A partir da v8.1, a Origem de dados é pré-configurada imediatamente após a instalação. Não é necessária qualquer configuração. Siga os passos abaixo para alterar o Data Source, se necessário.

1 Para definir a fonte de dados, no menu superior, clique em **Settings** (Definições). No menu do lado esquerdo, clique em **Data Source** (Fonte de dados).
2 Introduza o nome de utilizador para iniciar sessão na base de dados da Dell.
3 Introduza a palavra-passe para iniciar sessão na base de dados da Dell.
4 Introduza o nome de anfitrião para iniciar sessão na base de dados da Dell.
5 Introduza o nome da base de dados para iniciar sessão na base de dados da Dell.
6 Introduza o número máximo de ligações inativas permitidas. A predefinição é 2.
7 Introduza o número máximo de ligações (ativas) permitidas. A predefinição é 10.
8 Introduza o tempo de espera máximo (número máximo de milissegundos de espera pela ligação). -1 é indefinido
9 Para verificar o URL da base de dados e testar a conetividade entre o Dell Compliance Reporter e a base de dados da Dell, clique em **Test Connection** (Testar ligação).
10 Clique em **Update** (Atualizar). Para ignorar as informações, clique em Cancelar.

As tarefas administrativas estão concluídas O resto deste capítulo abordará a Autenticação do Windows e pode ser ignorado se a Autenticação do SQL for utilizada no Dell Compliance Reporter.

Se necessário, avance para Create a Self-Signed Certificate and Generate a Certificate Signing Request (Criar um certificado autoassinado e Gerar pedido de assinatura de certificado) ou Export a Certificate to .PFX Using the Certificate Management Console (Exportar um certificado para .PFX utilizando a consola de gestão de certificados).

Configurar autenticação do Windows com o Compliance Reporter

A partir da v8.1, a Origem de dados é pré-configurada imediatamente após a instalação. Não é necessária qualquer configuração. Siga os passos abaixo para alterar o Data Source, se necessário.

1 Introduza o nome de utilizador para iniciar sessão na base de dados da Dell.
2 Deixe a palavra-passe em branco. Quando o utilizador de domínio iniciar sessão, a sua palavra-passe será transferida para a base de dados.
3 Introduza o nome de anfitrião para iniciar sessão na base de dados da Dell.
4 Introduza o nome da base de dados para iniciar sessão na base de dados da Dell.
5 Introduza o número máximo de ligações inativas permitidas. A predefinição é 2.

6 Introduza o número máximo de ligações (ativas) permitidas. A predefinição é 10.

7 Introduza o tempo de espera máximo (número máximo de milissegundos de espera pela ligação). -1 é indefinido

8 Para verificar o URL da base de dados e testar a conetividade entre o Dell Compliance Reporter e a base de dados da dell, clique em **Test Connection** (Testar ligação).

9 Clique em **Update** (Atualizar). Para ignorar as informações, clique em Cancelar.

As tarefas administrativas estão concluídas **Se necessário**, avance para Create a Self-Signed Certificate and Generate a Certificate Signing Request (Criar um certificado autoassinado e Gerar pedido de assinatura de certificado) ou Export a Certificate to .PFX Using the Certificate Management Console (Exportar um certificado para .PFX utilizando a consola de gestão de certificados).

Realizar Cópias de Segurança

Tendo em vista a recuperação de desastres, certifique-se de que são feitas semanalmente cópias de segurança das seguintes localizações, com diferenciais noturnos.

Cópias de segurança do Enterprise Server

Realize regularmente cópias de segurança dos ficheiros que estão armazenados na localização que selecionou para a cópia de segurança do ficheiro de configuração durante a instalação (passo 10 na página 27 ou Atualização/Migração (passo 6 na página 68). É aceitável a realização de cópias de segurança semanais destes dados, uma vez que raramente são alterados e que podem ser reconfigurados manualmente, se necessário. Os ficheiros mais importantes contêm as informações necessárias para estabelecer ligação à base de dados:

<Pasta de instalação>\Enterprise Edition\Compatibility Server\conf\server_config.xml

<Pasta de instalação>\Enterprise Edition\Compatibility Server\conf\secretKeyStore

<Pasta de instalação>\Enterprise Edition\Compatibility Server\conf\gkresource.xml

Cópias de segurança do SQL Server

Realize cópias de segurança completas noturnas com registo transacional ativado e realize cópias de segurança da base de dados diferencial a cada 3-4 horas. Se estiver disponível uma cópia de segurança de base de dados, a recomendação seria que os registos transacionais e/ou tarefas de envio de registos sejam realizadas em intervalos de 15 minutos (ou intervalos menores, se possível). Como sempre, recomendamos que sejam seguidas as melhores práticas de utilização de base de dados para a base de dados da Dell e que o software Dell esteja incluído no plano de recuperação de desastres da sua organização.

Para mais informações sobre as melhores práticas do SQL Server, consulte The following list explains SQL server best practices, which should be implemented when Dell Data Protection is installed if not already implemented (A lista seguinte explica as melhores práticas do SQL Server, que devem ser implementadas quando o Dell Data Protection for instalado, caso ainda não esteja).

Cópias de segurança do PostgreSQL Server

Os eventos de auditoria são armazenados no servidor PostgreSQL, que deve ser alvo de uma cópia de segurança regular. Para obter instruções sobre cópias de segurança, consulte https://www.postgresql.org/docs/9.5/static/backup.html.

A Dell recomenda que sejam seguidas as melhores práticas de utilização da base de dados para a base de dados PostgreSQL e que o software Dell esteja incluído no plano de recuperação de desastres da sua organização.

7

Descrições de componentes Dell

A tabela seguinte descreve cada componente e a sua função.

Nome	Descrição	Necessária para
Compliance Reporter	Oferece uma visão abrangente do ambiente, tendo em vista a elaboração de relatórios de auditoria e conformidade. Um componente do Dell Enterprise Server.	Relatório
Key Server	Negocia, autentica e encripta uma ligação de cliente utilizando APIs Kerberos. Requer o acesso à base de dados do SQL para extrair os dados de chave. Um componente do Dell Enterprise Server.	Utilitários Dell Admin
Server Configuration Tool	Configura a comunicação da base de dados com o Core Server e o Compatibility Server/ Security Server. Utilizado para inicializar a base de dados após a instalação ou para migrar a base de dados para um esquema mais recente. Utilizado para controlar os serviços Dell. Um componente do Dell Enterprise Server.	Todos
Remote Management ConsoleEnterprise Server Console	Consola de administração e centro de controlo para implementação na empresa inteira. Um componente do Dell Enterprise Server.	Todos
Core Server	Gere o fluxo das políticas, as licenças e o registo para PBA (Preboot Authentication), SED Management, BitLocker Manager, Threat Protection e Advanced Threat Protection. Processa dados de inventário para utilização pelo Compliance Reporter e pela Remote Management Console. Reúne e armazena os dados de autenticação. Controla o acesso baseado em funções. Um componente do Dell Enterprise Server.	Todos
Security Server	Comunica com o Policy Proxy; gere obtenções de chaves forenses, ativações de clientes, produtos Data Guardian, comunicação SED-PBA e comunicação Active Directory para autenticação ou reconciliação, incluindo validação de identidade para autenticação na Remote Management Console. Requer o acesso à base de dados SQL.	Todos

Nome	Descrição	Necessária para
	Um componente do Dell Enterprise Server.	
Compatibility Server	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 neste serviço. Um componente do Dell Enterprise Server.	Todos
Message Broker Service	Trata da comunicação entre serviços do Enterprise Server. Prepara as informações de políticas criadas pelo Compatibility Server para colocação em fila de policy proxy Requer o acesso à base de dados SQL. Um componente do Dell Enterprise Server.	Todos
Device Server	Suporta ativações e recuperação de palavra-passe. Um componente do Dell Enterprise Server.	Enterprise Edition para Mac Enterprise Edition para Windows Proteções portáteis CREDActivate
Plug-ins do Device Server	Oferece suporte para vários componentes. Um componente do Dell Enterprise Server.	Todos
Identity Server	Trata dos pedidos de autenticação de domínio. Requer uma conta Active Directory. Tem de ser a conta utilizada para aceder a SQL quando a Autenticação do Windows é utilizada. Um componente do Dell Enterprise Server.	Todos
Policy Proxy	Oferece uma linha de comunicação com base na rede de forma a proporcionar atualizações de políticas de segurança e atualizações de inventário. Um componente do Dell Enterprise Server.	Enterprise Edition para Mac Enterprise Edition para Windows Mobile Edition para Mobile Device Security
Security Token Services (STS)	Utilizado para ajudar a criar um canal de autenticação seguro entre a interface do utilizador do Dell Enterprise Server e os Serviços de back end da Dell.	Todos
Gestor de dispositivos EAS	Ativa a funcionalidade Instalado no servidor de Acesso para Cliente do Exchange	Gestão do Exchange ActiveSync de dispositivos móveis.
Gestor da Caixa de correio do EAS	O agente da caixa de correio que está instalado no servidor de Caixa de correio do Exchange.	Gestão do Exchange ActiveSync de dispositivos móveis.

8

Melhores práticas do SQL Server

A lista seguinte explica as melhores práticas acerca do SQL Server, as quais devem ser implementadas quando o Dell Data Protection for instalado (se ainda não estiver).

1 Certifique-se de que o tamanho do bloco NTFS onde se encontram o ficheiro de dados e o ficheiro de registo é de 64 KB. As extensões do SQL Server (unidade básica do SQL Storage) são de 64 KB.

   Para obter mais informações, procure "Understanding Pages and Extents" (Compreender páginas e extensões) nos artigos TechNet da Microsoft.

   - Microsoft SQL Server 2008 - http://technet.microsoft.com/en-us/library/ms190969%28v=sql.100%29
   - Microsoft SQL Server 2008 R2 - http://technet.microsoft.com/en-us/library/ms190969(v=sql.105).aspx

2 Como orientação geral, defina a quantidade máxima da memória do SQL Server para 80% da memória instalada.

   Para obter mais informações, procure "Server Memory Server Configuration Options" (Opções de configuração de memória do servidor" nos artigos TechNet da Microsoft.

   - Microsoft SQL Server 2008 - http://technet.microsoft.com/en-us/library/ms178067%28v=sql.100%29
   - Microsoft SQL Server 2008 R2 - http://technet.microsoft.com/en-us/library/ms178067%28v=sql.105%29
   - Microsoft SQL Server 2012 - https://technet.microsoft.com/en-us/library/ms178067(v=sql.110)
   - Microsoft SQL Server 2014 - https://technet.microsoft.com/en-us/library/ms178067(v=sql.120)
   - Microsoft SQL Server 2016 - https://technet.microsoft.com/en-us/library/ms178067(v=sql.130)

3 Defina -t1222 nas propriedades de arranque da instância para garantir que as informações de impasse são capturadas, se ocorrer um.

   Para obter mais informações, procure "Trace Flags (Transact-SQL)" (Sinalizadores de rastreio (Transact-SQL)" nos artigos TechNet da Microsoft.

   - Microsoft SQL Server 2008 - http://technet.microsoft.com/en-us/library/ms188396%28v=sql.100%29
   - Microsoft SQL Server 2008 R2 - http://technet.microsoft.com/en-us/library/ms188396%28v=sql.105%29
   - Microsoft SQL Server 2012 - https://msdn.microsoft.com/en-us/library/ms188396.aspx
   - Microsoft SQL Server 2014 - https://msdn.microsoft.com/en-us/library/ms188396.aspx
   - Microsoft SQL Server 2016 - https://msdn.microsoft.com/en-us/library/ms188396.aspx

4 Certifique-se de que todos os índices são abrangidos por um trabalho de manutenção semanal para reconstruir os índices.

Certificados

Criar um certificado autoassinado e gerar um pedido de assinatura de certificado

Esta seção detalha os passos necessários para criar um certificado autoassinado para os componentes baseados em Java. Este processo **não pode** ser utilizado para criar um certificado autoassinado para componentes baseados em .NET.

Recomendamos a utilização de um certificado autoassinado *apenas* num ambiente de não produção.

Se a sua organização requerer um certificado de servidor SSL, ou se precisar de criar um certificado por outras razões, esta secção descreve o processo para criar uma keystore Java utilizando a aplicação Keytool.

Se a sua organização planear utilizar smart cards para autenticação, tem de utilizar a aplicação Keytool para importar a cadeia de certificação completa utilizada no certificado do utilizador do smart card.

A aplicação Keytool cria chaves privadas que são transmitidas no formato de Solicitação de Assinatura de Certificado (CSR) a uma Autoridade de Certificação (AC), como VeriSign® ou Entrust®. Com base nesta CSR, a AC irá então criar um certificado de servidor assinado. O certificado de servidor é depois transferido para um ficheiro, juntamente com o certificado da autoridade assinante. De seguida, os certificados são importados para o ficheiro cacerts.

Gerar um novo par de chaves e um certificado autoassinado

1 Navegue para o diretório **conf** do Dell Compliance Reporter, do Dell Security Server, ou do Dell Device Server.

2 Faça uma cópia de segurança da base de dados de certificados predefinida:

Clique em **Start** > **Run** (Iniciar > Executar) e escreva `move cacerts cacerts.old`.

3 Adicione a aplicação Keytool ao caminho do sistema. Escreva o seguinte comando numa janela de comandos:

```
set path=%path%;<Dell Java Install Dir>\bin
```

4 Para gerar um certificado, execute a aplicação Keytool como indicado:

```
keytool -genkey -keyalg RSA -sigalg SHA1withRSA -alias Dell -keystore .\cacerts
```

5 Introduza as informações seguintes à medida que forem solicitadas pela aplicação Keytool.

> **NOTA:**
> Faça uma cópia de segurança dos ficheiros de configuração antes de editá-los. Mude apenas os parâmetros especificados. Se mudar outros dados nestes ficheiros, incluindo as etiquetas, pode corromper o sistema e causar a sua falha. A **Dell** não pode garantir que os problemas resultantes de alterações não autorizadas a estes ficheiros possam ser resolvidos sem a reinstalação do **Dell**Enterprise Server.

- *Keystore password* (Palavra-passe da Keystore): introduza uma palavra-passe (os caracteres não suportados são <>;&" ') e defina a variável no ficheiro **conf** do componente com o mesmo valor, conforme se segue:

<Compliance Reporter install dir>\conf\eserver.properties. Defina o valor eserver.keystore.password =

<Device Server install dir>\conf\eserver.properties. Defina o valor eserver.keystore.password =

<Security Server install dir>\conf\eserver.properties. Defina o valor eserver.keystore.password =

- *Nome completamente qualificado do servidor*: introduza o nome completamente qualificado do servidor onde está instalado o componente com o qual está a trabalhar. Este nome completamente qualificado inclui o nome de anfitrião e o nome do domínio (exemplo: server.domain.com).
- *Unidade organizacional*: introduza o valor adequado (por exemplo, Segurança).
- *Organização*: introduza o valor apropriado (por exemplo, Dell).
- *Cidade ou localização*:introduza o valor apropriado (por exemplo, Lisboa).
- *Estado ou região*: introduza o nome não abreviado do estado ou da região (por exemplo, Mondego).
- Código de país de duas letras.
- O utilitário solicita que confirme se a informação está correta. Se for o caso, escreva `yes` (sim).

  Caso contrário escreva `no` (não). A aplicação Keytool apresenta os valores introduzidos anteriormente. Clique em **Enter** para aceitar o valor ou altere o valor e clique em **Enter**.
- *Key password for alias* (Palavra-passe para alias): se não introduzir outra palavra-passe aqui, esta palavra-passe é predefinida como a palavra-passe da Keystore.

Solicitar um certificado assinado de uma autoridade de certificação

Use este procedimento para gerar uma Solicitação de Assinatura de Certificado (CSR) para o certificado autoassinado criado em Generate a New Key Pair and a Self-Signed Certificate (Gerar um novo par de chaves e um certificado autoassinado).

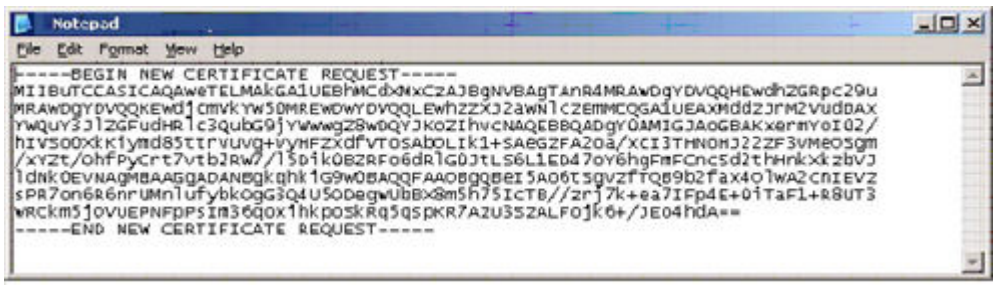
1 Substitua o mesmo valor utilizado anteriormente para <**certificatealias**>:

```
keytool -certreq -sigalg SHA1withRSA -alias <certificate-alias> -keystore .\cacerts -file
<csr-filename>
```

Por exemplo, `keytool -certreq -sigalg SHA1withRSA -alias sslkey -keystore .\cacerts -file Dell.csr`

O ficheiro .csr irá conter o par BEGIN/END que será utilizado durante a criação do certificado na AC.

Exemplo de um ficheiro .CSR



2 Siga o seu processo organizacional para adquirir um certificado do servidor SSL de uma Autoridade de certificação. Envie o conteúdo do <csr-filename> para assinatura.

> **NOTA:**
> Existem vários métodos para solicitar um certificado válido. É apresentado um exemplo de método em **Example Method to Request a Certificate** (Exemplo de método para solicitar um certificado).

3 Quando receber o certificado assinado, guarde-o num ficheiro.

4 Como recomendação, faça uma cópia de segurança deste certificado para o caso de ocorrer algum erro durante o processo de importação. Esta cópia de segurança evitará que tenha de recomeçar o processo.

Importar um certificado de raiz

Se a autoridade de certificação do certificado de raiz for o Verisign (mas não o teste de Verisign), ignore o procedimento seguinte e importe o certificado assinado.

O certificado de raiz da autoridade de certificação valida certificados assinados.

1 Realize **um** dos seguintes procedimentos:

- Transfira o certificado de raiz da autoridade de certificação e guarde-o num ficheiro.
- Obtenha o certificado de raiz do Enterprise Directory Server.

2 Realize **um** dos seguintes procedimentos:

- Se pretender ativar o SSL para o DellCompliance Reporter, Dell Security Server ou Dell Device Server, mude para o diretório **conf** do componente.
- Se pretender ativar o SSL entre o Dell Enterprise Server e o Enterprise Directory Server, mude para <**Dell install dir>\Java Runtimes\jre1.x.x_xx\lib\security** (a palavra-passe predefinida para JRE cacerts é **changeit**).

3 Execute a aplicação Keytool conforme descrito a seguir para instalar o certificado de raiz:

```
keytool -import -trustcacerts -alias <ca-cert-alias> -keystore .\cacerts -file <ca-cert-filename>
```

Por exemplo, `keytool -import -alias Entrust -keystore .\cacerts -file .\Entrust.cer`

Exemplo de método para solicitar um certificado

Um exemplo de método para solicitar um certificado é utilizar um Web browser para aceder ao Microsoft CA Server que será configurado internamente pela sua organização.

1 Navegue até ao Microsoft CA Server. O endereço IP será fornecido pela sua organização.

2 Selecione **Solicitar certificado** e clique em **Seguinte**.

Serviços de certificados da Microsoft

3 Selecione **Solicitação avançada** e clique em **Seguinte**.

Escolher tipo de pedido

4 Selecione a opção para **Enviar uma solicitação de certificado utilizando um ficheiro PKCS #10 com codificação de base 64** e clique em **Seguinte**.

Pedido de certificado avançado

5 Cole o conteúdo da solicitação de CSR na caixa de texto. Selecione um modelo de certificado do **Web Server** e clique em **Enviar**.

Submeter um pedido guardado

6 Guarde o certificado. Selecione **Codificação DER** e clique em **Transferir certificado AC**.

Transferir certificado AC

7 Guarde o certificado. Selecione **Codificação DER** e clique em **Transferir caminho da certificação AC**.

Transferir caminho da certificação AC

8 Importe o certificado da autoridade assinante convertido. Volte à janela DOS. Escreva:

```
keytool -import -trustcacerts -file <csr-filename> -keystore cacerts
```

9 Agora que o certificado da autoridade assinante foi importado, o certificado do servidor pode ser importado (a cadeia de confiança pode ser estabelecida). Escreva:

```
keytool -import -alias sslkey -file <csr-filename> -keystore cacerts
```

Utilize o alias do certificado autoassinado para emparelhar a solicitação de CSR com o certificado do servidor.

10 A lista do ficheiro cacerts irá mostrar que o certificado do servidor tem uma **cadeia de certificação com um comprimento** de **2**, o que indica que o certificado não é autoassinado. Escreva:

```
keytool -list -v -keystore cacerts
```

A impressão digital do segundo certificado na cadeia é o certificado da autoridade assinante importado (que também é mostrado na lista, abaixo do certificado de servidor).

Exportar um certificado para .PFX utilizando a consola de gestão de certificados

Quando tiver um certificado no formato de ficheiro .crt na MMC, tem de o converter para um ficheiro .pfx para poder utilizá-lo com a aplicação Keytool quando o Dell Security Server é utilizado no modo DMZ *e* quando importa um certificado do Dell Manager para a Dell Server Configuration Tool.

1 Abra a Consola de Gestão da Microsoft (MMC - Microsoft Management Console).
2 Clique em **File** > **Add/Remove Snap-in** (Ficheiro > Adicionar/Remover Snap-in).
3 Clique em **Add** (Adicionar).
4 Na janela *Add Standalone Snap-in* (Adicionar Snap-in autónomo), selecione **Certificates** (Certificados) e clique em **Add** (Adicionar).
5 Selecione **Computer Account** (Conta de computador) e clique em **Next** (Seguinte).
6 Na janela *Select Computer* (Selecionar computador), selecione **Local computer (the computer this console is running on)** (Computador local (o computador onde esta consola é executada)) e clique em **Finish** (Concluir).
7 Clique em **Fechar**.
8 Clique em **OK**.
9 Na pasta *Console Root* (Raiz da consola), expanda *Certificates (Local Computer)* (Certificados (computador local)).
10 Aceda à pasta *Personal* (Pessoal) e localize o certificado pretendido.
11 Realce o certificado pretendido, clique com o botão direito do rato em **All Tasks** > **Export** (Todas as tarefas > Exportar).
12 Quando o assistente para exportar certificados abrir, clique em **Next** (Seguinte).
13 Selecione **Yes, export the private key** (Sim, exportar a chave privada) e clique em **Next** (Seguinte).
14 Selecione **Personal Information Exchange - PKCS #12 (.PFX)** e depois selecione as subopções **Include all certificates in the certification path if possible** (Incluir todos os certificados no caminho de certificação, se possível) e **Export all extended properties** (Exportar todas as propriedades expandidas). Clique em **Seguinte**.
15 Introduza e confirme uma palavra-passe. Esta pode ser qualquer palavra-passe da sua escolha. Escolha uma palavra-passe que seja fácil de recordar, mas difícil de outros adivinharem. Clique em **Seguinte**.
16 Clique em **Browse** (Procurar) para navegar para o local onde gostaria de guardar o ficheiro.
17 No campo `File Name` (Nome do ficheiro), introduza um nome para guardar o ficheiro como. Clique em **Guardar**.
18 Clique em **Seguinte**.
19 Clique em **Concluir**.

É apresentada uma mensagem indicando que a exportação foi realizada com êxito. Feche a MMC.

Adicionar um certificado fidedigno de assinatura ao Security Server quando foi utilizado um certificado SSL não fidedigno

1 Pare o Security Server, se este estiver a ser executado.

2 Faça uma cópia de segurança do ficheiro cacerts em <Security Server install dir>\conf\.

Utilize a aplicação Keytool para completar o seguinte:

3 Exporte o PFX fidedigno para um ficheiro de texto e documente o alias:

```
keytool -list -v -keystore "
```

4 Importe o PFX para o ficheiro cacerts em <Security Server install dir>\conf\.

```
keytool -importkeystore -v -srckeystore "
```

5 Modifique o valor keystore.alias.signing em <Security Server install dir>\conf\application.properties.

```
keystore.alias.signing=AliasNamePreviouslyDocumented
```

Inicie o Security Server.