はじめに

Dell Data Security 実装サービス

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 Encryption、Endpoint Security Suite Enterprise、および Data Guardian のスイートのドキュメントに使用されている登録商標および商標（Dell™、Dell のロゴ、Dell Precision™、OptiPlex™、ControlVault™、Latitude™、XPS®、および KACE™）は、Dell Inc. の商標です。Cylance®、CylancePROTECT、および Cylance のロゴは、米国およびその他の国における Cylance, Inc. の登録商標です。McAfee® および McAfee のロゴは、米国およびその他の国における McAfee, Inc. の商標または登録商標です。Intel ®、Pentium ®、Intel Core Inside Duo®、Itanium®、および Xeon ® は米国およびその他の国における Intel Corporation の登録商標です。Adobe®、Acrobat®、および Flash® は、Adobe Systems Incorporated の登録商標です。Authen Tec® および Eikon® は、Authen Tec の登録商標です。AMD® は、Advanced Micro Devices, Inc. の登録商標です。Microsoft®、Windows®、および Windows Server®、Internet Explorer®、Windows Vista®、Windows 7®、Windows 10®、Azure®、Active Directory®、Access®、BitLocker®、BitLocker To Go®、Excel®、Hyper-V®、Outlook®、PowerPoint®、Word®、OneDrive®、SQL Server®、および Visual C++® は、米国および / またはその他の国における Microsoft Corporation の商標または登録商標です。VMware® は、米国およびその他の国における VMware, Inc. の登録商標または商標です。Box® は、Box の登録商標です。Dropbox ℠ は、Dropbox, Inc のサービスマークです。Google™、Android™、Google™ Chrome™、Gmail™、および Google™ Play は、米国およびその他の国における Google Inc. の商標または登録商標です。Apple®、App Store℠、Apple Remote Desktop™、Boot Camp™、FileVault™、iPad®、iPhone®、iPod®、iPod touch®、iPod shuffle®、および iPod nano®、Macintosh®、および Safari® は、米国およびその他の国における Google Inc. のサービスマーク、商標、または登録商標です。EnCase™ および Guidance Software® は、Guidance Software の商標または登録商標です。Entrust® は、米国およびその他の国における Entrust®, Inc. の登録商標です。Mozilla® Firefox® は、米国およびその他の国における Mozilla Foundation の登録商標です。iOS® は同社の商標または米国およびその他の特定の国で Cisco Systems, Inc. の登録商標であり、ライセンスに使用されます。Oracle® および Java® は、Oracle および / またはその関連会社の登録商標です。Travelstar® は、米国およびその他の国における HGST, Inc. の登録商標です。UNIX® は、The Open Group の登録商標です。VALIDITY™ は、米国およびその他の国における Validity Sensors, Inc. の商標です。VeriSign® およびその他の関連標章は、米国およびその他の国における VeriSign, Inc. またはその関連会社あるいは子会社の商標または登録商標であり、Symantec Corporation にライセンス供与されています。KVM on IP® は、Video Products の登録商標です。Yahoo!® は、Yahoo! Inc. の登録商標です Bing® は、Microsoft Inc. の登録商標です。Ask® は、IAC Publishing, LLC の登録商標です。その他の名称は、それぞれの所有者の商標である場合があります。

はじめに

2019 - 06

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
    - 物理環境または仮想化環境で実行されている Windows ベースのアプリケーションです。
  - ***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

    デルサーバのインストール / 移行手順については、『*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。
- 初期ポリシーの設定
  - ***Security Management Server*** - support.dell.com にある『*Security Management Server* インストールおよび移行ガイド』の「管理タスク」の項、および管理コンソールから利用できる *AdminHelp* を参照してください。
  - ***Security Management Server Virtual*** - support.dell.com にある『*Security Management Server Virtual* クイックスタートおよびインストールガイド』の「管理コンソール管理タスク」の項、および管理コンソールから利用できる *AdminHelp* を参照してください。
- クライアントパッケージ
  クライアントの要件やソフトウェアのインストールドキュメントについては、導入に応じて適切な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。
- 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 ユーザーにはローカル管理者権限はありますか?
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、FDE、BitLocker Manager（BLM）、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、FDE、BitLocker Manager（BLM）、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オペレーティングシステム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

クライアントドキュメント

インストール要件、サポート対象のオペレーティングシステムバージョン、サポート対象の自己暗号化ドライブ、導入予定クライアントの手順については、以下の該当ドキュメントを参照してください。

Encryption Enterprise（Windows） - 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* 詳細インストールガイド - インストールガイド（カスタムインストールのためのスイッチおよびパラメーターの詳細情報）
- *Dell Data Security* コンソールのユーザーガイド - ユーザー向けの指示

Encryption Enterprise（Mac） - www.dell.com/support/home/us/en/04/product-support/product/dell-data-protection-encryption/manuals にある『*Encryption Enterprise for Mac* 管理者ガイド』を参照してください。インストールおよび導入手順も記述されています。

Endpoint Security Suite Enterprise（Windows） - 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* 詳細インストールガイド - インストールガイド（カスタムインストールのためのスイッチおよびパラメーターの詳細情報）
- *Endpoint Security Suite Enterprise Advanced Threat Prevention* クイック スタート ガイド - 管理の手順 ポリシーの推奨事項、脅威の識別と管理、トラブルシューティングなど）。
- *Dell Data Security Console* ユーザーガイド - ユーザー向けの指示

Endpoint Security Suite Enterprise（Mac） - 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* 管理者ガイド - 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* 管理者ガイド - インストール、アクティブ化および操作手順。
- *Dell Data Guardian* ユーザーガイド - ユーザーのためのインストール、アクティブ化、操作手順

サポート対象の自己暗号化ドライブについては、https://www.dell.com/support/article/us/en/04/sln296720 を参照してください。

サーバドキュメント

インストール要件、サポート対象オペレーティングシステムバージョン、導入デルサーバの構成については、以下の該当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* 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/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* 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/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 のインストール開始前に、導入 Dell Server に応じ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。

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

Security Management Server 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 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（同じサーバを使用している場合）。アンインストールの詳細については、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 を参照してください。
- ☐ 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。導入予定クライアントでの手順については、「クライアントドキュメント」を参照してください。

メモ:
すべての新規の実装は、新規データベースへの、Encryption、Endpoint Security Suite Enterprise、または Data Guardian ソフトウェアの初期インストールから始める必要があります。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。POC の実行中に暗号化されたエンドポイントはいずれも、デルによるインストール作業開始前に復号化または再構築する必要があります。

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 2012 R2（Standard または Datacenter）、2016（Standard または Datacenter）、Windows Server 2019（Standard または Datacenter）がインストールされている。これらのオペレーティングシステムは物理または仮想ハードウェアにインストールできます。
- ☐ 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 の実稼動導入環境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 8000、8050、8081、8084、8888、61613 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 2012 R2 にインストールする前に UAC を無効にしておく。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 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。

  メモ: インストールディレクトリが保護対象ディレクトリとして指定されていない限り、UAC が強制的に無効にされることはなくなりました。

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。

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/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

  http://www.dell.com/support の製品ページから、次の手順を実行します。

  1 **ドライバおよびダウンロード** を選択します。
  2 オペレーティングシステムのリストから、ダウンロードする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。
  3 該当するソフトウェアで、**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」でご購入いただいた場合は、Dell Digital Deliver を使用してターゲットコンピュータにソフトウェアを配信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 の **SoftwareDownloads** フォルダにあります。

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、FTP 資格情報が記載された元の電子メールにあります。「お客様通知電子メールの例」を参照してください。このキーは、http://www.dell.com/support および https://ddpe.credant.com.からアプリケーションをダウンロードしたときにも含まれています。
- ライセンスファイルは、FTP サイトの **Client Licenses** 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 Data Guardian、Encryption、Enterprise 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 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 : dds.<domain.com>
  - フロントエンドサーバ : dds-fe.<domain.com>

メモ:
Split-DNS では、内部と外部で同じ DNS 名のユーザーが許可されます。つまり、内部では dds.<domain.com> を内部の c-name として指定して Dell Security Management Server (バックエンド) につなげ、外部では dds.<domain.com> の A レコードを指定して該当のポート (Security Management Server のポートに関する項を参照) をフロントエンドサーバに転送することができます。DNS ラウンドロビンまたはロードバランサーを利用して、負荷を各種フロントエンド (複数存在する場合) に分散できます。

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。公的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) は、デルサーバのインストールに使用されているすべてのサーバ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、実稼働コンピュータをテストに使用することを**お勧めしません**。実稼働コンピュータは、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 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（同じサーバを使用している場合）。アンインストールの詳細については、次を参照してください： 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

- ☐ 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。導入予定クライアントでの手順については、「クライアントドキュメント」を参照してください。

メモ:
すべての新規の実装は、新規データベースへの、Encryption、Endpoint Security Suite Enterprise、または Data Guardian ソフトウェアの初期インストールから始める必要があります。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。POC の実行中に暗号化されたエンドポイントはいずれも、デルによるインストール作業開始前に復号化または再構築する必要があります。

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 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/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

  http://www.dell.com/support の製品ページから、次の手順を実行します。

  1. **ドライバおよびダウンロード** を選択します。
  2. オペレーティングシステムのリストから、ダウンロードする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。
  3. 該当するソフトウェアで、**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」でご購入いただいた場合は、Dell Digital Deliver を使用してターゲットコンピュータにソフトウェアを配信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、ddpe.credant.com サイトの **Client Licenses** 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。

Security Management Server Virtual 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 : dds.<domain.com>
  - フロントエンドサーバ : dds-fe.<domain.com>

メモ:
Split-DNS では、内部と外部で同じ DNS 名のユーザーが許可されます。つまり、内部では dds.<domain.com> を内部の c-name として指定して Dell Security Management Server (バックエンド) につなげ、外部では dds.<domain.com> の A レコードを指定して該当のポート (Security Management Server Virtual のポートに関する項を参照) をフロントエンドサーバに転送することができます。DNS ラウンドロビンまたはロードバランサーを利用して、負荷を各種フロントエンド (複数存在する場合) に分散できます。

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。

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、実稼働コンピュータをテストに使用することを**お勧めしません**。実稼働コンピュータは、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 2012 R2 (Standard または Datacenter)、Windows Server 2016 (Standard または Datacenter)、Windows Server 2019 (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。
- ☐ 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 8000、8050、8081、8084、8443、8888、61613 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 2012 R2 にインストールする前に UAC を無効にしておく。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 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。このキーは、http://www.dell.com/support および https://ddpe.credant.com.からアプリケーションをダウンロードしたときにも含まれています。
- ☐ ライセンスファイルは、CFT サイトの **Client Licenses** 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。

新規および既存の 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 の **SoftwareDownloads** フォルダにあります。
- ☐ Data Guardian、Encryption Enterprise、Endpoint Security Suite Enterprise を「on-the-box」でご購入いただいた場合は、ソフトウェアの Dell Digital Delivery での出荷も可能です。www.dell.com/support または ddpe.credant.com からダウンロードすることもできます。

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、環境内にあるすべてのエンドポイントへの適用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。インストール数がライセンス数を上回っている場合は、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 が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。

DNS レコードは文書化されていますか?

- ☐ ハードウェアが変更されている場合、アップデート用に DNS レコードが文書化され、ステージングされているかを検証します。

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。公的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、実稼働コンピュータをテストに使用することを**お勧めしません**。実稼働コンピュータは、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。

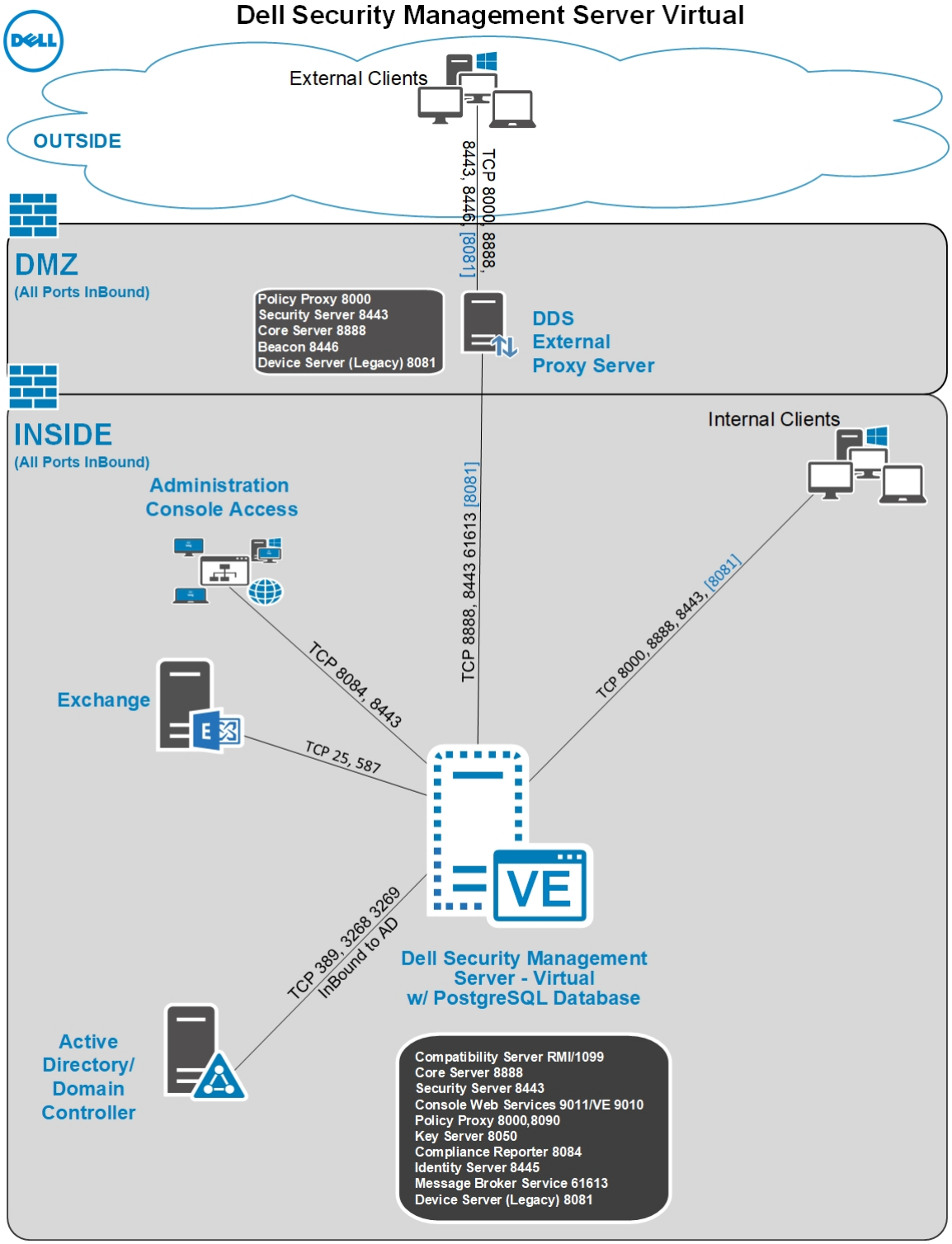
- Security Management Server のアーキテクチャの設計
- Security Management Server Virtual のアーキテクチャの設計

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

Dell Encryption、Endpoint Security Suite Enterprise、および Data Guardian の各ソリューションは非常に拡張性の高い製品で、組織内の暗号化を目的としたエンドポイントの数に基づいて拡張可能です。

アーキテクチャコンポーネント

以下は、Dell Security Management Server Virtual の基本的な導入です。



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
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。
管理コンソール	HTTPS/ 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。
Core Server	HTTPS/ 8887（クローズ）	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。
Core Server HA (高可用性)	HTTPS/ 8888	管理コンソール、Preboot Authentication、SED Management、FDE、BitLocker Manager、Threat Protection、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 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。
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。ユーザーグループに基づいてデータを処理します。
Message Broker サービス	TCP/ 61616（クローズ） 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）	デルサーバ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。
Identity Server	8445（クローズ）	SED Management の認証などのドメイン認証要求を処理します。
Forensic Server	HTTPS/ 8448	適切な権限を持った管理者が、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管理コンソールから取得できるようにします。 Forensic API に必要です。
Inventory Server	8887	インベントリキューを処理します。
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。 Encryption Enterprise（Windows および Mac）に必要です。
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

名前	デフォルトポート	説明
		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。
クライアント認証	HTTPS/ 8449	クライアントサーバがデルサーバを認証できるようにします。 Server Encryption に必要です。
コールバックビーコン	HTTP/TCP 8446	フロントエンドサーバで、Data Guardian の保護 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された各 Office ファイルに挿入されることを許可します。

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

Dell Encryption、Endpoint Security Suite Enterprise、および Data Guardian の各ソリューションは非常に拡張性の高い製品で、組織内の暗号化を目的としたエンドポイントの数に基づいて拡張可能です。

アーキテクチャコンポーネント

以下に、ほとんどの環境に適した推奨ハードウェア構成を示します。

Security Management Server

- オペレーティング システム：Windows Server 2012 R2（Standard、Datacenter 64 ビット）、Windows Server 2016（Standard、Datacenter 64 ビット）、Windows Server 2019（Standard、Datacenter）
- 仮想 / 物理マシン
- CPU：4 コア
- RAM：16.00 GB
- ドライブ C：ログおよびアプリケーションデータベース用に空きディスク容量 30 GB

メモ: PostgreSQL 内に保存されているローカルイベントデータベースで最大 10 GB を消費することがあります。

プロキシサーバー

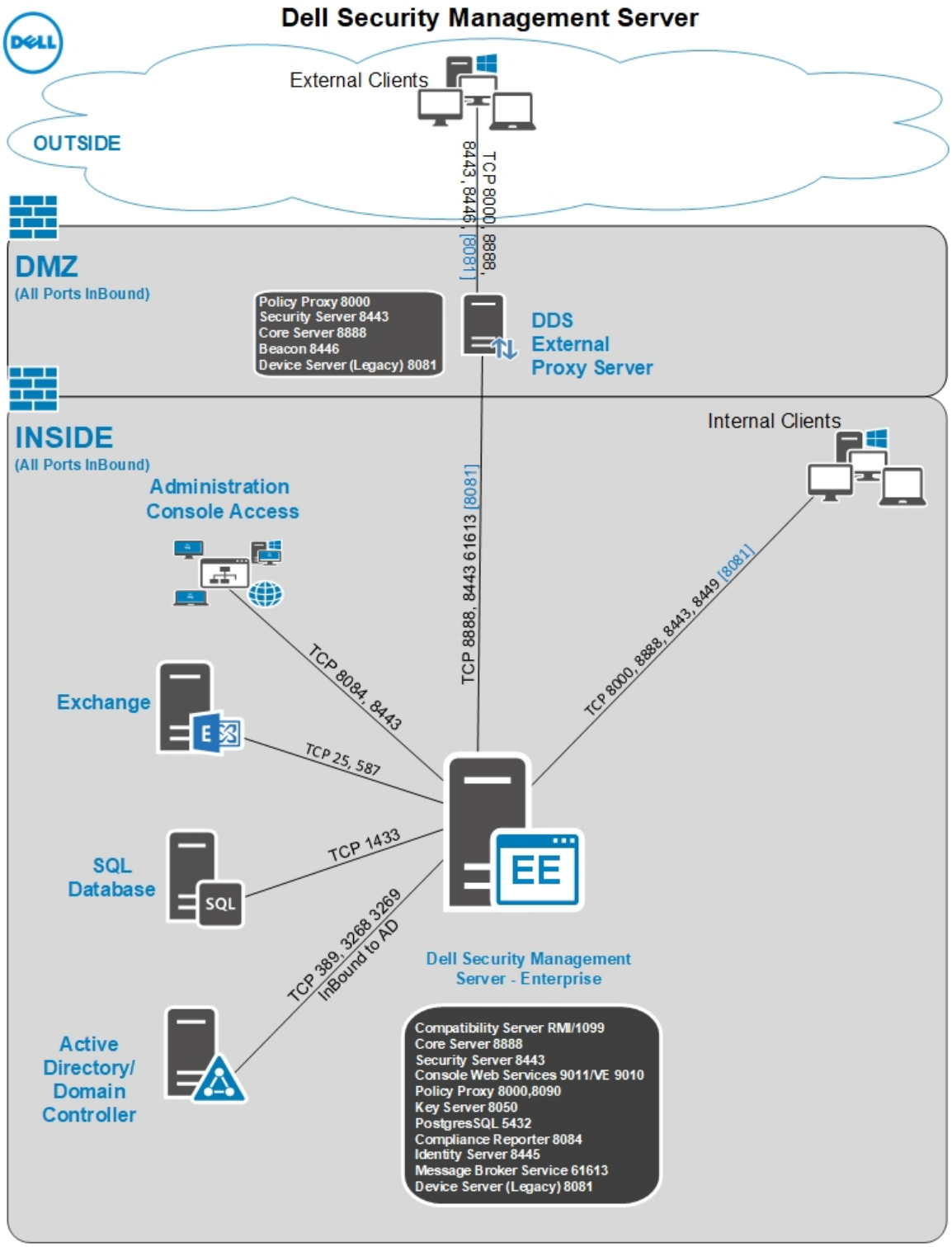
- オペレーティング システム：Windows Server 2012 R2（Standard、Datacenter 64 ビット）、Windows Server 2016（Standard、Datacenter 64 ビット）、Windows Server 2019（Standard、Datacenter）
- 仮想 / 物理マシン
- CPU：2 コア
- RAM：8.00 GB
- ドライブ C：ログ用に空きディスク容量 20 GB

SQL Server のハードウェア仕様

- CPU：4 コア
- RAM：24.00 GB
- データドライブ：空きディスク容量 100 ~ 150 GB（環境によって異なる）
- ログドライブ：空きディスク容量 50 GB（環境によって異なる）

ⓘ | **メモ: ほとんどの環境で上記の情報が有効です。そうでない場合は、「SQL Server ベストプラクティス」を参照してください。**

以下は、Dell Security Management Server の基本的な導入です。



ⓘ | **メモ: 組織に 20,000 を超えるエンドポイントがある場合は、Dell ProSupport に問い合わせてサポートを受けてください。**

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
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。
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。
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。
Device Server	HTTPS/ 8081	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（ Windows および Mac ）に必要です。
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、SED-PBA 通信、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。
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。ユーザーグループに基づいてデータを処理します。
Message Broker サービス	TCP/ 61616 および STOMP/ 61613	デルサーバ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。 SQL データベースアクセスが必要です。
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。
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。
LDAP	TCP/	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

名前	デフォルトポート	説明
	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)	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。
Microsoft SQL データベース	TCP/ 1433	デフォルトの SQL Server 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。
クライアント認証	HTTPS/ 8449	クライアントサーバがデルサーバを認証できるようにします。Server Encryption に必要です。
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。

6

SQL Server ベストプラクティス

以下に、SQL Server のベストプラクティスを説明するリストを示します。ベストプラクティスをまだ実装していない場合は、Dell Security のインストール時に実装するようにしてください。

1 データファイルおよびログファイルが格納される NTFS ブロックサイズが 64 KB になっていることを確認します。SQL Server エクステント（SQL ストレージの基本単位）は 64 KB です。

詳細については、Microsoft の TechNet 記事、「Understanding Pages and Extents」（ページとエクステントについて）を検索してください。

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

2 一般的なガイドラインとして、SQL Server の最大メモリ数は、インストールされているメモリの 80 パーセントに設定します。

詳細については、Microsoft の TechNet 記事「*Server Memory Server Configuration Options*」（サーバメモリに関するサーバ設定オプション）を検索してください。

- 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 インスタンスのスタートアッププロパティで -t1222 を設定して、デッドロックが発生した場合にその情報を取得できるようにします。

詳細については、Microsoft の TechNet 記事、「Trace Flags (Transact-SQL)」（トレースフラグ（Transact-SQL））を検索してください。

- 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 すべてのインデックスが、インデックスを再構築するための週次メンテナンスジョブの対象になっていることを確認します。

7

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電子メールの例です。

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