Getting Started

Dell Data Security Implementation Services

December 2023
Rev. A01

DELL Technologies

Notas, avisos e advertências

NOTA: NOTA fornece informações importantes para ajudar você a usar melhor o computador.

CUIDADO: Um AVISO indica possíveis danos ao hardware ou perda de dados e ensina como evitar o problema.

ATENÇÃO: Uma ADVERTÊNCIA indica possíveis danos à propriedade, lesões corporais ou risco de morte.

Contents

1

Fases de implementação

O processo de implementação básica contém estas fases:

- Executar Início e análise de requisitos
- Concluir Lista de verificação de preparação - implementação inicial ou Lista de verificação de preparação - upgrade/migração
- Instalar ou fazer upgrade/migrar ***um*** *dos produtos a seguir:*
  - ***Security Management Server***
    - Gerenciamento centralizado de dispositivos
    - Um aplicativo baseado no Windows que é executado em um ambiente físico ou virtualizado.
  - ***Security Management Server Virtual***
    - Gerenciamento centralizado de até 3.500 dispositivos
    - Executado em um ambiente virtualizado

    Para obter instruções sobre a instalação/migração do Dell Server, consulte o *Guia de instalação e migração do Security Management Server* ou o *Guia de instalação e de início rápido 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 *Security Management Server Guia de instalação e migração*, *Tarefas administrativas*, disponível em support.dell.com e *AdminHelp*, disponível no Management Console
  - ***Security Management Server Virtual*** - consulte *Security Management Server Virtual Guia de instalação e de início rápido*, *Tarefas administrativas do Management Console*, disponível em support.dell.com e *AdminHelp*, disponível no Management Console
- Montar o pacote do cliente

  Para obter os requisitos e os documentos de instalação de software, selecione os documentos em questão, de acordo com a 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*
  - Para obter estes documentos, consulte os documentos do cliente do Dell Data Security.
- Participar na transferência de conhecimentos básicos do administrador do Dell Security
- Implementar as práticas recomendadas
- Coordenar o piloto ou o suporte à implementação com o Dell Client Services

2

Início e análise de requisitos

Antes da instalação, é importante entender o seu ambiente e os objetivos comerciais e técnicos do seu projeto, a fim de implementar o Dell Data Security satisfatoriamente e alcançar esses objetivos. Assegure-se de que você tem um entendimento pleno dos requisitos gerais de segurança de dados de sua organização.

A seguir encontram-se algumas perguntas-chave comuns que ajudam o Dell Client Servicesl a entender seu ambiente e seus requisitos:

1. Qual o tipo de negócios da sua organização (serviços de saúde, etc.)?
2. Com quais requisitos de conformidade normativa você trabalha (HIPAA/HITECH, PCI, etc.)?
3. Qual o tamanho de sua organização (número de usuários, número de locais físicos, etc.)?
4. Qual o número visado de endpoints para a implementação? Há planos de expandir além desse número no futuro?
5. Os usuários têm privilégios de administrador local?
6. Quais dados e dispositivos você precisa gerenciar e criptografar (discos fixos locais, USB, etc.)?
7. Quais produtos você considera implementar?
    - Encryption Enterprise
        - Encryption (elegibilidade para DE) – Windows Encryption, Server Encryption, Encryption External Media, SED Management, Full Disk Encryption, BitLocker Manager e Criptografia de Mac.
        - Encryption External Media
    - Endpoint Security Suite Enterprise
        - Advanced Threat Prevention - com ou sem o recurso opcional de firewall cliente e proteção da Web (elegibilidade para ATP)
        - Encryption (elegibilidade para DE) – Windows Encryption, Server Encryption, Encryption External Media, SED Management, Full Disk Encryption, BitLocker Manager e Criptografia de Mac.
        - Encryption External Media
8. Que tipo de conectividade com o usuário sua organização suporta? Os tipos podem conter os seguintes:
    - Apenas conectividade LAN local
    - VPN e/ou usuários corporativos sem fio
    - Usuários remotos/desconectados (usuários não conectados diretamente à rede nem via VPN durante longos períodos de tempo)
    - Estações de trabalho sem domínio
9. Quais dados você precisa proteger no endpoint? Que tipo de dados os usuários típicos possuem no endpoint?
10. Quais aplicativos do usuário podem conter informações sigilosas? Quais são os tipos de arquivos dos aplicativos?
11. Quantos domínios você tem em seu ambiente? Quantos estão dentro do escopo da criptografia?
12. Quais sistemas operacionais e suas versões estão identificados para serem criptografados?
13. Você tem partições de inicialização alternativas configuradas em seus endpoints?
    a. Partição de recuperação do fabricante
    b. Estações de trabalho de inicialização dupla

Documentos do cliente

Para obter os requisitos de instalação, versões de sistema operacional compatíveis, SEDs compatíveis e instruções para os clientes que você planeja implantar, consulte os documentos aplicáveis, listados abaixo.

Encryption Enterprise (Windows) — consulte os seguintes documentos no endereço: 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 avançadas e parâmetros para instalações personalizadas.
- *Guia do usuário do Dell Data Security* - Instruções para usuários.

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 a instalação e instruções de 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 avançadas e parâmetros para instalações personalizadas.
- *Guia de início rápido do Endpoint Security Suite Enterprise Advanced Threat Prevention* - instruções de administração, incluindo recomendações de política, gerenciamento e identificação de ameaças e solução de problemas.
- *Guia do usuário do Dell Data Security* - Instruções aos usuários.

Endpoint Security Suite Enterprise (Mac) - consulte o seguinte documento no endereço: 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

Para saber mais sobre Self-Encrypting Drives compatíveis, consulte https://www.dell.com/support/article/us/en/04/sln296720.

Documentos do servidor

Para obter os requisitos de instalação, versões de sistemas operacionais suportados e as configurações do Dell Server que você pretende implementar, consulte o documento em questão 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

Security Management Server Virtual

- Consulte o *Guia de instalação e de início rápido 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

3

Lista de verificação de preparação - implementação inicial

Dependendo do Dell Server implantado, use a lista de verificação adequada para confirmar que todos os pré-requisitos foram atendidos antes de começar a instalação do Dell Encryption ou do Endpoint Security Suite Enterprise.

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

Checklist da implementação inicial do Security Management Server

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

☐	O banco de dados e o aplicativo da POC tiveram um backup efetuado e foram desinstalados (no caso de uso de um mesmo servidor) antes do engajamento da instalação com a Dell. Para obter mais instruções sobre uma 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 usados durante o teste de POC foram descriptografados ou os principais pacotes foram obtidos por download. Para obter mais informações sobre os clients que você planeja implementar, consulte Documentos do client.

NOTA:

Todas as novas implementações precisam começar com um novo banco de dados e com a instalação do software Encryption ou Endpoint Security Suite Enterprise. O Dell Client Services não realizará uma nova implementação usando um ambiente POC. Todos os endpoints criptografados durante uma POC precisarão ser descriptografados ou recriados antes do engajamento da instalação com a Dell.

Os servidores atendem às especificações de hardware exigidas?

☐	Consulte Design da arquitetura do Dell Security Management Server.

Os servidores atendem às especificações de software exigidas?

☐	Windows Server 2012 R2 (Standard ou Datacenter), 2016 (Standard ou Datacenter), Windows Server 2019 (Standard ou Datacenter) ou Windows Server 2022: (Standard ou Datacenter) está instalado. Esses sistemas operacionais podem ser instalados no hardware físico ou virtual.
☐	Windows Installer 4.0 ou posterior está instalado.
☐	.NET Framework 4.6.1 está instalado.
☐	Microsoft SQL Native Client 2012 está instalado se estiver usando o SQL Server 2012 ou o SQL Server 2016. Se disponível, o SQL Native Client 2014 pode ser usado. **NOTA:** O SQL Express não é compatível com a implementação de produção do Security Management Server.

☐	O Firewall do Windows está desativado ou configurado para permitir as portas (de entrada) 8000, 8050, 8081, 8888 e 61613.
☐	A conectividade está disponível entre o Security Management Server e o Active Directory (AD) nas portas 88, 135, 389, 443, 636, 3268, 3269, 49125+ (RPC) (de entrada no AD).
☐	O UAC é desativado antes de fazer a instalação no Windows Server 2012 R2 quando instalando em C:\Program Files. O servidor precisa ser reiniciado para que essa alteração tenha efeito. (consulte Painel de controle do Windows > Contas de usuário). • Windows Server 2012 R2 - o instalador desativa o UAC. • Windows Server 2016 R2 - o instalador desativa o UAC. **NOTA:** Não é possível forçar a desativação do UAC, a menos que o diretório protegido esteja especificado no diretório de instalação.

As contas de serviço foram criadas satisfatoriamente?

☐	Conta de serviço com acesso somente leitura ao AD (LDAP) - uma conta de usuário básico/usuário de domínio é suficiente.
☐	A conta de serviço precisa ter direitos de administrador local sobre os servidores de aplicativos do Security Management Server.
☐	Para usar a autenticação do Windows para o banco de dados, você precisará de uma conta de serviços de domínio com direitos de administrador do sistema. A conta de usuário precisa estar no formato DOMÍNIO\Nomedeusuário e ter o esquema padrão de permissões do SQL Server: dbo e a Associação à função de banco de dados: dbo_owner, público.
☐	Para usar a autenticação SQL, a conta SQL usada precisa ter direitos de administrador do sistema no SQL Server. A conta de usuário precisa ter o esquema padrão de permissões do SQL Server: dbo e Associação à função de banco de dados: dbo_owner, público.

Foi feito o download do software?

Faça o download a partir do site Suporte Dell.

☐	O software client do Dell Data Security e os downloads do Security Management Server estão localizados na pasta **Drivers e downloads** 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 Na página do produto http://www.dell.com/support 1. Selecione **Drivers e Downloads**. 2. Na lista de sistemas operacionais, selecione o sistema operacional correto do produto para o qual você está fazendo o download. Por exemplo, para fazer download do Dell Enterprise Server, selecione **uma das opções de Windows Server.** 3. Embaixo do título do software em questão, selecione **Fazer download do arquivo**.
☐	Caso você tenha adquirido o Encryption ou o Endpoint Security Suite Enterprise “on-the-box”, o download do software poderá ser feito pelo computador de destino usando o Dell Digital Delivery.

OU

Fazer download a partir do site de transferência de arquivos (CFT) do Dell Data Security

☐	O software se encontra em https://ddpe.credant.com ou na pasta **Downloads de software**.

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

☐	A chave de licença está incluída no e-mail original com as credenciais do FTP - consulte o Exemplo de e-mail de notificação ao cliente. Esta chave está inclusa no download do aplicativo em http://www.dell.com/support e https://ddpe.credant.com.
☐	O arquivo de licença é um arquivo XML localizado no site FTP, na pasta **Client Licenses**.

NOTA:

Se você comprou suas licenças pela modalidade "on-the-box", não é necessário um arquivo de licença. Seu direito de uso será automaticamente obtido por download da Dell, após a ativação de qualquer novo client Data Guardian, Encryption, Enterprise ou Endpoint Security Suite Enterprise.

O banco de dados foi criado?

☐	(Opcional) Um novo banco de dados é criado em um servidor suportado - consulte Requisitos e arquitetura no *Guia de instalação e migração do Security Management Server*. O instalador do Security Management Server cria um banco de dados durante a instalação se ainda não houver um criado.
☐	O usuário do banco de dados de destino recebeu os direitos **db_owner**.

Um alias de DNS foi criado para os proxies de política e/ou para o Security Management Server com Split DNS para tráfego interno e externo?

Para fins de escalabilidade, é recomendável que você crie aliases de DNS. Isso permitirá que você acrescente serviços adicionais posteriormente ou componentes separados do aplicativo sem exigir atualização do client.

☐	Aliases de DNS foram criados, se desejado. Aliases de DNS sugeridos: • Security Management Server: dds.<domain.com> • Servidor front-end: dds-fe.<domain.com>

NOTA:

Com o Split-DNS, o usuário do mesmo DNS pode nomeá-lo interna e externamente. Isso significa que podemos fornecer internamente dds.<domain.com> como um c-name interno, direcioná-lo ao Dell Security Management Server (back-end). Além disso, externamente, podemos fornecer um a-record para o dds.<domain.com> e encaminhar as portas relevantes (consulte Portas para Security Management Server) para o servidor de front-end. Podemos aproveitar o round-robin do DNS ou um balanceamento de carga para distribuir a carga para os diversos front-ends (se existirem diversos deles).

Planeja usar certificados SSL?

☐	Contamos com uma Autoridade de certificação (CA) interna que pode ser usada para assinar os certificados, na qual todas as estações de trabalho do ambiente confiam, **ou** planejamos adquirir um certificado assinado usando uma Autoridade Certificadora pública, como a VeriSign ou a Entrust. Se você usa uma Autoridade de certificação pública, informe ao Engenheiro do Dell Client Services. O certificado contém toda a cadeia de confiança (raiz e intermediária) com assinaturas de chaves públicas e privadas.
☐	Os Nomes alternativos da entidade (SANs) na solicitação de certificado correspondem a todos os aliases de DNS fornecidos a todos os servidores sendo usados para a instalação do Dell Server. Não se aplica a curinga ou a solicitações de certificados autoassinados.
☐	O certificado é gerado em um formato .pfx.

Os requisitos de Controle de Mudanças foram identificados e comunicados à Dell?

☐	Envie quaisquer requisitos específicos de Controle de mudanças referentes à instalação do Encryption ou do Endpoint Security Suite Enterprise ao Dell Client Services antes do engajamento da instalação. Esses requisitos podem conter alterações em servidores de aplicativos, banco de dados e estações de trabalho client.

O hardware de teste está preparado?

☐	Prepare pelo menos três computadores com sua imagem de computador corporativo a serem usados para teste. A Dell recomenda que você **não** use sistemas em produção para fazer testes. Os computadores em produção devem ser usados durante um piloto de produção, após as políticas de criptografia serem definidas e testadas usando o 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)?

☐	O banco de dados e o aplicativo da POC tiveram um backup efetuado e foram desinstalados (no caso de uso de um mesmo servidor) antes do engajamento da instalação com a Dell. Para obter mais instruções sobre uma 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 usados durante o teste de POC foram descriptografados ou os principais pacotes foram obtidos por download. Para obter mais informações sobre os clients que você planeja implementar, consulte Documentos do client.

NOTA:

Todas as novas implementações precisam começar com um novo banco de dados e com a instalação do software Encryption ou Endpoint Security Suite Enterprise. O Dell Client Services não realizará uma nova implementação usando um ambiente POC. Todos os endpoints criptografados durante uma POC precisarão ser descriptografados ou recriados antes do engajamento da instalação com a Dell.

As contas de serviço foram criadas satisfatoriamente?

☐	Conta de serviço com acesso somente leitura ao AD (LDAP) - uma conta de usuário básico/usuário de domínio é suficiente.

Foi feito o download do software?

☐	O software client do Dell Data Security e os downloads do Security Management Server estão localizados na pasta **Drivers e downloads** 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 Na página do produto http://www.dell.com/support 1. Selecione **Drivers e Downloads**.

	2. Na lista de sistemas operacionais, selecione o sistema operacional correto do produto para o qual você está fazendo o download. Por exemplo, para fazer download do Dell Enterprise Server, selecione **uma das opções de Windows Server.** 3. Embaixo do título do software em questão, selecione **Fazer download do arquivo**.
☐	Caso você tenha adquirido o Encryption ou o Endpoint Security Suite Enterprise “on-the-box”, o download do software poderá ser feito pelo computador de destino usando o Dell Digital Delivery.

Os arquivos de licença estão disponíveis?

☐	O arquivo de licença é um arquivo XML localizado no site ddpe.credant.com, na pasta **Client Licenses**.

NOTA:

Se você comprou suas licenças pela modalidade "on-the-box", não é necessário um arquivo de licença. Seu direito de uso será automaticamente obtido por download da Dell, após a ativação de qualquer novo cliente Encryption ou Endpoint Security Suite Enterprise.

Os servidores atendem às especificações de hardware exigidas?

☐	Consulte Design da arquitetura do Security Management Server Virtual.

Um alias de DNS foi criado para os proxies de política e/ou para o Security Management Server Virtual com Split DNS para tráfego interno e externo?

Para fins de escalabilidade, é recomendável que você crie aliases de DNS. Isso permitirá que você acrescente serviços adicionais posteriormente ou componentes separados do aplicativo sem exigir atualização do client.

☐	Aliases de DNS foram criados, se desejado. Aliases de DNS sugeridos: • Security Management Server: dds.<domain.com> • Servidor front-end: dds-fe.<domain.com>

NOTA:

Com o Split-DNS, o usuário do mesmo DNS pode nomeá-lo interna e externamente. Isso significa que podemos fornecer internamente dds.<domain.com> como um c-name interno, direcioná-lo ao Dell Security Management Server (back-end). Além disso, externamente, podemos fornecer um a-record para o dds.<domain.com> e encaminhar as portas relevantes (consulte Portas para Security Management Server Virtual) para o servidor de front-end. Podemos aproveitar o round-robin do DNS ou um balanceamento de carga para distribuir a carga para os diversos front-ends (se existirem diversos deles).

Planeja usar certificados SSL?

☐	Contamos com uma Autoridade de certificação (CA) interna que pode ser usada para assinar os certificados, na qual todas as estações de trabalho do ambiente confiam, **ou** planejamos adquirir um certificado assinado usando uma Autoridade Certificadora pública, como a VeriSign ou a Entrust. Se você usa uma Autoridade Certificadora pública, informe ao Engenheiro do Dell Client Services.

Os requisitos de Controle de Mudanças foram identificados e comunicados à Dell?

☐	Envie quaisquer requisitos específicos de Controle de mudanças referentes à instalação do Encryption ou do Endpoint Security Suite Enterprise ao Dell Client Services antes do engajamento da instalação. Esses requisitos podem conter alterações em servidores de aplicativos, banco de dados e estações de trabalho client.

O hardware de teste está preparado?

☐	Prepare pelo menos três computadores com sua imagem de computador corporativo a serem usados para teste. A Dell recomenda que você **não** use sistemas em produção para fazer testes. Os computadores

	em produção devem ser usados durante um piloto de produção, após as políticas de criptografia serem definidas e testadas usando o Plano de Teste fornecido pela Dell.

4

Checklist de preparação - upgrade/migração

Essa checklist se aplica apenas ao Security Management Server.

NOTA:

Atualize o Security Management Server Virtual do menu Configuração Básica no terminal do Dell Server. Para obter mais informações, consulte o *Guia de instalação e de início rápido do Security Management Server Virtual*.

Use a seguinte checklist para confirmar que todos os pré-requisitos foram atendidos antes de começar a atualizar o Encryption ou o Endpoint Security Suite Enterprise.

Os servidores atendem às especificações de software exigidas?

☐	O Windows Server 2012 R2 (Standard ou Datacenter), o Windows Server 2016 (Standard ou Datacenter), o Windows Server 2019 (Standard ou Datacenter) ou o Windows Server 2022 (Standard ou Datacenter) está instalado. Como alternativa, um ambiente virtualizado pode ser instalado. **NOTA:** A atualização para o Dell Server v11.0 ou superior exige o Windows Server 2019 ou superior.
☐	Windows Installer 4.0 ou posterior está instalado.
☐	.NET Framework 4.6.1 está instalado.
☐	Microsoft SQL Native Client 2012 está instalado se estiver usando o SQL Server 2012 ou o SQL Server 2016. Se disponível, o SQL Native Client 2014 pode ser usado. **NOTA:** SQL Express não é suportado com Security Management Server.
☐	O Firewall do Windows está desativado ou configurado para permitir as portas (de entrada) 8000, 8050, 8081, 8443, 8888 e 61613.
☐	A conectividade está disponível entre o Security Management Server e o Active Directory (AD) nas portas 88, 135, 389, 443, 636, 3268, 3269, 49125+ (RPC) (de entrada no AD).
☐	O UAC é desativado antes de fazer a instalação no Windows Server 2012 R2 quando instalando em C:\Program Files. O servidor precisa ser reiniciado para que essa alteração tenha efeito. (consulte Painel de controle do Windows > Contas de usuário). • Windows Server 2012 R2 - o instalador desativa o UAC. • Windows Server 2016 R2 - o instalador desativa o UAC.

As contas de serviço foram criadas satisfatoriamente?

☐	Conta de serviço com acesso somente leitura ao AD (LDAP) - uma conta de usuário básico/usuário de domínio é suficiente.
☐	A conta de serviço precisa ter direitos de administrador local sobre os servidores de aplicativos do Security Management Server.
☐	Para usar a autenticação do Windows para o banco de dados, você precisará de uma conta de serviços de domínio com direitos de administrador do sistema. A conta de usuário precisa estar no formato DOMÍNIO\Nomedeusuário e ter o esquema padrão de permissões do SQL Server: dbo e a Associação à função de banco de dados: dbo_owner, público.
☐	Para usar a autenticação SQL, a conta SQL usada precisa ter direitos de administrador do sistema no SQL Server. A conta de usuário precisa ter o esquema padrão de permissões do SQL Server: dbo e Associação à função de banco de dados: dbo_owner, público.

O banco de dados e todos os arquivos necessários estão salvos em backup?

☐	Toda a instalação existente é salva em backup em um local alternativo. O backup deve conter o banco de dados SQL, o secretKeyStore e os arquivos de configuração.
☐	Confirme que esses arquivos mais críticos, que armazenam as informações necessárias para a conexão com o banco de dados, estão salvos em backup: <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 arquivo de licença estão disponíveis?

☐	A chave de licença está incluída no e-mail original com as credenciais do CFT - consulte o Exemplo de e-mail de notificação ao cliente. Esta chave está inclusa no download do aplicativo em http://www.dell.com/support e https://ddpe.credant.com.
☐	O arquivo de licença é um arquivo XML localizado no site CFT, na pasta **Client Licenses**.

NOTA:

Se você comprou suas licenças pela modalidade "on-the-box", não é necessário um arquivo de licença. Seu direito de uso é automaticamente obtido por download da Dell, após a ativação de qualquer novo client Encryption ou Endpoint Security Suite Enterprise.

Foi feito o download do software novo e existente do Dell Data Security?

Faça o download a partir do site de transferência de arquivos (CFT) do Dell Data Security.

☐	O software se encontra em https://ddpe.credant.com ou na pasta **Downloads de software**.
☐	Se você comprou o Encryption Enterprise ou o Endpoint Security Suite Enterprise ,OTB (on-the-box, pronto para uso) o software é entregue opcionalmente usando o Dell Digital Delivery. Como alternativa, o software pode ser baixado no site www.dell.com/support ou ddpe.credant.com, respectivamente.

Há licenças de endpoint suficientes?

Antes de fazer o upgrade, assegure-se de que tem licenças de clients suficientes para cobrir todos os endpoints de seu ambiente. Se sua instalação atualmente excede sua contagem de licenças, entre em contato com um Representante de Vendas Dell antes de fazer o upgrade ou a migração. O Dell Data Security executa a validação das licenças e impede as ativações caso não haja licenças disponíveis.

☐	Tenho licenças suficientes para cobrir meu ambiente.

Os registros DNS estão documentados?

☐	Confira se os registros de DNS estão documentadas e preparados para atualização, caso o hardware tenha sido alterado.

Planeja usar certificados SSL?

☐	Contamos com uma Autoridade de certificação (CA) interna que pode ser usada para assinar os certificados, na qual todas as estações de trabalho do ambiente confiam, **ou** planejamos adquirir um certificado assinado usando uma Autoridade Certificadora pública, como a VeriSign ou a Entrust. Se você usa uma Autoridade de certificação pública, informe ao Engenheiro do Dell Client Services. O certificado contém toda a cadeia de confiança (raiz e intermediária) com assinaturas de chaves públicas e privadas.

☐	Os Nomes alternativos da entidade (SANs) na solicitação de certificado correspondem a todos os aliases de DNS fornecidos a todos os servidores sendo usados para a instalação do Dell Enterprise Server. Não se aplica a curinga ou a solicitações de certificados autoassinados.
☐	O certificado é gerado em um formato .pfx.

Os requisitos de Controle de Mudanças foram identificados e comunicados à Dell?

☐	Envie quaisquer requisitos específicos de Controle de mudanças referentes à instalação do Encryption ou do Endpoint Security Suite Enterprise ao Dell Client Services antes do engajamento da instalação. Esses requisitos podem conter alterações em servidores de aplicativos, banco de dados e estações de trabalho client.

O hardware de teste está preparado?

☐	Prepare pelo menos três computadores com sua imagem de computador corporativo a serem usados para teste. A Dell recomenda que você **não** use computadores em produção para fazer testes. Os computadores em produção devem ser usados durante um piloto de produção, após as políticas de criptografia serem definidas e testadas usando o Plano de Teste fornecido pela Dell.

5

Arquitetura

Esta seção detalha as recomendações de design de arquitetura para implementação do Dell Data Security. Selecione o Dell Server que você implementará:

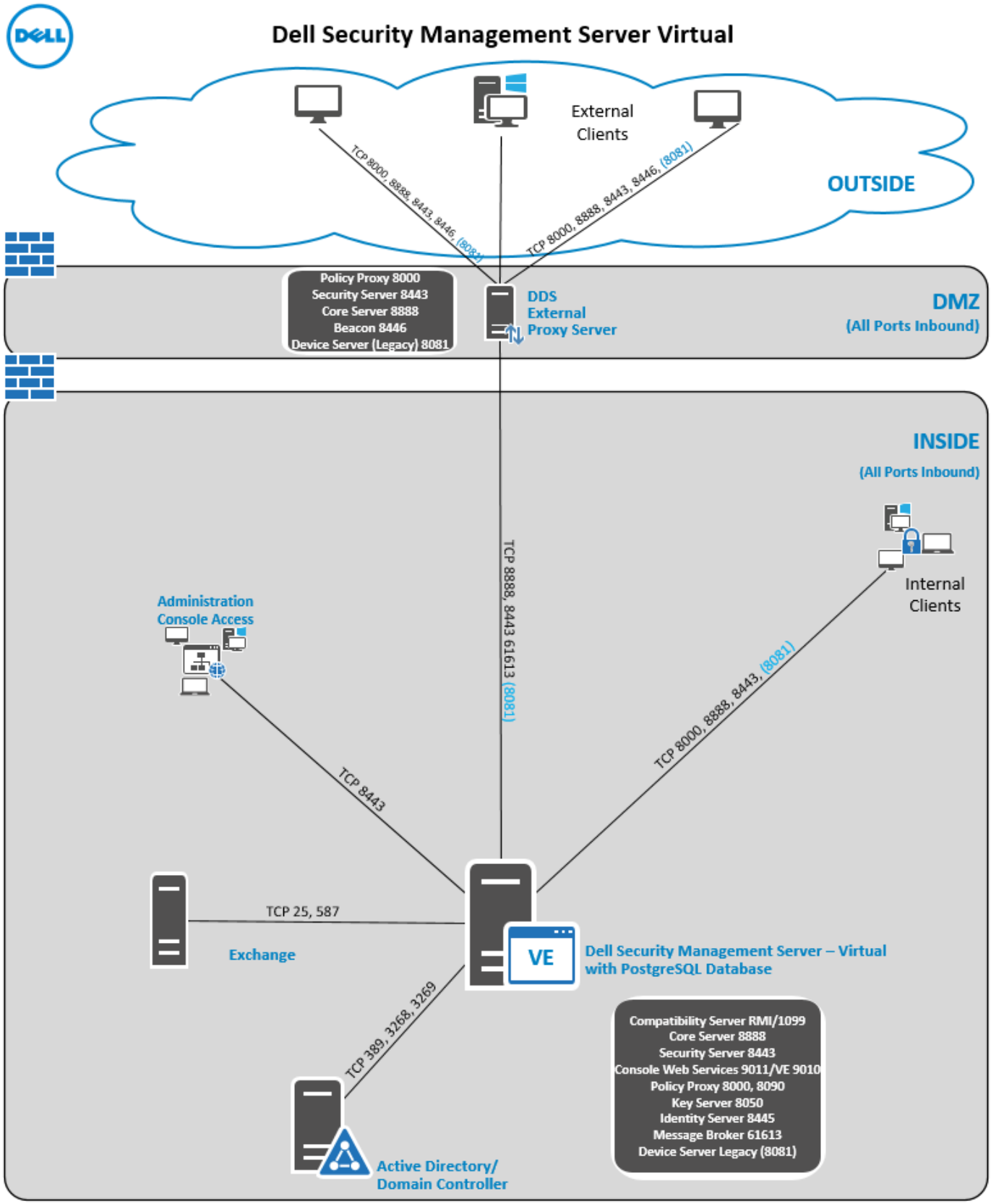
- Design da arquitetura do Security Management Server
- Design da arquitetura do Security Management Server Virtual

Design da arquitetura do Security Management Server Virtual

As soluções do Encryption Enterprise e Endpoint Security Suite Enterprise são produtos altamente escaláveis, de acordo com a quantidade de pontos de extremidade que se deseja criptografar em sua organização.

Componentes da arquitetura

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



Portas

A tabela a seguir descreve cada componente e sua função.

Nome	Porta padrão	Descrição
Access Group Service	TCP/ 8006	Gerencia várias permissões e acesso de grupo para vários produtos do Dell Security. **NOTA:** A porta 8006 não está protegida no momento. Certifique-se de que essa porta seja filtrada corretamente por meio de um firewall. Esta porta é apenas interna.
Management Console	HTTPS/ 8443	A central de controles e o console de administração da implementação de toda a empresa.
Core Server	HTTPS/ 8887 (fechado)	Gerencia o fluxo de política, as licenças, o registro para Preboot Authentication, SED Management, BitLocker Manager, Threat Protection e Advanced Threat Prevention. Processa os dados de inventário para uso pelo console de gerenciamento. Coleta e armazena os dados de autenticação. Controla o acesso baseado em função.
Core Server HA (Alta disponibilidade)	HTTPS/ 8888	Um serviço de alta disponibilidade que permite maior segurança e desempenho das conexões HTTPS com o Management Console, Preboot Authentication, SED Management, FDE, BitLocker Manager, Threat Protection e Advanced Threat Prevention.
Security Server	HTTPS/ 8443	Comunica-se com o Policy Proxy; gerencia as recuperações de chaves forense, ativações de clientes, comunicação SED-PBA e Full Disk Encryption-PBA.
Compatibility Server	TCP/ 1099 (fechada)	Um serviço para gerenciar a arquitetura empresarial. Coleta e armazena os dados iniciais de inventário durante a ativação e os dados de política durante as migrações. Processa os dados baseados em grupos de usuário. **NOTA:** A porta 1099 deve ser filtrada por um firewall. A Dell sugere que essa porta seja apenas interna.
Message Broker Service	TCP/ 61616 (fechado) e STOMP/ 61613 (fechada	Lida com a comunicação entre os serviços do Dell Server. Armazena as informações de políticas criadas pelo Compatibility Server para o enfileiramento do Policy Proxy. **NOTA:** A porta 61616 deve ser filtrada por um firewall. A Dell

Nome	Porta padrão	Descrição
	ou, caso configurado para DMZ, porta 61613 aberta)	recomenda que essa porta seja apenas interna. **NOTA:** A porta 61613 só deve ser aberta para os Security Management Servers configurados no modo Front-End.
Identity Server	8445 (fechado)	Trata as solicitações de autenticação de domínio, incluindo autenticação do SED Management.
Forensic Server	HTTPS/ 8448	Permite que administradores com privilégios adequados obtenham as chaves de criptografia do Management Console para o uso em tarefas de desbloqueio ou descriptografia de dados. Necessário para Forensic API.
Inventory Server	8887	Processa a fila de inventário.
Policy Proxy	TCP/ 8000	Fornece um caminho de comunicação baseado na rede para fornecer atualizações da política de segurança e atualizações de inventário. Necessário para Encryption Enterprise (Windows e Mac)
PostGres	TCP/ 5432	Banco de dados local usado para dados de eventos. **NOTA:** A porta 5432 deve ser filtrada por um firewall. A Dell recomenda que essa porta seja apenas interna.
LDAP	389/636, 3268/3269 RPC - 135, 49125+	Porta 389 – Esta porta é usada para solicitar informações a partir do controlador de domínio local. As solicitações de LDAP enviadas para a porta 389 podem ser usadas para buscar objetos apenas dentro do domínio doméstico do catálogo global. No entanto, o aplicativo de solicitação pode obter todos os atributos para esses objetos. Por exemplo, uma solicitação à porta 389 poderia ser usada para obter um departamento do usuário. Porta 3268 – Esta porta é usada para dúvidas especificamente voltadas ao catálogo global. As solicitações de LDAP enviadas para a porta 3268 podem ser usadas para buscar objetos em toda a floresta. No entanto, apenas os atributos marcados para replicação para o catálogo global

Nome	Porta padrão	Descrição
		podem ser devolvidos. Por exemplo, o departamento de um usuário poderia não ser devolvido usando a porta 3268 já que esse atributo não é replicado para o catálogo global.
Client Authentication	HTTPS/ 8449	Permite que os servidores clientes autentiquem com o Dell Server. Necessário para Server Encryption

Design da arquitetura do Security Management Server

As soluções Encryption Enterprise e Endpoint Security Suite Enterprise são produtos altamente escaláveis, de acordo com a quantidade endpoints que se deseja criptografar em sua organização.

Componentes da arquitetura

Abaixo estão as configurações sugeridas de hardware que atendem à maioria dos ambientes.

Security Management Server

- Sistema operacional: Windows Server 2012 R2 (Standard, Datacenter 64-bit), Windows Server 2016 (Standard, Datacenter 64-bit), Windows Server 2019 (Standard, Datacenter), Windows Server 2022 (Standard ou Datacenter)
- Máquina virtual ou física
- CPU: 4 núcleos
- RAM: 16 GB
- Unidade C: 30 GB de espaço em disco disponível para os registros e bases de dados da aplicação

  NOTA: Até 10 GB podem ser consumidos para um banco de dados de evento local armazenado no PostgreSQL.

Servidor proxy

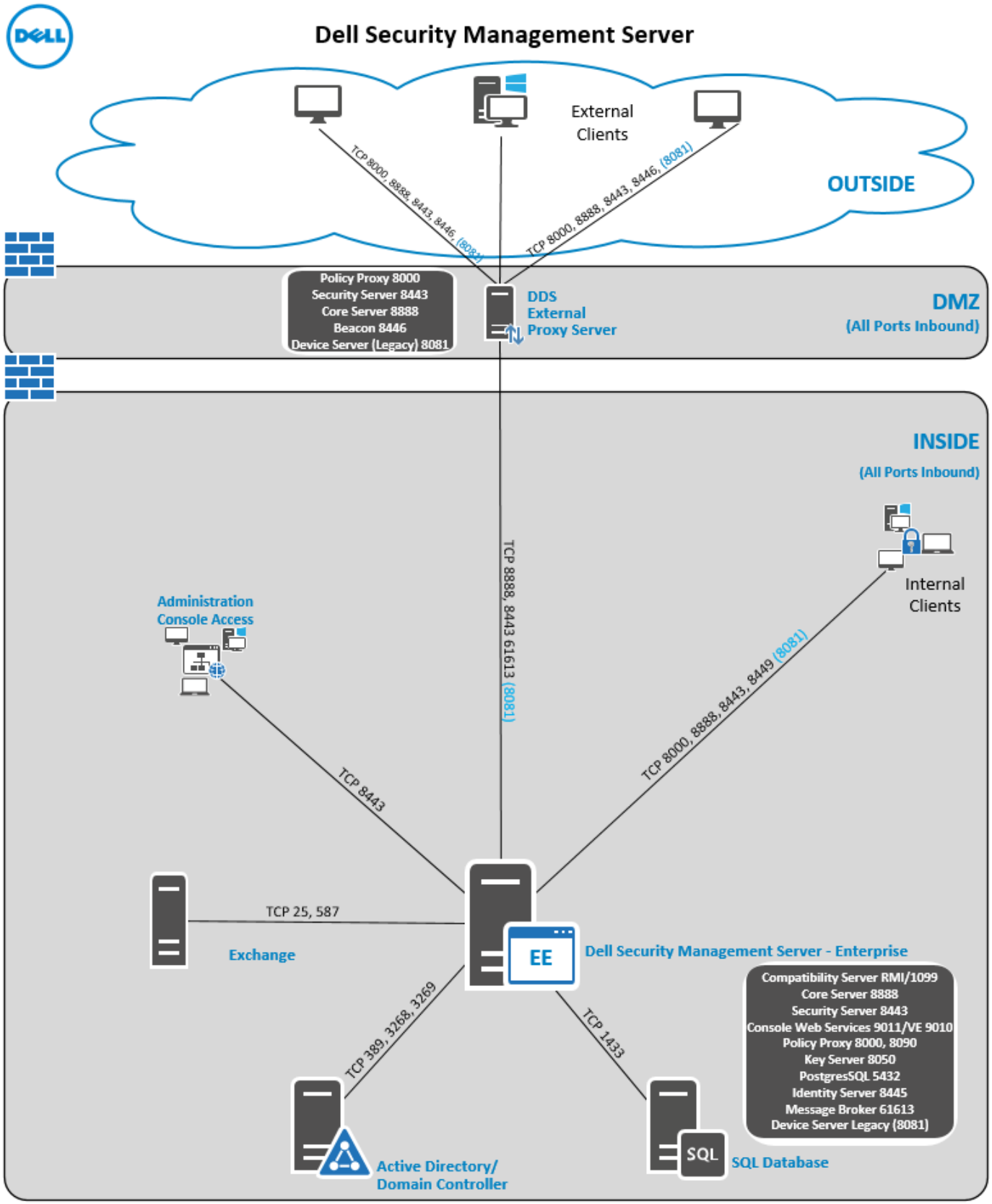
- Sistema operacional: Windows Server 2012 R2 (Standard, Datacenter 64-bit), Windows Server 2016 (Standard, Datacenter 64-bit), Windows Server 2019 (Standard, Datacenter), Windows Server 2022 (Standard ou Datacenter)
- Máquina virtual ou
- CPU: 2 núcleos
- RAM: 8 GB
- Unidade C: 20 GB de espaço em disco disponível para os registros

Especificações do hardware do SQL Server

- CPU: 4 núcleos
- RAM: 24 GB
- Unidade de dados: 100–150 GB de espaço em disco disponível (este valor pode variar de acordo com ambiente).
- Unidade de registro: 50 GB de espaço em disco disponível (este valor pode variar de acordo com ambiente).

  NOTA: A Dell Technologies recomenda que se siga as Práticas recomendadas do SQL Server, apesar das informações acima mencionadas cobrirem 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 endpoints, entre em contato com o Dell ProSupport para obter assistência.

Portas

A tabela a seguir descreve cada componente e sua função.

Nome	Porta padrão	Descrição
Serviço ACL	TCP/ 8006	Gerencia várias permissões e acesso de grupo para vários produtos do Dell Security. **NOTA:** A porta 8006 não está protegida. Certifique-se de que essa porta seja filtrada corretamente por meio de um firewall. Esta porta é apenas interna.
Management Console	HTTP(S)/ 8443	A central de controles e o console de administração da implementação de toda a empresa.
Core Server	HTTPS/ 8888	Gerencia o fluxo de política, as licenças, o registro para Preboot Authentication, SED Management, BitLocker Manager, Threat Protection e Advanced Threat Prevention. Processa os dados de inventário para uso pelo console de gerenciamento. Coleta e armazena os dados de autenticação. Controla o acesso baseado em função.
Device Server	HTTPS/ 8081	Suporta ativações e a recuperação de senha. Um componente do Security Management Server. Necessário para Encryption Enterprise (Windows e Mac)
Security Server	HTTPS/ 8443	Comunica-se com o Proxy de política; gerencia as recuperações de chaves forense, ativações de clients, comunicação SED-PBA e Full Disk Encryption-PBA e Active Directory para autenticação e reconciliação. Isso inclui a validação de identidade para autenticação no console de gerenciamento. Precisa de acesso ao banco de dados SQL.
Compatibility Server	TCP/ 1099	Um serviço para gerenciar a arquitetura empresarial. Coleta e armazena os dados iniciais de inventário durante a ativação e os dados de política durante as migrações. Processa os dados baseados em grupos de usuário. **NOTA:** A porta 1099 deve ser filtrada por um firewall. A Dell Technologies recomenda que essa porta seja apenas interna.

Nome	Porta padrão	Descrição
Message Broker Service	TCP/ 61616 e STOMP/ 61613	Lida com a comunicação entre os serviços do Dell Server. Prepara as informações de política que o Compatibility Server cria para o enfileiramento do proxy de política. Precisa de acesso ao banco de dados SQL. **NOTA:** A porta 61616 deve ser filtrada por um firewall. A Dell Technologies recomenda que essa porta seja apenas interna. **NOTA:** Somente abra a porta 61613 para os Security Management Servers configurados no modo front-end.
Key Server	TCP/ 8050	Negocia, autentica e criptografa uma conexão de um cliente usando APIs Kerberos. Precisa de acesso ao banco de dados SQL para obter os dados de chave.
Policy Proxy	TCP/ 8000	Fornece um caminho de comunicação baseado na rede para fornecer atualizações da política de segurança e atualizações de inventário.
PostGres	TCP/ 5432	Banco de dados local usado para dados de eventos. **NOTA:** A porta 5432 deve ser filtrada por um firewall. A Dell Technologies recomenda que essa porta seja apenas interna.
LDAP	TCP/ 389/636 (controlador de domínio local), 3268/3269 (catálogo global) TCP/ 135/ 49125+ (RPC)	Porta 389 – Esta porta é usada para solicitar informações a partir do controlador de domínio local. As solicitações de LDAP enviadas para a porta 389 podem ser usadas para buscar objetos apenas dentro do domínio doméstico do catálogo global. No entanto, o aplicativo de solicitação pode obter todos os atributos para esses objetos. Por exemplo, uma solicitação à porta 389 poderia ser usada para obter um departamento do usuário. Porta 3268 — esta porta é usada para dúvidas especificamente voltadas ao catálogo global. As solicitações de LDAP enviadas para a porta 3268 podem ser usadas para buscar objetos em toda a floresta. No entanto, apenas os atributos marcados para replicação para o catálogo global podem ser devolvidos. Por exemplo, o

Nome	Porta padrão	Descrição
		departamento de um usuário poderia não ser devolvido usando a porta 3268 já que esse atributo não é replicado para o catálogo global.
Microsoft SQL Database	TCP/ 1433	A porta padrão do SQL Server é 1433, e as portas client recebem um valor aleatório entre 1024 e 5000.
Client Authentication	HTTPS/ 8449	Permite que os servidores client sejam autenticados com o Dell Server. Necessário para Server Encryption.

6

Práticas recomendadas do SQL

A lista a seguir explica as boas práticas do SQL Server que precisam ser implementadas quando o Dell Security for instalado, caso ainda não tenham sido implementadas.

1. Certifique-se de que o tamanho de bloco do NTFS onde residem os arquivos de dados e o arquivo de registro é de 64 KB. As extensões do SQL Server (unidade básica do SQL Storage) são de 64 KB.

   Para obter mais informações, procure por "Compreendendo páginas e extensões" nos artigos da TechNet da Microsoft.

2. Como diretriz geral, defina a quantidade máxima de memória do SQL Server como 80% da memória instalada.

   Para obter mais informações, pesquise nos artigos da TechNet da Microsoft por *Opções de configuração do servidor de memória do servidor*.

   - 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 inicialização de instância para garantir que, na ocorrência de um impasse, as respectivas informações sejam capturadas.

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

   - 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 estejam cobertos por uma rotina de manutenção semanal que os reconstrua.

5. Confirme se as permissões e os recursos são apropriados para o banco de dados aproveitado pelo Security Management Server. Para obter mais informações, consulte o artigo da base de conhecimento 124909.

7

Exemplo de e-mail de notificação ao cliente

Depois de comprar o Dell Data Security, você receberá um e-mail de DellDataSecurity@Dell.com. Abaixo está um exemplo do e-mail, o qual conterá suas credenciais do CFT e as 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