Dell Data Protection

『Enterprise Server インストールおよびマイグレーションガイド v9.7』

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。

『Enterprise Server インストールおよびマイグレーションガイド 』

2017 - 04

Rev. A01

目次

1

Dell Enterprise Server はじめに

Dell Enterprise Server について

Enterprise Server は Dell ソリューションのセキュリティ管理部分です。管理者は、リモート管理コンソールを使用して、企業全体のエンドポイント、ポリシーの適用、および保護の状態を監視できます。

Enterprise Server には次の機能があります。

- デバイスの一元管理
- 役割ベースのセキュリティポリシーの作成と管理
- 管理者がサポートするデバイス復元
- 管理者職務の分割
- セキュリティポリシーの自動分配
- コンポーネント間での通信のための信頼済みパス
- 固有暗号化キーの生成および自動かつセキュアなキーエスクロー
- 一元的なコンプライアンス監査とレポート

Dell ProSupport へのお問い合わせ

Dell Data Protection 製品向けの 24 時間 365 日対応電話サポート（877-459-7304、内線 431003）に電話をかけてください。

さらに、dell.com/support で Dell Data Protection 製品のオンラインサポートもご利用いただけます。オンラインサポートでは、ドライバ、マニュアル、テクニカルアドバイザリー、よくあるご質問（FAQ）、および緊急の問題を取り扱っています。

適切なサポート担当者に迅速におつなぎするためにも、お電話の際はお客様のサービスコードをご用意ください。

米国外の電話番号については、Dell ProSupport の国際電話番号をチェックしてください。

2

Dell Enterprise Server の要件とアーキテクチャ

この項では、Dell Data Protection 実装の際の、ハードウェアとソフトウェアの要件および、アーキテクチャデザインの推奨に関する詳細を説明しています。

Dell Enterprise Server の要件

Dell Enterprise Server のコンポーネントには、Dell インストールメディアで提供されているソフトウェアの他に、ハードウェアとソフトウェアの要件があります。インストール作業またはアップグレード / 移行作業を続行する前に、インストール環境が要件を満たしていることを確認してください。

インストールを開始する前に、すべてのパッチとアップデートがインストールに使用されるサーバーに適用されていることを確認します。

Dell Enterprise Server の必要条件

次の表では、Dell Enterprise Server をインストールする前に配置しておく必要があるソフトウェアについて詳しく説明します。これらの必要条件をインストールするリンクおよび手順については、「インストール前の設定」で詳しく説明しています。

適用される各ソフトウェア項目は、インストーラがその項目をインストールすると明記されていない限り、インストールを開始する前にインストールする必要があります。インストールしない場合、インストールは失敗します。

Dell Enterprise Server のハードウェア

前提条件

- **Visual C++ 2010 再頒布可能パッケージ**

  インストールされていない場合、インストーラが自動でインストールします。
- **Visual C++ 2013 再頒布可能パッケージ**

  インストールされていない場合、インストーラが自動でインストールします。
- **Visual C++ 2015 再頒布可能パッケージ**

  インストールされていない場合、インストーラが自動でインストールします。
- **.NET Framework バージョン 3.5 SP1**
- **.NET Framework バージョン 4.5**

  Microsoft は、.NET Framework バージョン 4.5 のセキュリティアップデートを公開しました。
- **SQL Native Client 2012**

  SQL Server 2012 または SQL Server 2016 を使用している場合。

  インストールされていない場合、インストーラが自動でインストールします。

次の表では、Dell Enterprise Server の 最小 ハードウェア要件について詳しく説明します。導入のサイズに応じた拡張に関する詳細は、「Dell Enterprise Server アーキテクチャデザイン」を参照してください。

ハードウェア要件

プロセッサ

Core Duo、Core 2 Duo、Core i3、Core i5、Core i7、Xeon、Itanium、または AMD と同等のプロセッサを含む、少なくともデュアルコアの現行 CPU（2 GHz+）

単一サーバー構成は現行のクアッドコア CPU（2 GHz+）

RAM

最小 8 GB（構成に基づく）

単一サーバー構成は 16GB

空きディスク容量

+-1.5 GB の空きディスク容量（その他仮想ページング領域が必要）

単一サーバー構成は 20GB 以上の空きディスク容量（その他仮想ページング容量が必要）

ネットワークカード

10/100/1000 ネットワークインタフェースカード

その他

TCP/IPv4 がインストール済み、かつ有効化済み

Dell Enterprise Server のソフトウェア

次の表では、Dell Enterprise Server とプロキシサーバーのソフトウェア要件の詳細を説明しています。

メモ: UAC はインストール前に無効にする必要があります。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 Server 2012 R2 および Windows Server 2016 では、インストーラは UAC を無効にします。

メモ: Dell Policy Proxy（インストールされている場合）のレジストリの場所：HKLM\SOFTWARE\Wow6432Node\Dell

メモ: Windows Server のレジストリの場所：HKLM\SOFTWARE\Dell

Dell Enterprise Server - バックエンドサーバーおよび Dell フロントエンドサーバー

- **Windows Server 2008 R2 SP0-SP1 64 ビット**

  - Standard Edition

  - Enterprise Edition
- **Windows Server 2008 SP2 64 ビット**

  - Standard Edition

  - Enterprise Edition
- **Windows Server 2012 R2**

  - Standard Edition

  - Datacenter Edition
- **Windows Server 2016**

- Standard Edition

- Datacenter Edition

Exchange ActiveSync サーバー

Mobile Edition を使用する場合は、次の Exchange ActiveSync サーバがサポートされます。このコンポーネントは、フロントエンド Exchange サーバーにインストールされます。

- Exchange ActiveSync 12.0 – Exchange Server 2007 のコンポーネント
- Exchange ActiveSync 12.1 – Exchange Server 2007 SP1 のコンポーネント
- Exchange ActiveSync 14.0 – Exchange Server 2010 のコンポーネント
- Exchange ActiveSync 14.1 – Exchange Server 2010 SP1 のコンポーネント

Microsoft メッセージキュー（ MSMQ ）を Exchange Server にインストールおよび設定する必要があります。

LDAP リポジトリ

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

Dell Enterprise Server コンポーネントの推奨仮想環境

Dell Enterprise 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。

Dell Enterprise Server v9.7 は、Hyper-V Server（ フルまたはコアインストール ）で、および 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。

Dell Enterprise Server v9.7 は、VMware ESXi 5.5 および VMware ESXi 6.0 で動作が確認済みです。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。

メモ: Dell Enterprise 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。

データベース

- **SQL Server 2008 および SQL Server 2008 R2 -** Standard Edition / Enterprise Edition
- **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

メモ: Express Edition は、実稼働環境ではサポートされません。Express Edition は、POC および評価でのみ使用できます。

Dell Data Protection リモート管理コンソールおよび Compliance Reporter

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

メモ: お使いのブラウザで cookie を受け入れる必要があります。

Dell Enterprise Server の言語サポート

リモート管理コンソールは、複数言語ユーザーフェース（MUI）に対応しており、次の言語をサポートします。

言語サポート	
EN - 英語	JA - 日本語
ES - スペイン語	KO - 韓国語
FR - フランス語	PT-BR - ポルトガル語（ブラジル）
IT - イタリア語	PT-PT - ポルトガル語（ポルトガル（イベリア））
DE - ドイツ語	

Dell Enterprise Server アーキテクチャデザイン

Dell Encryption、Endpoint Security Suite、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 ~ 60,000 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。すべての Dell Enterprise Server のコンポーネントは、単一のサーバーにインストールすることができます。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

Dell Enterprise 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

単一サーバーの構成

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（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）

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

Dell Enterprise Server

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）

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 ~ 40,000 エンドポイント

このアーキテクチャは、20,000 から 40,000 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

Dell Enterprise 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 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）

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

40,000 ~ 60,000 エンドポイント

このアーキテクチャは、40,000 から 60,000 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。

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

Dell Enterprise 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 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）

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 Dell Enterprise Server があります。2 台目の Dell Enterprise 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 Enterprise 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

Dell Enterprise 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。

Dell Enterprise Server v9.7 は、Hyper-V Server (フルまたはコアインストール) で、および 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。

Dell Enterprise Server v9.7 は、VMware ESXi 5.5 および VMware ESXi 6.0 で動作が確認済みです。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。

メモ: Dell Enterprise 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。

3

インストール前の設定

作業を開始する前に、Dell Enterprise Server に関連する最新の回避策または既知の問題について『Enterprise Server Technical Advisories』（Enterprise Server テクニカルアドバイザリー）をお読みください。

Dell Enterprise Server をインストールするサーバーのインストール前の設定は非常に重要です。Dell Enterprise Server を円滑にインストールするためにこの項を特に注意してお読みください。

設定

1 有効な場合は、Internet Explorer セキュリティ強化の構成（ESC）を無効にします。ブラウザのセキュリティオプションで、サーバー URL を信頼済みサイトに追加します。サーバーを再起動します。

2 各コンポーネントの次のポートを開きます。

内部：

Active Directory 通信：TCP/389

電子メール通信（オプション）：25

対フロントエンド（必要な場合）：

外部 Dell Policy Proxy から Dell Message Broker への通信：TCP/61616 および STOMP/61613

バックエンド Dell Security Server への通信：HTTPS/8443

バックエンド Dell Core Server への通信：HTTPS/8888 および 9000

RMI ポートへの通信 - 1099

バックエンド Dell Device Server への通信：HTTP(S)/8443 - お使いの Dell Enterprise Server が v7.7 以降の場合。お使いの Dell Enterprise Server が v7.7 より前の場合は、HTTP（S）/8081 です。

ビーコンサーバ：HTTP/8446（Data Guardian を使用している場合）

外部（必要な場合）：

SQL データベース：TCP/1433

リモート管理コンソール：HTTPS/8443

LDAP：TCP/389/636（ローカルドメインコントローラ）、TCP/3268/3269（グローバルカタログ）、TCP/135/49125+（RPC）

Dell Compatibility Server：TCP/1099

Dell Compliance Reporter：HTTP（S）/8084（インストール時に自動的に設定）

Dell Identity Server：HTTPS/8445

Dell Core Server：HTTPS/8888 および 9000（8888 はインストール時に自動的に設定）

Dell Device Server：HTTP（S）/8443（Dell Enterprise Server v7.7 以降）または HTTP（S）/8081（v7.7 より前の Dell Enterprise Server）

Dell Key Server：TCP/8050

Dell Policy Proxy：TCP/8000

Dell Security Server：HTTPS/8443

クライアントの認証：HTTPS/8449（サーバ暗号化を使用している場合）

Advanced Threat Prevention を使用している場合、クライアント通信：HTTPS/TCP/443

メモ:
Enterprise Edition クライアントライセンスが工場から付与される場合、または工場からライセンスを購入する場合は、資格を有効にするために、ドメインコントローラで GPO を設定します（これは Enterprise Edition を実行するサーバーではない場合があります）。サーバーとの通信に送信ポート 443 が使用可能であることを確認します。ポート 443 が何らかの理由でブロックされている場合、資格機能は機能しません。詳細については、『Enterprise Edition Advanced Installation Guide』（Enterprise Edition アドバンスインストールガイド）を参照してください。

Dell データベースの作成

3 Dell Enterprise Server に対して SQL データベースが設定されていない場合、インストール中にインストーラによってデータベースが作成されます。Dell Enterprise Server をインストールする前にデータベースをセットアップする場合は、以下の指示に従って SQL Management Studio で SQL データベースおよび SQL ユーザーを作成してください。**まだデータベースが存在しない場合はインストーラがデータベースを作成するため、これらの手順はオプションです。**

Dell Enterprise Server をインストールする際は、「既存データベースでのバックエンドサーバーのインストール」の手順に従ってください。

Dell Enterprise Server は、SQL および Windows 認証の両方に対応しています。デフォルトの認証方法は SQL 認証です。

データベースを作成してから、db_owner 権限を持つ Dell データベースユーザーを作成します。db_owner では、許可の割り当て、データベースのバックアップと復元、オブジェクトの作成と削除、ユーザーアカウントと役割の制限なしでの管理が可能です。また、このユーザーがストアドプロシージャを実行する許可 / 権限を持っていることを確認します。

デフォルト以外の SQL Server インスタンスを使用するときは、Dell Enterprise Server をインストールした後、サーバー設定ツールの データベース タブで、そのインスタンスの動的ポートを指定する必要があります。詳細については、「サーバー設定ツール」を参照してください。その代替として、SQL Server Browser サービスを有効化して、UDP ポート 1434 が開放されていることを確認します。詳細については https://msdn.microsoft.com/en-us/library/hh510203(v=sql.120).aspx を参照してください。

SQL データベース、または SQL インスタンスのどちらかが非デフォルトの照合順序で設定されている場合は、非デフォルトの照合順序が大文字と小文字を区別するものである必要があります。照合順序のリストと、大文字と小文字の区別については、https://msdn.microsoft.com/en-us/library/ms144250(v=sql.105).aspx を参照してください。

SQL データベースおよび SQL ユーザーを SQL Management Studio で作成するには、以下を 1 つ選びます。

Windows 認証を使用して新しい Windows SQL Server データベースを作成するには、次の手順を実行します。

a **スタート** > **すべてのプログラム** > **Microsoft SQL Server** > **Management Studio** をクリックします。

b データベース フォルダを右クリックし、新規データベース をクリックします。データベースのプロパティ ダイアログが表示されます。

c データベース名を入力し、**OK** をクリックします。

d セキュリティフォルダを展開し、**ログイン** を右クリックします。

e **新しいログイン** をクリックし、新規データベースの所有者を作成します。

f 名前 フィールドにユーザー名を入力します。

g 認証オプションの *Windows* 認証を選択します。

h **ユーザーマッピング** を選択し、新規データベースをハイライトします。

i データベースの役割（db_owner）を選択し、**OK** をクリックします。

または

SQL Server 認証を使用して新しい SQL Server データベースを作成するには、次の手順を実行します。

a **スタート** > **すべてのプログラム** > **Microsoft SQL Server** > **Management Studio** をクリックします。

b データベースフォルダを右クリックし、**新規データベース** をクリックします。データベースのプロパティダイアログが表示されます。

c データベース名を入力し、**OK** をクリックします。

d セキュリティフォルダを展開し、**ログイン** を右クリックします。

e **新しいログイン** をクリックし、新規データベースの所有者を作成します。

f 名前 フィールドにユーザー名を入力します。

g 認証オプションの *SQL Server* 認証を選択します。パスワードを入力し、確認します。

h **パスワードの期限を適用する** を選択解除します。

i **ユーザーマッピング** を選択し、新しいデータベースをハイライトします。

j データベースの役割（db_owner）を選択し、**OK** をクリックします。

Visual C++ 2010/2013/2015 再頒布可能パッケージのインストール

4 Visual C++ 2010、2013、および 2015 再頒布可能パッケージをインストールしていない場合はインストールします。必要な場合は、Dell Enterprise Server インストーラにこれらのコンポーネントのインストールを許可できます。

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

.NET Framework 4.5 のインストール

5 .NET Framework 4.5 をインストールしていない場合はインストールします。

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

SQL Native Client 2012 のインストール

6 *SQL Server 2012* または *SQL Server 2016* を使用している場合は、SQL Native Client 2012 をインストールします。必要な場合は、Dell Enterprise Server インストーラにこのコンポーネントのインストールを許可できます。

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

Microsoft CA（MSCEP）の設定

この手順は、iOS を Mobile Edition で使用する場合のみ、MSCEP を実行しているサーバ上で完了する必要があります。

7 MSCEP を設定します。

Windows Server 2008 R2 は、Enterprise Edition である必要があります。***Standard Edition* は、*MSCEP* にインストールする役割を許可しません**：

a Server Manager を開きます。左側のメニューで、**サーバーの役割** を選択し、**Active Directory 証明書サービス** のボックスをオンにします。**次へ** をクリックします。役割の追加ウィザードで、次の手順に進みます。

AD CS > 役割サービス で、**証明機関** と **証明機関 Web 登録** 役割サービスのボックスをオンにします。**Web サーバー IIS に必要な役割サービスの追加** を選択します（求められた場合）。**次へ** をクリックします。

AD CS > セットアップの種類で、**スタンドアロン** を選択します。**次へ** をクリックします。

AD CS > *CA* の種類で、**下位 CA** を選択します。**次へ** をクリックします。

AD CS > 秘密キーで、**新しい秘密キーを作成する** を選択します。**次へ** をクリックします。

AD CS > 秘密キー > 暗号化で、**RSA#Microsoft ソフトウェアキー記憶域プロバイダー**、**2048**、および **SHA1** のデフォルト値をそのままにします。**次へ** をクリックします。

AD CS > 秘密キー > *CA* の名前で、すべてのデフォルト値をそのままにします。**次へ** をクリックします。

AD CS > 秘密キー > 証明書の要求 で、**親 CA に証明書の要求を送信する** を選択します。**参照手段：CA 名** を選択します。**親 CA** を参照し、選択します。**次へ** をクリックします。

AD CS > 証明書データベースで、デフォルト値をそのままにします。**次へ** をクリックします。

Web Server（IIS） で、**次へ** をクリックします。

Web Server（IIS） > 役割サービスで、デフォルト値をそのままにします。**次へ** をクリックします。

確認で、**インストール** をクリックします。

結果で、結果を確認し、**閉じる** をクリックします。

サーバマネージャ > 役割 で、*Active Directory* 証明書サービスの **役割サービスの追加** を選択します。

役割サービスの選択ウィンドウが表示されたら、**ネットワークデバイス登録サービス** のボックスをオンにします。**次へ** をクリックします。

ローカルサーバーの IIS_IUSRS のユーザーグループに対する証明書要求を承認するときにネットワークデバイス登録サービスを使用する必要があるユーザーアカウントを追加します。この形式はドメイン\ユーザー名です。**OK** をクリックします。

ユーザーアカウントの指定 ウィンドウで、IIS_IUSRS グループに追加されたユーザーを選択します。**次へ** をクリックします。

登録機関情報の指定ウィンドウで、必要な情報 と オプション情報の追加のデフォルト値をそのままにします。**次へ** をクリックします。

登録機関の暗号化の設定ウィンドウで、デフォルト値をそのままにします。**次へ** をクリックします。

インストールオプションの確認 ウィンドウで、**インストール** をクリックします。

インストールの結果ウィンドウで、結果を確認し、**閉じる** をクリックします。

Server Manager を閉じます。

b レジストリキーを次のように変更します。

HKLM\SOFTWARE\Microsoft\Cryptography\MSCEP\EnforcePassword

"EnforcePassword"=dword:00000000

c IIS マネージャを開きます。**\<ServerName> \Sites\Default Web Site\CertSrv\mscep_admin** にアクセスします。

認証 を開き、**匿名認証** を有効にします。

d **スタート** > **ファイル名を指定して実行** をクリックします。*certsrv.msc* と入力し、**Enter** をクリックします。

certsrv ウィンドウが表示されたら、サーバー名を右クリックし、**プロパティ** を選択して、**ポリシーモジュール**タブをクリックします。

プロパティ をクリックし、**証明書テンプレートに操作が設定されている場合はそれに従い、設定されていない場合は自動的に証明書を発行する を選択します。OK** をクリックします。

e IIS Manager を閉じます。

f サーバーを再起動します。検証するために、Internet Explorer を開き、アドレスバーに次のように入力します

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

MSCEP Windows Server 2008 R2 のセットアップが完了しました。

Windows Server 2012 R2 または Windows Server 2016：

a 「Network Device Enrollment Service (NDES) in Active Directory Certificate Services (AD CS)」の記事に記載されているセットアップ手順に従ってください。

b レジストリキーを次のように変更します。

HKLM\SOFTWARE\Microsoft\Cryptography\MSCEP\EnforcePassword

"EnforcePassword"=dword:00000000

c IIS マネージャを開きます。**\<ServerName\Sites\Default Web Site\CertSrv\mscep_admin** にアクセスします。

認証 を開き、**匿名認証** を有効にします。

d **スタート** > **ファイル名を指定して実行** をクリックします。*certsrv.msc* と入力し、**Enter** をクリックします。

certsrv ウィンドウが表示されたら、サーバー名を右クリックし、**プロパティ** を選択して、**ポリシーモジュール**タブをクリックします。

プロパティ をクリックし、**証明書テンプレートに操作が設定されている場合はそれに従い、設定されていない場合は自動的に証明書を発行する を選択します。OK** をクリックします。

e IIS Manager を閉じます。

f サーバーを再起動します。検証するために、Internet Explorer を開き、アドレスバーに次のように入力します

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

MSCEP Windows Server 2012 R2/Windows Server 2016 のセットアップが完了しました。

Microsoft メッセージキュー（ MSMQ ）のインストール / 設定

この手順は、Mobile Edition を使用する場合のみ完了する必要があります。これは、EAS デバイスマネージャおよび EAS メールボックスマネージャ の通信を可能にする前提条件です。

8 Windows Server 2008 または Windows Server 2008 R2 にインストールします（ Exchange 環境をホストしているサーバー上 ）: http://msdn.microsoft.com/en-us/library/aa967729.aspx

または

Windows Server 2012 R2 にインストールします

a Server Manager を開きます。

b **管理** > **役割と機能の追加** の順に移動します。

c 作業を開始する前に の画面で **次へ** をクリックします。

d **役割ベースまたは機能ベースのインストール** を選択して、**次へ** をクリックします。

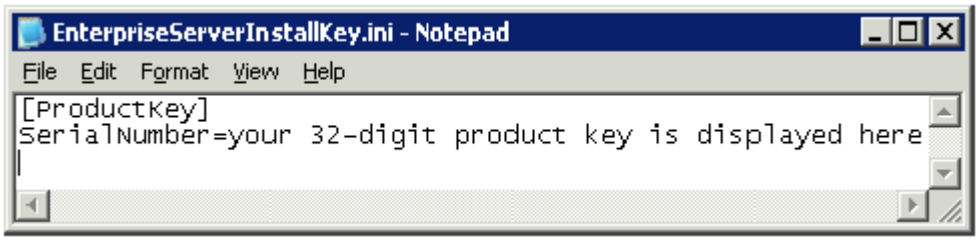
e 機能をインストールするサーバーを選択して、**次へ** をクリックします。

f サーバーの役割は選択しないでください。**次へ** をクリックします。

g 機能 で、**メッセージキュー** を選択して、**インストール** をクリックします。

オプション

9 **新規インストールの場合** - プロダクトキー（ ファイルの名前は *EnterpriseServerInstallKey.ini* ）を C:\Windows にコピーして、Dell Enterprise Server インストーラで 32 文字のプロダクトキーが自動的に入力されるようにします。



サーバーのインストール前の設定が完了しました。「インストールまたはアップグレード / 移行」に進みます。

4

インストールまたはアップグレード / 移行

本章では、次の操作に対する手順を説明します。

- 新規インストール - 新しい Dell Enterprise Server をインストールします。
- アップグレード / 移行 - 既存の Dell Enterprise Server v8.0 以降からアップグレードします。
- Dell Enterprise Server のアンインストール - 必要に応じて、現在のインストールを削除します。

  インストールに複数のメインサーバー（バックエンド）を含める必要がある場合は、デル ProSupport 担当者にお問い合わせください。

インストールまたはアップグレード / 移行を開始する前に

作業を開始する前に、該当する「インストール前の設定」の手順が完了していることを確認します。

Dell Enterprise Server のインストールに関連する最新の回避策または既知の問題については、『Enterprise Server Technical Advisories』（Enterprise Server テクニカルアドバイザリー）をお読みください。

ユーザー アカウント制御（UAC）が有効になっている場合は、無効にする必要があります。Windows Server 2012 R2 では、インストーラが UAC を無効化します。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。

インストール中にデータベースを設定するために Windows または SQL 認証資格情報が必要です。Windows 認証を選択した場合、ログインしているユーザーの資格情報が使用されます。ユーザーはシステム管理者権限と SQL データベースを作成および管理する（データベースの作成、ユーザーの追加、許可の割り当て）権限を有していなければなりません。SQL 認証の場合も、使用されるアカウントはこれらと同様の権限を有している必要があります。これら資格情報は、インストール中のみ使用されます。インストール後の製品は、これらの資格情報を使用することはありません。

また、インストール中に Dell サービスが SQL サーバーにアクセスするのに使用するサービスランタイム認証資格情報も指定する必要があります。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。

アクセス権限の有無またはデータベースへのアクセス可否について不明な場合は、インストールを開始する前に、データベース管理者に問い合わせて確認してください。

デルでは、データベースのベストプラクティスを Dell データベースに使用し、組織の災害復旧計画に Dell ソフトウェアを含めることを推奨します。

DMZ 内に Dell コンポーネントをデプロイする場合は、攻撃から適切に保護されていることを確認してください。

本番稼働の場合、デルでは、専用サーバーに SQL Server をインストールすることを強く推奨します。

フロントエンドサーバーをインストールして設定する前に、バックエンドサーバーをインストールすることがベストプラクティスです。

インストールログファイルは次のディレクトリにあります：C:\ProgramData\Dell\Dell Data Protection\Installer Logs

新規インストール

バックエンドサーバーインストールには、2 つのオプションのどちらかを選択します。

- バックエンドサーバーと新規データベースのインストール - 新規の Dell Enterprise Server と、新規データベースをインストールします。
- 既存データベースでのバックエンドサーバーのインストール - 新しい Dell Enterprise Server をインストールして、インストール前の設定 中に作成された SQL データベースまたは v9.x 以降の既存の SQL データベースに接続します（スキーマバージョンがインストールする Dell Enterprise Server のバ

ージョンに一致する場合)。v8.x 以降のデータベースは、最新バージョンのサーバー設定ツールで最新のスキーマに移行する必要があります。サーバー設定ツールを使用したデータベース移行の手順については、「データベースの移行」を参照してください。最新のサーバー設定ツールを入手、または v8.0 より前のデータベースに移行するには、デル ProSupport に問い合わせてサポートを受けてください。

メモ:

Dell Enterprise Server v8.x 以降を実行している場合、「**バックエンドサーバーのアップグレード / 移行**」の手順を参照してください。

フロントエンドサーバーをインストールする場合は、バックエンドサーバーのインストールを行ってからこのインストールを実行します。

- フロントエンドサーバーのインストール - バックエンドサーバーと通信するようにフロントエンドサーバーをインストールします。

バックエンドサーバーと新規データベースのインストール

1 Dell インストールメディアで、Dell Enterprise Server ディレクトリに移動します。Enterprise Server-x64 を、Enterprise Server をインストールするサーバのルートディレクトリに**解凍** (コピー / 貼り付けまたはドラッグ / ドロップではなく) します。**コピー / 貼り付けまたはドラッグ / ドロップを行うと、エラーが発生し、インストールが失敗します。**

2 **setup.exe** をダブルクリックします。

3 *InstallShield* ウィザードでインストールの言語を選択し、**OK** をクリックします。

4 前提条件対象のものがインストールされていない場合、それらをインストールするように伝えるメッセージが表示されます。**インストール** をクリックします。

5 ようこそ ダイアログで **次へ** をクリックします。

6 ライセンス契約を読み、その条件に同意して **次へ** をクリックします。

7 「インストール前の設定」において、オプションで 手順 9 を完了した場合は、**次へ** をクリックします。完了していない場合は、32 文字のプロダクトキーを入力し、**次へ** をクリックします。プロダクトキーはファイル「*EnterpriseServerInstallKey.ini*」にあります。

8 **バックエンドインストール** を選択し、**次へ** をクリックします。

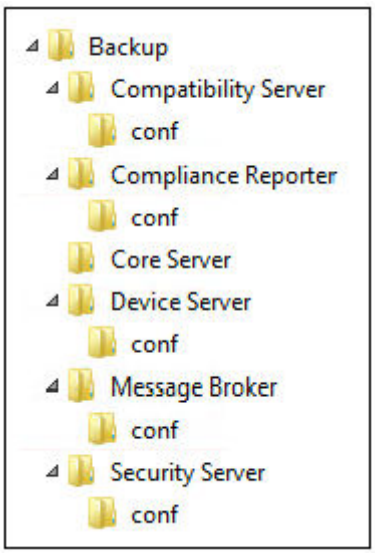
9 Dell Enterprise Server を、デフォルトの場所の C:\Program Files\Dell にインストールするには、**次へ** をクリックします。それ以外の場所にインストールする場合は、**変更** をクリックして異なる場所を選択し、**次へ** をクリックします。

10 バックアップ設定ファイルを保存する場所を選択するには、**変更** をクリックして希望のフォルダに移動してから **次へ** をクリックします。

デルでは、バックアップの場所にリモートネットワークの場所または外部のドライブを選択することを推奨します。

サーバー設定ツールで行われた変更を含む、インストール後に設定ファイルに対して行われた変更は、これらのフォルダに手動でバックアップする必要があります。設定ファイルは、サーバーを手動で復元するのに使用される全情報のうちの重要な要素です。

メモ: このインストール中にインストーラによって作成されたフォルダの構造 (例は下記参照) は変更しないでください。



11 使用するデジタル証明書のタイプを選択することができます。**デジタル証明書は信頼のおける証明書認証局からのものを使用することが強く推奨されます。**
以下のオプション「a」または「b」を選択します。

a CA 機関から購入された既存の証明書を使用するには、**既存証明書のインポート** を選択し、**次へ** をクリックします。
参照 をクリックして、証明書のパスを入力します。

この証明書に関連付けられているパスワードを入力します。キーストアファイルは .p12 または pfx である必要があります。手順については、「証明書管理コンソールを使用した証明書の .PFX へのエクスポート」を参照してください。

次へ をクリックします。

> **メモ:**
> この設定を使用するには、インポートされるエクスポート済み CA 証明書に完全な信頼チェーンがある必要があります。不明な場合は、CA 証明書を再エクスポートし、「証明書のエクスポートウィザード」で次のオプションが選択されていることを確認します。
>
> - Personal Information Exchange - PKCS#12 (.PFX)
> - 可能な場合は証明書パスにすべての証明書を含める
> - すべての拡張プロパティをエクスポートする

または

b 自己署名証明書を作成する場合は、**自己署名証明書を作成してキーストアにインポートする を選択して 次へ** をクリックします。
自己署名証明書の作成 ダイアログで、次の情報を入力します。

完全修飾コンピュータ名 (例 : computername.domain.com)

組織

組織単位 (例 : Security)

都市

州 (正式名)

国 : 国を表す 2 文字の略語

次へ をクリックします。

> **メモ:**
> 証明書は、デフォルトで 1 年で期限切れになります。

12 サーバー暗号化 (SE) では、使用するデジタル証明書のタイプを選択することができます。デジタル証明書は信頼のおける証明書認証局からのものを使用することが強く推奨されます。
以下のオプション「a」または「b」を選択します。

a CA 機関から購入された既存の証明書を使用するには、**既存証明書のインポート** を選択し、**次へ** をクリックします。
参照 をクリックして、証明書のパスを入力します。

この証明書に関連付けられているパスワードを入力します。キーストアファイルは .p12 または pfx である必要があります。手順については、「証明書管理コンソールを使用した証明書の .PFX へのエクスポート」を参照してください。

次へ をクリックします。

メモ:
この設定を使用するには、インポートされるエクスポート済み CA 証明書に完全な信頼チェーンがある必要があります。不明な場合は、CA 証明書を再エクスポートし、「証明書のエクスポートウィザード」で次のオプションが選択されていることを確認します。

- Personal Information Exchange - PKCS#12 (.PFX)
- 可能な場合は証明書パスにすべての証明書を含める
- すべての拡張プロパティをエクスポートする

または

b 自己署名証明書を作成する場合は、**自己署名証明書を作成してキーストアにインポートする を選択して 次へ** をクリックします。
Create Self-Signed Certificate (自己署名証明書の作成) ダイアログで、次の情報を入力します。

完全修飾コンピュータ名 (例 : computername.domain.com)

組織

組織単位 (例 : Security)

都市

州 (正式名)

国 : 国を表す 2 文字の略語

次へ をクリックします。

メモ:
証明書は、デフォルトで 1 年で期限切れになります。

13 バックエンドサーバーインストール設定ダイアログから、ホスト名とポートを表示または編集できます。

- デフォルトのホスト名とポートを使用する場合は、バックエンドサーバーインストール設定 ダイアログで、**次へ** をクリックします。
- フロントエンドサーバーを使用している場合は、**ネットワークでのクライアントとの内部通信、または DMZ 内でのクライアントとの外部通信を行うためにフロントエンドの連携** を選択して、フロントエンドのセキュリティサーバーのホスト名を入力します (server.domain.com など)。
- ホスト名を表示または編集するには、**ホスト名の編集** をクリックします。必要に応じて、ホスト名を編集します。Dell はデフォルトの使用を推奨します。

メモ: ホスト名に下線 (「_」) は使用できません。

終了したら、**OK** をクリックします。

- ポートを表示または編集するには、**ポートの編集** をクリックします。必要に応じて、ポートを編集します。Dell はデフォルトの使用を推奨します。終了したら、**OK** をクリックします。

14 新規データベースを作成するには、次の手順に従います。

a **参照** をクリックして、データベースをインストールするサーバーを選択します。

b Dell Data Protection データベースを設定するためにインストーラが使用する認証メソッドを選択します。製品がインストールされた後は、ここで指定された資格情報を使用することはありません。

- **現在のユーザーの Windows 認証資格情報**

  Windows 認証を選択すると、Windows へのログイン時に使用されたものと同じ資格情報が認証に使用されます (ユーザ名 フィールドとパスワード フィールドは編集できなくなります)。アカウントではシステム管理者権限があること、SQL サーバーを管理することができることを確認してください。

  または

- **以下の資格情報を使った SQL server 認証**

SQL 認証を使用する場合、使用する SQL アカウントには SQL サーバーに対するシステム管理者権限が必要です。

インストーラは、データベースの作成、ユーザーの追加、およびアクセス権限の割り当ての許可を持つ SQL サーバーに認証する必要があります。

c データベースカタログを指定します。
新規データベースカタログの名前を入力します。次に表示されるダイアログで、新規カタログの作成を促すプロンプトが表示されます。

d **次へ** をクリックします。

e **はい** をクリックして、インストーラにデータベースを作成させることを確認します。前の画面に戻って設定を変更するには、**いいえ** をクリックします。

15 製品が使用するための認証メソッドを選択します。このステップによりアカウントと製品が関連付けられます。

- **Windows 認証**

  以下の資格情報を使用した Windows 認証 を選択し、製品が使用する資格情報を入力してから、**次へ** をクリックします。

  アカウントではシステム管理者権限があること、SQL サーバーを管理することができることを確認してください。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。

  これらの資格情報も Dell サービスが Dell Enterprise Server で作業する際に使用されます。

  または

- **SQL Server 認証**

  以下の資格情報を使用した SQL サーバー認証 を選択し、Dell サービスが Dell Enterprise Server で作業する際に使用する SQL サーバー資格情報を入力して、**次へ** をクリックします。

  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。

16 プログラムインストールの準備完了 ダイアログで、**インストール** をクリックします。
ステータスは、インストールプロセスの全体を通して進捗状況ダイアログに表示されます。

17 インストールが完了したら、**終了** をクリックします。
これでバックエンドサーバーインストールタスクは完了です。

Dell サービスはインストール終了時に再起動されます。サーバーを再起動する必要はありません。

既存データベースでのバックエンドサーバーのインストール

メモ:
Dell Enterprise Server v8.x 以降を実行している場合、バックエンドサーバーのアップグレード / 移行の手順を参照してください。

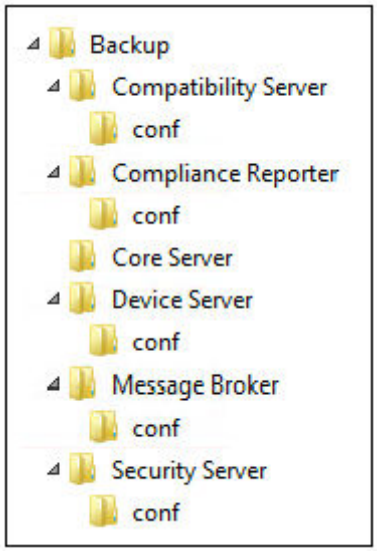
新しい Dell Enterprise Server をインストールして、「インストール前の設定」中に作成された SQL データベースまたは v9.x 以降の既存の SQL データベースに接続することができます（スキーマバージョンがインストールする Dell Enterprise Server のバージョンに一致する場合）。

v8.x 以降のデータベースは、最新バージョンのサーバー設定ツールで最新のスキーマに移行する必要があります。サーバー設定ツールを使用したデータベース移行の手順については、「データベースの移行」を参照してください。最新のサーバー設定ツールを入手、または **v8.0 より前のデータベースに移行するには**、デル ProSupport に問い合わせてサポートを受けてください。

インストールの実行元のユーザーアカウントには、SQL データベース用のデータベース所有者権限が必要です。アクセス権限の有無またはデータベースへのアクセス可否について不明な場合は、インストールを開始する前に、データベース管理者に問い合わせて確認してください。

既存のデータベースが Dell Enterprise Server で事前にインストールされている場合は、インストールを開始する前に、データベース、設定ファイルおよび secretKeyStore がバックアップされていること、Dell Enterprise Server をインストールするサーバーからアクセス可能であることを確認します。これらのファ

イルは、Dell Enterprise Server と既存のデータベースを設定するときに必要になります。インストール中、インストーラによって作成されたフォルダの構造（例は下記参照）は変更しないでください。



1 Dell インストールメディアで、Dell Enterprise Server ディレクトリに移動します。Enterprise Server-x64 を、Enterprise Server をインストールするサーバのルートディレクトリに**解凍**（コピー / 貼り付けまたはドラッグ / ドロップではなく）します。**コピー / 貼り付けまたはドラッグ / ドロップを行うと、エラーが発生し、インストールが失敗します。**

2 **setup.exe** をダブルクリックします。

3 *InstallShield* ウィザードでインストールの言語を選択し、**OK** をクリックします。

4 前提条件対象のものがインストールされていない場合、それらをインストールするように伝えるメッセージが表示されます。**インストール** をクリックします。

5 ようこそ ダイアログで **次へ** をクリックします。

6 ライセンス契約を読み、その条件に同意して **次へ** をクリックします。

7 「インストール前の設定」において、オプションで手順 9 を完了した場合は、**次へ** をクリックします。完了していない場合は、32 文字のプロダクトキーを入力し、**次へ** をクリックします。プロダクトキーはファイル「*EnterpriseServerInstallKey.ini*」にあります。

8 **バックエンドインストール** および **リカバリインストール** を選択し、**次へ** をクリックします。

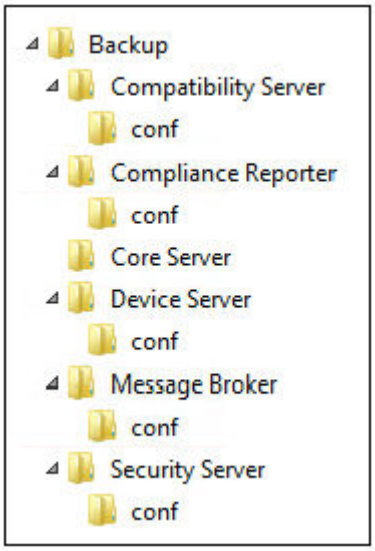
9 Dell Enterprise Server を、デフォルトの場所の C:\Program Files\Dell にインストールするには、**次へ** をクリックします。それ以外の場所にインストールする場合は、**変更** をクリックして異なる場所を選択し、**次へ** をクリックします。

10 バックアップ設定ファイルを保存する場所を選択するには、**変更** をクリックして希望のフォルダに移動してから **次へ** をクリックします。

デルでは、バックアップの場所にリモートネットワークの場所または外部のドライブを選択することを推奨します。

サーバー設定ツールで行われた変更を含む、インストール後に設定ファイルに対して行われた変更は、これらのフォルダに手動でバックアップする必要があります。設定ファイルは、サーバーを手動で復元するのに使用される全情報のうちの重要な要素です。

メモ: インストール中、インストーラによって作成されたフォルダの構造（例は下記参照）は変更しないでください。



11 使用するデジタル証明書のタイプを選択することができます。**デジタル証明書は信頼のおける証明書認証局からのものを使用することが強く推奨されます。**

以下のオプション「a」または「b」を選択します。

a CA 機関から購入された既存の証明書を使用するには、**既存証明書のインポート** を選択し、**次へ** をクリックします。

参照 をクリックして、証明書のパスを入力します。

この証明書に関連付けられているパスワードを入力します。キーストアファイルは .p12 または pfx である必要があります。手順については、「証明書管理コンソールを使用した証明書の .PFX へのエクスポート」を参照してください。

次へ をクリックします。

> **メモ:**
> この設定を使用するには、インポートされるエクスポート済み CA 証明書に完全な信頼チェーンがある必要があります。不明な場合は、CA 証明書を再エクスポートし、「証明書のエクスポートウィザード」で次のオプションが選択されていることを確認します。
>
> - Personal Information Exchange - PKCS#12 (.PFX)
> - 可能な場合は証明書パスにすべての証明書を含める
> - すべての拡張プロパティをエクスポートする

または

b 自己署名証明書を作成する場合は、**自己署名証明書を作成してキーストアにインポートする を選択して 次へ** をクリックします。

Create Self-Signed Certificate (自己署名証明書の作成) ダイアログで、次の情報を入力します。

完全修飾コンピュータ名 (例 : computername.domain.com)

組織

組織単位 (例 : Security)

都市

州 (正式名)

国 : 国を表す 2 文字の略語

次へ をクリックします。

メモ:
証明書は、デフォルトで 1 年で期限切れになります。

12 サーバー暗号化（SE）では、使用するデジタル証明書のタイプを選択することができます。デジタル証明書は信頼のおける証明書認証局からのものを使用することが強く推奨されます。
以下のオプション「a」または「b」を選択します。

a CA 機関から購入された既存の証明書を使用するには、**既存証明書のインポート** を選択し、**次へ** をクリックします。
参照 をクリックして、証明書のパスを入力します。

この証明書に関連付けられているパスワードを入力します。キーストアファイルは .p12 または pfx である必要があります。手順については、「証明書管理コンソールを使用した証明書の .PFX へのエクスポート」を参照してください。

次へ をクリックします。

メモ:
この設定を使用するには、インポートされるエクスポート済み CA 証明書に完全な信頼チェーンがある必要があります。不明な場合は、CA 証明書を再エクスポートし、「証明書のエクスポートウィザード」で次のオプションが選択されていることを確認します。

- Personal Information Exchange - PKCS#12（.PFX）
- 可能な場合は証明書パスにすべての証明書を含める
- すべての拡張プロパティをエクスポートする

b 自己署名証明書を作成する場合は、**自己署名証明書を作成してキーストアにインポートする を選択して 次へ** をクリックします。
Create Self-Signed Certificate（自己署名証明書の作成）ダイアログで、次の情報を入力します。

完全修飾コンピュータ名（例：computername.domain.com）

組織

組織単位（例：Security）

都市

州（正式名）

国：国を表す 2 文字の略語

次へ をクリックします。

メモ:
証明書は、デフォルトで 1 年で期限切れになります。

13 バックエンドサーバーインストール設定ダイアログから、ホスト名とポートを表示または編集できます。

- デフォルトのホスト名とポートを使用する場合は、バックエンドサーバーインストール設定 ダイアログで、**次へ** をクリックします。
- フロントエンドサーバーを使用している場合は、**ネットワークでのクライアントとの内部通信、または DMZ 内でのクライアントとの外部通信を行うためにフロントエンドの連携** を選択して、フロントエンドのセキュリティサーバーのホスト名を入力します（server.domain.com など）。
- ホスト名を表示または編集するには、**ホスト名の編集** をクリックします。必要に応じて、ホスト名を編集します。Dell はデフォルトの使用を推奨します。

メモ: ホスト名に下線（「_」）は使用できません。

終了したら、**OK** をクリックします。

- ポートを表示または編集するには、**ポートの編集** をクリックします。必要に応じて、ポートを編集します。Dell はデフォルトの使用を推奨します。
終了したら、**OK** をクリックします。

14 インストーラが使用するための認証メソッドを指定します。

a **参照** をクリックしてデータベースが存在するサーバを選択します。

b 認証タイプを選択します。

- **現在のユーザーの Windows 認証資格情報**

  Windows 認証を選択すると、Windows へのログイン時に使用されたものと同じ資格情報が認証に使用されます (ユーザ名 フィールドとパスワード フィールドは編集できなくなります)。アカウントではシステム管理者権限があること、SQL サーバーを管理することができることを確認してください。

  または

- **以下の資格情報を使った SQL server 認証**

  SQL 認証を使用する場合、使用する SQL アカウントには SQL サーバーに対するシステム管理者権限が必要です。

  インストーラは、データベースの作成、ユーザーの追加、およびアクセス権限の割り当ての許可を持つ SQL サーバーに認証する必要があります。

c **参照** をクリックして、既存のデータベースカタログの名前を選択します。

d **次へ** をクリックします。

15 製品が使用するための認証メソッドを選択します。これは製品がデータベースおよびデルのサービスで作業するのに使用するアカウントです。

- **Windows 認証の使用**

  以下の資格情報を使用した Windows 認証 を選択し、製品が使用するアカウントの資格情報を入力してから、**次へ** をクリックします。

  アカウントではシステム管理者権限があること、SQL サーバーを管理することができることを確認してください。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。

  または

- **SQL Server 認証の使用**

  以下の資格情報を使った SQL Server 認証 を選択し、SQL Server 資格情報を入力してから **次へ** をクリックします。

  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。

  インストーラがデータベースの問題を検出すると、Existing Database Error (既存のデータベースにエラー) ダイアログが表示されます。ダイアログ内のオプションは状況により異なります。

  - データベーススキーマは以前のバージョンのものとなります。(手順 a を参照してください。)
  - このデータベースには、現在インストール中のバージョンに一致するデータベーススキーマがすでに含まれています。(手順 b を参照してください。)

  a データベーススキーマが以前のバージョンのものである場合は、**インストーラを終了して、このインストールを終了する** を選択します。次にデータベースをバックアップする必要があります。
  次のオプションはデル *ProSupport* からの指示のもとでのみ使用します。

  - **このデータベースを現在のスキーマに移行する** オプションは、故障したサーバー実装から良好なデータベースを復元するのに使用します。このオプションでは \Backup フォルダ内の復元ファイルを使用してデータベースに再接続し、その後データベースを現在のスキーマに移行します。正しいバージョンの Enterprise Server を再インストールし、最新のインストーラを実行してアップグレードをするという方法を試した後にのみ、このオプションを使用するようにしてください。
  - **データベースの移行なしで続行する** オプションでは、データベースを完全に設定せずに Enterprise Server ファイルをインストールします。後にサーバー設定ツールを使用してデータベースの設定を手動で行う必要があります。また、その後も手動での変更が必要になります。

  b データベーススキーマが現行バージョンのスキーマになっているが、Dell Enterprise Server バックエンドに接続されていない場合は、リカバリとしてみなされます。このダイアログが表示される場合は、次の操作を行います。

  - 選択したデータベースのインストールを続行するには、**復元インストールモード** を選択します。

- 異なるデータベースを選ぶには、**新規データベースを選択する** を選択します。
- インストールを終了するには、**インストーラを終了して、このインストールを終了する** を選択します。

c **次へ** をクリックします。

16 プログラムインストールの準備完了 ダイアログで、**インストール** をクリックします。

ステータスは、インストールプロセスの全体を通して進捗状況ダイアログに表示されます。

インストールが完了したら、**終了** をクリックします。

これでバックエンドサーバーインストールタスクは完了です。

Dell サービスはインストール終了時に再起動されます。サーバーを再起動する必要はありません。

フロントエンドサーバのインストール

フロントエンドサーバのインストールは、Dell Enterprise Server を使用するフロントエンド (DMZ モード) オプションを提供します。DMZ 内に Dell コンポーネントをデプロイする場合は、攻撃から適切に保護されていることを確認してください。

メモ: ビーコンサービスは、保護 Office モードを実行する際に、Data Guardian によって保護されるすべてのファイルにコールバックビーコンを挿入する Data Guardian コールバックビーコンをサポートするこのインストールの一部としてインストールされます。これによって、任意の場所の任意のデバイスと Dell Front End Server 間の通信が可能になります。コールバックビーコンを使用する前に、必要なネットワークセキュリティが設定されていることを確認します。コールバックビーコンの有効化ポリシーはデフォルトで有効です。

このインストールを実行するには、DMZ サーバーの完全修飾ホスト名が必要になります。

1 Dell インストールメディアで、Dell Enterprise Server ディレクトリに移動します。Dell Enterprise Server-x64 を、Enterprise Server をインストールするサーバのルートディレクトリに**解凍** (コピー / 貼り付けまたはドラッグ / ドロップではなく) します。**コピー /貼り付けまたはドラッグ /ドロップを行うと、エラーが発生し、インストールが失敗します。**

2 **setup.exe** をダブルクリックします。

3 *InstallShield* ウィザードでインストールの言語を選択し、**OK** をクリックします。

4 前提条件対象のものがインストールされていない場合、それらをインストールするように伝えるメッセージが表示されます。**インストール** をクリックします。

5 ようこそ ダイアログで **次へ** をクリックします。

6 ライセンス契約を読み、その条件に同意して **次へ** をクリックします。

7 プロダクトキーを入力します。

8 **フロントエンドインストール** を選択し、**次へ** をクリックします。

9 フロントエンドサーバーをデフォルトの C:\Program Files\Dell にインストールする場合は、**次へ** をクリックします。それ以外の場所にインストールする場合は、**変更** をクリックして異なる場所を選択し、**次へ** をクリックします。

10 使用するデジタル証明書のタイプを選択することができます。**デジタル証明書は信頼のおける証明書認証局からのものを使用することが強く推奨されます。**
以下のオプション「a」または「b」を選択します。

a CA 機関から購入された既存の証明書を使用するには、**既存証明書のインポート** を選択し、**次へ** をクリックします。
参照 をクリックして、証明書のパスを入力します。

この証明書に関連付けられているパスワードを入力します。キーストアファイルは .p12 または pfx である必要があります。手順については、「証明書管理コンソールを使用した証明書の .PFX へのエクスポート」を参照してください。

次へ をクリックします。

メモ:
この設定を使用するには、インポートされるエクスポート済み CA 証明書に完全な信頼チェーンがある必要があります。不明な場合は、CA 証明書を再エクスポートし、「証明書のエクスポートウィザード」で次のオプションが選択されていることを確認します。

- Personal Information Exchange - PKCS#12（.PFX）
- 可能な場合は証明書パスにすべての証明書を含める
- すべての拡張プロパティをエクスポートする

b 自己署名証明書を作成する場合は、**自己署名証明書を作成してキーストアにインポートする を選択して 次へ** をクリックします。
Create Self-Signed Certificate（自己署名証明書の作成）ダイアログで、次の情報を入力します。

完全修飾コンピュータ名（例：computername.domain.com）

組織

組織単位（例：Security）

都市

州（正式名）

国：国を表す 2 文字の略語

次へ をクリックします。

メモ:
証明書は、デフォルトで 1 年で期限切れになります。

11 フロントエンドサーバーセットアップ ダイアログでバックエンドサーバーの完全修飾ホスト名または DNS エイリアスを入力して **Enterprise Edition** を選択し、**次へ** をクリックします。

12 フロントエンドサーバーインストールの設定ダイアログから、ホスト名とポートを表示または編集できます。

- デフォルトのホスト名とポートを使用する場合は、フロントエンドサーバーインストールの設定 ダイアログで、**次へ** をクリックします。
- ホスト名を表示または編集する場合は、フロントエンドサーバーセットアップ ダイアログで **ホスト名の編集** をクリックします。必要に応じて、ホスト名を編集します。Dell はデフォルトの使用を推奨します。

メモ:
ホスト名に下線（「_」）は使用できません。

プロキシはインストールに設定する必要がない場合のみ非選択にしてください。このダイアログでプロキシを選択しないとインストールされません。

終了したら、**OK** をクリックします。

- ポートを表示または編集する場合は、フロントエンドサーバーセットアップダイアログで **外向きポートの編集**、または **内部接続ポートの編集** のいずれかをクリックします。必要に応じて、ポートを編集します。Dell はデフォルトの使用を推奨します。

フロントエンドのホスト名の編集 ダイアログでプロキシの選択を解除すると、そのポートは 外部ポート または 内部ポート ダイアログには表示されません。

終了したら、**OK** をクリックします。

13 プログラムインストールの準備完了 ダイアログで、**インストール** をクリックします。
ステータスは、インストールプロセスの全体を通して進捗状況ダイアログに表示されます。

14 インストールが完了したら、**終了** をクリックします。
これでフロントエンドサーバーインストールタスクは完了です。

アップグレード / 移行

Dell Enterprise Server v8.0 以降を Dell Enterprise Server v9.x にアップグレードできます。サーバーのバージョンが v8.0 以前の場合、v8.0 にアップグレードしてから v9.x にアップグレードします。

アップグレード / 移行を開始する前に

作業を開始する前に、「インストール前の設定」がすべて完了していることを確認します。これは Mobile Edition を導入する場合は、特に重要です。

Dell Enterprise Server のインストールに関連する最新の回避策または既知の問題については、『*Enterprise Server* テクニカルアドバイザリー』をお読みください。

インストールの実行元のユーザーアカウントには、SQL データベース用のデータベース所有者権限が必要です。アクセス権限の有無またはデータベースへのアクセス可否について不明な場合は、インストールを開始する前に、データベース管理者に問い合わせて確認してください。

デルでは、データベースのベストプラクティスを Dell データベースに使用し、組織の災害復旧計画に Dell ソフトウェアを含めることを推奨します。

DMZ 内に Dell コンポーネントをデプロイする場合は、攻撃から適切に保護されていることを確認してください。

本番稼働の場合、デルでは、専用サーバーに SQL Server をインストールすることを推奨します。

ポリシーの機能を十分に活用するには、Dell Enterprise Server および Client の両方を最新バージョンに更新することを推奨します。

Dell Enterprise Server v9.x は以下をサポートします。

- Enterprise Edition：
  - Windows クライアント v7.x/8.x
  - Mac クライアント v7.x/8.x
  - SED クライアント v8.x
  - Authentication v8.x
  - BitLocker Manager v7.2x+ および v8.x
  - Data Guardian v1.x
- Endpoint Security Suite v1.x
- Endpoint Security Suite Enterprise v1.x
- Mobile Edition v7.x/v8.x
- Dell Enterprise Server v8.x 以降からのアップグレード / 移行。(v8.x より前の Dell Enterprise Server から移行する際は、デル ProSupport に問い合わせてサポートを受けてください。)

新しいポリシーが導入されたバージョンに Dell Enterprise Server をアップグレード / 移行する場合は、更新されたポリシーをアップグレード / 移行後にコミットして、デフォルト値ではなく、独自のポリシー設定が新しいポリシーに実装されるようにしてください。

一般的に推奨されるアップグレードパスは Dell Enterprise Server およびそのコンポーネントをアップグレード / 移行し、次に Client をインストール / アップグレードすることです。

ポリシーの変更の適用

1 リモート管理コンソールに Dell 管理者としてログインします。

2 左側のメニューで、**管理** > **コミット**.をクリックします。

3 コメント フィールドで変更の説明を入力します。

4 **ポリシーのコミット** をクリックします。

5 コミットが完了したら、リモート管理コンソールからログオフします。

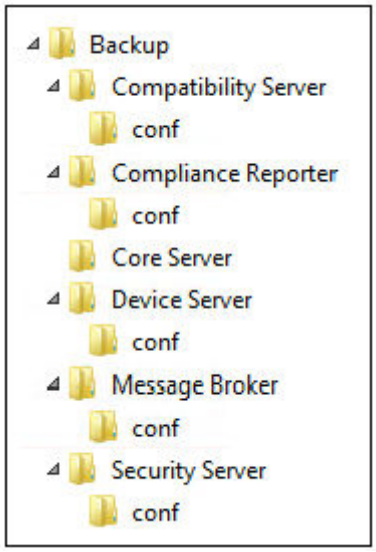
すべての Dell サービスが実行されていることを確認します。

6 Windows の スタート メニューから、**スタート** > **ファイル名を指定して実行** をクリックします。*services.msc* と入力し、**OK** をクリックします。サービスが開いたら、各 Dell サービスに移動し、必要に応じて、**サービスの開始** をクリックします。

既存のインストールのバックアップ

7 既存のすべてのインストールのバックアップを別の場所に作成します。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。アップグレード / 移行の完了後、既存のインストールからのファイルがいくつか必要になります。

メモ:
インストール中、インストーラによって作成されたフォルダの構造（例は下記参照）は変更しないでください。



バックエンドサーバーのアップグレード / 移行

1 Dell インストールメディアで、Dell Enterprise Server ディレクトリに移動します。Dell Enterprise Server-x64 を、Enterprise Server をインストールするサーバのルートディレクトリに**解凍**（コピー / 貼り付けまたはドラッグ / ドロップではなく）します。**コピー /貼り付けまたはドラッグ /ドロップを行うと、エラーが発生し、インストールが失敗します。**

2 **setup.exe** をダブルクリックします。

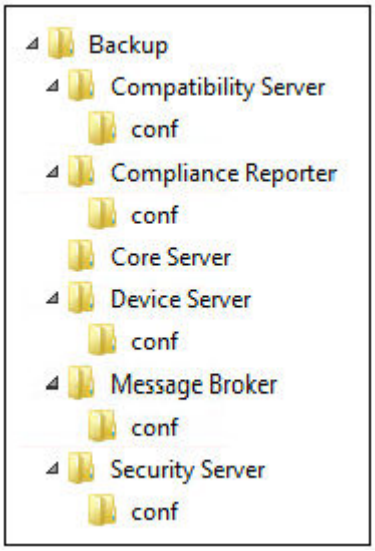
3 *InstallShield* ウィザードでインストールの言語を選択し、**OK** をクリックします。

4 ようこそ ダイアログで **次へ** をクリックします。

5 ライセンス契約を読み、その条件に同意して **次へ** をクリックします。

6 バックアップ設定ファイルを保存する場所を選択するには、**変更** をクリックして希望のフォルダに移動してから **次へ** をクリックします。
デルでは、バックアップの場所にリモートネットワークの場所または外部のドライブを選択することを推奨します。

インストール中、インストーラによって作成されたフォルダの構造（例は下記参照）は変更しないでください。



7 インストーラが的確に既存のデータベースを検出すると、ダイアログは自動入力されます。
既存のデータベースに接続するには、使用する認証メソッドを指定します。製品がインストールされた後は、ここで指定された資格情報を使用しません。

a データベースの認証タイプを選択します。

- **現在のユーザーの Windows 認証資格情報**

  Windows 認証を選択すると、Windows へのログイン時に使用されたものと同じ資格情報が認証に使用されます (ユーザ名 フィールドとパスワード フィールドは編集できなくなります)。

  アカウントではシステム管理者権限があること、SQL サーバーを管理することができることを確認してください。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。

  または

- **以下の資格情報を使った SQL server 認証**

  SQL 認証を使用する場合、使用する SQL アカウントには SQL サーバーに対するシステム管理者権限が必要です。

  インストーラは、データベースの作成、ユーザーの追加、およびアクセス権限の割り当ての許可を持つ SQL サーバーに認証する必要があります。

b **次へ** をクリックします。

8 サービスランタイムアカウント情報が事前に入力されていない場合は、インストール後に製品が使用する認証メソッドを指定します。

a 認証タイプを選択します。

b SQL Server へアクセスするために Dell サービスが使用する、ドメインサービスのアカウントのユーザー名およびパスワードを入力して、**Next**(次へ) をクリックします。

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。

9 データベースのバックアップを作成していない場合は、インストールを続行する前にバックアップを作成する**必要があります。データベースのアップグレードを元に戻すことはできません。**データベースがバックアップされた後にのみ、**はい。データベースはバックアップされています。** を選択して、**次へ** をクリックします。

10 **インストール** をクリックしてインストールを開始します。
ステータスは、アップグレードプロセスの全体を通して進捗状況ダイアログに表示されます。

11 インストールが完了したら、**終了** をクリックします。
Dell サービスは移行終了時に再起動されます。サーバーを再起動する必要はありません。

インストーラは手順 12 ~ 13 を自動的に実行します。これらの値に注目して変更が適切に行われたかを確認することが重要です。

12 バックアップされたインストールで、<Compatibility Server install dir>\conf\secretKeyStore を新しいインストールにコピー / 貼り付けします。
<Compatibility Server install dir>\conf\secretKeyStore に貼り付けます。

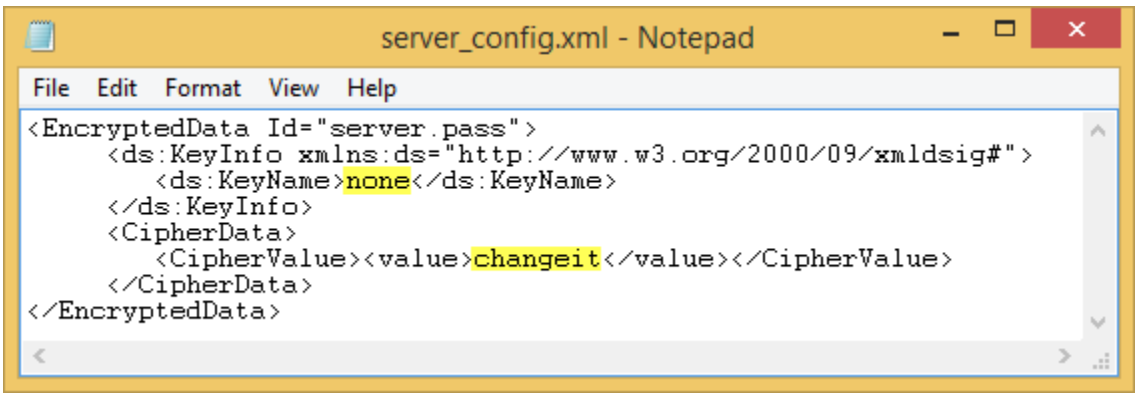
13 新しいインストールで、<Compatibility Server install dir>\conf\server_config.xml を開き、次のように、**server.pass** 値を、バックアップした <Compatibility Server install dir>\conf\server_config.xml の値に置き換えます。

server.pass に関する手順：

パスワードがわかっている場合は、server_config.xml ファイルの例を参照し、次のように変更します。

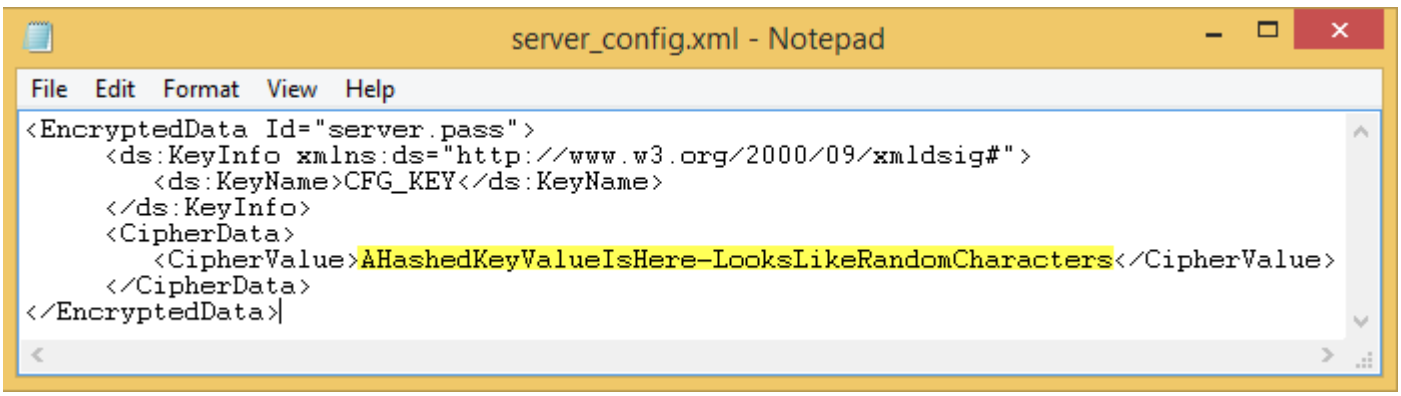
- *KeyName*（**CFG_KEY** 値）を編集して **none** にします。
- プレインテキストパスワードを入力し、*<value> </value>* で囲みます。この例では **<value>changeit</value>** となっています。
- Dell Enterprise Server が起動すると、このプレインテキストパスワードはハッシュされ、ハッシュされた値がプレインテキストに置き換えられます。

既知のパスワード



パスワードがわからない場合は、バックアップされた <Compatibility Server install dir>\conf\server_config.xml ファイルから図 4-2 にあるセクションに似たセクションを新しい *server_config.xml* ファイルの対応するセクションにカットアンドペーストします。

不明なパスワード



ファイルを保存して閉じます。

メモ:
上記以外の場合に、server_config.xml 内の server.pass 値を編集して **Dell** Enterprise Server のパスワードを変更しないでください。この値を変更すると、データベースにアクセスできなくなります。

これでバックエンドサーバー移行タスクは完了です。

フロントエンドサーバーのアップグレード / 移行

メモ: v9.5 で開始すると、ビーコンサービスはデフォルトのホスト名とポート 8446 を使用して、このアップグレードの一部としてインストールされます。ビーコンサービスは、保護 Office モードを実行する際に、Data Guardian によって保護されるすべてのファイルにコールバックビーコンを挿入する Data Guardian コールバックビーコンをサポートします。これによって、任意の場所の任意のデバイスと Dell Front End Server 間の通信が可能になります。コールバックビーコンの有効化ポリシーはデフォルトで有効です。コールバックビーコンを使用する前に、必要なネットワークセキュリティが設定されていることを確認します。

1 Dell インストールメディアで、Dell Enterprise Server ディレクトリに移動します。Dell Enterprise Server-x64 を、Enterprise Server をインストールするサーバのルートディレクトリに**解凍** (コピー / 貼り付けまたはドラッグ / ドロップではなく) します。**コピー /貼り付けまたはドラッグ /ドロップを行うと、エラーが発生し、インストールが失敗します。**

2 **setup.exe** をダブルクリックします。

3 *InstallShield* ウィザードでインストールの言語を選択し、**OK** をクリックします。

4 前提条件対象のものがインストールされていない場合、それらをインストールするように伝えるメッセージが表示されます。**インストール** をクリックします。

5 ようこそ ダイアログで **次へ** をクリックします。

6 ライセンス契約を読み、その条件に同意して **次へ** をクリックします。

7 プログラムインストールの準備完了 ダイアログで、**インストール** をクリックします。

ステータスは、インストールプロセスの全体を通して進捗状況ダイアログに表示されます。

8 インストールが完了したら、**終了** をクリックします。

9 バックエンドサーバーがフロントエンドサーバーと通信するように設定します。

a バックエンドサーバーで、<Security Server install dir>\conf\ に移動して、application.properties ファイルを開きます。

b publicdns.server.host を探し、外部で解決可能なホスト名を設定します。

c publicdns.server.port を探し、ポートを設定します (デフォルト値は 8443)。

Dell サービスはインストール終了時に再起動されます。インストール後の設定が完了するまでサーバーを再起動する必要はありません。

切断モードのインストール

切断モードは、インターネットおよびセキュアではない LAN または他のネットワークから Enterprise Server を分離します。Enterprise Server は、切断モードでインストールされた後、切断モードに保持され、接続モードに戻すことはできません。

Enterprise Server は、コマンドラインを使用して切断モードでインストールされます。

次の表には、使用可能なスイッチが一覧表示されています。

スイッチ	意味
/v	*.exe 内の .msi に変数を渡します。
/s	サイレントモード

次の表には、使用可能な表示オプションが一覧表示されています。

オプション	意味
/q	進行状況ダイアログなし、処理完了後に自動で再起動
/qb	**キャンセル** ボタンを含む進行状況ダイアログ
/qn	ユーザーインタフェースなし

次の表は、インストールで使用できるパラメータの詳細です。これらのパラメータは、コマンドラインで指定することもできますし、プロパティを使用してファイルから呼び出すこともできます。

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

パラメータ

AGREE_TO_LICENSE=Yes - この値は「Yes」である必要があります。

PRODUCT_SN=xxxxx - 標準的な場所にライセンス情報を持っている場合は任意です。そうでない場合はこちらに入力します。

INSTALLDIR=<path> - オプション。

BACKUPDIR=<path> - ここにリカバリファイルが保存されます。

メモ: このインストール中にインストーラによって作成されたフォルダの構造（例は下記参照）は変更しないでください。

AIRGAP=1 - 切断モードで Enterprise Server をインストールするには、この値は「1」である必要があります。

SSL_TYPE=n - n が 1 の場合は CA 機関から購入した既存の証明書をインポートし、2 の場合は自己署名証明書を作成します。SSL_TYPE 値は、必要な SSL プロパティを決定します。

以下は SSL_TYPE=1 で必要です：

SSL_CERT_PASSWORD=xxxxx

SSL_CERT_PATH=xxxxx

以下は SSL_TYPE=2 で必要です：

SSL_CITYNAME

SSL_DOMAINNAME

SSL_ORGNAME

SSL_UNITNAME

SSL_COUNTRY - オプション、デフォルト = "US"

SSL_STATENAME

SSOS_TYPE=n - n が 1 の場合は CA 機関から購入した既存の証明書をインポートし、2 の場合は自己署名証明書を作成します。SSOS_TYPE 値は、必要な SSOS プロパティを決定します。

以下は SSOS_TYPE=1 で必要です：

SSOS_CERT_PASSWORD=xxxxx

SSOS_CERT_PATH=xxxxx

以下は SSOS_TYPE=2 で必要です：

SSOS_CITYNAME

SSOS_DOMAINNAME

SSOS_ORGNAME

SSOS_UNITNAME

SSOS_COUNTRY - オプション、デフォルト = "US"

SSOS_STATENAME

パラメータ

DISPLAY_SQLSERVER - この値は、サーバ、インスタンスおよびポート情報を取得するために解析されます。

例：

DISPLAY_SQLSERVER=SQL_server\Server_instance, port

IS_AUTO_CREATE_SQLSERVER=FALSE - オプション。デフォルト値はデータベースが作成されていないことを意味する FALSE です。データベースはサーバ上にすでに存在している必要があります。

新しいデータベースを作成するには、この値を TRUE に設定します。

IS_SQLSERVER_AUTHENTICATION=0 - オプション。デフォルト値は 0 で、現在ログインしているユーザーの Windows 認証用資格情報が SQL サーバの認証に使用されるように指定します。SQL 認証を使用するには、この値を 1 に設定します。

メモ: インストーラは、データベースの作成、ユーザーの追加、およびアクセス権限の割り当ての許可を持つ SQL Server に認証する必要があります。この資格情報は、インストール時の資格情報であり、実行時の資格情報ではありません。

SQL 認証を使用する場合は、以下が必要です。

IS_SQLSERVER_USERNAME

IS_SQLSERVER_PASSWORD

EE_SQLSERVER_AUTHENTICATION - 必須。製品が使用するための認証メソッドを指定します。このステップによりアカウントと製品が関連付けられます。これらの資格情報もデルサービスが Enterprise Server で作業する際に使用されます。Windows 認証を使用するには、この値を 0 に設定します。SQL 認証を使用するには、値を 1 に設定します。

メモ: アカウントではシステム管理者権限があること、SQL サーバを管理することができることを確認してください。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。

SQL_EE_USERNAME - 必須。Windows 認証で、この形式を使用します：ドメイン\ユーザー名。SQL 認証で、ユーザー名を指定します。

SQL_EE_PASSWORD - 必須。Windows ユーザー名または SQL ユーザー名に関連付けられているパスワードを指定します。

SQL 認証を使用する場合は（ EE_SQLSERVER_AUTHENTICATION=1 ）、次が有効です。

RUNAS_KEYSERVER_USER - キーサーバをこの形式の Windows ユーザー名「として実行」に設定します：ドメイン\ユーザー。これは、Windows のユーザーアカウントである必要があります。

RUNAS_KEYSERVER_PSWD - キーサーバを Windows のユーザーアカウントに関連付けられている Windows パスワード「として実行」に設定します。

SQL_ADD_LOGIN=T - オプション。デフォルトは null です（ このログインは追加されません ）。値が T に設定されており、SQL_EE_USERNAME がログインまたはデータベースのユーザーではない場合は、インストーラはユーザーの SQL 認証用資格情報を追加し、権限を設定して製品に資格情報が使用できるようにしようとします。

以下は、ホスト名のパラメータです。必要に応じて、ホスト名を編集します。Dell はデフォルトの使用を推奨します。形式は `server.domain.com` である必要があります。

メモ: ホスト名に下線（「_」）は使用できません。

CORESERVERHOST - オプション。Core Server ホスト名。

RMIHOST - オプション。Compatibility Server ホスト名。

REPORTERHOST - オプション。Compliance Reporter ホスト名。

DEVICEHOST - オプション。Device Server ホスト名。

KEYSERVERHOST - オプション。Key Server ホスト名。

パラメータ

TIGAHOST - オプション。Security Server ホスト名。

SMTP_HOST - オプション。SMTP ホスト名。

ACTIVEMQHOST - オプション。Message Broker ホスト名。

以下はポートのパラメータです。必要に応じて、ポートを編集します。デルはデフォルトの使用を推奨します

SERVERPORT_CLIENTAUTH - オプション。

REPORTERPORT - オプション。

DEVICEPORT - オプション。

KEYSERVERPORT - オプション。

GKPORT - オプション。

TIGAPORT - オプション。

SMTP_PORT - オプション。

ACTIVEMQ_TCP - オプション。

ACTIVEMQ_STOMP - オプション。

切断モードでの Enterprise Server のインストール

次の例では、ファイルにリストされたインストールパラメータを使用して、進行状況ダイアログにより、サイレントモードで Enterprise Server をインストールします。`C:\mysetups\eeoptions.txt\" "`

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

Dell Enterprise Server のアンインストール

1. Dell インストールメディアで、Dell Enterprise Server ディレクトリに移動します。Dell Enterprise Server-x64 を、Enterprise Server をアンインストールするサーバのルートディレクトリに**解凍**（コピー / 貼り付けまたはドラッグ / ドロップではなく）します。**コピー /貼り付けまたはドラッグ /ドロップを行うと、エラーが発生し、インストールが失敗します。**
2. **setup.exe** をダブルクリックします。
3. ようこそ ダイアログで **次へ** をクリックします。
4. プログラムの削除 ダイアログで、**削除** をクリックします。
   ステータスは、アンインストールプロセスの全体を通して進捗状況ダイアログに表示されます。
5. アンインストールが完了したら、**終了** をクリックします。

5

インストール後の設定

Dell Enterprise Server の設定に関連する最新の回避策または既知の問題について『Enterprise Server Technical Advisories』(Enterprise Server テクニカルアドバイザリー) をお読みください。

Dell Enterprise Server を初めてインストールするのか、既存のインストールをアップグレードするのかによって、環境のコンポーネントをいくつか構成する必要があります。

EAS 管理のインストールおよび設定

本項は、Mobile Edition を使用する場合に完了する必要があります。使用しない場合は、本項を省略し、「DMZ モード構成の Dell Security Server」に進みます。

前提条件

- EAS メールボックスマネージャサービスのログインアカウントは、Exchange ActiveSync ポリシーの作成 / 変更、ユーザーメールボックスへのポリシーの割り当て、および ActiveSync デバイスに関する情報をクエリする許可を持つアカウントである必要があります。
- ファイルを変更してサービスを再起動するには、EAS 設定ユーティリティを管理者権限で実行する必要があります。
- Dell Policy Proxy へのネットワーク接続が必要です。
- Dell Policy Proxy の FQDN を用意します。
- Dell Policy Proxy ポート番号を用意します。
- Exchange 環境をホストするサーバーに Microsoft メッセージキュー (MSMQ) がインストール / 設定されている必要があります。インストール / 設定されていない場合は、「Microsoft メッセージキュー (MSMQ) のインストール / 設定」を参照してください。

導入プロセス時

Exchange ActiveSync を使用して、Mobile Edition 経由でモバイルデバイスを管理する予定の場合、Exchange Server 環境を設定する必要があります。

EAS デバイスマネージャのインストール

1 Dell インストールメディアで EAS 管理フォルダに移動します。EAS デバイスマネージャフォルダで、setup.exe を *Exchange Client Access Server* にコピーします。

2 **setup.exe** をダブルクリックして、インストールを開始します。お使いの環境に複数の *Exchange Client Access Server* がある場合、それぞれの環境でこのインストーラを実行します。

3 インストール用言語を選択して **OK** をクリックします。

4 ようこそ 画面が表示されたら、**次へ** をクリックします。

5 ライセンス契約を読み、条項に同意して、

6 **次へ** をクリックして EAS デバイスマネージャをデフォルトの場所 **C:\Inetpub\wwwroot\Dell\EAS Device Manager** にインストールします。

7 インストールを開始する準備ができました 画面で **インストール** をクリックします。
ステータスウィンドウにインストールの進捗状況が表示されます。

8 必要に応じて Windows インストーラログを表示するボックスにチェックを入れ、**終了** をクリックします。

EAS メールボックスマネージャのインストール

1 Dell インストールメディアで EAS 管理フォルダに移動します。EAS Mailbox Manager フォルダで、setup.exe を *Exchange Mailbox Server* にコピーします。

2 **setup.exe** をダブルクリックして、インストールを開始します。お使いの環境に複数の *Exchange Mailbox Server* がある場合、それぞれの環境でこのインストーラを実行します。

3 インストール用言語を選択して **OK** をクリックします。

4 ようこそ 画面が表示されたら **次へ** をクリックします。

5 ライセンス契約を読み、条項に同意して、

6 **次へ** をクリックして、デフォルトの場所である **C:\Program Files\Dell\EAS Mailbox Manager** に EAS メールボックスマネージャをインストールします。

7 ログオン情報 画面で、ログオンしてこのサービスを使用するユーザーアカウントの資格情報を入力します。

ユーザー名：ドメイン\ユーザー名

パスワード：このユーザー名に関連付けられているパスワード

次へ をクリックします。

8 インストールを開始する準備ができました 画面で **インストール** をクリックします。

ステータスウィンドウにインストールの進捗状況が表示されます。

9 必要に応じて Windows インストーラログを表示するボックスにチェックを入れ、**終了** をクリックします。

EAS 設定ユーティリティの使用

1 同じコンピュータで **スタート** > **Dell** > **EAS 設定ユーティリティ** > **EAS 設定** と移動して、EAS 設定ユーティリティを実行します。

2 **セットアップ** をクリックして EAS 管理を設定します。

3 以下の情報を入力します。

Dell Policy Proxy の FQDN

Dell Policy Proxy ポート（デフォルトのポートは 8090）

Dell Policy Proxy のポーリング間隔（デフォルトは 1 分）

EAS デバイスマネージャをレポート限定モードで実行するボックスを選択します（導入時の推奨）。

> **メモ:**
> レポート限定モードを使用すると、不明なデバイス / ユーザーによる Exchange ActiveSync へのアクセスが許可されますが、トラフィックは引き続きユーザーに報告されます。導入が完了して稼働しはじめたら、この設定を変更してセキュリティを厳しくすることができます。

OK をクリックします。

4 成功メッセージが表示されます。**はい** をクリックして IIS と EAS メールボックスマネージャサービスを再起動します。

5 終了したら **終了** をクリックします。

EAS 管理の設定

導入が完了して稼働しはじめ、セキュリティを厳しくする準備が整えば、次の手順に従います。

1 **スタート** > **Dell** > **EAS 設定ユーティリティ** > **EAS 設定** と移動して、EAS 設定ユーティリティを実行します。

2 **セットアップ** をクリックして EAS 管理を設定します。

3 以下の情報を入力します。

Dell Policy Proxy の FQDN

Dell Policy Proxy ポート（デフォルトのポートは 8090）

Dell Policy Proxy のポーリング間隔（デフォルトは 1 分）

EAS デバイスマネージャをレポート限定モードで実行するボックスを選択解除します。

OK をクリックします。

4 成功メッセージが表示されます。**はい** をクリックして IIS と EAS メールボックスマネージャサービスを再起動します。

5 終了したら **終了** をクリックします。

DMZ モード構成の Dell Security Server

Dell Security Server が DMZ とプライベートネットワークに導入され、DMZ サーバーのみが信頼できる証明機関（CA）からのドメイン証明書を持っている場合は、その信頼できる証明書をプライベートネットワークの Dell Security Server の Java キーストアに追加するために、手動でいくつかの手順を実行する必要があります。

信頼できる証明書が使用される場合は、この項を省略し、「APN 登録」に進みます。

メモ: DMZ サーバーおよびプライベートネットワークサーバーの両方に対して信頼できる証明機関からのドメイン証明書を使用することを強く推奨します。

Keytool を使用した DMZ ドメイン証明書のインポート

重要:

Keytool の手順を続行する前に、既存の **Dell** Security Server の cacerts をバックアップします。設定エラーが発生した場合は、保存したファイルに復元できます。

前提

- Dell Security Server が、非信頼証明書を使用してインストールされています。
- DMZ モードの Dell Security Server が、署名された証明書（Entrust、Verisign など）を使用してインストールされています。
- .pfx 証明書ファイルが利用可能です。お使いの証明書を .pfx に変換する必要がある場合は、証明書管理コンソールを使用した証明書の .PFX へのエクスポート を参照します。

プロセス

1 Keytool をシステムパスに追加します。

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

2 Keytool を使用して、インポートする信頼できるドメイン証明書の内容をリストします。リストされたエイリアス名をメモします。

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

3 Keytool を使用して、署名された証明書の内容を Dell Security Server の cacerts ファイルにインポートします。

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

-srcalias について、署名された証明書のエクスポート済み内容からこの情報を収集する必要があります。

-destalias について、これは選択した任意の場所です。

4 <Security Server install dir>\conf\ ディレクトリの現在の cacerts ファイルをバックアップし、Dell Security Server で新しく作成された cacerts ファイルと置き換えます。

application.properties ファイルの変更

application.properties ファイルを変更して署名証明書のエイリアスを指定します。

1 <Security Server install dir>\conf\application.properties にアクセスします。
2 次の情報を変更します。
keystore.alias.signing=<この値は上記 手順 3 の `-destalias` の値に変更します>
3 Dell Security Server サービスを再起動します。

APN 登録

iOS デバイスで Mobile Edition for Mobile Device Security を使用する予定の場合は、APN 登録ウィザードを使用する必要があります。

- CSR の作成
- Apple プッシュ証明書の作成
- プッシュ証明書のアップロード

iOS デバイスで Mobile Edition for Mobile Device Security を使用しない予定の場合は、本項を省略し、「サーバ設定ツール」に進みます。

Apple プッシュ通知サービス (APN) を使用すると、iOS デバイスと無線で安全な通信を行えます。APN は、Dell Enterprise Server とチェックインするために iOS デバイスに通知を送信するために使用されます。APN はデバイスに通知のみを送信し、データは送信されません。

プロセス

1 ブラウザを開き、https://<FQDN-of-security-server>:8443/csrweb にアクセスします。
2 APN 登録ウィザードログイン ダイアログで、Dell 管理者の資格情報を入力し、**ログイン** をクリックします。
3 実行する手順を説明するダイアログが表示されます。**次へ** をクリックします。

手順 I : CSR の作成

4 以下の情報を入力します。

電子メール : 電子メールアドレスとして任意の UPN を使用できますが、APN 証明書を保持する管理者のアカウントを使用することを推奨します。

共通名 : この電子メールアドレスに関連付けられた共通名を入力します。

CSR の生成 をクリックします。

5 CSR の生成後に、簡単にアクセスできる場所にファイルを保存します。
6 **次へ** をクリックします。

手順 II : Apple プッシュ証明書の作成

7 **Apple Push Certificate Portal** のリンクをクリックします。Apple ID とパスワードを使用してログインします。
8 使用条件を読み、同意を示すために **同意する** をクリックします。
9 **参照** をクリックし、次に アップロード をクリックして作成した CSR を**アップロード**します。
10 サードパーティサーバーの証明書 ページで、**ダウンロード** をクリックします。簡単にアクセスできる場所にファイルを保存します。
11 APN 登録ウィザードに戻り、**次へ** をクリックします。

手順 III : プッシュ証明書のアップロード

12 次の情報を入力します (手順 I : CSR の作成 で使用したのと同じ資格情報を使用します)。

電子メール:

コマンド名：

証明書ファイルのプッシュ：**参照** をクリックして、手順 7 で保存されたファイルを指定します。**アップロード** をクリックします。

13 成功メッセージが表示されます。**終了** をクリックします。

Dell Enterprise Server を使用した APN 証明書の登録が完了しました。

サーバー設定ツール

インストール終了後に環境設定が必要になった場合は、Dell サーバー設定ツールを使用して変更します。

Dell サーバー設定ツールでは、次の操作を行うことができます。

- 新規またはアップデートされた証明書の追加
- Dell Manager 証明書のインポート
- ID 証明書のインポート
- サーバー SSL 証明書または Mobile Edition の設定
- Data Guardian または電子メールサービスの SMTP の設定
- データベース名、場所、または資格情報の変更
- データベースの移行

Dell Core Server および Dell Compatibility Server を Dell サーバー設定ツールと同時に実行することはできません。Dell Core Server サービスと Dell Compatibility Server サービスを サービス（**スタート > ファイル名を指定して実行**し、***services.msc*** と入力します）で停止した後で、Dell サーバー設定ツールを起動します。

Dell サーバー設定ツールを起動するには、**スタート** > **プログラム** > **Dell** > **Enterprise Edition** > **サーバー設定ツール** > **サーバー設定ツールを実行する** を選択します。

Dell サーバー設定ツールのログは、C:\Program Files\Dell\Enterprise Edition\Configuration Tool\Logs に保存されます。

新規またはアップデートされた証明書の追加

証明書は、自己署名証明書または署名付き証明書のどちらを使用するか選択できます。

- **自己署名証明書**は、作成者自身によって署名されます。自己署名証明書は、パイロットや POC などに適しています。実稼働環境では、デルは、パブリック CA 署名付き証明書またはドメイン署名付き証明書を推奨します。
- **署名付き**（パブリック CA 署名付きまたはドメイン署名付き）証明書は、パブリック CA またはドメインにより署名されます。パブリック認証機関（CA）により署名された証明書の場合は、通常、署名元 CA の証明書が Microsoft 証明書ストアにすでに存在するので、信頼チェーンは自動的に確立されます。ドメイン CA 署名付き証明書の場合は、ワークステーションがドメインに所属していれば、ドメインから提供される署名元 CA の証明書はワークステーションの Microsoft 証明書ストアに追加されているので、信頼チェーンが作成されます。

証明書の設定の影響を受けるコンポーネントは以下のとおりです。

- Java サービス（例：Dell Device Server など）
- .NET アプリケーション（Dell Core Server）
- 起動前認証用に使用されるスマートカードの検証（Dell Security Server）
- Dell Manager に送信されるポリシーバンドルの署名に使用される秘密暗号化キーのインポート Dell Manager は、自己暗号化ドライブ、または BitLocker Manager が搭載されたリモート管理の Enterprise Edition クライアントの SSL 検証を実行します。
- クライアントワークステーション：
  - BitLocker Manager を実行しているワークステーション
  - Enterprise Edition（Windows クライアント）を実行しているワークステーション

- Endpoint Security Suite を実行しているワークステーション
- Endpoint Security Suite Enterprise を実行しているワークステーション

使用する証明書の種類に関する情報 *:*

スマートカードを使用した起動前認証には Dell Security Server での SSL 検証が必要です。Dell Manager は、Dell Core Server への接続時に SSL 検証を実行します。これらの種類の接続の場合は、署名元 CA がキーストアに含まれている必要があります (対象の Dell サーバーコンポーネントに応じて、Java キーストアまたは Microsoft キーストアのいずれかになります)。自己署名証明書が選択された場合は、次のオプションを使用できます。

- 起動前認証用に使用されるスマートカードの検証 :
  - Dell Security Server Java キーストアに「Root Agency」署名証明書と完全な信頼チェーンをインポートします。詳細については、「自己署名証明書の作成と証明書署名要求の生成」を参照してください。完全な信頼チェーンがインポートされる必要があります。

Dell Manager :

- Microsoft キーストアにあるワークステーションの「信頼されたルート証明機関」(「ローカルコンピュータ」用) に「Root Agency」署名証明書 (生成された自己署名証明書からのもの) を挿入します。
- Server サイド SSL 検証の動作を変更します。Server サイド SSL 信頼検証を無効にするには、設定 タブの **信頼チェーンチェックの無効化** をチェックします。

証明書の作成方法には、高速 と 詳細 の 2 つがあります。

いずれか **ひとつ** の方法を選択します。

- 高速 – すべてのコンポーネントに対して自己署名付き証明書を生成する場合はこの方法を選択します。これは最も簡単な方法ですが、自己署名証明書は、パイロットや POC などにのみ適しています。実稼働環境では、デルは、パブリック CA 署名付き証明書またはドメイン署名付き証明書を推奨します。
- 詳細 – 各コンポーネントを個別に設定する場合はこの方法を選択します。

高速

1 最上部のメニューから、**アクション** > **証明書の設定** を選択します。

2 設定ウィザードが起動されたら、**高速** を選択し、**次へ** をクリックします。Enterprise Server のインストール時に作成された自己署名付き証明書の情報が使用されます (利用可能な場合)。

3 最上部のメニューから **設定** > **保存** を選択します。プロンプトが表示されたら、保存を確定します。

証明書のセットアップが完了しました。本項の残りの部分では、証明書の詳細な作成方法について詳しく説明します。

詳細

証明書を作成するには、自己署名付き証明書の生成 と 現在の設定の使用 の 2 つの方法があります。いずれか**ひとつ**のパスを選択します。

- 方法 1 – 自己署名付き証明書の生成
- 方法 2 – 現在の設定の使用

方法 1 – 自己署名付き証明書の生成

1 最上部のメニューから、**アクション** > **証明書の設定** を選択します。

2 設定ウィザードが起動されたら、**詳細** を選択し、**次へ** をクリックします。

3 **自己署名証明書の生成** を選択し、**次へ** をクリックします。Enterprise Server のインストール時に作成された自己署名付き証明書の情報が使用されます (利用可能な場合)。

4 最上部のメニューから **設定** > **保存** を選択します。プロンプトが表示されたら、保存を確定します。

証明書のセットアップが完了しました。本項の残りの部分では、証明書その他の作成方法について詳しく説明します。

方法 2 - 現在の設定の使用

1 最上部のメニューから、**アクション** > **証明書の設定** を選択します。

2 設定ウィザードが起動されたら、**詳細** を選択し、**次へ** をクリックします。

3 **現在の設定の使用** を選択し、**次へ** をクリックします。

4 *Compatibility Server SSL* 証明書ウィンドウで、**自己署名証明書の生成** を選択し、**次へ** をクリックします。Enterprise Server のインストール時に作成された自己署名付き証明書の情報が使用されます（利用可能な場合）。

次へ をクリックします。

5 *Core Server SSL* 証明書 ウィンドウで、以下のいずれかを選択します。

- 証明書の選択 - 既存の証明書を使用する場合はこのオプションを選択します。**次へ** をクリックします。

  既存の証明書の場所を参照して、既存の証明書に関連付けられているパスワードを入力し、**次へ** をクリックします。

  完了したら、**終了** をクリックします。
- 自己署名付き証明書の生成 - Enterprise Server のインストール時に作成された自己署名付き証明書の情報が使用されます（利用可能な場合）。このオプションを選択すると メッセージセキュリティ証明書 ウィンドウが表示されず（オプション 現在の設定の使用 を選択すると表示されます）、Dell Compatibility Server 用に作成された証明書が使用されます。

  完全修飾コンピュータ名が正しいことを確認します。**次へ** をクリックします。

  同じ名前の証明書がすでにあることを示す警告メッセージが表示されます。使用するかどうかを尋ねるメッセージが表示されたら、**はい** をクリックします。

  完了したら、**終了** をクリックします。
- 現在の設定の使用 - 証明書の設定を Dell Enterprise Server の初期構成後に随時変更する場合にこのオプションを選択します。このオプションでは、すでに設定済みの証明書はそのまま残ります。このオプションを選択すると、メッセージセキュリティ証明書 ウィンドウに進みます。

  メッセージセキュリティ証明書 ウィンドウで、次のいずれか**ひとつ**を選択します。

  - 証明書の選択 - 既存の証明書を使用する場合はこのオプションを選択します。**次へ** をクリックします。

    既存の証明書の場所を参照して、既存の証明書に関連付けられているパスワードを入力し、**次へ** をクリックします。

    完了したら、**終了** をクリックします。
  - 自己署名付き証明書の生成 - Enterprise Server のインストール時に作成された自己署名付き証明書の情報が使用されます(利用可能な場合)。

    次へ をクリックします。

    完了したら、**終了** をクリックします。

証明書のセットアップが完了しました。

変更が完了したら、次の手順に従います。

1 最上部のメニューから **設定** > **保存** を選択します。プロンプトが表示されたら、保存を確定します。

2 Dell サーバー設定ツールを閉じます。

3 **スタート** > **ファイル名を指定して実行** をクリックします。*services.msc* と入力し、**OK** をクリックします。サービス が開いたら、各 Dell サービスに移動し、**サービスの開始** をクリックします。

Dell Manager 証明書のインポート

自己暗号化ドライブ、または BitLocker Manager が搭載された Enterprise Edition のリモート管理クライアントが導入に含まれている場合は、新しく作成した（または既存の）証明書をインポートする必要があります。Dell Manager の証明書は、Enterprise Edition のリモートで管理されているクライアン

トおよび BitLocker Manager へ送られた、ポリシーバンドルにサインするための、プライベートキーを保護する手段として使用されます。この証明書は他の証明書のいずれにも無関係にすることができます。さらに、このキーが漏洩した場合は、これを新しいキーと交換することが可能で、Dell Manager はポリシーバンドルを復号化できない場合に新しい公開鍵を要求します。

1 Microsoft 管理コンソールを開きます。
2 **ファイル** > **スナップインの追加と削除** をクリックします。
3 **追加** をクリックします。
4 スタンドアロンスナップインの追加 ウィンドウで **証明書** を選択し、**追加** をクリックします。
5 **コンピュータアカウント** を選択し、**次へ** をクリックします。
6 コンピュータの選択ウィンドウで **ローカルコンピュータ（このコンソールが実行されているコンピュータ）** を選択し、**終了** をクリックします。
7 **閉じる** をクリックします。
8 **OK** をクリックします。
9 コンソールルートフォルダで、証明書 *（ローカルコンピュータ）* を展開します。
10 パーソナルフォルダを展開し、必要な証明書を見つけます。
11 目的の証明書をハイライトし、**全てのタスク** > **エクスポート** を右クリックします。
12 証明書のエクスポートウィザードが開いたら、**次へ** をクリックします。
13 **はい、秘密キーをエクスポートします** を選択し、**次へ** をクリックします。
14 **Personal Information Exchange - PKCS #12（.PFX）** を選択してから、サブオプションの **可能な場合は証明書パスにすべての証明書を含める** と **すべての拡張プロパティをエクスポートする** を選択します。**次へ** をクリックします。
15 パスワードを入力し、確認します。ここにはどのようなパスワードを選んでも問題ありません。自分に覚えやすく、他人にはわかりにくいパスワードを選んでください。**次へ** をクリックします。
16 **参照** をクリックしてファイルを保存する場所を指定します。
17 *ファイル名* フィールドに、保存するファイルの名前を入力します。**保存** をクリックします。
18 **次へ** をクリックします。
19 **終了** をクリックします。
20 正しくエクスポートされたことを知らせるメッセージが表示されます。MMC を閉じます。
21 Dell サーバー設定ツールに戻ります。
22 最上部のメニューから、**アクション** > **マネージャ証明書のインポート** を選択します。
23 エクスポートしたファイルが保存されている場所に移動します。ファイルを選択し、**開く** をクリックします。
24 そのファイルに関連付けられているパスワードを入力し、**OK** をクリックします。

これで Dell Manager 証明書のインポートが完了しました。

変更が完了したら、次の手順に従います。

1 最上部のメニューから **設定** > **保存** を選択します。プロンプトが表示されたら、保存を確定します。
2 Dell サーバー設定ツールを閉じます。
3 **スタート** > **ファイル名を指定して実行** をクリックします。*services.msc* と入力し、**OK** をクリックします。サービス が開いたら、各 Dell サービスに移動し、**サービスの開始** をクリックします。

ID 証明書のインポート

導入にサーバーの暗号化が含まれている場合は、新しく作成した（または既存の）証明書をインポートする必要があります。ID 証明書は、クライアントサーバーに送信されるポリシーバンドルの署名に使用する秘密キーを保護します。この証明書は他の証明書のいずれにも無関係にすることができます。

1 最上部のメニューから、**アクション** > **ID 証明書のインポート** を選択します。

2 証明書を参照して選択し、**次へ** をクリックします。

3 証明書パスワードのプロンプトで、既存の証明書に関連付けられているパスワードを入力します。

4 Windows アカウントダイアログで、いずれかのオプションを選択します。

   a ID 証明書に関連付けられている資格情報を変更するには、**ID 証明書で異なる Windows アカウント資格情報を使用する** を選択します。

   b 現在ログオンしているアカウントの資格情報を継続して使用するには、**次へ** をクリックします。

5 最上部のメニューから **設定** > **保存** を選択します。プロンプトが表示されたら、保存を確定します。

サーバー SSL 証明書または Mobile Edition の設定

サーバー設定ツールで、**設定**タブをクリックします。

Dell Manager：

Server サイド Dell Manager SSL 信頼検証を無効にするには、**信頼チェーン確認の無効化** をオンにします。

SCEP：

Mobile Edition を使用している場合は、SCEP をホスティングするサーバの URL を入力します。

変更が完了したら、次の手順に従います。

1 最上部のメニューから **設定** > **保存** を選択します。プロンプトが表示されたら、保存を確定します。

2 Dell サーバー設定ツールを閉じます。

3 **スタート** > **ファイル名を指定して実行** をクリックします。*services.msc* と入力し、**OK** をクリックします。サービス が開いたら、各 Dell サービスに移動し、**サービスの開始** をクリックします。

Data Guardian または電子メールサービスの SMTP の設定

サーバー設定ツールで、**SMTP** タブをクリックします。

このタブで Data Guardian の SMTP を設定します。Data Guardian 以外で、他の目的のために SMTP を設定する必要がある場合は、管理者用ヘルプのトピック「SMTP サーバのライセンス電子メール通知の有効化」を参照してください。

以下の情報を入力します。

1 ホスト名：フィールドに、SMTP サーバーの FQDN（ smtpservername.domain.com など ）を入力します。

2 ユーザー名：フィールドに、メールサーバーにログインするユーザー名を入力します。書式は、DOMAIN\jdoe、jdoe、あるいは組織の要件に従ったものになります。

3 パスワード：フィールドに、このユーザー名に関連付けられているパスワードを入力します。

4 送信元アドレス：フィールドに、電子メールの送信元アドレスを入力します。これはユーザー名のアカウントと同じものでも（ jdoe@domain.com ）、指定されたユーザー名が電子メールを送信するアクセス権のある別のアカウント（ CloudRegistration@domain.com ）でもかまいません。

5 ポート：フィールドにポート番号（ 通常は 25 ）を入力します。

6 認証：メニューで 正 または 誤 のいずれかを選択します。

変更が完了したら、次の手順に従います。

1 最上部のメニューから **設定** > **保存** を選択します。プロンプトが表示されたら、保存を確定します。

2 Dell サーバー設定ツールを閉じます。

3 **スタート** > **ファイル名を指定して実行** をクリックします。*services.msc* と入力し、**OK** をクリックします。サービス が開いたら、各 Dell サービスに移動し、**サービスの開始** をクリックします。

データベース名、場所、または資格情報の変更

サーバー設定ツールで、データベースタブをクリックします。

1 *サーバー名：* フィールドに、データベースをホスティングしているサーバーの完全修飾ドメインネーム（ インスタンス名がある場合はインスタンス名も含む ）を入力します。例：SQLTest.domain.com\DellDB。

IP アドレスも使用できますが、デルは、完全修飾ドメインネームを使用することを推奨します。

2 *サーバーポート：* フィールドにポート番号を入力します。

デフォルト以外の SQL Server インスタンスを使用するときは、ポート：フィールドでインスタンスの動的ポートを指定する必要があります。その代替として、SQL Server Browser サービスを有効化して、UDP ポート 1434 が開放されていることを確認します。詳細については https://msdn.microsoft.com/en-us/library/hh510203(v=sql.120).aspx を参照してください。

3 *データベース* フィールドに、データベースの名前を入力します。

4 認証 ：フィールドで、**Windows 認証** または **SQL Server 認証** を選択します。Windows 認証を選択すると、Windows へのログイン時に使用されたものと同じ資格情報が認証に使用されます（ ユーザ名 フィールドと パスワード フィールドは編集できなくなります ）。

5 *ユーザー名：* フィールドには、このデータベースに関連付けられている適切なユーザー名を入力します。

6 *パスワード：* フィールドに、ユーザー名 フィールドにリストされたユーザー名のパスワードを入力します。

7 最上部のメニューから **設定** > **保存** を選択します。プロンプトが表示されたら、保存を確定します。

8 データベース設定をテストするには、最上部メニューから、**アクション** > **データベース設定のテスト** を選択します。設定ウィザードが起動します。

9 設定のテストウィンドウでテストに関する情報を読み、**次へ** をクリックします。

10 データベース タブで Windows 認証 を選択した場合は、任意で代替の資格情報を入力し、Dell Enterprise Server の実行に使用されるものと同じ資格情報の使用を許可することができます。**次へ** をクリックします。

11 設定のテストウィンドウに、接続設定テスト、互換性テスト、およびデータベース移行テストの結果が表示されます。

12 **終了** をクリックします。

メモ:

SQL データベース、または SQL インスタンスのどちらかが非デフォルトの照合順序で設定されている場合は、非デフォルトの照合順序が大文字と小文字を区別するものである必要があります。照合順序のリストと、大文字と小文字の区別については、https://msdn.microsoft.com/en-us/library/ms144250(v=sql.105).aspx を参照してください。

変更が完了したら、次の手順に従います。

1 最上部のメニューから **設定** > **保存** を選択します。プロンプトが表示されたら、保存を確定します。

2 Dell サーバー設定ツールを閉じます。

3 **スタート** > **ファイル名を指定して実行** をクリックします。*services.msc* と入力し、**OK** をクリックします。サービス が開いたら、各 Dell サービスに移動し、**サービスの開始** をクリックします。

データベースの移行

最新バージョンのサーバー設定ツールを使用して、v8.x データベースと最新のスキーマに移行することができます。最新のサーバー設定ツールを入手、または v8.0 より前のデータベースに移行するには、デル ProSupport に問い合わせてサポートを受けてください。

サーバー設定ツールで、データベースタブをクリックします。

1 既存の Dell データベースをまだバックアップしていない場合は、**今すぐ行ってください**。

2 最上部のメニューから、**アクション** > **データベースの移行** を選択します。設定ウィザードが起動します。

3 エンタープライズデータベースの移行ウィンドウに警告が表示されます。データベース全体をバックアップ済みか、既存のデータベースのバックアップを取る必要がないことを確認してください。**次へ** をクリックします。

データベースの移行ウィンドウに、移行の状態を示す情報メッセージが表示されます。

完了したら、エラーがないか確認します。

メモ: エラーメッセージに  **が付いている場合は、データベースタスクが失敗しており、是正処置を取らなければデータベースの移行を適切に実行できません。完了 をクリックして、データベースエラーを修正し、本項の手順を再度開始します。**

4 **終了** をクリックします。

移行が完了したら、以下の操作を実行します。

1 最上部のメニューから **設定** > **保存** を選択します。プロンプトが表示されたら、保存を確定します。

2 Dell サーバー設定ツールを閉じます。

3 **スタート** > **ファイル名を指定して実行** をクリックします。*services.msc* と入力し、**OK** をクリックします。サービス が開いたら、各 Dell サービスに移動し、**サービスの開始** をクリックします。

6

管理作業

Dell 管理者役割の割り当て

1 Dell 管理者として、このアドレスにてリモート管理コンソールにログインします : https://server.domain.com:8443/webui/ 。デフォルトの資格情報は **superadmin/changeit** です。
2 左ペインで **ポピュレーション** > **ドメイン** をクリックします。
3 ユーザーを追加する対象であるドメインをクリックします。
4 ドメイン詳細 ページで、**メンバー** タブをクリックします。
5 **ユーザーの追加** をクリックします。
6 ユーザー名を共通名、UPN (Universal Principal Name)、または sAMAccountName で検索するためのフィルタを入力します。ワイルドカード文字は * です。

共通名、UPN (Universal Principal Name)、および sAMAccountName は、各ユーザーのエンタープライズディレクトリサーバーで定義されている必要があります。ユーザーがドメインまたはグループのメンバーであるにもかかわらず、管理のドメインまたはグループのメンバーリストに表示されない場合は、エンタープライズディレクトリサーバーでそのユーザーの 3 つの名前がすべて正しく定義されていることを確認してください。

クエリでは、一致が見つかるまで、共通名、UPN、sAMAccountName の順に自動的に検索します。

7 ディレクトリユーザーリストから、ドメインに追加するユーザーを選択します。複数のユーザーを選択するには、<Shift><click> または <Ctrl><click> を使用します。
8 **追加** をクリックします。
9 メニューバーから、指定したユーザーの **詳細とアクション** タブをクリックします。
10 メニューバーをスクロールして、**管理者** タブを選択します。
11 管理者の役割を選択して、このユーザーに追加します。
12 **保存** をクリックします。

Dell 管理者役割でのログイン

1 リモート管理コンソール Enterprise Server からログアウトします。
2 リモート管理コンソール Enterprise Server にログインし、ドメインユーザー証明書でログインします。

クライアントアクセスライセンスのアップロード

クライアントアクセスライセンスは、初回購入時またはクライアントアクセスライセンスを追加した場合には初回購入後に、インストールファイルとは別に付与されています。

1 左側のペインで、**管理** をクリックします。
2 **ライセンス管理** をクリックします。
3 **ファイルを選択する** をクリックし、クライアントライセンス ファイルを探して選択します。

ポリシーのコミット

インストールが完了したらポリシーをコミットします。

ポリシーの変更を保存し、ポリシーのインストール後、またはそれ以後にポリシーをコミットするには、次の手順に従います。

1 左側のペインで、**管理** > **コミット** をクリックします。
2 コメント フィールドで変更の説明を入力します。
3 **ポリシーのコミット** をクリックします。

Dell Compliance Reporter の設定

1 左側のペインで、**Compliance Reporter** をクリックします。
2 Dell Compliance Reporter が起動されたら、デフォルトの資格情報 *superadmin/changeit* を使用してログインします。
3 2 つの異なる認証方法がサポートされます。設定するには、次のいずれかを選択します。

- Compliance Reporter を使用した SQL 認証の設定
- Compliance Reporter を使用した Windows 認証の設定

Compliance Reporter を使用した SQL 認証の設定

v8.1 では、データソースはデフォルトで事前に設定されています。設定を行う必要はありません。次の手順を使用してデータソースを変更します（必要な場合）。

1 データソースを設定するには、最上部のメニューで **設定** をクリックします。左側のメニューで、**データソース** をクリックします。
2 Dell データベースへのログインに使用するユーザー名を入力します。
3 Dell データベースへのログインに使用するパスワードを入力します。
4 Dell データベースへのログインに使用するホスト名を入力します。
5 Dell データベースへのログインに使用するデータベース名を入力します。
6 許容される最大アイドル接続時間を入力します。デフォルトは 2 です。
7 許容される最大接続数（アクティブ）を入力します。デフォルトは 10 です。
8 最大待機時間（接続を待機するミリ秒単位の最大時間）を入力します。-1 は無制限です。
9 データベース URL を検証し、Dell Compliance Reporter と Dell データベースの接続をテストするには、**接続のテスト** をクリックします。
10 **アップデート** をクリックします。情報を破棄するには、キャンセル をクリックします。
管理タスクが完了しました。本章の残りの部分では、Windows 認証について説明します。SQL 認証が Dell Compliance Reporter に使用されている場合は、省略できます。

必要な場合は、「自己署名証明書の作成と証明書署名要求の生成」または「証明書管理コンソールを使用した証明書の .PFX へのエクスポート」に進みます。

Compliance Reporter を使用した Windows 認証の設定

v8.1 では、データソースはデフォルトで事前に設定されています。設定を行う必要はありません。次の手順を使用してデータソースを変更します（必要な場合）。

1 Dell データベースへのログインに使用するユーザー名を入力します。
2 パスワードは空白のままにしてください。ドメインユーザーがログインすると、ユーザーのパスワードがデータベースに渡されます。
3 Dell データベースへのログインに使用するホスト名を入力します。
4 Dell データベースへのログインに使用するデータベース名を入力します。
5 許容される最大アイドル接続時間を入力します。デフォルトは 2 です。
6 許容される最大接続数（アクティブ）を入力します。デフォルトは 10 です。
7 最大待機時間（接続を待機するミリ秒単位の最大時間）を入力します。-1 は無制限です。
8 データベース URL を検証し、Dell Compliance Reporter と Dell データベースの接続をテストするには、**接続のテスト** をクリックします。

9 **アップデート** をクリックします。情報を破棄するには、キャンセル をクリックします。

管理タスクが完了しました。**必要な場合**は、「自己署名証明書の作成と証明書署名要求の生成」または「証明書管理コンソールを使用した証明書の .PFX へのエクスポート」に進みます。

バックアップの実行

災害復旧目的のため、次の場所が夜間に作成される差分で毎週バックアップされるようにしてください。

Enterprise Server のバックアップ

インストール中（27 ページ の 手順 10 ）、またはアップグレード / 移行中（68 ページ の 手順 6 ）に設定ファイルのバックアップ用に選択した場所に、保存したファイルを定期的にバックアップしてください。このデータはほとんど変更されることがなく、必要に応じて手動で再設定できるため、週次バックアップでも十分です。最も重要なファイルには、データベースに接続するための情報が保存されています。

<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

SQL Server のバックアップ

トランザクションログを有効にして、夜間の完全バックアップを実行し、3 ~ 4 時間ごとに差分データベースバックアップを実行します。バックアップデータベースが使用可能な場合、トランザクションログおよび/またはログ配布タスクは 15 分 (可能な場合はそれ以下) 間隔で実行することが推奨されます。通常通り、データベースのベストプラクティスを Dell データベースに使用し、組織の災害復旧計画に Dell ソフトウェアを含めることが推奨されます。

SQL Server のベストプラクティスの追加情報については、「次のリストは、SQL Server ベストプラクティスを説明しています。ベストプラクティスがまだ実装されていない場合は、Dell Data Protection のインストール時に実装するようにしてください」を参照してください。

PostgreSQL Server のバックアップ

日常的にバックアップする必要がある、監査イベントは、PostgreSQL サーバに保存されます。バックアップ手順については、「https://www.postgresql.org/docs/9.5/static/backup.html」を参照してください。

デルでは、データベースのベストプラクティスを PostgreSQL データベースに使用し、組織の災害復旧計画にデルソフトウェアを含めることを推奨します。

7

Dell コンポーネントの説明

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	説明	必須とされる機能
Compliance Reporter	監査とコンプライアンスのレポートにより、環境の詳細なビューを提供します。 Dell Enterprise Server のコンポーネントです。	レポート
Key Server	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。 Dell Enterprise Server のコンポーネントです。	Dell 管理ユーティリティー
サーバー設定ツール	Core Server および Compatibility Server/ Security Server とのデータベース通信を設定します。インストール時のデータベースの初期化、または新しいスキーマへのデータベースの移行に使用されます。Dell サービスの制御に使用します。 Dell Enterprise Server のコンポーネントです。	すべて
リモート管理コンソール Enterprise Server 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。 Dell Enterprise Server のコンポーネントです。	すべて
Core Server	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 Protection 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。 Dell Enterprise Server のコンポーネントです。	すべて
Security Server	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 通信を管理します。SQL データベースアクセスが必要です。 Dell Enterprise Server のコンポーネントです。	すべて
Compatibility Server	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	すべて

名前	説明	必須とされる機能
	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。 Dell Enterprise Server のコンポーネントです。	
Message Broker サービス	Enterprise 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。 SQL データベースアクセスが必要です。 Dell Enterprise Server のコンポーネントです。	すべて
Device Server	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。 Dell Enterprise Server のコンポーネントです。	Mac 用の Enterprise Edition Windows 用の Enterprise Edition Handheld Shield CREDActivate
Device Server プラグイン	さまざまなコンポーネントをサポートします。 Dell Enterprise Server のコンポーネントです。	すべて
Identity Server	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。 Dell Enterprise Server のコンポーネントです。	すべて
Policy Proxy	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。 Dell Enterprise Server のコンポーネントです。	Mac 用の Enterprise Edition Windows 用の Enterprise Edition Mobile Edition for Mobile Device Security
セキュリティトークンサービス (STS)	Dell Enterprise Server ユーザーインタフェースと Dell バックエンドサービス間の安全な認証チャネルの作成を支援するために使用されます。	すべて
EAS Device Manager	無線機能を有効にします。Exchange クライアントアクセスサーバーにインストールされています。	モバイルデバイスの Exchange ActiveSync 管理。
EAS メールボックスマネージャ	Exchange メールボックスサーバーにインストールされたメールボックスエージェント。	モバイルデバイスの Exchange ActiveSync 管理。

8

SQL Server ベストプラクティス

次のリストは、SQL Server ベストプラクティスを説明しています。ベストプラクティスがまだ実装されていない場合は、Dell Data Protection 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 - http://technet.microsoft.com/en-us/library/ms190969%28v=sql.100%29
- Microsoft SQL Server 2008 R2 - http://technet.microsoft.com/en-us/library/ms190969(v=sql.105).aspx

2 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」（サーバーメモリに関するサーバー構成オプション）を検索してください。

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

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

4 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。

9

証明書

自己署名証明書の作成と証明書署名要求の生成

このセクションでは、Java ベースのコンポーネントの自己署名証明書を作成する手順について詳しく説明します。このプロセスは、.NET ベースのコンポーネントの自己署名証明書の作成には使用 **できません**。

実稼動環境でない環境では自己署名証明書のみを推奨します。

組織で SSL サーバー証明書が必要な場合、または他の理由で証明書を作成する必要がある場合は、このセクションで、Keytool を使用した Java キーストアの作成プロセスが説明されています。

組織が認証にスマートカードを使用することを計画している場合は、Keytool を使用してスマートカードユーザーの証明書で使用される信頼の完全証明書チェーンをインポートする必要があります。

Keytool は、証明書署名要求 (CSR) の形式で、VeriSign® や Entrust® などの証明機関 (CA) に渡される秘密鍵を作成します。その後、CA はこの CSR に基づいて署名したサーバー証明書を作成します。サーバー証明書は、署名機関証明書とともにファイルにダウンロードされます。その後、証明書は cacerts ファイルにインポートされます。

新しいキーペアと自己署名証明書の生成

1 **conf** ディレクトリ (Dell Compliance Reporter、Dell Security Server、または Dell Device Server) に移動します。

2 デフォルトの証明書データベースをバックアップします。

スタート > **ファイル名を指定して実行** をクリックして、`move cacerts cacerts.old` と入力します。

3 Keytool をシステムパスに追加します。コマンドプロンプトで次のコマンドを入力します。

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

4 証明書を生成するため、次のようにして Keytool を実行します。

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

5 Keytool プロンプトが表示されたら次の情報を入力します。

> **メモ:**
> 設定ファイルは、編集する前にバックアップしてください。指定されたパラメータのみを変更してください。これらのファイル内のその他のデータ (タグを含む) を変更すると、システムの破損や障害が発生するおそれがあります。**デル**は、これらのファイルの許可されてない変更に起因する問題が、**Dell** Enterprise Server の再インストールなしで解決できることを保証できません。

- キーストアのパスワード : パスワードを入力し (サポートされていない文字は <>;&" ')、コンポーネント **conf** ファイル内の変数を次のように同じ値に設定します。

  <Compliance Reporter install dir>\conf\eserver.properties.Set the value eserver.keystore.password =

  <Device Server install dir>\conf\eserver.properties.Set the value eserver.keystore.password =

  <Security Server install dir>\conf\eserver.properties.Set the value eserver.keystore.password =

- 完全修飾サーバー名：現在作業中のコンポーネントがインストールされているサーバーの完全修飾名を入力します。この完全修飾名には、ホスト名とドメイン名を含めます（例：server.domain.com）。
- 組織単位：適切な値を入力します（例：セキュリティ）。
- 組織：適切な値を入力します（例：デル）。
- 市区町村：適切な値を入力します（例：Dallas）。
- 都道府県：省略形でない都道府県の名前を入力します（たとえば、Texas）。
- 2 文字の国コード。
- ユーティリティによって、情報が正しいことを確認するように求められます。情報が正しい場合は、はいと入力します。

  情報が正しくない場合は、no と入力します。Keytool は以前に入力された各値を表示します。**Enter** をクリックして値を受け入れるか、値を変更して **Enter** をクリックします。
- 別名のキーパスワード：ここに別のパスワードを入力しなかった場合は、このパスワードがデフォルトでキーストアのパスワードになります。

証明機関からの署名付き証明書の要求

次の手順に従って、「新しいキーペアと自己署名証明書の生成」で作成された自己署名付き証明書の証明書署名要求（CSR）を生成します。

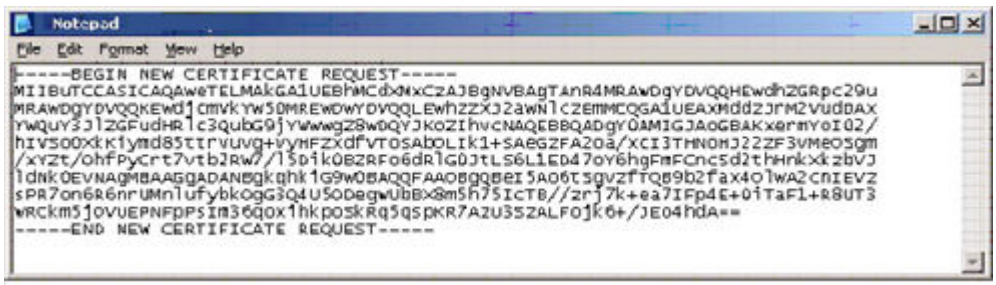
1 <**certificatealias**> で以前に使用した値と同じ値を代入します。

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

例：`keytool -certreq -sigalg SHA1withRSA -alias sslkey -keystore .\cacerts -file Dell.csr`

.csr ファイルには、CA 上での証明書の作成時に使用される BEGIN/END ペアが含まれます。

例 .CSR ファイル



2 証明機関からの SSL サーバー証明書の取得には、所属組織のプロセスに従います。署名用に <csr-filename> の内容を送信します。

> **メモ:**
> 有効な証明書を要求する方法は数通りあります。方法の例を、「**証明書の要求方法の例**」に示します。

3 署名付き証明書を受信したら、ファイルに保存します。

4 ベストプラクティスとして、インポートプロセスでエラーが発生した場合に備え、この証明書をバックアップします。このバックアップにより、プロセスをやり直す必要が生じるのを防ぐことができます。

ルート証明書のインポート

ルート証明書の証明機関が Verisign（Verisign Test ではない）の場合は、この手順をスキップして次の手順に進み、署名付き証明書をインポートしてください。

証明機関のルート証明書により、署名付き証明書を認証します。

1 次の**いずれか**を実行します。

- 証明機関のルート証明書をダウンロードして、ファイルに保存します。
- エンタープライズディレクトリサーバーのルート証明書を取得します。

2 次の**いずれか**を実行します。

- Dell Compliance Reporter、Dell Security Server、または Dell Device Server に対して SSL を有効にする場合は、コンポーネントの **conf** ディレクトリに変更します。
- Dell Enterprise Server とエンタープライズディレクトリサーバー間の SSL を有効にする場合は、< **Dell install dir>\Java Runtimes \jre1.x.x_xx\lib\security** に変更します（ JRE cacerts のデフォルトのパスワードは **changeit** です ）。

3 次のようにして Keytool を実行し、ルート証明書をインストールします。

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

例： `keytool -import -alias Entrust -keystore .\cacerts -file .\Entrust.cer`

証明書の要求方法の例

証明書の要求方法の 1 つの例は、Web ブラウザを使用して、組織によって社内的に設定されている Microsoft CA Server にアクセスする方法です。

1 Microsoft CA Server に移動します。IP アドレスは、組織によって提供されます。

2 **証明書の要求** を選択し、**次へ** をクリックします。

Microsoft 証明書サービス

3 **高度な要求** を選択し、**次へ** をクリックします。

Choose Request Type（ 要求タイプを選択する ）

4 **base64 エンコード PKCS #10 ファイルを使用して証明書要求を送信する** オプションを選択し、**次へ** をクリックします。

Advanced Certificate Request（ 高度な証明書の要求 ）

5 CSR 要求の内容をテキストボックスに貼り付けます。**Web Server** の証明書テンプレートを選択し、**送信** をクリックします。

Submit a Saved Request（ 保存した要求の提出 ）

6 証明書を保存します。**DER encoded** を選択し、**CA 証明書のダウンロード** をクリックします。

Download CA Certificate（ CA 証明書のダウンロード ）

7 証明書を保存します。**DER encoded** を選択し、**Download CA certification path** をクリックします。

Download CA Certification Path（ CA 証明パスのダウンロード ）

8 変換された署名機関証明書をインポートします。DOS ウィンドウに戻ります。タイプ：

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

9 署名機関証明書がインポートされたので、次にサーバー証明書をインポートできます（ 信頼チェーンを確立できます ）。タイプ：

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

自己署名証明書の別名を使用して、CSR 要求とサーバー証明書をペアにします。

10 cacerts ファイルのリストは、**サーバー証明書** が長さ **2** の証明書チェーンを持つことを示しています。これは、証明書が自己署名されていないことを示しています。タイプ：

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

チェーン内の 2 番目の証明書の証明書指紋は、インポートされた署名機関証明書です（リストのサーバー証明書の下にもリストされます）

証明書管理コンソールを使用した証明書の .PFX へのエクスポート

MMC で .crt ファイル形式の証明書がある場合は、Keytool で使用するためにその証明書を .pfx ファイルに変換する必要があります（Dell Security Server が DMZ モードで使用されるとき、および Dell Manager 証明書を Dell サーバー構成ツールにインポートするとき）。

1 Microsoft 管理コンソールを開きます。
2 **ファイル** > **スナップインの追加と削除** をクリックします。
3 **追加** をクリックします。
4 スタンドアロンスナップインの追加 ウィンドウで **証明書** を選択し、**追加** をクリックします。
5 **コンピュータアカウント** を選択し、**次へ** をクリックします。
6 コンピュータの選択ウィンドウで **ローカルコンピュータ（このコンソールが実行されているコンピュータ）** を選択し、**終了** をクリックします。
7 **閉じる** をクリックします。
8 **OK** をクリックします。
9 コンソールルートフォルダで、証明書（ローカルコンピュータ）を展開します。
10 パーソナルフォルダを展開し、必要な証明書を見つけます。
11 目的の証明書をハイライトし、**全てのタスク** > **エクスポート** を右クリックします。
12 証明書のエクスポートウィザードが開いたら、**次へ** をクリックします。
13 **はい、秘密キーをエクスポートします** を選択し、**次へ** をクリックします。
14 **Personal Information Exchange - PKCS #12（.PFX）** を選択してから、サブオプションの **可能な場合は証明書パスにすべての証明書を含める** と **すべての拡張プロパティをエクスポートする** を選択します。**次へ** をクリックします。
15 パスワードを入力し、確認します。ここにはどのようなパスワードを選んでも問題ありません。自分に覚えやすく、他人にはわかりにくいパスワードを選んでください。**次へ** をクリックします。
16 **参照** をクリックしてファイルを保存する場所を指定します。
17 *ファイル名* フィールドに、保存するファイルの名前を入力します。**保存** をクリックします。
18 **次へ** をクリックします。
19 **終了** をクリックします。

正しくエクスポートされたことを知らせるメッセージが表示されます。MMC を閉じます。

SSL に非信頼証明書が使用された場合の信頼署名証明書の Security Server への追加

1 Security Server サービスを停止します（実行されている場合）。
2 <Security Server install dir>\conf\ の cacerts ファイルをバックアップします。

Keytool を使用して次の手順を実行します。

3 信頼 PFX をテキストファイルに次の場所にエクスポートし、エイリアスを文書化します。

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

4 PFX を <Security Server install dir>\conf\ の cacerts ファイルにインポートします。

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

5 <Security Server install dir>\conf\application.properties で keystore.alias.signing の値を変更します。

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

Security Server サービスを開始します。