Dell Data Security

Dell Data Security v9.9 - はじめに

メモ、注意、警告

メモ: 製品を使いやすくするための重要な情報を説明しています。

注意: ハードウェアの損傷やデータの損失の可能性を示し、その問題を回避するための方法を説明しています。

警告: 物的損害、けが、または死亡の原因となる可能性があることを示しています。

Dell Data Security - はじめに

2017 - 10

Rev. A01

目次

1

実装フェーズ

基本的な実装プロセスは、これらのフェーズで構成されます。

- 「キックオフと要件確認」を実行する
- 「準備チェックリスト - 初期実装」または「準備チェックリスト - アップグレード / 移行」を完了する
- 次の**いずれか**をインストールまたはアップグレード/ 移行します。
  - ***Security Management Server***
    - デバイスの一元管理
    - Microsoft Windows サーバ上、または仮想化環境で実行されます
  - ***Security Management Server Virtual***
    - 最大 3500 台のデバイスの一元管理
    - 仮想環境で実行されます

    Dell Server の詳細については、*Security Management Server* / インストールおよび移行ガイド または *Security Management Server Virtual* クイックスタートおよびインストールガイド を参照してください。これらのドキュメントを入手するには、「Dell Data Security Server に関するドキュメント」を参照してください。

    クライアントの要件やソフトウェアのインストールの手順については、施された展開に適切な文書を参照してください。

    - *Encryption Enterprise* 基本インストールガイドまたは *Encryption Enterprise* 詳細インストールガイド
    - *Endpoint Security Suite Enterprise* 基本インストールガイド または *Endpoint Security Suite Enterprise* 詳細インストールガイド
    - *Advanced Threat Prevention* 管理者ガイド
    - *Encryption Personal* インストールガイド
    - *Encryption Enterprise for Mac* 管理者ガイド
    - *Endpoint Security Suite Enterprise for Mac* の管理者ガイド
    - *Dell Data Guardian* の管理者ガイド
    - *Dell Data Guardian* のユーザーガイド

      これらのドキュメントを入手するには、「Dell Data Security クライアントのドキュメント」を参照してください。
- 初期ポリシーの設定
  - *Security Management Server* - リモート管理コンソールから利用できる *Security Management Server* / インストールおよび移行ガイド、管理タスク および *AdminHelp* を参照してください
  - *Security Management Server Virtual* - リモート管理コンソールから利用できる *Security Management Server Virtual* **クイックスタートおよびインストールガイド**、リモート管理コンソール管理タスク および *AdminHelp* を参照してください
- テスト計画の実行
- クライアントパッケージ
- Dell Security Administrator ベーシックナレッジトランスファーへの参加
- ベストプラクティスの実装
- デルクライアントサービスとのパイロットまたは導入サポートの調整

2

キックオフと要件確認

プロジェクトのビジネスおよび技術的な目標を達成するために Dell Data Security を正しく実装するには、インストールの前に、お使いの環境と、これらの目的を理解しておくことが重要です。組織全体のデータセキュリティ要件を十分に理解しておくようにしてください。

次の質問は、デルクライアントサービスチームがお使いの環境と要件を理解するために役立つ、一般的な主要質問です。

1 組織のビジネスタイプは何ですか（医療機関など）?
2 規制順守要件はありますか（HIPAA/HITECH、PCI、など）?
3 組織の規模は（ユーザー数、物理的場所の数、など）?
4 導入するエンドポイントの目標数は? エンドポイント数を将来拡張する予定はありますか?
5 エンドユーザーにローカル管理者権限がありますか?
6 管理および暗号化する必要があるデータおよびデバイスは何ですか（ローカル固定ディスク、USB、など）?
7 導入を検討している製品は何ですか?

- Encryption Enterprise
  - Encryption（DE 資格）- Windows Encryption、Server Encryption、Encryption External Media、SED Management、Advanced Authentication、BitLocker Manager（BLM）、および Mac Encryption
  - Encryption External Media
- Endpoint Security Suite Enterprise
  - Advanced Threat Prevention - オプションの Client Firewall および Web Protection（ATP 資格）の有無を問わない
  - Encryption（DE 資格）- Windows Encryption、Server Encryption、Encryption External Media、SED Management、Advanced Authentication、BitLocker Manager（BLM）、および Mac Encryption
  - Encryption External Media
- Dell Data Guardian（CE 資格）

8 組織でサポートされているユーザー接続のタイプは何ですか? これには、次のようなタイプがあります。

- ローカル LAN 接続のみ
- VPN ベース、および / または企業ワイヤレスユーザー
- リモートユーザー / 切断されたユーザー（直接または VPN 経由のいずれかでネットワークに長期間接続されていないユーザー）
- 非ドメインワークステーション

9 エンドポイントで保護する必要のあるデータはどのデータですか? 標準的なユーザーがエンドポイントで使用しているデータのタイプは何ですか?
10 重要情報を含まれる可能性があるユーザーアプリケーションは何ですか? アプリケーションのファイルタイプは何ですか?
11 お使いの環境内のドメインの数は? 暗号化の対象範囲となっているドメインの数は?
12 暗号化の対象になるオペレーティングシステムと OS バージョンは何ですか?
13 エンドポイントに代替ブートパーティションを設定していますか?

a メーカーリカバリパーティション
b デュアルブートワークステーション

Dell Data Security クライアントのドキュメント

展開したい Dell Data Security 製品のインストール要件、サポートされている OS バージョンおよび SSED の詳細については、以下の適切なドキュメントを参照してください。

Encryption Enterprise（Windows クライアント） - www.dell.com/support/home/us/en/04/product-support/product/dell-data-protection-encryption/manuals にある次のドキュメントを参照してください。

- *Encryption Enterprise* 基本インストールガイド - Encryption Enterprise のインストールガイド。
- Encryption Enterprise 詳細インストールガイド - Encryption Enterprise のインストールガイド（カスタムインストール用の高度なスイッチおよびパラメーター付き）。
- *Dell Data Security* コンソールのユーザーガイド- Advanced Authentication のエンドユーザー向けの指示。

Encryption Enterprise *（Mac クライアント）* - www.dell.com/support/home/us/en/04/product-support/product/dell-data-protection-encryption/manuals にある『Encryption Enterprise の管理者ガイドを参照してください。この管理者ガイドには、インストールと導入の手順が記載されています。

Endpoint Security Suite Enterprise（Windows クライアント） - www.dell.com/support/home/us/en/19/product-support/product/dell-dp-endpt-security-suite-enterprise/manuals にある次のドキュメントを参照してください。

- *Endpoint Security Suite Enterprise* 基本インストールガイド- Endpoint Security Suite Enterprise のインストールガイド。
- *Endpoint Security Suite Enterprise* 詳細インストールガイド 詳細インストールガイド- Endpoint Security Suite Enterprise のインストールガイド（カスタムインストール用の高度なスイッチおよびパラメーター付き）。
- *Advanced Threat Prevention* クイックスタートガイド- Advanced Threat Prevention 管理の手順（ポリシーの推奨事項、脅威の識別と管理、およびトラブルシューティングを含む）。
- *Dell Data Security* コンソールのユーザーガイド- Endpoint Security Suite Enterprise のエンドユーザー向けの指示。

Endpoint Security Suite Enterprise **（Mac クライアント）** - www.dell.com/support/home/us/en/19/product-support/product/dell-dp-endpt-security-suite-enterprise/manuals にある次のドキュメントを参照してください。

- *Endpoint Security Suite Enterprise for Mac* の管理者ガイド *）* - Endpoint Security Suite Enterprise for Mac のインストールガイド。

Dell Data Guardian - www.dell.com/support/home/us/en/19/product-support/product/dell-data-guardian/manuals にある次のドキュメントを参照してください。

- *Dell Data Guardian* の管理者ガイド- Data Guardian のエンドユーザー向けのインストール、アクティブ化および操作手順。
- *Dell Data Guardian* のユーザーガイド- Data Guardian のエンドユーザー向けのインストール、アクティブ化および操作手順。

Dell Data Security Server に関するドキュメント

展開したい Dell Data Security Server のインストール要件、サポートされている OS バージョンや構成の詳細については、以下の適切なドキュメントを参照してください。

Security Management Server

- 次のリンクから『*Security Management Server Installation and Migration Guide*』*（Security Management Server* インストールおよび移行ガイド *）*を参照してください。

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

  または

  www.dell.com/support/home/us/en/04/product-support/product/dell-dp-endpt-security-suite/manuals

  または

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

または

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

Security Management Server Virtual

- 次のリンクから、『Security Management Server Virtual Quick Start and Installation Guide』*(Security Management Server Virtual* クイックスタートおよびインストールガイド *)* を参照してください。

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

  または

  www.dell.com/support/home/us/en/04/product-support/product/dell-dp-endpt-security-suite/manuals

  または

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

  または

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

3

準備チェックリスト - 初期実装

Dell Encryption、Endpoint Security Suite Enterprise、または Data Guardian のインストールを開始する前に、展開された Dell Server に基づいた適切なチェックリストを参照して、すべての前提条件が満たされていることを確認します。

- Dell Security Management Server のチェックリスト
- Dell Security Management Server Virtual のチェックリスト

Security Management Server 初期実装のチェックリスト

Proof of Concept（POC）環境のクリーンアップは完了していますか（該当する場合）？

- ☐ デルでインストール作業を行う前に、Proof of Concept 用のデータベースおよびアプリケーションがバックアップされ、アンインストールされている（同じサーバーを使用している場合）。
- ☐ Proof of Concept（PoC）テスト中に使用されたすべての実稼働エンドポイントが複合化されている、または主要バンドルがダウンロードされています。
- ☐ Proof of Concept のアプリケーションが環境から削除されました。

メモ:
すべての新規実装は、新しいデータベースおよび Encryption、Endpoint Security Suite Enterprise、または Data Guardian のソフトウェアのインストールから開始される必要があります。デルクライアントサービスは、POC 環境を使用した新規実装は行いません。Proof of Concept の実行中に暗号化されたエンドポイントは、いずれもデルとのインストール作業開始前に復号化または再構築される必要があります。

サーバーはハードウェアの必須要件を満たしていますか?

- ☐ 「Dell Security Management Server アーキテクチャの設計」を参照してください。

サーバーはソフトウェア必須要件を満たしていますか?

- ☐ Windows Server 2008 SP2 64 ビット（Standard または Enterprise）; 2008 R2 SP0-SP1 64-bit（Standard または Enterprise）; 2012 R2（Standard または Datacenter）あるいは 2016（Standard または Datacenter）がインストールされている。または、仮想化環境にインストールすることもできます。詳細については、「仮想化」を参照してください。
- ☐ Windows Installer 4.0 以降がインストールされている。
- ☐ .NET Framework 4.5 がインストールされている。
- ☐ SQL Server 2012 または SQL Server 2016 を使用している場合、Microsoft SQL Native Client 2012 がインストールされている。もし利用可能であれば、SQL Native Client 2014 も使用できます。

  メモ: SQL Express は Security Management Server ではサポートされていません。
- ☐ Windows ファイアウォールが無効化されている、または（インバウンド）ポート 443、1099、1433、8000、8050、8081、8084、8443、8445、8446、8888、9000、9011、61613、61616 を許可するように設定されている。

- ポート 88、135、389、443、636、3268、3269、49125+（RPC）（AD へのインバウンド）経由の Security Management Server と Active Directory（AD）間での接続が利用可能になっている。

- C:\Program Files にインストールする際は、Windows Server 2008/2008 R2 上でインストールする前に UAC を無効にします。変更を有効にするためにはサーバーを再起動する必要があります。（Windows コントロールパネル > ユーザーアカウントを参照）

  - Windows Server 2008 SP2 64 ビット / Windows Server 2008 R2 SP0-SP1 64 ビット
  - Windows Server 2012 R2 では、インストーラが UAC を無効にします。
  - Windows Server 2016 R2 では、インストーラが UAC を無効にします。

サービスアカウントが正しく作成されていますか?

- AD への読み取り専用アクセス（LDAP）付きのサービスアカウント - ベーシックのユーザー/ドメインのユーザーアカウントが適切です。

- サービスアカウントには、Dell Security Management Server アプリケーションサーバに対するローカル管理者権限が必要です。

- データベースで Windows での認証を実行したい場合は、システム管理者の権限を所持するドメインサービスアカウントが必要です。ユーザーアカウントは DOMAIN\\Username フォーマットであり、SQL Server 許可のデフォルトスキーマ： dbo およびデータベース役割メンバーシップ：db_owner を「public」にする必要があります。

- SQL 認証を使用する場合、使用する SQL アカウントには SQL Server に対するシステム管理者権限が必要です。ユーザーアカウントには、SQL Server 許可のデフォルトスキーマ： dbo およびデータベース役割メンバーシップ： db_owner を public にする必要があります。

ソフトウェアはダウンロードされていますか？

Dell Support ウェブサイトからダウンロードします。

- Dell Data Security クライアントソフトウェアと Security Management Server のダウンロードファイルは、次の場所の **ドライバおよびダウンロード** フォルダにあります。

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

  または

  www.dell.com/support/home/us/en/04/product-support/product/dell-dp-endpt-security-suite/research?rvps=y

  または

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

  または

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

  www.dell.com/support からこのフォルダに移動するには、次の手順を実行します。

  1 デルサポートのウェブページで、**すべての製品から選択**、**ソフトウェアおよびセキュリティ**、**エンドポイントセキュリティソリューション** の順に選択します。
  2 **Encryption**、**Endpoint Security Suite Enterprise**、または **Data Guardian** を選択し、次に **ドライバおよびダウンロード** を選択します。
  3 オペレーティングシステムのプルダウンリストからダウンロードしたい製品の正しいオペレーティングシステムを選択します。例えば、Dell Enterprise Server をダウンロードしたい場合は、「**Windows Server オプションのいずれか**」を選択します。
  4 選択したいソフトウェアから「ファイルのダウンロード」を選択します。

- Encryption または Endpoint Security Suite Enterprise を「on-the-box」で購入された場合は、ソフトウェアは www.dell.com/support からダウンロードすることができます。「On-the-box」とは、デルの工場出荷時コンピュータイメージに含まれているソフトウェアを意味します。デルのコンピュータには、Encryption または Endpoint Security Suite Enterprise を出荷時にプレインストールすることができます。

または

Dell Data Security ファイル転送サイト（CFT）からダウンロードします

- ソフトウェアは、https://ddpe.credant.com または https://cft.credant.com の **SoftwareDownloads** フォルダにあります。
- Encryption または Endpoint Security Suite Enterprise を「on-the-box」で購入された場合は、ソフトウェアは www.dell.com/support からダウンロードすることができます。「On-the-box」とは、デルの工場出荷時コンピュータイメージに含まれているソフトウェアを意味します。デルのコンピュータには、Encryption または Endpoint Security Suite Enterprise を出荷時にプレインストールすることができます。

インストールキーおよびライセンスファイルは利用可能ですか?

- ライセンスキーは、CFT 資格情報が記載された元の電子メールに含まれています。「お客様通知電子メールの例」を参照してください。
- ライセンスファイルは、CFT サイトの **Client Licenses**（クライアントライセンス）フォルダにある XML ファイルです。

メモ:
ライセンスを「on-the-box」でご購入いただいた場合は、ライセンスファイルは必要ありません。この権利は、新しい Encryption または Endpoint Security Suite Enterprise クライアントのアクティブ化と同時に、デルから自動的にダウンロードされます。

データベースが作成されていますか?

- （オプション）新しいデータベースがサポートされているサーバに作成されます。*Security Management Server / インストールおよび移行ガイド* の「Requirements and Architecture」（要件とアーキテクチャ）を参照してください。Security Management Server のインストーラは、データベースがすでに作成されていない場合、インストール中にデータベースを作成します。
- ターゲットデータベースユーザーには **db_owner** 権限が付与されています。

Security Management Server および / または内部と外部のトラフィックに対する Split DNS 付きの Policy Proxies に対して DNS エイリアスは作成されていますか？

拡張性のため、DNS エイリアスを作成することをお勧めします。これにより、クライアントのアップデートを必要とすることなく、後でサーバーを追加したり、アプリケーションのコンポーネントを分離させることができます。

- 必要に応じて、DNS エイリアスが作成されている。DNS エイリアス例：
  - Security Management Server：ddpe-es.<domain.com>
  - フロントエンドサーバー： ddpe-fe.<domain.com>

メモ:
スプリット DNS では、内部および外部両方のフロントエンドサービスに同一 DNS 名を使用することができ、スプリット DNS が必要となる場合もあります。スプリット DNS は、お使いのクライアントに単一のアドレスを使用することを可能にし、アップグレードの実行時や将来のソリューションを拡張する時に柔軟性を提供します。スプリット DNS の使用時におけるフロントエンドサーバー用 CNAME の例は、ddpe-fe.<domain.com> です。

SSL 証明書の計画はありますか?

- 証明書の署名に使用でき、環境内のすべてのワークステーションで信頼される社内認証機関（CA）がある、**または** VeriSign もしくは Entrust といったパブリック認証機関を使用して署名済み証明書を購入する計画がある。パブリック認証機関を使用している場合は、デルクライアントサービスのエンジニアにお知らせください。証明書には、公開キーおよび秘密キーの署名が付いた Entire Chain of Trust (Root および Intermediate) が含まれています。
- Certificate Request の Subject Alternate Names (SANs) が Dell Enterprise Server のインストールに使用されているすべてのサーバーに付与されているすべての DNS エイリアスに一致します。Wildcard または Self Signed の証明書の要求には適用されません。

- ☐ 証明書は .pfx 形式で生成されます。

Change Control 要件を特定し、それをデルに伝えましたか?

- ☐ インストール実施前に、Encryption、Endpoint Security Suite Enterprise、または Data Guardian のインストールに必要となるすべての具体的な Change Control 要件をデルクライアントサービスに提出してください。これらの要件には、アプリケーションサーバー、データベース、およびクライアントワークステーションへの変更が含まれる場合があります。

テストハードウェアの準備は整っていますか?

- ☐ テストに使用するため、少なくとも 3 台のコンピュータを会社のコンピューターイメージで準備してください。デルは、テスト用にライブシステムを使用することを **お勧めしません**。ライブシステムは、暗号化ポリシーが定義され、デル提供のテスト計画を使用したテストが行われた後の実稼働パイロット期間中に使用するようにしてください。

Security Management Server Virtual の初期実装チェックリスト

Proof of Concept（POC）環境のクリーンアップは完了していますか（該当する場合）?

- ☐ デルでインストール作業を行う前に、Proof of Concept（PoC）用のデータベースおよびアプリケーションがバックアップされ、アンインストールされています（同じサーバーを使用している場合）。
- ☐ Proof of Concept（PoC）テスト中に使用されたすべての実稼働エンドポイントが複合化されている、または主要バンドルがダウンロードされています。
- ☐ Proof of Concept のアプリケーションが環境から削除されました。

メモ:

すべての新規実装は、新しいデータベースおよび Encryption、Endpoint Security Suite Enterprise、または Data Guardian のソフトウェアのインストールから開始される必要があります。デルクライアントサービスは、POC 環境を使用した新規実装は行いません。Proof of Concept の実行中に暗号化されたエンドポイントは、いずれもデルとのインストール作業開始前に復号化または再構築される必要があります。

サービスアカウントが正しく作成されていますか?

- ☐ AD への読み取り専用アクセス（LDAP）付きのサービスアカウント - ベーシックのユーザー/ドメインのユーザーアカウントが適切です。

ソフトウェアはダウンロードされていますか?

- ☐ Dell Data Security クライアントソフトウェアと Security Management Server Virtual のダウンロードファイルは、次の場所の **ドライバおよびダウンロード** フォルダにあります。

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

  または

  www.dell.com/support/home/us/en/04/product-support/product/dell-dp-endpt-security-suite/research?rvps=y

  または

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

  または

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

www.dell.com/support からこのフォルダに移動するには、次の手順を実行します。

1 デルサポートのウェブページで、**すべての製品から選択**、**ソフトウェアおよびセキュリティ**、**エンドポイントセキュリティソリューション** の順に選択します。
2 **Encryption**、**Endpoint Security Suite Enterprise**、または **Data Guardian** を選択し、次に **ドライバおよびダウンロード** を選択します。
3 オペレーティングシステムのプルダウンリストからダウンロードしたい製品の正しいオペレーティングシステムを選択します。例えば、Dell Enterprise Server をダウンロードしたい場合は、「**Windows Server オプションのいずれか**」を選択します。
4 選択したいソフトウェアから「ファイルのダウンロード」を選択します。

- Encryption または Endpoint Security Suite Enterprise を「on-the-box」で購入された場合は、ソフトウェアは www.dell.com/support からダウンロードすることができます。「On-the-box」とは、デルの工場出荷時コンピュータイメージに含まれているソフトウェアを意味します。デルのコンピュータには、Encryption または Endpoint Security Suite Enterprise を出荷時にプレインストールすることができます。

ライセンスファイルが使用可能ですか?

- ライセンスファイルは、CFT サイトの **Client Licenses**（クライアントライセンス）フォルダにある XML ファイルです。

メモ:
ライセンスを「on-the-box」でご購入いただいた場合は、ライセンスファイルは必要ありません。この権利は、新しい Encryption または Endpoint Security Suite Enterprise クライアントのアクティブ化と同時に、デルから自動的にダウンロードされます。

サーバーはハードウェアの必須要件を満たしていますか?

- 「Security Management Server Virtual アーキテクチャの設計」を参照してください。

SSL 証明書の計画はありますか?

- 証明書の署名に使用でき、環境内のすべてのワークステーションで信頼される社内認証機関(CA)がある、**または** VeriSign もしくは Entrust といったパブリック認証機関を使用して署名済み証明書を購入する計画がある。パブリック認証機関を使用している場合は、デルクライアントサービスのエンジニアにお知らせください。

Change Control 要件を特定し、それをデルに伝えましたか?

- インストール実施前に、Encryption、Endpoint Security Suite Enterprise、または Data Guardian のインストールに必要となるすべての具体的な Change Control 要件をデルクライアントサービスに提出してください。これらの要件には、アプリケーションサーバー、データベース、およびクライアントワークステーションへの変更が含まれる場合があります。

テストハードウェアの準備は整っていますか?

- テストに使用するため、少なくとも 3 台のコンピュータを会社のコンピューターイメージで準備してください。デルは、テスト用にライブシステムを使用することを **お勧めしません**。ライブシステムは、暗号化ポリシーが定義され、デル提供のテスト計画を使用したテストが行われた後の実稼働パイロット期間中に使用するようにしてください。

4

準備チェックリスト - アップグレード / 移行

このチェックリストは Security Management Server のみに該当するものです。

メモ:
お使いの Dell Server ターミナルの 基本設定 メニューから、Security Management Server Virtual をアップデートします。詳細については、*Security Management Server Virtual* クイックスタートおよびインストールガイド を参照してください。

Encryption、Endpoint Security Suite Enterprise、または Data Guardian のアップグレードを開始する前に、次のチェックリストを参照して、すべての前提条件が満たされていることを確認します。

サーバーはソフトウェア必須要件を満たしていますか?

- ☐ Windows Server 2008 SP2 64 ビット (Standard または Enterprise) ; 2008 R2 SP0-SP1 64-bit (Standard または Enterprise) ; 2012 R2 (Standard または Datacenter) あるいは 2016 (Standard または Datacenter) がインストールされている。または、仮想化環境にインストールすることもできます。詳細については、「仮想化」を参照してください。
- ☐ Windows Installer 4.0 以降がインストールされている。
- ☐ .NET Framework 4.5 がインストールされている。
- ☐ SQL Server 2012 または SQL Server 2016 を使用している場合、Microsoft SQL Native Client 2012 がインストールされている。もし利用可能であれば、SQL Native Client 2014 も使用できます。

  メモ: SQL Express は Security Management Server ではサポートされていません。
- ☐ Windows ファイアウォールが無効化されている、または (インバウンド) ポート 443、1099、1433、8000、8050、8081、8084、8443、8445、8446、8888、9000、9011、61613、61616 を許可するように設定されている。
- ☐ ポート 88、135、389、443、636、3268、3269、49125+ (RPC) (AD へのインバウンド) 経由の Security Management Server と Active Directory (AD) 間での接続が利用可能になっている。
- ☐ C:\Program Files にインストールする際は、Windows Server 2008/2008 R2 上でインストールする前に UAC を無効にします。変更を有効にするためにはサーバーを再起動する必要があります。(Windows コントロールパネル > ユーザーアカウントを参照)
  - Windows Server 2008 SP2 64 ビット / Windows Server 2008 R2 SP0-SP1 64 ビット
  - Windows Server 2012 R2 では、インストーラが UAC を無効にします。
  - Windows Server 2016 R2 では、インストーラが UAC を無効にします。

サービスアカウントが正しく作成されていますか?

- ☐ AD への読み取り専用アクセス (LDAP) 付きのサービスアカウント - ベーシックのユーザー/ドメインのユーザーアカウントが適切です。
- ☐ サービスアカウントには、Security Management Server アプリケーションサーバに対するローカル管理者権限が必要です。
- ☐ データベースで Windows での認証を実行したい場合は、システム管理者の権限を所持するドメインサービスアカウントが必要です。ユーザーアカウントは DOMAIN\\Username フォーマットであり、SQL Server 許可のデフォルトスキーマ : dbo およびデータベース役割メンバーシップ : db_owner を「public」にする必要があります。

- SQL 認証を使用する場合、使用する SQL アカウントには SQL Server に対するシステム管理者権限が必要です。ユーザーアカウントには、SQL Server 許可のデフォルトスキーマ： dbo およびデータベース役割メンバーシップ： db_owner を public にする必要があります。

データベースおよびすべての必要なファイルはバックアップされていますか？

- 既存のすべてのインストールが別の場所にバックアップされています。バックアップには、SQL データベース、secretKeyStore および設定ファイルを含めるようにしてください。
- データベースへの接続に必要な情報を保持する、次の最も重要なファイルがバックアップされていることを確認してください。

  <インストール先フォルダ>\Enterprise Edition\Compatibility Server\conf\server_config.xml

  <インストール先フォルダ>\Enterprise Edition\Compatibility Server\conf\secretKeyStore

  <インストール先フォルダ>\Enterprise Edition\Compatibility Server\conf\gkresource.xml

インストールキーおよびライセンスファイルは利用可能ですか?

- ライセンスキーは、CFT 資格情報が記載された元の電子メールに含まれています。「お客様通知電子メールの例」を参照してください。
- ライセンスファイルは、CFT サイトの **Client Licenses**（クライアントライセンス）フォルダにある XML ファイルです。

メモ:
ライセンスを「on-the-box」でご購入いただいた場合は、ライセンスファイルは必要ありません。この権利は、新しい Encryption または Endpoint Security Suite Enterprise クライアントのアクティブ化と同時に、デルから自動的にダウンロードされます。

新しいおよび既存の Dell Data Security ソフトウェアはダウンロードされていますか？

Dell Data Security ファイル転送サイト（CFT）からダウンロードします。

- ソフトウェアは、https://ddpe.credant.com または https://cft.credant.com の **SoftwareDownloads** フォルダにあります。
- Encryption または Endpoint Security Suite Enterprise を「on-the-box」で購入された場合は、ソフトウェアは www.dell.com/support からダウンロードすることができます。「On-the-box」とは、デルの工場出荷時コンピュータイメージに含まれているソフトウェアを意味します。デルのコンピュータには、Encryption または Endpoint Security Suite Enterprise を出荷時にプレインストールすることができます。

十分なエンドポイントライセンスがありますか?

アップグレード前に、お使いの環境内にあるすべてのエンドポイントに適用するために十分な数のクライアントライセンスがあることを確認してください。現在インストール数がライセンス数を上回っている場合、アップグレードまたは移行前にデルのセールス担当者にお問い合わせください。Dell Data Security はライセンスの検証を実行し、使用可能なライセンスがない場合にはアクティブ化は行われません。

- 環境内で適用するために十分なライセンスがある。

SSL 証明書の計画はありますか?

- 証明書の署名に使用でき、環境内のすべてのワークステーションで信頼される社内認証機関(CA)がある、**または** VeriSign もしくは Entrust といったパブリック認証機関を使用して署名済み証明書を購入する計画がある。パブリック認証機関を使用している場合は、デルクライアントサービスのエンジニアにお知らせください。証明書には、公開キーおよび秘密キーの署名が付いた Entire Chain of Trust (Root および Intermediate) が含まれています。
- Certificate Request の Subject Alternate Names (SANs) が Dell Enterprise Server のインストールに使用されているすべてのサーバーに付与されているすべての DNS エイリアスに一致します。Wildcard または Self Signed の証明書の要求には適用されません。

- ☐ 証明書は .pfx 形式で生成されます。

Change Control 要件を特定し、それをデルに伝えましたか?

- ☐ インストール実施前に、Encryption、Endpoint Security Suite Enterprise、または Data Guardian のインストールに必要となるすべての具体的な Change Control 要件をデルクライアントサービスに提出してください。これらの要件には、アプリケーションサーバー、データベース、およびクライアントワークステーションへの変更が含まれる場合があります。

テストハードウェアの準備は整っていますか?

- ☐ テストに使用するため、少なくとも 3 台のコンピュータを会社のコンピューターイメージで準備してください。デルは、テスト用にライブシステムを使用することを **お勧めしません**。ライブシステムは、暗号化ポリシーが定義され、デル提供のテスト計画を使用したテストが行われた後の実稼働パイロット期間中に使用するようにしてください。

5

アーキテクチャ

この項では、Dell Data Security の実装におけるアーキテクチャデザインの推奨に関する詳細を説明します。展開したい Dell Server を選択してください。

- Security Management Server のアーキテクチャの設計
- Security Management Server Virtual のアーキテクチャの設計

Security Management Server アーキテクチャの設計

Dell Encryption、Endpoint Security Suite Enterprise、および Data Guardian ソリューションは、組織の規模と暗号化対象のエンドポイントの数に応じて拡張できる、拡張性の高い製品です。本項では、アーキテクチャを 5,000 ~ 50,000 またはそれ以上のエンドポイントに拡張するためのガイドラインを説明します。

メモ: 組織に 50,000 を超えるエンドポイントがある場合は、デル ProSupport に問い合わせてサポートを受けてください。

メモ:

各項にリストされた各コンポーネントには、それぞれ最小ハードウェア要件が設定されています。これは、ほぼすべての環境で最適なパフォーマンスを確保するための要件です。これらのコンポーネントに十分なリソースを割り当てないと、パフォーマンスの劣化、またはアプリケーションの動作問題につながるおそれがあります。

最大 5,000 のエンドポイント

このアーキテクチャは、1 から 5,000 のエンドポイントを持つほとんどの小規模 ~ 中規模企業に対応するものです。

アーキテクチャコンポーネント

Security Management Server

Windows Server 2008 R2 SP0-SP1 64 ビット/Windows Server 2008 SP2 64 ビット - Standard または Enterprise Edition

Windows Server 2012 R2 - Standard または Datacenter Edition

Windows Server 2016 - Standard または Datacenter Edition

シングルサーバ構成 - 概念検証用

次の推奨事項は、通常のクライアント通信レベルよりも高くで最大のパフォーマンスを発揮できるようにするものです。

16 GB、20 GB 以上の空きディスク容量（および仮想ページング容量）、現行世代のクアッドコア CPU（2 GHz 以上）

フロントエンドサーバーと併用されるサーバーの構成

最低 8 GB メモリ（構成に依存する）、120 GB HDD（SSD を推奨）、±1.5 GB の空きディスク容量（および仮想ページング容量）、最低でも現行世代のデュアルコア CPU（2 GHz 以上）（Core Duo、Core 2 Duo、Core i3、Core i5、Core i7、Xeon、Itanium、または AMD の同等製品を含む）

Dell 外部フロントエンドサーバー

Windows Server 2008 R2 SP0-SP1 64 ビット/Windows Server 2008 SP2 64 ビット - Standard または Enterprise Edition

Windows Server 2012 R2 - Standard または Datacenter Edition

Windows Server 2016 - Standard または Datacenter Edition

最低 8 GB（構成に依存する）、±1.5 GB の空きディスク容量（および仮想ページング容量）、最低でも現行世代のデュアルコア CPU（2 GHz 以上）（Core Duo、Core 2 Duo、Core i3、Core i5、Core i7、Xeon、Itanium、または AMD の同等製品を含む）

SQL Server

SQL Server 2008、SQL Server 2008 R2、および SQL Server 2008 SP4（KB3045311 付属）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

5,000 ~ 20,000 エンドポイント

このアーキテクチャは、5,000 から 20,000 のエンドポイントが存在する環境に対応するものです。追加の負荷を分散するためにフロントエンドサーバーが追加されますが、このサーバーは約 15,000 ~ 20,000 のエンドポイントを処理するよう設計されています。オプションで、インターネット経由でのポリシーの公開、および / またはエンドポイントのアクティブ化のために、フロントエンドサーバーを DMZ に設置することができます。

アーキテクチャコンポーネント

Security Management Server

最低 12GB メモリ（構成に依存する）、250 GB HDD（SSD を推奨）、±1.5 GB の空きディスク容量（および仮想ページング容量）、最低でも現行世代のデュアルコア CPU（2 GHz 以上）（Core Duo、Core 2 Duo、Core i3、Core i5、Core i7、Xeon、Itanium、または AMD の同等製品を含む）

Dell 内部フロントエンドサーバー（1）および Dell 外部フロントエンドサーバー（1）

Windows Server 2008 R2 SP0-SP1 64 ビット/Windows Server 2008 SP2 64 ビット - Standard または Enterprise Edition

Windows Server 2012 R2 - Standard または Datacenter Edition

Windows Server 2016 - Standard または Datacenter Edition

最低 8 GB（構成に依存する）、±1.5 GB の空きディスク容量（および仮想ページング容量）、最低でも現行世代のデュアルコア CPU（2 GHz 以上）（Core Duo、Core 2 Duo、Core i3、Core i5、Core i7、Xeon、Itanium、または AMD の同等製品を含む）

SQL Server

SQL Server 2008、SQL Server 2008 R2、および SQL Server 2008 SP4（KB3045311 付属）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 ~ 50,000 エンドポイント

このアーキテクチャは、20,000 から 50,000 のエンドポイントが存在する環境に対応するものです。追加の負荷を分散するためにフロントエンドサーバーが追加されます。各フロントエンドサーバーは、約 15,000 ~ 20,000 のエンドポイントを処理するよう設計されています。オプションで、エンドポイントのアクティブ化、および / またはインターネット経由でのポリシーの公開のために、フロントエンドサーバーを DMZ に設置することができます。

アーキテクチャコンポーネント

Security Management Server

Windows Server 2008 R2 SP0-SP1 64 ビット/Windows Server 2008 SP2 64 ビット - Standard または Enterprise Edition

Windows Server 2012 R2 - Standard または Datacenter Edition

Windows Server 2016 - Standard または Datacenter Edition

最低 16 GB メモリ(構成に依存する)、320 GB HDD(SSD 推奨)、±1.5 GB の空きディスク容量(および仮想ページング容量)、新型クアッドコア CPU の最小 (2 GHz 以上)、Xeon または AMD 同等を含む

Dell 内部フロントエンドサーバー (2) および Dell 外部フロントエンドサーバー (1)

Windows Server 2008 R2 SP0-SP1 64 ビット/Windows Server 2008 SP2 64 ビット - Standard または Enterprise Edition

Windows Server 2012 R2 - Standard または Datacenter Edition

Windows Server 2016 - Standard または Datacenter Edition

最低 8 GB (構成に依存する)、±1.5 GB の空きディスク容量 (および仮想ページング容量)、最低でも現行世代のデュアルコア CPU (2 GHz 以上) (Core Duo、Core 2 Duo、Core i3、Core i5、Core i7、Xeon、Itanium、または AMD の同等製品を含む)

SQL Server

SQL Server 2008、SQL Server 2008 R2、および SQL Server 2008 SP4 (KB3045311 付属) 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

50,000 以上のエンドポイント

このアーキテクチャは 50,000 以上のエンドポイントに対応します。追加の負荷を分散するためにフロントエンドサーバーが追加されます。各フロントエンドサーバーは、約 15,000 ~ 20,000 のエンドポイントを処理するよう設計されています。オプションで、エンドポイントのアクティブ化、および / またはインターネット経由でのポリシーの公開のために、フロントエンドサーバーを DMZ に設置することができます。

メモ:
組織に 50,000 を超えるエンドポイントがある場合は、デル ProSupport に問い合わせてサポートを受けてください。

アーキテクチャコンポーネント

Security Management Server

Windows Server 2008 R2 SP0-SP1 64 ビット/Windows Server 2008 SP2 64 ビット - Standard または Enterprise Edition

Windows Server 2012 R2 - Standard または Datacenter Edition

Windows Server 2016 - Standard または Datacenter Edition

最低 24 GB メモリ (構成に依存する)、500 GB HDD (SSD 推奨)、±1.5 GB の空きディスク容量 (および仮想ページング容量)、新型 8 コア CPU の最小 (2 GHz 以上)、Xeon または AMD 同等を含む

Dell 内部フロントエンドサーバー (2) および Dell 外部フロントエンドサーバー (1)

Windows Server 2008 R2 SP0-SP1 64 ビット/Windows Server 2008 SP2 64 ビット - Standard または Enterprise Edition

Windows Server 2012 R2 - Standard または Datacenter Edition

Windows Server 2016 - Standard または Datacenter Edition

最低 8 GB（構成に依存する）、±1.5 GB の空きディスク容量（および仮想ページング容量）、最低でも現行世代のデュアルコア CPU（2 GHz 以上）（Core Duo、Core 2 Duo、Core i3、Core i5、Core i7、Xeon、Itanium、または AMD の同等製品を含む）

SQL Server

SQL Server 2008、SQL Server 2008 R2、および SQL Server 2008 SP4（KB3045311 付属）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

高可用性についての考慮事項

このアーキテクチャは、最大 60,000 エンドポイントをサポートする可用性の高いアーキテクチャを形容するものです。これには、アクティブ / パッシブ設定でセットアップされた 2 台の Security Management Server があります。2 台目の Dell Server にフェイルオーバーするには、プライマリノードでサービスを停止して DNS エイリアス（CNAME）を 2 台目のノードにポイントさせます。2 台目のノードでサービスを開始し、リモート管理コンソールを起動してアプリケーションが正しく動作していることを確認します。2 台目（パッシブ）のノード上のサービスは、通常のメンテナンスおよびパッチ中にサービスが不意に開始されることを防ぐため、「手動」として設定してください。

組織では、SQL Cluster データベースサーバーの使用を選択することもできます。この設定では、クラスタ IP またはホスト名を使用するように Dell Server を設定してください。

メモ:
データベースのレプリケーションはサポートされません。

クライアントトラフィックは、3 台の内部フロントエンドサーバー間に分散されます。オプションで、エンドポイントのアクティブ化、および / またはインターネット経由でのポリシーの公開のために、フロントエンドサーバーを DMZ に設置することもできます。

仮想化

Security Management Server は、オプションで仮想環境にインストールできます。次の環境のみが推奨されます。

Security Management Server v9.9 は、Hyper-V Server（フルまたはコアインストール）で、Windows Server 2012 R2 または Windows Server 2016 の役割として動作確認済みです。

- Hyper-V Server（フルまたはコアインストール）
  - 64 ビット x86 CPU（必須）
  - 少なくとも 2 コアが搭載されたホストコンピュータ
  - 最小 8 GB RAM（推奨）
  - オペレーティングシステムは必要ありません
  - ハードウェアは Hyper-V 最小要件を満たしている必要があります
  - イメージ専用リソース用に最小 4 GB の RAM
  - 第 1 世代の仮想マシンとして実行する必要があります
  - 詳細については、https://technet.microsoft.com/en-us/library/hh923062.aspx を参照してください。

Security Management Server v9.9 は、VMware ESXi 5.5、VMware ESXi 6.0、および VMware ESXi 6.5 で動作確認済みです。潜在的な脆弱性を修正するため、VMWare ESXi にすべてのパッチとアップデートを適用します。

メモ: VMware ESXi および Windows Server 2012 R2 または Windows Server 2016 を実行する場合は、VMXNET3 イーサネットアダプタが推奨されます。

- VMware ESXi 5.5
  - 64 ビット x86 CPU（必須）
  - 少なくとも 2 コアが搭載されたホストコンピュータ
  - 最小 8 GB RAM（推奨）
  - オペレーティングシステムは必要ありません
  - 対応ホストオペレーティングシステムの完全なリストについては、http://www.vmware.com/resources/compatibility/search.php を参照してください。
  - ハードウェアは VMware 最小要件を満たしている必要があります
  - イメージ専用リソース用に最小 4 GB の RAM
  - 詳細については、http://pubs.vmware.com/vsphere-55/index.jsp を参照してください。
- VMware ESXi 6.0
  - 64 ビット x86 CPU（必須）
  - 少なくとも 2 コアが搭載されたホストコンピュータ
  - 最小 8 GB RAM（推奨）
  - オペレーティングシステムは必要ありません
  - 対応ホストオペレーティングシステムの完全なリストについては、http://www.vmware.com/resources/compatibility/search.php を参照してください。
  - ハードウェアは VMware 最小要件を満たしている必要があります
  - イメージ専用リソース用に最小 4 GB の RAM
  - 詳細については、http://pubs.vmware.com/vsphere-60/index.jsp を参照してください。
- VMware ESXi 6.5
  - 64 ビット x86 CPU（必須）
  - 少なくとも 2 コアが搭載されたホストコンピュータ
  - 最小 8 GB RAM（推奨）
  - オペレーティングシステムは必要ありません
  - 対応ホストオペレーティングシステムの完全なリストについては、http://www.vmware.com/resources/compatibility/search.php を参照してください。
  - ハードウェアは VMware 最小要件を満たしている必要があります
  - イメージ専用リソース用に最小 4 GB の RAM
  - 詳細については、http://pubs.vmware.com/vsphere-65/index.jsp を参照してください。

メモ: Security Management Server をホストしている SQL Server データベースは、別のコンピュータ上で実行する必要があります。

SQL Server

さらに大規模な環境では、SQL クラスタなどの冗長システム上で SQL データベースサーバを実行して、可用性とデータ継続性を確保することを強くお勧めします。また、トランザクションログを有効にして完全バックアップを毎日実行し、ユーザー / デバイスのアクティブ化によって新規に生成されたすべてのキーを回復可能にしておくこともお勧めします。

データベースのメンテナンスタスクには、すべてのデータベースインデックスの再構築と統計収集を含めるようにしてください。

Security Management Server ポート

以下の表は、各コンポーネントとその機能について説明しています。

名前	デフォルトポート	説明	必須とされる機能
Compliance Reporter	HTTP(S)/ 8084	監査とコンプライアンスのレポートのために、環境の詳細ビューを提供します。 Security Management Server のコンポーネント	レポート
リモート管理コンソール	HTTP(S)/ 8443	企業全体での導入に対応する管理コンソールとコントロールセンター。 Security Management Server のコンポーネント	すべて
Core Server	HTTPS/ 8888 および 9000	ポリシーフロー、ライセンス、起動前認証の登録、SED Management、BitLocker Manager、Threat Protection、Advanced Threat Prevention を管理します。Compliance Reporter およびリモート管理コンソールが使用するインベントリデータを処理します。認証データを収集し、保管します。役割に基づいたアクセスを制御します。 Security Management Server のコンポーネント	すべて
Device Server	HTTPS/ 8443 HTTPS/ 8081 (バックエンドの Dell Device Server へ	アクティベーションとパスワードの復元をサポートします。 Security Management Server のコンポーネント	Encryption Enterprise for Mac Encryption Enterprise CREDActivate
Security Server	HTTPS/ 8443	Policy Proxy との通信を行います。また、フォレンジックキーの取得、クライアントのアクティベーション、Data Guardian 製品、SED-PBA 通信、およびリモート管理コンソールへの認証のための ID 検証を含む認証または仲裁のための Active Directory を管理します。SQL データベースアクセスが必要です。 Security Management Server のコンポーネント	すべて
Compatibility Server	TCP/ 1099	エンタープライズアーキテクチャを管理するためのサービスです。アクティベーション中の初期インベントリデータおよび移行時のポリシーデータを収集、保管します。このサービスのユーザーグループに基づいてデータを処理します。 Security Management Server のコンポーネント	すべて
Message Broker サービス	TCP/ 61616	Security Management Server のサービス間の通信を処理します。ポリシープロキシのキュー操作のために Compatibility Server によって作成されるポリシー情報をステージします。	すべて

名前	デフォルトポート	説明	必須とされる機能
	および STOMP/ 61613	SQL データベースアクセスが必要です。 Security Management Server のコンポーネント	
Identity Server	HTTPS/ 8445	SED Manager の認証を含むドメイン認証要求を処理します。 Active Directory アカウントが必要です。Windows 認証が使用されている場合は、SQL にアクセスするために使用するアカウントである必要があります。 Security Management Server のコンポーネント	すべて
Key Server	TCP/ 8050	Kerberos API を使用して、クライアント接続のネゴシエーション、認証、暗号化を行います。 重要なデータの取得には SQL データベースのアクセスが必要です。 Security Management Server のコンポーネント	Dell 管理ユーティリティー
Policy Proxy	TCP/ 8000	セキュリティポリシーのアップデートとインベントリのアップデートを配信するためのネットワークベースの通信パスを提供します。 Security Management Server のコンポーネント	Encryption Enterprise for Mac Encryption Enterprise
LDAP	TCP/ 389/636 (ローカルドメインコントローラ)、3268/3269 (グローバルカタログ) TCP/ 135/ 49125+ (RPC)	ポート 389 - このポートはローカルドメインコントローラからの情報の要求に使用されます。ポート 389 に送信される LDAP 要求は、グローバルカタログのホームドメイン内にあるオブジェクトの検索にのみ使用できます。ただし、要求側のアプリケーションは、これらのオブジェクトに対するすべての属性を取得できます。たとえば、ポート 389 への要求は、ユーザーの部門を取得するために使用することができます。 **ポート 3268** - このポートは、特にグローバルカタログをターゲットとするクエリ用に使用されます。ポート 3268 に送信される LDAP 要求は、フォレスト全体でのオブジェクトの検索に使用することができます。ただし、返されるのはグローバルカタログへのリプリケーション用にマークされた属性のみです。たとえば、ポート 3268 を使用してユーザーの部門は返すことはできません。これは、この属性がグローバルカタログに複製されないためです。	すべて
Microsoft SQL データベース	TCP/ 1433	デフォルトの SQL サーバーポートは 1433 であり、クライアントポートには 1024 から 5000 の間の値がランダムに割り当てられます。	すべて
クライアント認証	HTTPS/ 8449	クライアントサーバが Security Management Server を介して認証することを許可します。	Server Encryption (SE)

名前	デフォルトポート	説明	必須とされる機能
コールバックビーコン	HTTP/TCP 8446	Data Guardian の保護付き Office モードを実行するときに、コールバックビーコンが保護付きの各 Office ファイルに挿入されることを許可します。	オプション。Data Guardian で使用
Advanced Threat Prevention を使用するクライアント通信	HTTPS/TCP/443	Advanced Threat Prevention を使用する場合のクライアント通信	Advanced Threat Prevention

Security Management Server Virtual アーキテクチャの設計

このアーキテクチャは、1 から 3500 のエンドポイントを持つ小規模 ~ 中規模企業に対応するものです。オプションで、インターネット経由でのポリシーの公開、および / またはエンドポイントのアクティブ化のために、フロントエンドサーバーを DMZ に設置することができます。

ハードウェアの仕様

- Security Management Server Virtual
- VMware Workstation 11、VMware Workstation 12.5、VMware ESXi 5.5、ESXi 6.0、または ESXi 6.5
- VMware Workstation 11 または VMware Workstation 12.5 には 4 GB RAM。ESXi 5.5、ESXi 6.0、または ESXi 6.5 には 8 GB RAM
- 80 GB の空きディスク容量
- 2+ Ghz のプロセッサ、Dual Core 以上

要件の詳細については、『*Security Management Server Virtual Quick Start Guide and Installation Guide*』(Security Management Server Virtual クイックスタートガイドおよびインストールガイド) を参照してください。

Dell 外部フロントエンドサーバー

- Windows Server 2008 R2 SP0-SP1 64 ビット/Windows Server 2008 SP2 64 ビット - Standard または Enterprise Edition/Windows Server 2012 R2 - Standard または Datacenter Edition/Windows Server 2016 - Standard Datacenter Edition
- 最低 +2 GB の専用 RAM / 4 GB の専用 RAM 推奨
- 1.5 GB の空きディスク容量 (その他仮想ページング容量が必要)
- 2 GHz Core Duo 以上

Security Management Server Virtual ポート

以下の表は、各コンポーネントとその機能について説明しています。

名前	デフォルトポート	説明	必須とされる機能
Compliance Reporter	HTTP(S)/ 8084	監査とコンプライアンスのレポートのために、環境の詳細ビューを提供します。 Security Management Server Virtual のコンポーネント	レポート
リモート管理コンソール		企業全体での導入に対応する管理コンソールとコントロールセンター。 Security Management Server Virtual のコンポーネント	すべて

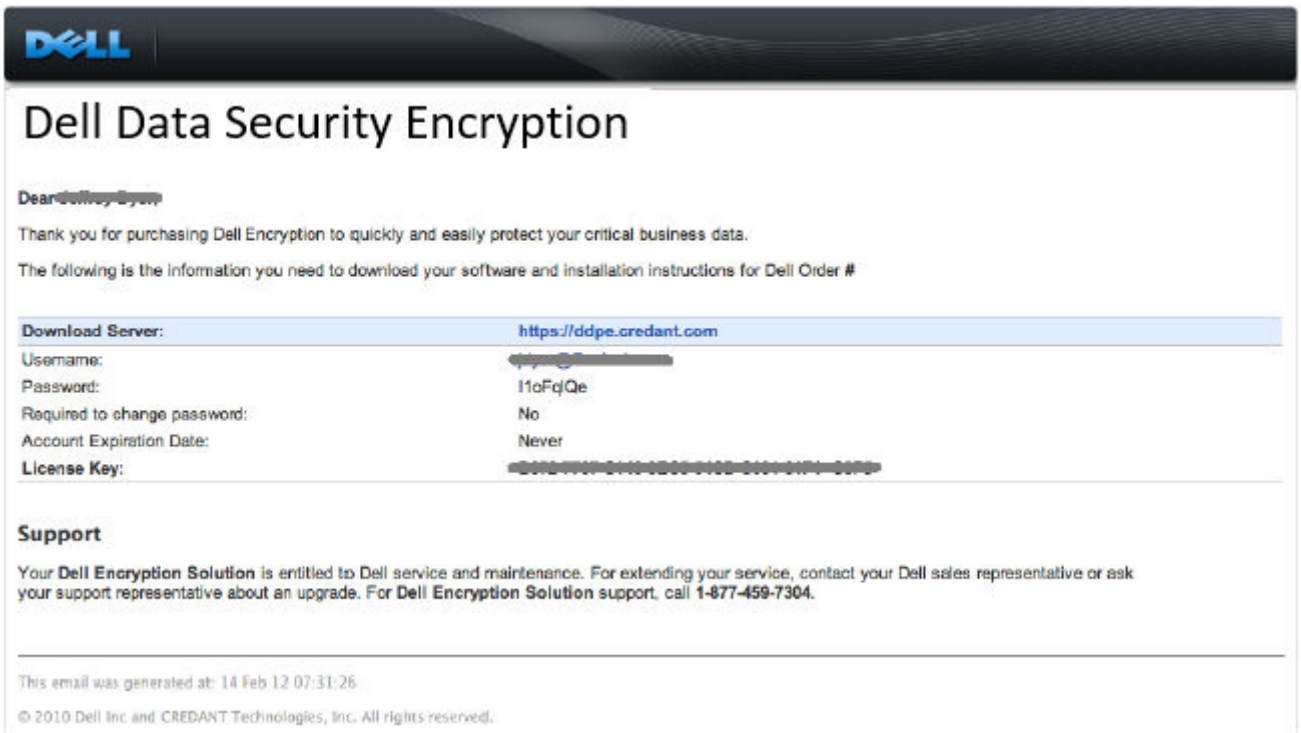
名前	デフォルトポート	説明	必須とされる機能
Core Server	HTTPS/ 8888	ポリシーフロー、ライセンス、起動前認証の登録、SED Management、BitLocker Manager、Threat Protection、Advanced Threat Prevention を管理します。Compliance Reporter およびリモート管理コンソールが使用するインベントリデータを処理します。認証データを収集し、保管します。役割に基づいたアクセスを制御します。 Security Management Server Virtual のコンポーネント	すべて
Core Server HA (高可用性)	HTTPS/ 8888	Remote Management Console、Preboot Authentication、SED Management、BitLocker Manager、Threat Protection および Advanced Threat Prevention による HTTPS 接続のセキュリティおよびパフォーマンスの強化を可能にする高可用性サービスです。 Security Management Server Virtual のコンポーネント	すべて
Security Server	HTTPS/ 8443	Policy Proxy との通信を行います。また、フォレンジックキーの取得、クライアントのアクティベーション、Data Guardian 製品、および SED-PBA 通信を管理します。 Security Management Server Virtual のコンポーネント	すべて
Compatibility Server	TCP/ 1099 (閉鎖)	エンタープライズアーキテクチャを管理するためのサービスです。アクティベーション中の初期インベントリデータおよび移行時のポリシーデータを収集、保管します。このサービスのユーザーグループに基づいてデータを処理します。 Security Management Server Virtual のコンポーネント	すべて
Message Broker サービス	TCP/ 61616 および STOMP/ 61613 (閉鎖、または DMZ 用に設定済みの場合は 61613 が開放)	Security Management Server Virtual のサービス間の通信を処理します。ポリシープロキシのキュー操作のために Compatibility Server によって作成されるポリシー情報をステージします。 Security Management Server Virtual のコンポーネント	すべて
Identity Server	8445	SED Manager の認証を含むドメイン認証要求を処理します。 Active Directory アカウントが必要です。 Security Management Server Virtual のコンポーネント	すべて

名前	デフォルトポート	説明	必須とされる機能
Forensic Server	HTTPS/ 8448	適切な権限を持った管理者にデータのロック解除または復号化のタスクに使用される暗号化キーを Remote Management Console から取得することを可能にします。 Security Management Server Virtual のコンポーネント	フォレンジック API
Inventory Server	8887	インベントリキューを処理します。 Security Management Server Virtual のコンポーネント	すべて
Policy Proxy	TCP/ 8000/8090	セキュリティポリシーのアップデートとインベントリのアップデートを配信するためのネットワークベースの通信パスを提供します。 Security Management Server Virtual のコンポーネント	Encryption Enterprise for Mac Encryption Enterprise
LDAP	389/636、3268/3269 RPC - 135、49125+	**ポート 389** - このポートはローカルドメインコントローラからの情報の要求に使用されます。ポート 389 に送信される LDAP 要求は、グローバルカタログのホームドメイン内にあるオブジェクトの検索にのみ使用できます。ただし、要求側のアプリケーションは、これらのオブジェクトに対するすべての属性を取得できます。たとえば、ポート 389 への要求は、ユーザーの部門を取得するために使用することができます。 **ポート 3268** - このポートは、特にグローバルカタログをターゲットとするクエリ用に使用されます。ポート 3268 に送信される LDAP 要求は、フォレスト全体でのオブジェクトの検索に使用することができます。ただし、返されるのはグローバルカタログへのリプリケーション用にマークされた属性のみです。たとえば、ポート 3268 を使用してユーザーの部門は返すことはできません。これは、この属性がグローバルカタログに複製されないためです。	すべて
クライアント認証	HTTPS/ 8449	クライアントサーバが Security Management Server Virtual に対して認証することを許可します。	サーバー暗号化
コールバックビーコン	HTTP/TCP 8446	Data Guardian の保護付き Office モードを実行するときに、コールバックビーコンが保護付きの各 Office ファイルに挿入されることを許可します。	オプション。Data Guardian で使用
Advanced Threat Prevention を使用するクライアント通信	HTTPS/TCP/443	Advanced Threat Prevention を使用する場合のクライアント通信	Advanced Threat Prevention

6

お客様通知電子メールの例

Dell Data Security のご購入後、DellDataSecurity@Dell.com からの電子メールを受け取ります。以下は、お客様の CFT 資格情報とライセンスキー情報が記載された Dell Encryption 電子メールの例です。



Dell Data Security Encryption

Dear [redacted]

Thank you for purchasing Dell Encryption to quickly and easily protect your critical business data.

The following is the information you need to download your software and installation instructions for Dell Order #

Download Server:	https://ddpe.credant.com
Username:	[redacted]
Password:	I1oFqJQe
Required to change password:	No
Account Expiration Date:	Never
License Key:	[redacted]

Support

Your **Dell Encryption Solution** is entitled to Dell service and maintenance. For extending your service, contact your Dell sales representative or ask your support representative about an upgrade. For **Dell Encryption Solution** support, call **1-877-459-7304.**

This email was generated at: 14 Feb 12 07:31:26