Introdução

Serviços de implementação do Dell Data Security

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.

Introdução

2019 - 06

Rev. A01

Índice

1

Fases de implementação

O processo básico de implementação inclui três fases:

- Execute Introdução e revisão dos requisitos
- Preencha a Lista de verificação de preparação - Implementação inicial ou Lista de verificação de preparação - Atualização/migração
- Instalar ou atualizar/migrar ***um*** dos seguintes:
  - ***Security Management Server***
    - Gestão centralizada de dispositivos
    - Uma aplicação baseada em Windows que é executada num ambiente físico ou virtual.
  - ***Security Management Server Virtual***
    - Gestão centralizada de até 3,500 dispositivos
    - Funciona num ambiente virtualizado

    Para obter informações sobre a instalação/migração do Dell Server, consulte o *Guia de instalação e migração do Security Management Server* ou o *Guia de início rápido e instalação do Security Management Server Virtual*. Para obter estes documentos, consulte os documentos do Dell Data Security Server.
- Configurar a política inicial
  - ***Security Management Server*** - consulte o *Guia de instalação e migração do Security Management Server*, as *Tarefas Administrativas*, disponíveis em support.dell.com, e *AdminHelp*, disponível na Management Console
  - ***Security Management Server Virtual*** - consulte o *Guia de início rápido e instalação do Security Management Server Virtual*, as *Tarefas Administrativas da Management Console*, disponíveis em support.dell.com, e *AdminHelp*, disponível na Management Console
- Embalagem do cliente

  Para obter os requisitos do cliente e os documentos de instalação de software, selecione os documentos aplicáveis com base na sua implementação:
  - *Guia de instalação básica do Encryption Enterprise* ou *Guia de instalação avançada do Encryption Enterprise*
  - *Guia de instalação básica do Endpoint Security Suite Enterprise* ou *Guia de instalação avançada do Endpoint Security Suite Enterprise*
  - *Guia do administrador do Advanced Threat Prevention*
  - *Guia de instalação do Encryption Personal*
  - *Guia do administrador do Encryption Enterprise para Mac*
  - *Guia do administrador do Endpoint Security Suite Enterprise para Mac*
  - *Guia do Administrador do Dell Data Guardian*
  - *Guia do Utilizador do Dell Data Guardian*

    Para obter estes documentos, consulte os documentos do cliente Dell Data Security.
- Participar na transferência de conhecimentos básicos do Dell Security Administrator
- Implementar as Melhores práticas
- Coordenar o suporte de implementação ou piloto com o Dell Client Services

2

Introdução e revisão dos requisitos

Antes da instalação, é importante entender o seu ambiente e os objetivos comerciais e técnicos do seu projeto para implementar com êxito o Dell Data Security para cumprir estes objetivos. Certifique-se de que compreende totalmente os requisitos gerais de segurança de dados da sua organização.

A seguir apresentamos algumas das perguntas mais comuns para ajudar a equipa do Dell Client Services a entender o seu ambiente e requisitos:

1 Qual é a atividade da sua organização (cuidados de saúde, etc.)?
2 Quais são as exigências de conformidade regulamentar (HIPAA/HITECH, PCI, etc.)?
3 Qual é a dimensão da sua organização (número de utilizadores, número de locais físicos, etc.)?
4 Qual é o número de endpoints destinados à implementação? Existem planos para, no futuro, expandir para além deste número?
5 Os utilizadores têm privilégios de administrador local?
6 De que dados e dispositivos necessita para gerir e encriptar (discos fixos locais, USB, etc.)?
7 Quais produtos está a considerar para a implementação?

- Encryption Enterprise
  - Encriptação (elegibilidade DE) – Windows Encryption, Server Encryption, Encryption External Media, SED Management, FDE, BitLocker Manager e Encriptação Mac.
  - Encryption External Media
- Endpoint Security Suite Enterprise
  - Advanced Threat Prevention - com ou sem Firewall para Cliente e Proteção Web (elegibilidade ATP) opcionais
  - Encriptação (elegibilidade DE) – Windows Encryption, Server Encryption, Encryption External Media, SED Management, FDE, BitLocker Manager e Encriptação Mac.
  - Encryption External Media
- Dell Data Guardian (elegibilidade CE)

8 Que tipo de conectividade de utilizador a sua organização suporta? Os tipos podem incluir os seguintes:

- Só conectividade de LAN local
- Conectividade baseada em VPN e/ou utilizadores empresariais de rede sem fios
- Utilizadores remotos/desligados (utilizadores não ligados à rede diretamente ou através de VPN por longos períodos de tempo)
- Estações de trabalho fora do domínio

9 Quais são os dados que necessita proteger no endpoint? Que tipo de dados os utilizadores típicos possuem no endpoint?
10 Quais as aplicações do utilizador que podem conter informações confidenciais? Quais são os tipos de ficheiro de aplicação?
11 Quantos domínios tem no seu ambiente? Quantos estão dentro do âmbito para encriptação?
12 Que sistemas operativos e versões de sistemas operativos estão destinados a encriptação?
13 Tem partições alternadas de arranque configuradas nos seus endpoints?

a Partição de recuperação do fabricante
b Estações de trabalho de arranque duplo

Documentos do cliente

Para aceder aos requisitos de instalação, às versões de sistema operativo suportadas, às unidades de encriptação automática suportadas e às instruções referentes aos clientes que pretende implementar, consulte os documentos aplicáveis listados abaixo.

Encryption Enterprise (Windows) - Consulte os documentos em: www.dell.com/support/home/us/en/04/product-support/product/dell-data-protection-encryption/manuals

- *Guia de instalação avançada do Encryption Enterprise* - Guia de instalação com opções e parâmetros avançados para instalações personalizadas.
- *Guia do utilizador da consola do Dell Data Security* - Instruções para utilizadores.

Encryption Enterprise (Mac) - Consulte o *Guia do administrador do Encryption Enterprise para Mac* em www.dell.com/support/home/us/en/04/product-support/product/dell-data-protection-encryption/manuals. Inclui as instruções de instalação e implementação.

Endpoint Security Suite Enterprise (Windows) - Consulte os documentos em: www.dell.com/support/home/us/en/19/product-support/product/dell-dp-endpt-security-suite-enterprise/manuals.

- *Guia de instalação avançada do Endpoint Security Suite Enterprise* - Guia de instalação com opções e parâmetros avançados para instalações personalizadas.
- *Guia de Introdução do* Endpoint Security Suite Enterprise Advanced Threat Prevention - Instruções para a administração, incluindo recomendações de políticas, identificação e gestão de ameaças e resolução de problemas.
- *Guia do utilizador da consola do Dell Data Security* - Instruções para utilizadores.

Endpoint Security Suite Enterprise (Mac) - Consulte o documento em: www.dell.com/support/home/us/en/19/product-support/product/dell-dp-endpt-security-suite-enterprise/manuals.

- *Guia do Administrador do Endpoint Security Suite Enterprise para Mac* - Guia de instalação

Dell Data Guardian - Consulte os documentos em: www.dell.com/support/home/us/en/19/product-support/product/dell-data-guardian/manuals

- *Guia de administrador do Dell Data Guardian* - Instruções de instalação, ativação e funcionamento.
- *Guia do utilizador do Dell Data Guardian* - Instalação, ativação e instruções de funcionamento para utilizadores.

Para obter informações sobre as unidades de encriptação automática, consulte https://www.dell.com/support/article/us/en/04/sln296720.

Documentos do servidor

Para obter os requisitos de instalação, as versões de sistema operativo suportadas e as configurações do servidor da Dell que deseja implementar, consulte o documento aplicável abaixo.

Security Management Server

- Consulte o *Guia de instalação e migração do Security Management Server*em

  www.dell.com/support/home/us/en/04/product-support/product/dell-data-protection-encryption/manuals

  ou

  www.dell.com/support/home/us/en/19/product-support/product/dell-dp-endpt-security-suite-enterprise/manuals

  ou

  www.dell.com/support/home/us/en/19/product-support/product/dell-data-guardian/manuals

Security Management Server Virtual

- Consulte o *Guia de início rápido e de instalação do Security Management Server Virtual* em

  www.dell.com/support/home/us/en/04/product-support/product/dell-data-protection-encryption/manuals

  ou

  www.dell.com/support/home/us/en/19/product-support/product/dell-dp-endpt-security-suite-enterprise/manuals

ou

www.dell.com/support/home/us/en/19/product-support/product/dell-data-guardian/manuals

3

Lista de verificação de preparação - Implementação inicial

Com base no Dell Server que implementar, utilize a lista de verificação adequada para se certificar de que cumpriu todos os pré-requisitos antes de começar a instalar o Dell Encryption, o Endpoint Security Suite Enterprise ou o Data Guardian.

- Lista de verificação do Security Management Server
- Lista de verificação do Security Management Server Virtual

Lista de verificação da implementação inicial do Security Management Server

A limpeza do ambiente de Prova de Conceito foi concluída (se aplicável)?

- ☐ Foi efetuada a cópia de segurança e a desinstalação da aplicação e da base de dados da prova de conceito (se estiver a utilizar o mesmo servidor) antes da atividade de instalação com a Dell. Para obter mais instruções sobre a desinstalação, consulte https://www.dell.com/support/manuals/us/en/04/dell-data-protection-encryption/enterpserverig/perform-back-ups?guid=guid-2669f62a-2567-49ea-8e72-4ad06fb82442&lang=en-us.
- ☐ Todos os endpoints de produção utilizados durante o teste da prova de conceito foram desencriptados ou pacotes de chaves foram transferidos. Para obter mais informações sobre os clientes que pretende implementar, consulte Documentos de cliente.

NOTA:
Todas as novas implementações têm de ser iniciadas com uma nova base de dados e uma nova instalação do software Encryption, Endpoint Security Suite Enterprise ou Data Guardian. O Dell Client Services não fará uma nova implementação utilizando um ambiente POC. Todos os endpoints encriptados durante uma POC terão de ser desencriptados ou reconstruídos antes da atividade de instalação com a Dell.

Os servidores cumprem as especificações de hardware necessárias?

- ☐ Consulte Arquitetura do Dell Security Management Server.

Os servidores cumprem as especificações de software necessárias?

- ☐ O Windows Server 2012 R2 (Standard ou Datacenter), 2016 (Standard ou Datacenter) ou Windows Server 2019 (Standard ou Datacenter) está instalado. Estes sistemas operativos podem ser instalados em hardware físico ou virtual.
- ☐ Windows Installer 4.0 ou versão posterior está instalado.
- ☐ O .NET Framework 4.5 está instalado.
- ☐ O Microsoft SQL Native Client 2012 está instalado, se estiver a utilizar o SQL Server 2012 ou SQL Server 2016. Se disponível, o SQL Native Client 2014 pode ser utilizado.

  NOTA: O SQL Express não é suportado com a implementação de produção do Security Management Server.

- ☐ O Windows Firewall está desativado ou configurado para permitir as portas (de entrada) 8000, 8050, 8081, 8084, 8888, 61613.
- ☐ A conectividade está disponível entre o Security Management Server e o Active Directory (AD) nas portas 88, 135, 389, 443, 636, 3268, 3269 e 49125+ (RPC) (de entrada para o AD).
- ☐ O UAC está desativado antes da instalação no Windows Server 2012 R2 ao instalar em C:\Program Files. O servidor tem de ser reiniciado para que esta alteração seja implementada. (consulte o Painel de controlo do Windows > Contas de utilizador).
  - Windows Server 2012 R2 - o programa de instalação desativa o UAC.
  - Windows Server 2016 R2 - o programa de instalação desativa o UAC.

  NOTA: A não ser que um diretório protegido seja especificado no diretório de instalação, o UAC já não é desativado à força.

As contas de serviços foram criadas com êxito?

- ☐ O acesso só de leitura ao AD (LDAP) - conta de utilizador básico/utilizador de domínio é suficiente.
- ☐ A conta de serviço deve ter direitos de administrador local para os servidores da aplicação Security Management Server.
- ☐ Para utilizar a autenticação do Windows para a base de dados, terá de ter uma conta de serviços de domínio com direitos de administrador do sistema. 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.
- ☐ Para utilizar a autenticação do SQL, a conta SQL utilizada deve ter direitos de administrador do sistema no 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.

O software foi transferido?

Efetue a transferência a partir do site de suporte da Dell.

- ☐ O software do cliente Dell Data Security e as transferências do Security Management Server estão localizados na pasta **Controladores e transferências** em

  www.dell.com/support/home/us/en/04/product-support/product/dell-data-protection-encryption/research

  ou

  www.dell.com/support/home/us/en/19/product-support/product/dell-dp-endpt-security-suite-enterprise/research

  ou

  www.dell.com/support/home/us/en/19/product-support/product/dell-data-guardian/research

  A partir da página do produto http://www.dell.com/support

  1 Selecione **Controladores e Transferências**.
  2 Na lista de sistemas operativos, selecione o sistema operativo correto para o produto que está a transferir. Por exemplo, para transferir o Dell Enterprise Server, selecione **uma das opções do Windows Server.**
  3 Sob o título de software aplicável, selecione **Transferir ficheiro**.
- ☐ Caso tenha adquirido o Encryption ou o Endpoint Security Suite Enterprise on-the-box, o software pode ser entregue no computador de destino através de Dell Digital Delivery.

OU

Efetue a transferência a partir do site de transferência de ficheiros (CFT) do Dell Data Security

- ☐ O software está localizado em https://ddpe.credant.com na pasta **Transferências de software**.

A chave de instalação e o ficheiro de licença estão disponíveis?

- ☐ A chave de licença está incluída no e-mail original com as credenciais de FTP - consulte Exemplo de e-mail de notificação ao cliente. Esta chave também é incluída na transferência da aplicação a partir de http://www.dell.com/support e https://ddpe.credant.com.
- ☐ O ficheiro de licença é um ficheiro XML localizado no site do FTP, na pasta de **Licenças cliente**.

NOTA:
Se tiver adquirido as suas licenças "on-the-box", nenhum ficheiro de licença será necessário. A elegibilidade será automaticamente transferida da Dell mediante a ativação de qualquer cliente novo de Data Guardian, Encryption, Enterprise ou Endpoint Security Suite Enterprise.

A base de dados foi criada?

- ☐ (Opcional) Foi criada uma nova base de dados num servidor suportado - consulte Requisitos e Arquitetura no *Guia de Instalação e Migração do Security Management Server*. O instalador do Security Management Server cria uma base de dados durante a instalação caso ainda não tenha sido criada uma.
- ☐ O utilizador de destino da base de dados recebeu direitos **db_owner**.

Aliases de DNS criados para o Security Management Server e/ou proxies de políticas com o Split-DNS para tráfego interno e externo?

É recomendado que crie aliases de DNS para escalabilidade. Isto permitirá adicionar servidores extra posteriormente ou separar componentes da aplicação sem a necessidade de atualização do cliente.

- ☐ Aliases de DNS são criados, se é o que pretende. Aliases sugeridos de DNS:
  - Security Management Server: dds.<domain.com>
  - Servidor de front-end: dds-fe.<domain.com>

NOTA:
O Split-DNS permite a utilização do mesmo nome DNS interna e externamente. Isto significa que internamente podemos fornecer o dds.<domain.com> como um c-name e direcioná-lo para o Dell Security Management Server (back-end), e que externamente podemos fornecer um a-record para o dds.<domain.com> e encaminhar as portas relevantes (consulte Portas do Security Management Server) para o servidor front-end. Poderíamos tirar partido de um DNS Round Robin ou de um balanceador de carga para distribuir a carga entre os vários front-ends (se existirem vários).

Planeia usar certificados SSL?

- ☐ Dispomos de uma Autoridade de Certificação (CA) interna que pode ser utilizada para assinar certificados e a mesma é tida como fidedigna por todas as estações de trabalho do ambiente **ou** planeamos adquirir um certificado assinado utilizando uma Autoridade de Certificação pública, como a VeriSign ou Entrust. Se utilizar uma Autoridade de Certificação pública, informe o técnico de assistência do Dell Client Services. O Certificado contém toda a Cadeia de certificação (Raiz e Intermediária) com assinaturas de Chaves Públicas e Privadas.
- ☐ Os nomes alternativos de requerente (SANs) no pedido de certificado correspondem a todos os aliases do DNS atribuídos a cada servidor utilizado para a instalação do Dell Server. Tal não se aplica aos pedidos de certificados de caráter universal ou autoassinados.
- ☐ O certificado é gerado para um formato .pfx.

Os requisitos de controlo de alterações foram identificados e comunicados à Dell?

- ☐ Envie quaisquer requisitos específicos de Controlo de Alterações para a instalação do Encryption, Endpoint Security Suite Enterprise ou Data Guardian ao Dell Client Services antes do processo de instalação. Estes requisitos podem incluir alterações ao(s) servidor(es) de aplicações, base de dados e estações de trabalho cliente.

O hardware de teste está preparado?

- ☐ Prepare pelo menos três computadores com a imagem do seu computador corporativo para serem utilizados para teste. A Dell recomenda que **não** utilize computadores de produção para efetuar o teste. Os computadores de produção devem ser utilizados durante uma produção piloto após as políticas de encriptação terem sido definidas e testadas com a utilização do Plano de Teste fornecido pela Dell.

Lista de verificação da implementação inicial do Security Management Server Virtual

A limpeza do ambiente de Prova de Conceito foi concluída (se aplicável)?

- ☐ Foi efetuada a cópia de segurança e a desinstalação da aplicação e da base de dados da prova de conceito (se estiver a utilizar o mesmo servidor) antes da atividade de instalação com a Dell. Para obter mais instruções sobre a desinstalação, consulte https://www.dell.com/support/manuals/us/en/04/dell-data-protection-encryption/enterpserverig/perform-back-ups?guid=guid-2669f62a-2567-49ea-8e72-4ad06fb82442&lang=en-us

- ☐ Todos os endpoints de produção utilizados durante o teste da prova de conceito foram desencriptados ou pacotes de chaves foram transferidos. Para obter mais informações sobre os clientes que pretende implementar, consulte Documentos de cliente.

NOTA:
Todas as novas implementações têm de ser iniciadas com uma nova base de dados e uma nova instalação do software Encryption, Endpoint Security Suite Enterprise ou Data Guardian. O Dell Client Services não fará uma nova implementação utilizando um ambiente POC. Todos os endpoints encriptados durante uma POC terão de ser desencriptados ou reconstruídos antes da atividade de instalação com a Dell.

As contas de serviços foram criadas com êxito?

- ☐ O acesso só de leitura ao AD (LDAP) - conta de utilizador básico/utilizador de domínio é suficiente.

O software foi transferido?

- ☐ O software do cliente Dell Data Security e as transferências do Security Management Server estão localizados na pasta **Controladores e transferências** em

  www.dell.com/support/home/us/en/04/product-support/product/dell-data-protection-encryption/research

  ou

  www.dell.com/support/home/us/en/19/product-support/product/dell-dp-endpt-security-suite-enterprise/research

  ou

  www.dell.com/support/home/us/en/19/product-support/product/dell-data-guardian/research

  A partir da página do produto http://www.dell.com/support

  1. Selecione **Controladores e Transferências**.
  2. Na lista de sistemas operativos, selecione o sistema operativo correto para o produto que está a transferir. Por exemplo, para transferir o Dell Enterprise Server, selecione **uma das opções do Windows Server.**

3 Sob o título de software aplicável, selecione **Transferir ficheiro**.

- Caso tenha adquirido o Encryption ou o Endpoint Security Suite Enterprise on-the-box, o software pode ser entregue no computador de destino através de Dell Digital Delivery.

O(s) ficheiro(s) de licença está/estão disponível(eis)?

- O ficheiro de licença é um ficheiro XML localizado no site ddpe.credant.com na pasta de **Licenças cliente**.

NOTA:
Se tiver adquirido as suas licenças "on-the-box", nenhum ficheiro de licença será necessário. A elegibilidade será automaticamente transferida da Dell mediante a ativação de qualquer cliente novo de Encryption ou Endpoint Security Suite Enterprise.

Os servidores cumprem as especificações de hardware necessárias?

- Consulte Arquitetura do Security Management Server Virtual.

Aliases de DNS criados para o Security Management Server Virtual e/ou proxies de políticas com o Split-DNS para tráfego interno e externo?

É recomendado que crie aliases de DNS para escalabilidade. Isto permitirá adicionar servidores extra posteriormente ou separar componentes da aplicação sem a necessidade de atualização do cliente.

- Aliases de DNS são criados, se é o que pretende. Aliases sugeridos de DNS:
  - Security Management Server: dds.<domain.com>
  - Servidor de front-end: dds-fe.<domain.com>

NOTA:
O Split-DNS permite a utilização do mesmo nome DNS interna e externamente. Isto significa que internamente podemos fornecer o dds.<domain.com> como um c-name e direcioná-lo para o Dell Security Management Server (back-end), e que externamente podemos fornecer um a-record para o dds.<domain.com> e encaminhar as portas relevantes (consulte Portas do Security Management Server Virtual) para o servidor front-end. Poderíamos tirar partido de um DNS Round Robin ou de um balanceador de carga para distribuir a carga entre os vários front-ends (se existirem vários).

Planeia usar certificados SSL?

- Dispomos de uma Autoridade de Certificação (CA) interna que pode ser utilizada para assinar certificados e a mesma é tida como fidedigna por todas as estações de trabalho do ambiente **ou** planeamos adquirir um certificado assinado utilizando uma Autoridade de Certificação pública, como a VeriSign ou Entrust. Se utilizar uma Autoridade de Certificação pública, informe o técnico de assistência do Dell Client Services.

Os requisitos de controlo de alterações foram identificados e comunicados à Dell?

- Envie quaisquer requisitos específicos de Controlo de Alterações para a instalação do Encryption, Endpoint Security Suite Enterprise ou Data Guardian ao Dell Client Services antes do processo de instalação. Estes requisitos podem incluir alterações ao(s) servidor(es) de aplicações, base de dados e estações de trabalho cliente.

O hardware de teste está preparado?

- Prepare pelo menos três computadores com a imagem do seu computador corporativo para serem utilizados para teste. A Dell recomenda que **não** utilize computadores de produção para efetuar o teste. Os computadores de produção devem ser utilizados

durante uma produção piloto após as políticas de encriptação terem sido definidas e testadas com a utilização do Plano de Teste fornecido pela Dell.

Lista de verificação de preparação - Atualização/migração

Esta lista de verificação só se aplica ao Security Management Server.

NOTA:
Atualize o Security Management Server Virtual a partir do menu de configuração básica no seu terminal do Dell Server. Para obter mais informações, consulte o *Guia de início rápido e de instalação do Security Management Server Virtual*.

Utilize a seguinte lista de verificação para se certificar de que cumpriu todos os pré-requisitos antes de começar a atualizar o Encryption, Endpoint Security Suite Enterprise ou Data Guardian.

Os servidores cumprem as especificações de software necessárias?

- ☐ O Windows Server 2012 R2 (Standard ou Datacenter), Windows Server 2016 (Standard ou Datacenter) ou Windows Server 2019 (Standard ou Datacenter) está instalado. Em alternativa, pode ser instalado um ambiente virtual.
- ☐ Windows Installer 4.0 ou versão posterior está instalado.
- ☐ O .NET Framework 4.5 está instalado.
- ☐ O Microsoft SQL Native Client 2012 está instalado, se estiver a utilizar o SQL Server 2012 ou SQL Server 2016. Se disponível, o SQL Native Client 2014 pode ser utilizado.

  NOTA: O SQL Express não é suportado com o Security Management Server.
- ☐ O Windows Firewall está desativado ou configurado para permitir as portas (de entrada) 8000, 8050, 8081, 8084, 8443, 8888, 61613.
- ☐ A conectividade está disponível entre o Security Management Server e o Active Directory (AD) nas portas 88, 135, 389, 443, 636, 3268, 3269 e 49125+ (RPC) (de entrada para o AD).
- ☐ O UAC está desativado antes da instalação no Windows Server 2012 R2 ao instalar em C:\Program Files. O servidor tem de ser reiniciado para que esta alteração seja implementada. (consulte o Painel de controlo do Windows > Contas de utilizador).
  - Windows Server 2012 R2 - o programa de instalação desativa o UAC.
  - Windows Server 2016 R2 - o programa de instalação desativa o UAC.

As contas de serviços foram criadas com êxito?

- ☐ O acesso só de leitura ao AD (LDAP) - conta de utilizador básico/utilizador de domínio é suficiente.
- ☐ A conta de serviço deve ter direitos de administrador local para os servidores da aplicação Security Management Server.
- ☐ Para utilizar a autenticação do Windows para a base de dados, terá de ter uma conta de serviços de domínio com direitos de administrador do sistema. 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.

- ☐ Para utilizar a autenticação do SQL, a conta SQL utilizada deve ter direitos de administrador do sistema no 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.

A base de dados e todos os ficheiros necessários têm cópia de segurança?

- ☐ Toda a instalação existente possui uma cópia de segurança numa localização alternativa. A cópia de segurança deve incluir a base de dados SQL, a secretKeyStore e os ficheiros de configuração.
- ☐ Certifique-se de que estes ficheiros mais importantes, que armazenam as informações necessárias para ligar à base de dados, têm uma cópia de segurança:

  <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

A chave de instalação e o ficheiro de licença estão disponíveis?

- ☐ A chave de licença está incluída no correio eletrónico original com as credenciais CFT - consulte Exemplo de correio eletrónico de notificação ao cliente. Esta chave também é incluída na transferência da aplicação a partir de http://www.dell.com/support e https://ddpe.credant.com.
- ☐ O ficheiro de licença é um ficheiro XML localizado no site do CFT na pasta de **Licenças cliente**.

NOTA:
Se tiver adquirido as suas licenças "on-the-box", nenhum ficheiro de licença será necessário. A elegibilidade é automaticamente transferida da Dell mediante a ativação de qualquer cliente novo de Encryption ou Endpoint Security Suite Enterprise.

O software novo e existente do Dell Data Security foi transferido?

Efetue a transferência a partir do site de transferência de ficheiros (CFT) do Dell Data Security.

- ☐ O software está localizado em https://ddpe.credant.com na pasta **Transferências de software**.
- ☐ Caso tenha adquirido o Data Guardian, o Encryption Enterprise ou o Endpoint Security Suite Enterprise on-the-box (OTB), o software é opcionalmente enviado através de Dell Digital Delivery. Em alternativa, o software pode ser transferido a partir de www.dell.com/support ou ddpe.credant.com, respetivamente.

Possui licenças de endpoint suficientes?

Antes da atualização, certifique-se de que tem licenças clientes suficientes para cobrir todos os endpoints do seu ambiente. Se as instalações excedem atualmente a contagem de licenças, contacte o seu representante de vendas da Dell antes de efetuar a atualização ou a migração. O Dell Data Security efetua a validação das licenças e impede as ativações no caso de não haver licenças disponíveis.

- ☐ Tenho licenças suficientes para cobrir o meu ambiente.

Os registos DNS estão documentados?

- ☐ Valida que os registos DNS estão documentados e agendados para atualização, caso o hardware tenha sido atualizado.

Planeia usar certificados SSL?

- ☐ Dispomos de uma Autoridade de Certificação (CA) interna que pode ser utilizada para assinar certificados e a mesma é tida como fidedigna por todas as estações de trabalho do ambiente **ou** planeamos adquirir um certificado assinado utilizando uma Autoridade de Certificação pública, como a VeriSign ou Entrust. Se utilizar uma Autoridade de Certificação pública, informe o técnico de assistência do Dell Client Services. O Certificado contém toda a Cadeia de certificação (Raiz e Intermediária) com assinaturas de Chaves Públicas e Privadas.

- ☐ Os Nomes alternativos de requerente (SANs) na Requisição de certificado correspondem a todos os aliases do DNS atribuídos a cada servidor utilizado para a instalação do Dell Enterprise Server. Tal não se aplica às Requisições de certificados de carácter universal ou autoassinados.

- ☐ O certificado é gerado para um formato .pfx.

Os requisitos de controlo de alterações foram identificados e comunicados à Dell?

- ☐ Envie quaisquer requisitos específicos de Controlo de Alterações para a instalação do Encryption, Endpoint Security Suite Enterprise ou Data Guardian ao Dell Client Services antes do processo de instalação. Estes requisitos podem incluir alterações ao(s) servidor(es) de aplicações, base de dados e estações de trabalho cliente.

O hardware de teste está preparado?

- ☐ Prepare pelo menos três computadores com a imagem do seu computador corporativo para serem utilizados para teste. A Dell recomenda que **não** utilize computadores de produção para efetuar o teste. Os computadores de produção devem ser utilizados durante uma produção piloto após as políticas de encriptação terem sido definidas e testadas com a utilização do Plano de Teste fornecido pela Dell.

5

Arquitetura

Esta secção especifica as recomendações de arquitetura para implementações do Dell Data Security. Selecione o Dell Server que irá implementar:

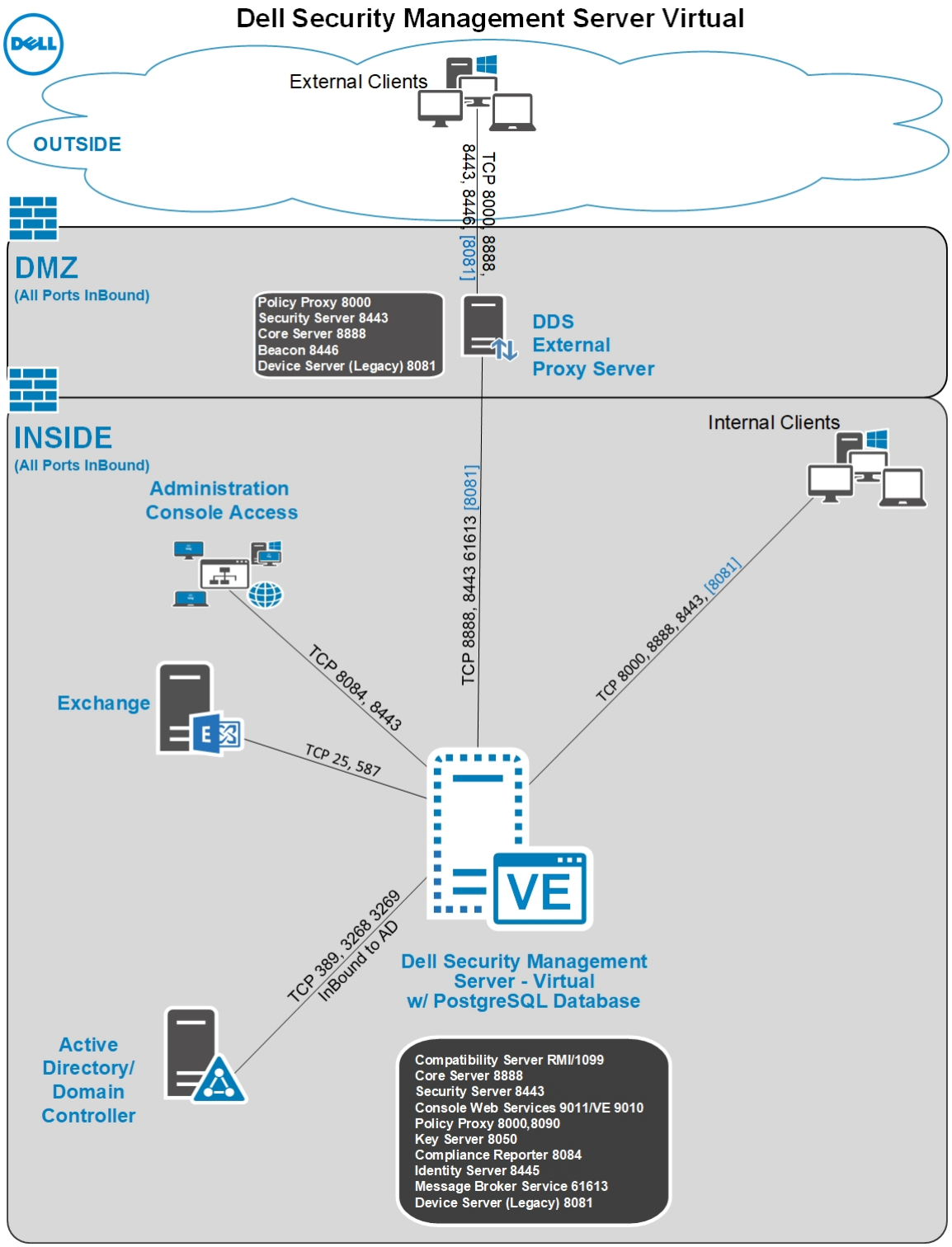
- Arquitetura do Security Management Server
- Arquitetura do Security Management Server Virtual

Arquitetura do Security Management Server Virtual

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

Componentes da arquitetura

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



Portas

A tabela seguinte descreve cada componente e a sua função.

Nome	Porta predefinida	Descrição
Compliance Reporter	HTTP(S)/ 8084	Oferece uma visão abrangente do ambiente, tendo em vista a elaboração de relatórios de auditoria e conformidade.
Management Console	HTTPS/ 8443	Consola de administração e centro de controlo para implementação na empresa inteira.
Core Server	HTTPS/ 8887 (fechada)	Gere o fluxo das políticas, as licenças e o registo para PBA (Preboot Authentication), SED Management, BitLocker Manager, Threat Protection e Advanced Threat Prevention. Processa dados de inventário para utilização pelo Compliance Reporter e pela Management Console. Reúne e armazena os dados de autenticação. Controla o acesso baseado em funções.
Core Server HA (Elevada Disponibilidade)	HTTPS/ 8888	Um serviço de elevada disponibilidade que permite o aumento da segurança e do desempenho das ligações HTTPS com a Management Console, Preboot Authentication, SED Management, FDE, BitLocker Manager, Threat Protection e Advanced Threat Prevention.
Security Server	HTTPS/ 8443	Comunica com o Policy Proxy; gere obtenções de chaves forenses, ativações de clientes, produtos Data Guardian e comunicação SED-PBA.
Compatibility Server	TCP/ 1099 (fechada)	Um serviço para gerir a arquitetura empresarial. Reúne e armazena os dados de inventário iniciais durante a ativação e os dados de políticas durante as migrações. Processa os dados com base nos grupos de utilizadores.
Message Broker Service	TCP/ 61616 (fechada) e STOMP/ 61613 (fechada ou, se configurado para DMZ, 61613 está aberta)	Trata da comunicação entre serviços do Dell Server. Prepara as informações de políticas criadas pelo Compatibility Server para colocação em fila de Policy Proxy.
Identity Server	8445 (fechada)	Trata dos pedidos de autenticação de domínio, incluindo a autenticação de SED Management.
Forensic Server	HTTPS/ 8448	Permite que os administradores com privilégios adequados obtenham chaves encriptadas da Management Console para utilizar no desbloqueio de dados ou nas tarefas de desencriptação. Necessário para API forense.
Inventory Server	8887	Processa a fila de inventário.
Policy Proxy	TCP/ 8000	Oferece uma linha de comunicação com base na rede de forma a proporcionar atualizações de políticas de segurança e atualizações de inventário. Necessário para Encryption Enterprise (Windows e Mac)

Nome	Porta predefinida	Descrição
LDAP	389/636, 3268/3269 RPC - 135, 49125+	Porta 389 - Esta porta é utilizada para o pedido de informações a partir do controlador de domínio local. Os pedidos de LDAP enviados à porta 389 podem ser utilizados para procurar objetos apenas dentro do domínio raiz do catálogo global. No entanto, a aplicação requerente pode obter todos os atributos para esses objetos. Por exemplo, um pedido na porta 389 poderia ser utilizado para obter um departamento de utilizador. Porta 3268 - Esta porta é utilizada para consultas especificamente direcionadas para o catálogo global. Os pedidos de LDAP enviados à porta 3268 podem ser utilizados para procurar objetos na floresta inteira. No entanto, apenas os atributos marcados para replicação para o catálogo global podem ser devolvidos. Por exemplo, um departamento de utilizador não poderia ser devolvido utilizando a porta 3268 uma vez que este atributo não é replicado para o catálogo global.
Client Authentication	HTTPS/ 8449	Permite aos servidores de cliente autenticarem com o Dell Server. Necessário para Server Encryption
Beacon de chamada de retorno	HTTP/TCP 8446	Num servidor front-end, isto permite que um sinalizador de chamada de retorno seja inserido em cada ficheiro protegido do Office ao executar o modo protegido do Office do Data Guardian.

Arquitetura do Security Management Server

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

Componentes da arquitetura

Abaixo encontram-se sugestões de configurações de hardware que se adequam à maioria dos ambientes.

Security Management Server

- Sistema Operativo: Windows Server 2012 R2 (Standard, Datacenter de 64 bits), Windows Server 2016 (Standard, Datacenter de 64 bits), Windows Server 2019 (Standard, Datacenter)
- Máquina virtual/física
- CPU: 4 Core(s)
- RAM: 16 GB
- Unidade C: 30 GB de espaço disponível no disco rígido para registos e bases de dados da aplicação

  NOTA: Podem ser consumidos até 10 GB para uma base de dados local guardada no PostgreSQL.

Servidor Proxy

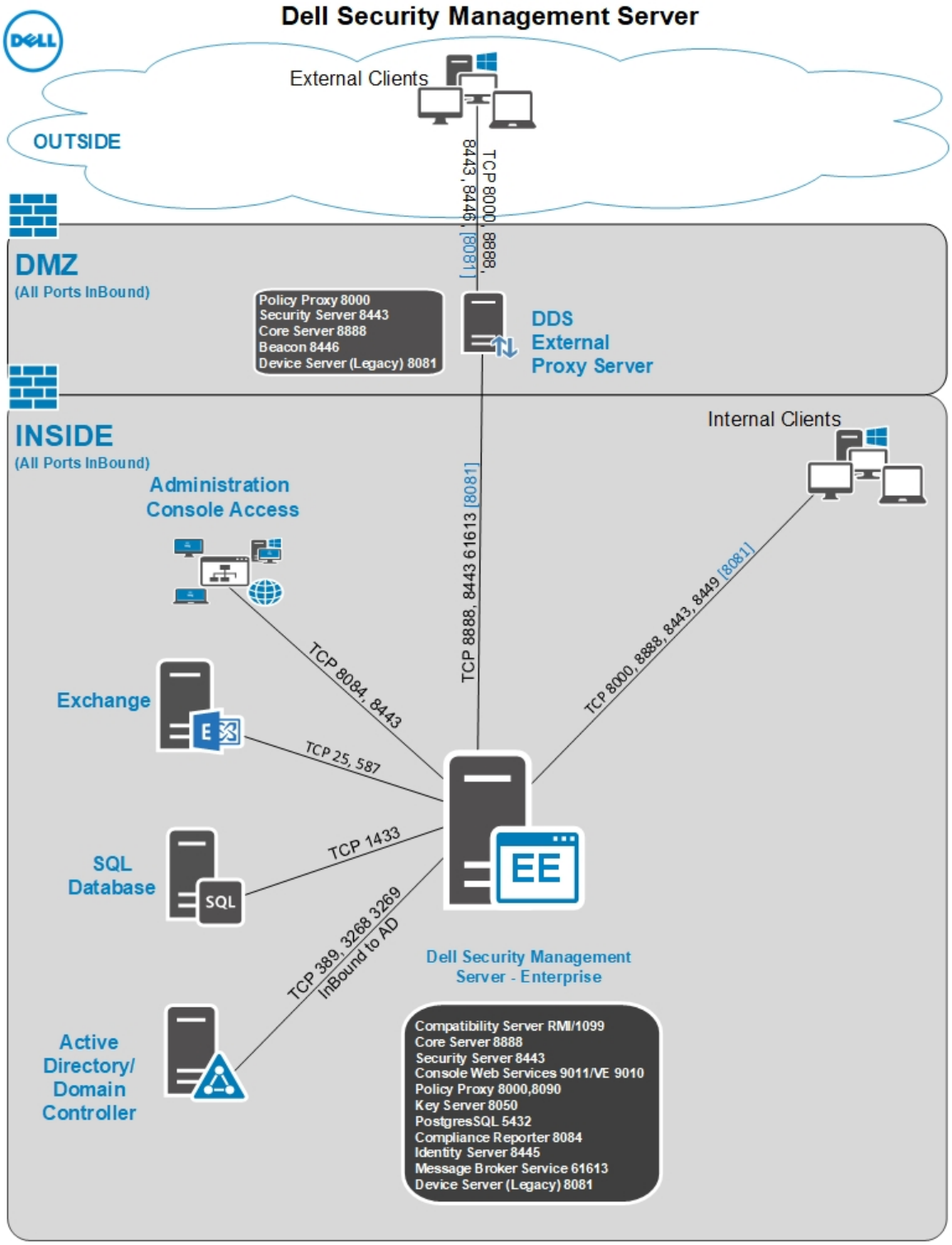
- Sistema Operativo: Windows Server 2012 R2 (Standard, Datacenter de 64 bits), Windows Server 2016 (Standard, Datacenter de 64 bits), Windows Server 2019 (Standard, Datacenter)
- Máquina virtual/física
- CPU: 2 Core(s)
- RAM: 8 GB
- Unidade C: 20 GB de espaço disponível no disco rígido para registos

Especificações do hardware do SQL Server

- CPU: 4 Core(s)
- RAM: 24 GB
- Unidade de dados: 100 -150 GB de espaço disponível no disco rígido (depende do ambiente)
- Unidade de registos: 50 GB de espaço disponível no disco rígido (depende do ambiente)

> **NOTA: A Dell recomenda seguir as Melhores práticas do SQL Server, mas as informações acima devem cobrir a maioria dos ambientes.**

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



NOTA: Se a organização tiver mais de 20 000 pontos terminais, contacte o Dell ProSupport para obter assistência.

Portas

A tabela seguinte descreve cada componente e a sua função.

Nome	Porta predefinida	Descrição
Compliance Reporter	HTTP(S)/ 8084	Oferece uma visão abrangente do ambiente, tendo em vista a elaboração de relatórios de auditoria e conformidade.
Management Console	HTTP(S)/ 8443	Consola de administração e centro de controlo para implementação na empresa inteira.
Core Server	HTTPS/ 8888	Gere o fluxo das políticas, as licenças e o registo para PBA (Preboot Authentication), SED Management, BitLocker Manager, Threat Protection e Advanced Threat Prevention. Processa dados de inventário para utilização pelo Compliance Reporter e pela Management Console. Reúne e armazena os dados de autenticação. Controla o acesso baseado em funções.
Device Server	HTTPS/ 8081	Suporta ativações e recuperação de palavra-passe. Um componente do Security Management Server. Necessário para Encryption Enterprise (Windows e Mac)
Security Server	HTTPS/ 8443	Comunica com o Policy Proxy; gera obtenções de chaves forenses, ativações de clientes, Data Guardian, comunicação SED-PBA e Active Directory para autenticação ou reconciliação, incluindo validação de identidades para autenticação na Management Console. Requer o acesso à base de dados SQL.
Compatibility Server	TCP/ 1099	Um serviço para gerir a arquitetura empresarial. Reúne e armazena os dados de inventário iniciais durante a ativação e os dados de políticas durante as migrações. Processa os dados com base nos grupos de utilizadores.
Message Broker Service	TCP/ 61616 e STOMP/ 61613	Trata da comunicação entre serviços do Dell 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.
Key Server	TCP/ 8050	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.
Policy Proxy	TCP/ 8000	Oferece uma linha de comunicação com base na rede de forma a proporcionar atualizações de políticas de segurança e atualizações de inventário.
LDAP	TCP/ 389/636 (controlador de domínio local), 3268/3269 (catálogo global) TCP/	Porta 389 - Esta porta é utilizada para o pedido de informações a partir do controlador de domínio local. Os pedidos de LDAP enviados à porta 389 podem ser utilizados para procurar objetos apenas dentro do domínio raiz do catálogo global. No entanto, a aplicação requerente pode obter todos os atributos para esses objetos. Por exemplo, um pedido na porta 389 poderia ser utilizado para obter um departamento de utilizador.

Nome	Porta predefinida	Descrição
	135/ 49125+ (RPC)	Porta 3268 - Esta porta é utilizada para consultas especificamente direcionadas para o catálogo global. Os pedidos de LDAP enviados à porta 3268 podem ser utilizados para procurar objetos na floresta inteira. No entanto, apenas os atributos marcados para replicação para o catálogo global podem ser devolvidos. Por exemplo, um departamento de utilizador não poderia ser devolvido utilizando a porta 3268 uma vez que este atributo não é replicado para o catálogo global.
Base de dados Microsoft SQL	TCP/ 1433	A porta do SQL Server predefinida é a 1433 e é atribuído um valor aleatório entre 1024 e 5000 às portas de cliente.
Client Authentication	HTTPS/ 8449	Permite aos servidores cliente autenticarem com o Dell Server. Necessário para Server Encryption.
Beacon de chamada de retorno	HTTP/TCP 8446	Permite que um beacon de chamada de retorno seja inserido em cada ficheiro protegido do Office ao executar o modo protegido do Office do Data Guardian.

6

Melhores práticas do SQL Server

A lista seguinte explica as melhores práticas do SQL Server, que devem ser aplicadas quando o Dell Security for instalado, se ainda não estiver implementado.

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 armazenamento do SQL) 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 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 do servidor de memória) nos artigos TechNet da Microsoft.

   - 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)
   - Microsoft SQL Server 2017 - 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 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
   - Microsoft SQL Server 2017 - 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.

Exemplo de correio eletrónico de notificação ao cliente

Após a sua aquisição do Dell Data Security, receberá um e-mail de DellDataSecurity@Dell.com. Abaixo encontra-se um exemplo de e-mail, que irá incluir as suas credenciais CFT e informações da chave de licença.

Dell Data Security

Thank you for purchasing Dell Encryption Enterprise - Order %USER.CUSTOM2%

Dell Encryption offers a comprehensive data-centric encryption solution that secures data wherever it goes while enabling IT end-users to do more. Listed below are helpful links and information about the support services that are available to you.

Get your Software

Download your software and its accompanying documentation.

Download Now

Username:	%USER.LOGIN%
Password:	%USER.PASSWORD%
Required to change password:	%USER.RESET_PASSWORD_AT_FIRST_LOGIN%
License Key:	xxxx-xxxx-xxxx-xxxx-xxxx-xxxx-xxxx-xxxx

Explore our top knowledge base solutions for Dell Encryption Enterprise.

ProSupport for Software

- Online Support: www.dell.com/datasecuritysupport
- 1.877.459.7304, Option 1, X4310039 - U.S. & Canada Only
- Outside the U.S., click here for a list of numbers

Need Support? CHAT NOW! Click Here

You will need your software service tag to open a Support ticket. This is a seven digit alphanumeric code located above or also can be found on your asset.

Other Products and Services

- Explore our Products
- Subscribe to our Newsletter
- Search our Knowledge Base
- Deployment and Training Services - please contact your sales representative for options