

Enterprise Vault™ アップグレードの手順

12.3

Enterprise Vault™: アップグレードの手順

最終更新日: 2018-03-16。

法的通知と登録商標

Copyright © 2018 Veritas Technologies LLC. All rights reserved.

Veritas、Veritas ロゴ、Enterprise Vault、Compliance Accelerator、Discovery Accelerator は、Veritas Technologies LLC または同社の米国およびその他の国における関連会社の商標または登録商標です。その他の会社名、製品名は各社の登録商標または商標です。

この製品には、Veritas 社がサードパーティへの帰属を示す必要があるサードパーティソフトウェア (「サードパーティプログラム」) が含まれる場合があります。一部のサードパーティプログラムはオープンソースまたは無償ソフトウェアライセンスの下で利用できます。ソフトウェアに付属している使用許諾契約は、それらのオープンソースまたは無償ソフトウェアライセンスで規定されている権利または義務を変更するものではありません。この Veritas 製品に付属するサードパーティの法的通知文書は次の場所で入手できます。

<https://www.veritas.com/about/legal/license-agreements>

本書に記載する製品は、使用、コピー、頒布、逆コンパイルおよびリバース・エンジニアリングを制限するライセンスに基づいて頒布されています。Veritas Technologies LLC からの書面による許可なく本書を複製することはできません。

文書は「現状有姿のまま」提供され、市販性、特定目的との適合性または権利を侵害していないことを含むすべての明示または黙示の条件、表明および保証は、そのような免責が法的に無効であるとされた場合を除き、免責されます。VERITAS TECHNOLOGIES LLC は本書の供給、実行、または使用に関連した付随的、間接的な損害に対する責任を負わないものとします。本書に含まれる情報は、事前の通知なく変更される場合があります。

ライセンス対象ソフトウェアおよび資料は、FAR 12.212 の規定によって商用コンピュータソフトウェアとみなされ、場合に応じて、FAR セクション 52.227-19「Commercial Computer Software - Restricted Rights」、DFARS 227.7202「Commercial Computer Software and Commercial Computer Software Documentation」、その後継規制の規定により、Veritas がオンプレミスとして提供したか、ホストサービスとして提供したかにかかわらず、制限された権利の対象となります。米政府による本ソフトウェアの使用、修正、複製のリリース、実演、表示または開示は、本使用許諾契約の条項に従ってのみ行われるものとします。

Veritas Technologies LLC
500 E Middlefield Road
Mountain View, CA 94043

<https://www.veritas.com>

テクニカルサポート

テクニカルサポートは、世界中にサポートセンターを設けています。すべてのサポートサービスは、サポート契約と、その時点でのエンタープライズテクニカルサポートポリシーに従って提供されます。サポートサービスとテクニカルサポートに連絡する方法について詳しくは、次の当社の Web サイトを参照してください。

https://www.veritas.com/support/ja_JP.html

次の URL で Veritas Account の情報を管理できます。

<https://my.veritas.com>

既存のサポート契約に関して当社に問い合わせる場合は、次に示すご利用の地域のサポート契約管理チームに電子メールでお問い合わせください。

全世界 (日本以外)

CustomerCare@veritas.com

日本

CustomerCare_Japan@veritas.com

テクニカルサポートに連絡する前に、Veritas Quick Assist (VQA) ツールを実行して製品のマニュアルに記載されているシステムの必要条件を満たしていることを確認してください。VQA は Veritas サポート Web サイトの次の記事からダウンロードできます。

https://www.veritas.com/support/en_US/vqa

マニュアル

最新版のマニュアルを確認してください。各マニュアルの 2 ページ目に最終更新日が表示されています。最新のマニュアルは Veritas の Web サイトで入手できます。

https://www.veritas.com/support/ja_JP/article.100040095

マニュアルのフィードバック

お客様のフィードバックは当社の財産です。改善点のご指摘やマニュアルの間違い、脱字などのご報告をお願いします。その際、マニュアルのタイトル、バージョン、章タイトル、セクションタイトルも合わせてご報告ください。フィードバックは次のアドレスに送信してください。

evdocs@veritas.com

次の Veritas コミュニティサイトでマニュアルの情報を参照したり、質問することもできます。

<https://www.veritas.com/community>

目次

第 1 章	本書について	9
	本書について	9
	Enterprise Vault についての詳しい情報の入手先	9
	Enterprise Vault トレーニングモジュール	12
第 2 章	開始する前の確認事項	13
	サーバーのアップグレードの流れ	13
	マニュアル	13
第 3 章	アップグレードする場合の注意事項	14
	Compliance Accelerator または Discovery Accelerator を装備した環境 でのアップグレード順序	14
	コマンドラインからの Enterprise Vault のサイレントインストール	16
	Enterprise Vault サーバーへの Outlook のインストール	16
	Outlook 2013 SP1 または 2016 へのアップグレード	17
	Enterprise Vault Web アプリケーションのセキュリティ保護	18
	弱いプロトコルと暗号のブロック	19
	アイテムに保持期間を適用する場合の一貫性の向上	20
	移動されたアイテムの場所を更新する際の影響を制限する	22
	Windows Server 2016 での Microsoft ファイル分類インフラストラクチャを 使用した分類	23
	Data Classification Services は Enterprise Vault 12.3 で利用可能なす べての種類の保持カテゴリをサポートしない	23
	Enterprise Vault との eDiscovery プラットフォーム互換性	24
	Enterprise Vault 11.0 または 11.0.1 からアップグレードする場合の追加 の注意事項	24
	ボルトサービスアカウントに必要な新しい SQL 権限	24
	Enterprise Vault 12.3 に必要な一貫した SQL 照合	24
	Enterprise Vault 検索の高速参照を有効にする	24
	コンテンツの変換設定の自動移行	25
第 4 章	システムのアップグレード手順	27
	アップグレード処理の概要	27

第 5 章	Enterprise Vault サーバーの準備	29
	Enterprise Vault サーバーの準備について	29
	システムのバックアップ	30
	Enterprise Vault データのバックアップ	30
	変更した言語ファイルのバックアップ	30
	必要な Windows 機能のアップデート	31
	Enterprise Vault Deployment Scanner の実行	31
	データベースの権限の設定	32
	MSMQ キューを空にすることを許可します。	32
	アーカイブと有効期限の確認	33
第 6 章	単一サーバー: Enterprise Vault サーバーソフトウェアのアップグレード	34
	単一 Enterprise Vault サーバーのアップグレードについて	34
	単一サーバーへのインストール	34
	Enterprise Vault データベースのアップグレード	36
	アップグレードされた Enterprise Vault データベースのバックアップ	37
	すべての Enterprise Vault サービスの起動	37
第 7 章	複数サーバー: Enterprise Vault サーバーソフトウェアのアップグレード	38
	複数の Enterprise Vault サーバーのアップグレードについて	38
	複数サーバーへのインストール	38
	Enterprise Vault データベースのアップグレード	40
	アップグレードされた Enterprise Vault データベースのバックアップ	41
	すべての Enterprise Vault サービスの起動	41
第 8 章	Veritas Cluster Server: Enterprise Vault サーバーソフトウェアのアップグレード	42
	Veritas クラスターのアップグレードについて	42
	Enterprise Vault サーバーソフトウェアのインストール	43
	Enterprise Vault データベースのアップグレード	45
	アップグレードされた Enterprise Vault データベースのバックアップ	46
	すべての Enterprise Vault サービスの起動	46

第 9 章	Windows Server フェールオーバークラスタリング: Enterprise Vault サーバーソフトウェアのアップ グレード	47
	Windows Server フェールオーバークラスタのアップグレードについて	47
	Enterprise Vault サーバーソフトウェアのインストール	48
	Enterprise Vault データベースのアップグレード	50
	アップグレードされた Enterprise Vault データベースのバックアップ	51
	すべての Enterprise Vault サービスの起動	51
第 10 章	スタンドアロン管理コンソールのアップグレード	52
	スタンドアロン管理コンソールのアップグレードについて	52
	スタンドアロン管理コンソールのアップグレード (ウィザード)	53
	Enterprise Vault のインストール (コマンドライン)	53
	アクティブ化の設定ファイルの作成 (Windows 7 のみ)	54
第 11 章	Enterprise Vault Reporting のアップグレード	55
	Enterprise Vault Reporting のアップグレード	55
	Enterprise Vault Reporting コンポーネントのインストール	56
	Enterprise Vault Reporting 設定ユーティリティの実行	57
第 12 章	MOM と SCOM のアップグレード	58
	MOM のアップグレード	58
	Enterprise Vault SCOM Management Pack のアップグレード	58
	付属の Management Pack について	59
	アップグレード手順について	59
第 13 章	Exchange Server フォームのアップグレード	61
	Exchange Server フォームのアップグレードについて	61
第 14 章	Domino メールボックスアーカイブのアップグレード	62
	Domino メールボックスアーカイブのアップグレードについて	62
	EVInstall.nsf の実行に必要な Domino クライアントのバージョン	62
	Domino メールボックスアーカイブのアップグレードの準備	63
	Domino メールボックスアーカイブのアップグレード	64
	メールファイルに対する Domino アーカイブユーザーのアクセス権の付与	65
	内部メール受信者の識別	66

	Domino プロビジョニングタスクの実行	68
第 15 章	FSA エージェントのアップグレード	69
	FSA エージェントおよび Enterprise Vault サーバーの互換性のあるバージョン	69
	FSA エージェントのアップグレードについて	70
	高可用性のためにクラスタ化された FSA エージェントサービスのアップグレード	71
	管理コンソールからの Windows の対象ファイルサーバーの FSA エージェントのアップグレード	72
	管理コンソールからの FSA レポート用プロキシサーバーの FSA エージェントのアップグレード	73
	FSA エージェントの手動アップグレード	75
第 16 章	Enterprise Vault Office Mail App のアップグレード	76
	Enterprise Vault Office Mail App のアップグレードについて	76
第 17 章	OWA Extensions のアップグレード	77
	OWA Extensions のアップグレードについて	77
	Enterprise Vault OWA 2010 Extensions のアップグレード	77
第 18 章	SharePoint Server コンポーネントのアップグレード	79
	SharePoint コンポーネントのアップグレードについて	79
	Enterprise Vault SharePoint コンポーネントのアップグレード	80
第 19 章	SMTP アーカイブのアップグレード	81
	SMTP ジャーナルの種類の設定の確認	81
	サポート対象でないアーカイブの種類に割り当てられた SMTP ターゲットの検索	85
	プロビジョニンググループへの既存のターゲットの移行	86
	SMTP アーカイブタスクのアカウントの権限の確認	87
	[ジャーナルレポートの処理] SMTP ポリシーの詳細設定の確認	87
	[選択したジャーナルのアーカイブ] サイトの設定の確認	88
	Skype for Business アーカイブおよび SMTP アーカイブの実装	89
	レガシー SMTP アーカイブコンポーネントのアップグレードについて	89

第 20 章	Enterprise Vault Search を使うように Enterprise Vault サイトをアップグレード	90
	Enterprise Vault 検索について	90
	Enterprise Vault による検索のサーバー必要条件	91
	Enterprise Vault Search ポリシーの定義	91
	権限のある Enterprise Vault 検索ユーザーによる他のユーザーのメールボックスへのアイテムの復元の許可	93
	Enterprise Vault による検索用のプロビジョニンググループの設定	94
	Enterprise Vault が検索プロビジョニンググループを処理する順序の変更	95
	Enterprise Vault による検索用のクライアントアクセスプロビジョニングタスクの作成と設定	96
	Enterprise Vault Search に対するユーザーのブラウザの構成	97
	Windows 10 での信頼されていないフォントのブロック機能の設定	98
	Forefront TMG とそれに類似する環境で使う Enterprise Vault 検索の設定	99
	Enterprise Vault 検索モバイル版の設定	99
	Enterprise Vault 検索モバイル版のインストール前作業の実行	100
	Enterprise Vault 検索モバイル版のインストール	102
	Enterprise Vault 検索モバイル版に実行できるログイン試行の最大数の設定	104
	Enterprise Vault 検索モバイル版のインストールの確認	105
第 21 章	Enterprise Vault API アプリケーションのアップグレード	106
	Enterprise Vault API ランタイムを使用する任意のアプリケーションのアップグレード	106

本書について

この章では以下の項目について説明しています。

- [本書について](#)
- [Enterprise Vault についての詳しい情報の入手先](#)

本書について

このマニュアルでは、Enterprise Vault のアップグレード方法について説明します。

Enterprise Vault の新しいインストールを実行する場合は、ReadMeFirst ファイルを参照してください。Enterprise Vault リリースメディアの Veritas Enterprise Vault® Documentation フォルダにある『Veritas Enterprise Vault™ インストール/設定』のインストール手順に従います。

ReadMeFirst ファイルと『インストール/設定』ガイドの最新バージョンは、[ドキュメントライブラリ](#)から入手できます。

Enterprise Vault についての詳しい情報の入手先

[表 1-1](#) に、Enterprise Vault に付属のマニュアルの一覧を示します。このマニュアルは、Veritas [ドキュメントライブラリ](#)から PDF および HTML 形式でも入手可能です。

表 1-1 Enterprise Vault マニュアルセット

マニュアル	コメント
Veritas Enterprise Vault ドキュメントライブラリ	<p>横断検索の可能な Windows のヘルプ (.chm) 形式の次のドキュメントがすべて含まれています。Acrobat (.pdf) 形式のマニュアルへのリンクも含まれています。</p> <p>このライブラリには、次を含む複数の操作でアクセスできます。</p> <ul style="list-style-type: none"> ■ Windows エクスプローラで Enterprise Vault インストール先フォルダのサブフォルダ Documentation¥language¥Administration Guides を参照し、EV_Help.chm ファイルを開きます。 ■ 管理コンソールの [ヘルプ] メニューで [Enterprise Vault のヘルプ] をクリックします。
導入および計画	Enterprise Vault の機能の概要を説明します。
Deployment Scanner	Enterprise Vault をインストールする前に必要なソフトウェアと設定を確認する方法を説明します。
インストールおよび設定	Enterprise Vault の設定に関する詳細な情報を提供します。
アップグレードの手順	既存の Enterprise Vault インストールを最新バージョンにアップグレードする方法を説明します。
Domino サーバーアーカイブの設定	Domino メールファイルとジャーナルデータベースからアイテムをアーカイブする方法を説明します。
Exchange Server アーカイブの設定	Microsoft Exchange ユーザーメールボックス、ジャーナルメールボックス、パブリックフォルダからアイテムをアーカイブする方法を説明します。
ファイルシステムアーカイブ (FSA) の設定	ネットワークファイルサーバーに保存されているファイルをアーカイブする方法を説明します。
IMAP の設定	Exchange アーカイブとインターネットメールアーカイブへの IMAP クライアントアクセスを設定する方法を説明します。
SharePoint Server アーカイブの設定	Microsoft SharePoint サーバーの文書をアーカイブする方法を説明します。
Skype for Business のアーカイブの設定	Skype For Business のセッションをアーカイブ化する方法を説明します。
SMTP アーカイブの設定	他のメッセージングサーバーから SMTP メッセージをアーカイブする方法を説明します。

マニュアル	コメント
Microsoft ファイル分類インフラストラクチャを使用した分類	Windows Server の新しいエディションに組み込まれた分類エンジンを使用して、新規と既存のすべてのアーカイブ済みコンテンツを分類する方法について説明します。
Veritas Information Classifier を使用した分類	Veritas Information Classifier を使用して、業界標準の分類ポリシーの包括的なセットを基準に新規とアーカイブ済みのすべてのコンテンツを評価する方法について説明します。Enterprise Vault を使用した分類を初めて行う場合は、以前の直観的でないファイル分類インフラストラクチャエンジンではなく、Veritas Information Classifier の使用をお勧めします。
管理者ガイド	日常的な管理を実行する方法を説明します。
PowerShell コマンドレット	Enterprise Vault PowerShell コマンドレットを実行して、さまざまな管理タスクを実行する方法を説明します。
監査	Enterprise Vault サーバー上でイベントの監査情報を収集する方法を説明します。
バックアップと回復	システムエラーが起きた場合にデータ損失を防止する効果的なバックアップ戦略の実装方法や、回復手段を利用する方法を説明します。
レポート	Enterprise Vault サーバー、アーカイブ、アーカイブ済みアイテムの状態に関するレポートを提供する、Enterprise Vault Reporting の実装方法を説明します。FSA レポートを設定すると、ファイルサーバーとそのボリューム用の追加レポートを利用できます。
NSF 移行	Domino ファイルと Notes NSF ファイルから内容を Enterprise Vault アーカイブにインポートする方法を説明します。
PST 移行	Outlook PST ファイルから内容を Enterprise Vault アーカイブに移行する方法を説明します。
ユーティリティ	Enterprise Vault のツールとユーティリティについて説明します。
レジストリ値	レジストリ値を一覧表示している参照用の文書で、さまざまな側面から Enterprise Vault の動作を修正する場合に使うことができます。
管理コンソールのヘルプ	Enterprise Vault 管理コンソールのヘルプ。
Enterprise Vault Operations Manager のヘルプ	Enterprise Vault Operations Manager のヘルプ。

サポートされているデバイスとソフトウェアのバージョンの最新情報について詳しくは、『Enterprise Vault [Compatibility Charts](#)』を参照してください。

Enterprise Vault トレーニングモジュール

Veritas 教育サービスでは、基本的な管理から詳細トピック、トラブルシューティングまで、Enterprise Vault の包括的なトレーニングを提供します。教室でのトレーニングや仮想トレーニングなど、さまざまな形式でトレーニングできます。

Enterprise Vault トレーニング、カリキュラムのパス、認定オプションについて詳しくは、<https://www.veritas.com/services/education-services> を参照してください。

開始する前の確認事項

この章では以下の項目について説明しています。

- [サーバーのアップグレードの流れ](#)
- [マニュアル](#)

サーバーのアップグレードの流れ

このマニュアルは Enterprise Vault 12.3 にアップグレードする方法を記述します。このバージョンにアップグレードできるのは、次のサーバーだけです。

- Enterprise Vault 11.0 または 11.0.1。
- Enterprise Vault 12.0 の最初のリリース、12.1、12.2。

メモ: インストールされた Enterprise Vault リリースの更新はアップグレードに影響しません。アップグレードの前に Enterprise Vault リリースの更新を削除する必要はありません。

マニュアル

Enterprise Vault のマニュアルは、Enterprise Vault メディアの Veritas Enterprise Vault\Documentation フォルダにあります。

サポートされているデバイスとソフトウェアのバージョンの最新情報については、『Enterprise Vault [Compatibility Charts](#)』を参照してください。

アップグレードする場合の注意事項

この章では以下の項目について説明しています。

- **Compliance Accelerator** または **Discovery Accelerator** を装備した環境でのアップグレード順序
- コマンドラインからの **Enterprise Vault** のサイレントインストール
- **Enterprise Vault** サーバーへの **Outlook** のインストール
- **Enterprise Vault Web** アプリケーションのセキュリティ保護
- 弱いプロトコルと暗号のブロック
- アイテムに保持期間を適用する場合の一貫性の向上
- **Windows Server 2016** での **Microsoft** ファイル分類インフラストラクチャを使用した分類
- **Data Classification Services** は **Enterprise Vault 12.3** で利用可能なすべての種類の保持カテゴリをサポートしない
- **Enterprise Vault** との **eDiscovery** プラットフォーム互換性
- **Enterprise Vault 11.0** または **11.0.1** からアップグレードする場合の追加の注意事項

Compliance Accelerator または Discovery Accelerator を装備した環境でのアップグレード順序

Compliance Accelerator と Discovery Accelerator 12.3 は、Enterprise Vault 11.0.1 以降と連携します。

アップグレードする順番

- 1 **Discovery Accelerator** を備えた環境の場合は、次の順序でアップグレードします。
 - **Discovery Accelerator** サーバーに **Discovery Accelerator 12.3** をインストールします。
 - **Discovery Accelerator** データベースをアップグレードします。
 - 各クライアントコンピュータに **Discovery Accelerator 12.3** クライアントソフトウェアをインストールします。
- 2 すべての **Enterprise Vault** サーバーで **Enterprise Vault** をバージョン **12.3** にアップグレードします。

メモ: **Compliance Accelerator** を備えた環境では、**Compliance Accelerator 12.3** にアップグレードするまで **Enterprise Vault** ストレージサーバーで **Enterprise Vault** ストレージサービスを開始しないでください。この順序でアップグレードすると、ランダムサンプリング機能がアップグレード前後にシームレスに働きます。

- 3 すべての **Compliance Accelerator** サーバーおよび **Discovery Accelerator** サーバーで **Enterprise Vault** をバージョン **12.3** にアップグレードします。
- 4 **Compliance Accelerator** を備えた環境の場合は、次の順序でアップグレードします。
 - **Compliance Accelerator** サーバーに **Compliance Accelerator 12.3** をインストールします。
 - **Compliance Accelerator** データベースをアップグレードします。
 - 各クライアントコンピュータに **Compliance Accelerator 12.3** クライアントソフトウェアをインストールします。

次の点に注意してください。

- **Enterprise Vault Storage** サーバーで **Enterprise Vault Storage** サービスを起動するのは、**Compliance Accelerator** を完全にアップグレードしてからにしてください。

サポート対象のバージョンとアップグレード方法について詳しくは、**Enterprise Vault Compatibility Charts** と「Supported upgrade paths for Enterprise Vault, Compliance Accelerator, Discovery Accelerator and Discovery Collector」(<https://www.veritas.com/docs/100023744>) の記事を参照してください。

Compliance Accelerator および **Discovery Accelerator** をアップグレードする方法について詳しくは、それぞれに付属するマニュアルを参照してください。

コマンドラインからの Enterprise Vault のサイレントインストール

Enterprise Vault のサイレントインストールのためのコマンドラインの構文が変更されました。現在は 2 つの新しいパラメータ、`/wait` および `/clone_wait` を含める必要があります。構文は次のとおりです。

```
start /wait "" "setup (x64).exe" /s /clone_wait  
/v"COMPONENTS=Option[|Option][...]"
```

詳しくは、『インストール/設定』ガイドの Enterprise Vault のインストール (コマンドライン) に関する項を参照してください。

Enterprise Vault サーバーへの Outlook のインストール

Exchange Server のアーカイブをサポートするには、Outlook を Enterprise Vault サーバーにインストールする必要があります。Enterprise Vault では現在 Outlook の次のバージョンをこの目的でサポートしています。

- Outlook 2013 SP1 (32 ビットバージョン)。
- Outlook 2016 (32 ビットバージョン)。16.0.4534.1001 以降のビルドバージョンが必要です。

どちらの場合も、Enterprise Vault は、ボリュームライセンスで利用可能な 32 ビット Outlook のバージョンの Windows インストーラ (MSI) をサポートします。Click-to-Run および 64 ビットバージョンはサポートしていません。Outlook のサポート対象バージョンの最新情報については、[Compatibility Charts](#) を参照してください。

Outlook を Enterprise Vault サーバーのデフォルトの電子メールクライアントにする必要があります。Enterprise Vault 管理サービスを起動すると、Outlook がデフォルトのクライアントとして設定されていることが確認されます。設定されていない場合は、デフォルトとして設定されます。

MAPI over HTTP および Outlook Anywhere (RPC over HTTP)

Exchange で有効にしたトランスポートプロトコル (MAPI over HTTP または Outlook Anywhere (以前の「RPC over HTTP」)) に合う Outlook のバージョンをインストールします。

表 3-1 Exchange トランスポートプロトコルおよび必要な Outlook のバージョン

Exchange のバージョン	Enterprise Vault サーバーの Outlook のバージョン	
	Outlook 2013 SP1	Outlook 2016
MAPI over HTTP が有効な Exchange Server 2013/2016	Enterprise Vault クライアントコンピュータから Exchange への MAPI over HTTP 接続はサポートされていますが、Enterprise Vault サーバー自体からの MAPI over HTTP 接続はサポートされていません。次の記事の指示に従って、サーバーの MAPI over HTTP を無効にします。 https://www.veritas.com/docs/100040583 MAPI over HTTP を無効にすると、Enterprise Vault は Exchange への接続を Outlook Anywhere に戻します。	サポート対象
Outlook Anywhere が有効な Exchange Server 2013/2016	サポート対象	サポートされていません。
RPC over HTTP が有効な Exchange Server 2010	サポート対象	サポートされていません。

パブリックフォルダのアーカイブ

Outlook 2013 SP1 を Enterprise Vault サーバーにインストールすることで、Exchange パブリックフォルダからのアーカイブもサポートできます。Outlook 2016 は、現在この用途にはサポートされません。

Outlook 2013 SP1 または 2016 へのアップグレード

メモ: Enterprise Vault サーバーに Outlook 2013 SP1 または 2016 がインストールされている場合は、Outlook のパフォーマンスカウンタを無効にする必要があります。Enterprise Vault サーバーに Outlook 2013 または 2016 を検出すると、Enterprise Vault 管理サービスは Outlook のパフォーマンスカウンタを自動的に無効にします。

Outlook 2013 SP1 または 2016 にアップグレードする方法

- 1 Enterprise Vault サーバー上で Enterprise Vault 管理サービスを停止します。
- 2 Outlook をインストールします。
- 3 すべての Enterprise Vault サービスを再起動します。

Enterprise Vault Web アプリケーションのセキュリティ保護

Enterprise Vault Web アプリケーションは IIS のデフォルト Web サイトで設定します。Enterprise Vault 12.3 以降の新規インストールでは、Enterprise Vault はデフォルトでポート 443 に HTTPS を設定し、各 Enterprise Vault 仮想ディレクトリで SSL を有効にします。

Enterprise Vault を 12.3 より前のバージョンからアップグレードしても、デフォルトの Web サイトおよび Enterprise Vault 仮想ディレクトリの既存の設定は変更されません。Enterprise Vault Web アプリケーションへの接続のセキュリティを確保するために、デフォルトの Web サイトで HTTPS バインドを手動で設定し、Enterprise Vault 仮想ディレクトリで SSL を有効にすることを強くお勧めします。次の手順では、これを行う方法について説明します。

クライアントが EnterpriseVault 仮想ディレクトリにアクセスするために使用するポートとプロトコルは、Enterprise Vault 管理コンソールのサイトプロパティの[全般]タブに表示されます。この設定を変更する前に、まず Enterprise Vault サイトの各サーバー上の IIS のデフォルト Web サイトに必要な変更を行ってください。

アイテムをアーカイブした後で、サイトプロパティのポートまたはプロトコルの設定を変更すると、既存のショートカットは動作しなくなります。Outlook と Notes のショートカットは、Enterprise Vault 管理コンソールのメールボックス同期機能を使って新しいプロトコルまたはポート情報に更新できますが、カスタマイズされたショートカット、FSA ショートカット、SharePoint ショートカットは更新できません。

証明書要求を作成し、IIS で SSL を実装する方法

- 1 SSL 証明書要求を作成して、信頼できる認証局に送信します。証明書には、Vault Site のエイリアス (Enterprise Vault サイトの DNS エイリアス) の短縮名と完全修飾ドメイン名の両方を含める必要があります。たとえば、EVServer1 と EVServer1.domain.com などが挙げられます。

適切なツールを使用して証明書を要求できます。たとえば、Enterprise Vault インストールフォルダにインストールした OpenSSL を使うことができます。Microsoft 管理コンソール (MMC) を使用して証明書要求を作成する方法については、<https://www.veritas.com/docs/100038186> のドキュメントを参照してください。

- 2 Enterprise Vault サーバーの IIS マネージャで次の手順を実行します。
 - サーバー証明書機能を使用して、新しい証明書をインストールします。
 - デフォルトの Web サイトにバインドしているサイトで、HTTPS プロトコルのバインドを追加して新しい証明書にリンクを作成します。デフォルト Web サイト用のプロトコルまたはポートを変更すると、Web サイトのすべての仮想ディレクトリに影響することに留意してください。

- 各 Enterprise Vault 仮想ディレクトリの [SSL 設定] ペインで、[SSL を要求] を選択します。

これらのタスクについては、<https://www.veritas.com/docs/100038186> のドキュメントも参照してください。

- 3 IIS で必要な変更を行ったら、Enterprise Vault 管理コンソールのサイトプロパティの [全般] タブで、ポートまたはプロトコルの設定を変更します。

弱いプロトコルと暗号のブロック

Enterprise Vault 12.3 の新規インストール、または Enterprise Vault 12.3 へのアップグレードを行う際、Enterprise Vault インストーラが弱いプロトコルと暗号を無効化するようになりました。Enterprise Vault は次のプロトコルを無効にします (これらを手動で有効化した場合を除く)。

- SSL 2.0
- SSL 3.0

弱いプロトコルは、

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols にあるレジストリ設定を使用して管理されます。前述の弱いプロトコルを手動で有効化した場合、レジストリ設定は Protocols サブキーの下にあります。この方法で有効にしたプロトコルは無効化されません。

メモ: 次の記事に示す手順に従って、TLS 1.0 プロトコルを手動で無効にすることもできます。

<https://www.veritas.com/docs/100041638>

TLS 1.0 を無効にすると、Enterprise Vault の一部の機能が正常に動作しない場合があります。前述の記事では、この機能を引き続き正常に動作させる方法を説明しています。

Enterprise Vault は次の暗号を無効にします。

- TLS_RSA_WITH_RC4_128_SHA
- TLS_RSA_WITH_RC4_128_MD5
- TLS_RSA_WITH_3DES_EDE_CBC_SHA

暗号は、HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Cryptography\Configuration\SSL\00010002 にあるレジストリ設定を使用して管理されます。

Enterprise Vault は、前述の弱い暗号をすべて無効にします。これは、Ciphers サブキーにあるレジストリ設定を使用して弱い暗号を有効にした場合でも当てはまります。

アイテムに保持期間を適用する場合の一貫性の向上

Vault Administration Console が変更されて、Enterprise Vault がアイテムに保持期間を適用する方法の一貫性とわかりやすさが向上しました。これらの変更の一部には、デフォルト動作に対する変更が含まれています。

表 3-2 管理コンソールの要素に対する変更

管理コンソールの要素	変更内容
<p>[Exchange メールボックスポリシー]ダイアログボックス > [既存のアイテム]タブ</p> <p>(Enterprise Vault 11.0 では、このタブは[移動されたアイテム])</p>	<p>このタブは削除されました。このタブの設定は、メールボックスフォルダ間でショートカットが移動されたアイテムに対する保持の割り当て方法に関連していました。この設定は、メールボックスフォルダ内の既存のショートカットアイテムにも適用されていました。[サイトプロパティ]ダイアログボックスの[アーカイブの設定]タブにある[既存のアイテムのカテゴリを更新]設定でも、このようなアイテムに対する保持の割り当て方法が制御されました。さまざまな設定名が存在し、それらの効果のさまざまな組み合わせが可能なことが、混乱を招いていました。</p> <p>このリリースでは、アイテムの移動動作を Enterprise Vault 全体で標準化しました。つまり、次のようになります。</p> <ul style="list-style-type: none"> ■ 移動したアイテムの場所は常に更新されます。 p.22 の「移動されたアイテムの場所を更新する際の影響を制限する」を参照してください。 ■ 移動したアイテムのカテゴリは更新されます。これは、サイトのアーカイブ設定と分類ポリシーの設定に従います。 ■ フォルダ内の他の既存アイテムのカテゴリは変更されません。 ■ 移動したアイテムのカテゴリは、元のカテゴリがユーザーによって選択されていた場合、カスタムフィルタによって設定されていた場合、または PST 移行によって設定されていた場合でも、更新されます。これもまた、サイトのアーカイブ設定と分類ポリシーの設定に従います。

管理コンソールの要素	変更内容
[サイトプロパティ]ダイアログボックス > [アーカイブの設定]タブ	<p>このタブの[ユーザー操作によってカテゴリを更新できるようにする]設定は、ユーザーがアーカイブ済みアイテムの保持カテゴリを更新する可能性のある操作を実行したときに Enterprise Vault が更新の実行を許可するかどうかを決定します。たとえば、ユーザーは、異なる保持カテゴリが適用されているフォルダ間でアーカイブ済みアイテムを移動することや、許可されている場合に Enterprise Vault Search でアイテムの保持カテゴリを変更することがあります。どちらの操作でも、アイテムの保持カテゴリが変更される可能性があります。次のオプションで、Enterprise Vault がこのようなアイテムの保持カテゴリを更新する状況を制御できるようになりました。</p> <ul style="list-style-type: none"> ■ 常に ■ アイテムの有効期限日が同じまたは以降か、レコードの種類が変更された場合
[分類ポリシープロパティ]ダイアログボックス > [設定]タブ	<p>このタブには、[ユーザー操作によって保持カテゴリが更新されないようにする]というオプションが追加されました。このオプションにより、Enterprise Vault 分類機能によってアーカイブ済みアイテムに割り当てられた保持カテゴリに対する不要な変更をブロックできます。たとえば、ユーザーがフォルダ間でアイテムを移動することによって、保持カテゴリが更新される可能性があります。</p> <p>すべての場合で保持カテゴリが更新されないようにすることができます。また、Enterprise Vault レコード管理機能を使用している場合は、アイテムのレコードタイプも変更されるときに保持カテゴリの更新を許可することができます。</p>

管理コンソールの要素	変更内容
<p>[保持カテゴリプロパティ]ダイアログボックス > [詳細]タブ</p> <p>(Enterprise Vault 12.1 以前では、このタブは[全般]と呼ばれていました)</p>	<p>このタブで利用可能なオプションは、次のとおりです。</p> <ul style="list-style-type: none"> ■ このカテゴリ内の期限切れアイテムの削除を禁止 ■ このカテゴリ内のアイテムのユーザーによる削除を禁止 <p>次の例について考えてみます。</p> <ul style="list-style-type: none"> ■ メールボックスフォルダ内のアイテムには、期限切れアイテムの自動削除時に保留が設定された保持カテゴリがあります。 ■ ユーザーは、このアイテムのショートカットを別のカテゴリが割り当てられたフォルダに移動します。フォルダのカテゴリには、保留が設定されていません。 <p>この場合、以前のリリースの Enterprise Vault はカテゴリを更新しませんでした。この動作が変更されました。Enterprise Vault は、ユーザー操作によってアイテムのカテゴリを更新できるようにするために、サイトと分類ポリシーの設定に従ってアイテムのカテゴリを更新します。この例では、カテゴリが更新されて、有効期限切れ時の自動削除の保留が解除されます。同様に、ユーザー操作によって、ユーザーによる削除を保留するよう指定する保持カテゴリから、保留しないよう指定する保持カテゴリに変更される可能性があります。このため、ユーザーによる削除の保留が解除されることがあります。</p>
<p>[検索ポリシープロパティ]ダイアログボックス > [機能]タブ</p>	<p>このタブには、[保持カテゴリの変更を許可]というオプションが追加されました。このオプションにより、Enterprise Vault Search ユーザーがそのアーカイブ内にあるアイテムの保持カテゴリを変更することを許可できます。デフォルトでは、このオプションはオフになっています。</p> <p>この設定は、上で説明されているサイトと分類ポリシーの設定に従います。</p>

Enterprise Vault 12.3 での保持の概要については、テクニカルノート「[Managing Retention](#)」を参照してください。

移動されたアイテムの場所を更新する際の影響を制限する

以前は、ユーザーがショートカットをメールボックスの別のフォルダに移動した場合に、**Enterprise Vault** によるアーカイブ内のアイテムの場所の更新を抑止できました。この機能を無効にするために、**Exchange Mailbox** ポリシーの[メールボックスに移動されたアイテムのアーカイブ場所を更新]は選択していませんでした。**Enterprise Vault 11.0** では、このオプションは[移動されたアイテム]タブにあります。**Enterprise Vault 12.0** では、このタブの名前が[既存のアイテム]に変更されました。

このリリースでは、**Enterprise Vault** は移動されたアイテムのアーカイブ場所を常に更新します。以前にこの機能を無効にし、メールボックスに多くのショートカットが含まれる場

合、Enterprise Vault はアップグレード後に移動されたアイテムのアーカイブ場所を更新しようとしています。メールボックスにすでに Enterprise Vault サーバーに対するアクセス不能な履歴ショートカットが含まれる場合、長いネットワークタイムアウトが発生することがあります。

このタイムアウトを防止するには、次の手順で説明されているように、有効なサイトエイリアスのリストを構成します。

有効なサイトエイリアスのリストの構成

- 1 Enterprise Vault 管理コンソールで、Exchange Mailbox ポリシーの[詳細]タブを開きます。
- 2 [一覧表示する設定の種類]で、[アーカイブ全般]を選択します。
- 3 [有効な Enterprise Vault サイトのエイリアス]を選択し、[変更]をクリックします。
- 4 有効なサイトエイリアスをセミコロンで区切ったリストを入力します。ショートカットの処理中に、Enterprise Vault はエイリアスがリストに記載されていないサイトへの接続を試みません。
- 5 [OK]をクリックしてダイアログボックスを閉じ、さらにプロパティを閉じます。
- 6 それぞれの Exchange Mailbox メールボックスポリシーに対して、前述の手順を繰り返します。

Windows Server 2016 での Microsoft ファイル分類インフラストラクチャを使用した分類

Microsoft ファイル分類インフラストラクチャを使用した Enterprise Vault 分類は、Windows Server 2016 ではサポートされません。

Data Classification Services は Enterprise Vault 12.3 で利用可能なすべての種類の保持カテゴリをサポートしない

Enterprise Vault 12.2 では、保持期間ではなく、固定の有効期限を指定する保持カテゴリを設定するオプションが導入されました。たとえば、固定の有効期限が 2021 年 12 月 31 日の保持カテゴリを作成して、この日に期限切れにするアイテムに保持カテゴリを割り当てることがことができます。

Enterprise Vault の Data Classification Services 機能では、固定の有効期限を指定した保持カテゴリをサポートしません。したがって、Data Classification Services で利用可能な保持カテゴリの一覧を定義する場合は、固定の有効期限を指定した保持カテゴリを除外する必要があります。

Enterprise Vault との eDiscovery プラットフォーム互換性

Enterprise Vault をアップグレードする前に、『[eDiscovery Platform Compatibility Matrix](#)』で Enterprise Vault との互換性の詳細を参照してください。

Enterprise Vault 11.0 または 11.0.1 からアップグレードする場合の追加の注意事項

Enterprise Vault 11.0 または 11.0.1 からアップグレードする場合は、次のセクションをお読みください。Enterprise Vault 12.0 オリジナルリリース以降からアップグレードする場合は、このセクションをスキップしても構いません。

ボルトサービスアカウントに必要な新しい SQL 権限

ボルトサービスアカウントには VIEW ANY DEFINITION 権限が必要です。詳しくは、『Veritas Enterprise Vault インストール/設定』ガイドの「SQL ログインアカウントの作成」を参照してください。

Enterprise Vault 12.3 に必要な一貫した SQL 照合

Enterprise Vault 12.3 では、マスターデータベースとすべての Enterprise Vault データベース全体の SQL で一貫した照合を実行する必要があります。一貫しない照合を実行するとアップグレードできないので、アップグレードの前に一貫した照合を実行する必要があります。一貫しない照合を修正する方法について詳しくは、次のテクニカルノートを参照してください。

<https://www.veritas.com/docs/100023860>

Enterprise Vault 検索の高速参照を有効にする

Enterprise Vault では、Enterprise Vault 検索で使用するためのメタデータインデックスを作成できます。これらのインデックスにより、アーカイブされた項目の高速参照が可能になります。アーカイブ用のメタデータインデックスがない場合、Enterprise Vault 検索はアーカイブ自体のインデックスを使用しますが、参照の速度は遅くなります。

Enterprise Vault はアーカイブの高速参照を自動的に有効化しません。

IMAP では常に高速参照が有効になっています。

高速参照を有効にするよう選択する場合は、次の方法で行うことができます：

- 管理コンソールを使用します。[サイトプロパティ]ダイアログボックスの[アーカイブ設定]タブで、特定のタイプのすべての新規または既存のアーカイブに対する高速参照

を有効にすることができます。たとえば、すべての **Exchange** メールボックスのアーカイブを有効にすることができます。

また、各アーカイブのプロパティを編集することで、アーカイブを個別に有効にすることができます。この方法は、数個のアーカイブを有効にする必要がある場合には適していません。

- **PowerShell cmdlet** を使用します。**New-EVMDSBuildTask cmdlet** を使用すると、多数のアーカイブの高速参照を有効にすることができます。

コンテンツの変換設定の自動移行

Enterprise Vault コンテンツ変換機能は、**Windows TIFF IFilter** 機能が提供する機能を使うように拡張されました。

以前はコンテンツの変換はレジストリ設定を使ってサーバーレベルで設定できました。このリリースではサイトレベルで設定します。そのため、**Enterprise Vault** サイトのストレージサーバー全体に一貫して実装されます。

この機能を使うには、**Enterprise Vault Administration Console** のサイトの詳細設定に新しい[コンテンツの変換]設定を追加します。アップグレード処理中に新しい設定がデフォルト値で各サイトに追加されます。

Enterprise Vault サーバーで以前に変換レジストリを設定している場合はアップグレード中に設定値が評価されます。サイトの各 **Enterprise Vault** サーバーで、既存のコンテンツの変換レジストリ設定を論理的にアップグレードして設定値が同等のサイト設定と一致する場合は削除します。サイト設定のデフォルト値とレジストリの設定値が異なる場合はレジストリの設定値がローカルの **Enterprise Vault** サーバーのサイト設定値のみを上書きします。

表 3-3 に、新しい[コンテンツの変換]のサイト設定と既存の変換のレジストリ設定の関連付けを示します。

表 3-3 [コンテンツの変換]のサイト設定とレジストリ設定

[コンテンツの変換]の詳しいサイトプロパティの設定名	関連付けられたレジストリ設定
変換から除外されるファイルの種類	Enterprise Vault¥ExcludedFileTypesFromConversion
テキストに変換されたファイルの種類	Enterprise Vault¥TextConversionFileTypes Enterprise Vault¥ConvertWordToText Enterprise Vault¥ConvertExcelToText Enterprise Vault¥ConvertRTFCoverToText
変換タイムアウト	Enterprise Vault¥ConversionTimeout

[コンテンツの変換]の詳しいサイトプロパティの設定名	関連付けられたレジストリ設定
アーカイブファイルの種類の変換タイムアウト	Enterprise Vault¥ ConversionTimeoutArchiveFiles
非表示のテキストを含める	Enterprise Vault¥ConversionIncludeHiddenText
非表示のスプレッドシートデータを含める	Enterprise Vault¥ ConversionIncludeHiddenSpreadsheetData
スプレッドシートの枠線の表示	Enterprise Vault¥ConversionSpreadsheetBorder
最大変換サイズ	Enterprise Vault¥MemLimitForTextConversionFallback
変換失敗イベントのログ	Storage¥FailedConversionEvents
テキストへのフォールバックイベントのログ	Storage¥FallbackConversionEvents
変換タイムアウトイベントのログ	Storage¥ConversionTimeoutEvents
ファイルの種類が認識されないイベントのログ	Storage¥UnrecognisedFileTypeEvents
最大変換サイズの超過イベントのログ	Storage¥RequestedAllocationSizeTooLargeEvents

システムのアップグレード手順

この章では以下の項目について説明しています。

- [アップグレード処理の概要](#)

アップグレード処理の概要

アップグレード処理の概要

- 1 お使いの環境に **Compliance Accelerator** または **Discovery Accelerator** が含まれている場合、これらのアプリケーションと **Enterprise Vault** をアップグレードする際の順序について理解しておく必要があります。

[p.14 の「Compliance Accelerator または Discovery Accelerator を装備した環境でのアップグレード順序」](#)を参照してください。
- 2 アップグレードに向けて **Enterprise Vault** サーバーを準備します。

[p.29 の「Enterprise Vault サーバーの準備について」](#)を参照してください。
- 3 各自のインストールに該当する章の説明に従って **Enterprise Vault** サーバーソフトウェアをインストールして設定します。

[p.34 の「単一 Enterprise Vault サーバーのアップグレードについて」](#)を参照してください。

[p.38 の「複数の Enterprise Vault サーバーのアップグレードについて」](#)を参照してください。

[p.42 の「Veritas クラスタのアップグレードについて」](#)を参照してください。

[p.47 の「Windows Server フェールオーバークラスタのアップグレードについて」](#)を参照してください。

- 4 Enterprise Vault 管理コンソールのみを実行しているコンピュータをアップグレードします。

p.52 の「[スタンドアロン管理コンソールのアップグレードについて](#)」を参照してください。

- 5 Enterprise Vault Reporting を実行しているコンピュータをアップグレードします。

p.55 の「[Enterprise Vault Reporting のアップグレード](#)」を参照してください。

- 6 必要に応じて、インストール後の作業を実行します。

- MOM と SCOM のアップグレード
p.58 の「[MOM のアップグレード](#)」を参照してください。
- Exchange Server フォームをアップグレードします。
p.61 の「[Exchange Server フォームのアップグレードについて](#)」を参照してください。
- Domino メールボックスアーカイブをアップグレードします。
p.62 の「[Domino メールボックスアーカイブのアップグレードについて](#)」を参照してください。
- FSA エージェントがインストールされている Windows サーバーの FSA エージェントをアップグレードします。
p.70 の「[FSA エージェントのアップグレードについて](#)」を参照してください。
- Enterprise Vault Office Mail App のアップグレード
p.76 の「[Enterprise Vault Office Mail App のアップグレードについて](#)」を参照してください。
- OWA Extensions をアップグレードします。
p.77 の「[OWA Extensions のアップグレードについて](#)」を参照してください。
- SharePoint Server コンポーネントをアップグレードします。
p.79 の「[SharePoint コンポーネントのアップグレードについて](#)」を参照してください。
- SMTP アーカイブをアップグレードします。
p.87 の「[SMTP アーカイブタスクのアカウントの権限の確認](#)」を参照してください。
- Enterprise Vault 検索を使用するために、Enterprise Vault サイトをアップグレードします。
p.90 の「[Enterprise Vault 検索について](#)」を参照してください。
- Enterprise Vault API アプリケーションをアップグレードします。
p.106 の「[Enterprise Vault API ランタイムを使用する任意のアプリケーションのアップグレード](#)」を参照してください。

Enterprise Vault サーバーの準備

この章では以下の項目について説明しています。

- [Enterprise Vault サーバーの準備について](#)
- [システムのバックアップ](#)
- [必要な Windows 機能のアップデート](#)
- [Enterprise Vault Deployment Scanner の実行](#)
- [データベースの権限の設定](#)
- [MSMQ キューを空にすることを許可します。](#)
- [アーカイブと有効期限の確認](#)

Enterprise Vault サーバーの準備について

Enterprise Vault ソフトウェアをアップグレードする前に、この章の説明に従ってアップグレードの準備を行う必要があります。

次の処理を記載順に実行します。

- システムをバックアップします。
p.30 の「[システムのバックアップ](#)」を参照してください。
- Enterprise Vault Deployment Scanner を実行します。
p.31 の「[Enterprise Vault Deployment Scanner の実行](#)」を参照してください。
- データベース権限を設定します。
p.32 の「[データベースの権限の設定](#)」を参照してください。
- MSMQ キューの削除を許可します。

p.32 の「[MSMQ キューを空にすることを許可します。](#)」を参照してください。

- アーカイブと有効期限を確認します。
p.33 の「[アーカイブと有効期限の確認](#)」を参照してください。
- Enterprise Vault が移動されたアイテムのアーカイブ場所を更新する際に、有効なサイトエイリアスを構成して影響を制限します。
p.20 の「[アイテムに保持期間を適用する場合の一貫性の向上](#)」を参照してください。

システムのバックアップ

Enterprise Vault のデータと変更したすべての言語ファイルをバックアップする必要があります。

SCOM を使っている場合、Management Pack のバックアップが必要になることがあります。

Enterprise Vault データのバックアップ

Enterprise Vault 環境をアップグレードする前に、通常のバックアップ手順に従って、すべての Enterprise Vault データをバックアップします。

『Veritas Enterprise Vault™ バックアップと回復』を参照してください。

メモ: データベースのバックアップを作成するときに、Veritas サポート Web サイトの次のテクニカルノートで説明しているデータベース保守の推奨手順を実行します。

<https://www.veritas.com/docs/100022023>

これらの保守の手順はデータベースを縮小し、テーブルのインデックスを再構築し、データベースの統計を更新します。そのような処理はもっとすばやく続行するためのデータベースのアップグレードを可能にします。

ボルトストアパーティションをバックアップすると、ストレージサービスによって関連するファイルがバックアップ済みとしてマーク付けされるため、WatchFile テーブルからエントリが削除されます。これらの作業は事前に定義された頻度でストレージサービスによって実行されます。アップグレードは、WatchFile テーブルのサイズが小さくなってから進めてください。そうしないと、アップグレード完了後のストレージサービスの再起動に時間がかかることがあります。<http://evserver/enterprisevault/usage.asp> にある使用状況レポートの [Awaiting Backup] 列で、ファイル数を確認することができます。

変更した言語ファイルのバックアップ

インストール手順によって、Enterprise Vault サーバーの次の言語フォルダが上書きされます。

Enterprise Vault¥Languages¥Mailbox Messages¥language

language は使用中の言語を示します。

インストールによって、Enterprise Vault フォルダ (たとえば C:¥Program Files (x86)¥Enterprise Vault) 内の使用中のファイルは修正されません。

language フォルダ内のファイルに適用した変更を維持する必要がある場合は、ファイルを別の場所にコピーしてください。

必要な Windows 機能のアップデート

Enterprise Vault インストールランチャーは、サーバーが必須条件となる Windows 機能を搭載していることを自動的に確認して、不足している機能を追加することができます。

インストールランチャーが追加可能な機能について詳しくは、「Enterprise Vault サーバーを自動的に準備する」(『インストールと設定』マニュアル)を参照してください。

[マイシステムの準備]オプションを実行する方法

- 1 サーバーに Enterprise Vault メディアをロードします。
- 2 Windows の自動再生がサーバーで有効になっている場合、Windows によって自動再生のダイアログボックスが表示されます。[Setup.exe の実行]をクリックします。
自動再生が有効になっていない場合、Windows エクスプローラでインストールメディアのルートフォルダを開き、Setup.exe ファイルをダブルクリックします。
インストールランチャーが開きます。
- 3 Install Launcher の左ペインのリストで、[Enterprise Vault]をクリックします。
- 4 [Server Preparation]をクリックします。
- 5 [Windows の機能]をクリックし、[マイシステムの準備]をクリックします。Windows の機能がすぐに追加され、メッセージは表示されません。機能が追加された後、サーバーは自動的に再起動される場合があります。

Enterprise Vault Deployment Scanner の実行

Enterprise Vault にアップグレードする前に、Deployment Scanner を実行して必要なソフトウェアと設定を確認することを推奨します。

Deployment Scanner を実行するときはボルトサービスアカウントを使ってください。

メモ: SQL Server を確認するように選択すると、レポートは[SQL databases contain entities with mixed collations]という警告を示すことがあります。問題を修正する方法について詳しくは次のテクニカルノートを参照してください。

<https://www.veritas.com/docs/100023860>

Deployment Scanner を実行した結果、設定を変更する場合は、必要に応じてシステムのバックアップを繰り返します。

Deployment Scanner を実行する方法

- 1 ボルトサービスアカウントへログインします。
- 2 Enterprise Vault メディアをロードします。
- 3 Windows の自動再生がサーバーで有効になっている場合、Windows によって自動再生のダイアログボックスが表示されます。[Setup.exe の実行]をクリックします。
自動再生が有効になっていない場合、Windows エクスプローラでインストールメディアのルートフォルダを開き、Setup.exe ファイルをダブルクリックします。
- 4 Veritas Enterprise Vault インストールランチャーウィンドウの左ペインで、Enterprise Vault、[サーバーの準備]の順にクリックします。
- 5 右ペインで[Deployment Scanner]、[Deployment Scanner の実行]の順にクリックします。Deployment Scanner が起動します。

データベースの権限の設定

Enterprise Vault をアップグレードする前に、ボルトサービスアカウントに必要なすべての権限が含まれていることを確認する必要があります。

ボルトサービスアカウントの権限は、『Veritas Enterprise Vault インストール/設定』の「SQL ログインアカウントの作成」セクションの手順で確認できます。

MSMQ キューを空にすることを許可します。

Enterprise Vault にアップグレードする前に、MSMQ キューを空にすることを推奨します。キューにまだアイテムがある Enterprise Vault をアップグレードする場合には、Enterprise Vault サービスはアップグレードの後で最初に開始するときにエラーイベントをログに記録することがあります。

アーカイブと有効期限の確認

アーカイブが開始される前に新しいインストールを確認する場合は、サーバーをアップグレードする前にアーカイブと有効期限を無効にします。インストールを確認したら、再度サーバーを有効にすることができます。

単一サーバー: Enterprise Vault サーバーソフトウェアのアップグレード

この章では以下の項目について説明しています。

- 単一 Enterprise Vault サーバーのアップグレードについて
- 単一サーバーへのインストール
- Enterprise Vault データベースのアップグレード
- アップグレードされた Enterprise Vault データベースのバックアップ
- すべての Enterprise Vault サービスの起動

単一 Enterprise Vault サーバーのアップグレードについて

この章では、Enterprise Vault サービスを実行するサーバーが 1 つのみである場合に Enterprise Vault サーバーソフトウェアとデータベースをアップグレードする方法について説明します。

この章の手順を記載順に実行します。

単一サーバーへのインストール

このセクションでは、Enterprise Vault サービスを実行するサーバーが 1 つのみである場合に Enterprise Vault サーバーソフトウェアをインストールする方法について説明します。

準備

単一サーバーで **Enterprise Vault** サーバーソフトウェアのアップグレードを準備する方法

- 1 ボルトサービスアカウントで **Enterprise Vault** サーバーにログインします。
- 2 **Enterprise Vault Admin Service** を停止します。これにより、**Admin Service** 自体と、他のすべての **Enterprise Vault** サービスが停止されます。
- 3 **Enterprise Vault** ファイルをロックする可能性があるその他のローカルまたはリモートのサービスまたはアプリケーションを停止します。次に例を示します。
 - **Enterprise Vault 管理コンソール**
 - **Enterprise Vault Accelerator Manager Service**
- 4 サーバーで実行されている他のアプリケーションを、コントロールパネル、コンピュータの管理、Windows サービス、Windows イベントビューアを含めすべて終了します。
- 5 **Enterprise Vault Domino Gateway** にインストールする場合は、**Enterprise Vault Domino Gateway** の **Domino** サーバーが停止していることと、ローカルで `EVInstall.nsf` がアクセスされていないことを確認します。

Enterprise Vault のインストール(ウィザード)

ウィザードを使って **Enterprise Vault** をインストールする方法

- 1 **Enterprise Vault** メディアをロードします。
- 2 **Windows** の自動再生がサーバーで有効になっている場合、**Windows** によって自動再生のダイアログボックスが表示されます。[**Setup.exe** の実行]をクリックします。
自動再生が有効になっていない場合、**Windows** エクスプローラでインストールメディアのルートフォルダを開き、`Setup.exe` ファイルをダブルクリックします。
- 3 [**Veritas Enterprise Vault Install Launcher**]ウィンドウの左ペインにあるリストで、[**Enterprise Vault**]をクリックします。
- 4 [サーバーのインストール]をクリックします。
- 5 右ペインで、[既存のサーバーのアップグレード]をクリックします。
- 6 [インストール]をクリックします。**Enterprise Vault** インストールウィザードが開始します。
- 7 インストールウィザードの手順に従って **Enterprise Vault** コンポーネントをアップグレードします。
- 8 インストールウィザードでサーバーの再起動を求めるメッセージが表示されたら、再起動してから、インストーラがアップグレードを完了できるようにボルトサービスアカウントとして再度ログインします。

Enterprise Vault のインストール(コマンドライン)

次の手順では、Enterprise Vault のインストールをアップグレードする方法について説明します。コンポーネントを追加または削除する場合は、『Veritas Enterprise Vault™ インストール/設定』の「Enterprise Vault のインストール」の章に記載されているコマンドラインオプションの詳しい説明を参照してください。

注意: サイレントインストール時にシステムの再起動が必要な場合は、サーバーが自動的に再起動します。サーバーが再起動したら、インストーラがアップグレードを完了できるようにボルトサービスアカウントで再度ログオンします。

コマンドラインを使って Enterprise Vault をインストールする方法

- 1 ボルトサービスアカウントで Enterprise Vault サーバーにログオンします。
- 2 Enterprise Vault メディアをロードします。
- 3 Windows の自動再生がサーバーで有効になっている場合、Windows によって自動再生のダイアログボックスが表示されます。自動再生のダイアログボックスを閉じます。
- 4 コマンドプロンプトウィンドウを開いて、Enterprise Vault メディアの次のフォルダに移動します。

```
¥Veritas Enterprise Vault¥Server¥x64
```

- 5 次のように `setup (x64).exe` を実行します。

```
"setup (x64).exe" /s
```
- 6 サーバーが再起動したら、インストーラがアップグレードを完了できるようにボルトサービスアカウントで再度ログオンします。

Enterprise Vault データベースのアップグレード

対象のサーバー上で Enterprise Vault サービスを開始する前に、Enterprise Vault データベースをアップグレードする必要があります。

Enterprise Vault には `Start-EVDatabaseUpgrade` という PowerShell コマンドレットが用意されています。このコマンドレットを使ってすべての Enterprise Vault データベースをアップグレードできます。

Enterprise Vault のデータベースをアップグレードする方法

- 1 対象の Enterprise Vault サーバーにボルトサービスアカウントを使ってログインします。
- 2 Enterprise Vault 管理シェルを実行します。

- 3 Enterprise Vault 管理シェルで、次のコマンドを実行します。

```
Start-EVDatabaseUpgrade
```

詳しい出力を表示する場合は `Start-EVDatabaseUpgrade -verbose` を実行することもできます。

- 4 `Start-EVDatabaseUpgrade` が終了するまで待機してすべてのデータベースのアップグレードを完了します。

アップグレードが完了したらアップグレードレポートでエラーを確認できます。

`Start-EVDatabaseUpgrade` は Enterprise Vault インストールフォルダ (たとえば、`C:\Program Files (x86)\Enterprise Vault`) の `Reports\DBUpgrade` サブフォルダにレポートを作成します。

アップグレードされた Enterprise Vault データベースのバックアップ

アップグレードされた Enterprise Vault データベースを次のようにバックアップします。

アップグレードされた Enterprise Vault データベースをバックアップする方法

- 1 Enterprise Vault サーバー上の Enterprise Vault サービスの実行を停止します。
- 2 すべての Enterprise Vault データベースをバックアップします。

すべての Enterprise Vault サービスの起動

対象のサーバー上の Enterprise Vault サービスすべてを起動します。

複数サーバー: Enterprise Vault サーバーソフトウェアのアップグレード

この章では以下の項目について説明しています。

- 複数の Enterprise Vault サーバーのアップグレードについて
- 複数サーバーへのインストール
- Enterprise Vault データベースのアップグレード
- アップグレードされた Enterprise Vault データベースのバックアップ
- すべての Enterprise Vault サービスの起動

複数の Enterprise Vault サーバーのアップグレードについて

この章では、Enterprise Vault サービスを実行する複数のサーバーがある場合に Enterprise Vault のサーバーソフトウェアとデータベースをアップグレードする方法について説明します。

この章の手順を記載順に実行します。

複数サーバーへのインストール

次の手順では、Enterprise Vault サービスを実行するすべてのサーバーに Enterprise Vault サーバーソフトウェアをインストールする方法について説明します。

Enterprise Vault サービスをインストールする各コンピュータで次の手順を実行します。

準備

Enterprise Vault サーバーソフトウェアのアップグレードを準備する方法

- 1 ボルトサービスアカウントで Enterprise Vault サーバーにログオンします。
- 2 Enterprise Vault Admin Service を停止します。これにより、Admin Service 自体と、他のすべての Enterprise Vault サービスが停止されます。
- 3 Enterprise Vault ファイルをロックする可能性があるその他のローカルまたはリモートのサービスまたはアプリケーションを停止します。次に例を示します。
 - Enterprise Vault 管理コンソール
 - Enterprise Vault Accelerator Manager Service
- 4 サーバーで実行されている他のアプリケーションを、コントロールパネル、コンピュータの管理、Windows サービス、Windows イベントビューアを含めすべて終了します。
- 5 Enterprise Vault Domino Gateway にインストールする場合は、Enterprise Vault Domino Gateway の Domino サーバーが停止していることと、ローカルで EVInstall.nsf がアクセスされていないことを確認します。

Enterprise Vault のインストール(ウィザード)

ウィザードを使って Enterprise Vault をインストールする方法

- 1 Enterprise Vault メディアをロードします。
- 2 Windows の自動再生がサーバーで有効になっている場合、Windows によって自動再生のダイアログボックスが表示されます。[Setup.exe の実行]をクリックします。
自動再生が有効になっていない場合、Windows エクスプローラでインストールメディアのルートフォルダを開き、Setup.exe ファイルをダブルクリックします。
- 3 [Veritas Enterprise Vault Install Launcher]ウィンドウの左ペインにあるリストで、[Enterprise Vault]をクリックします。
- 4 [サーバーのインストール]をクリックします。
- 5 右ペインで、[既存のサーバーのアップグレード]をクリックします。
- 6 [インストール]をクリックします。Enterprise Vault インストールウィザードが開始します。
- 7 インストールウィザードの手順に従って Enterprise Vault コンポーネントをアップグレードします。
- 8 インストールウィザードでサーバーの再起動を求めるメッセージが表示されたら、再起動してから、インストーラがアップグレードを完了できるようにボルトサービスアカウントとして再度ログオンします。

- 9 インストールの完了時に、インストーラによって Enterprise Vault サービスが再度有効になります。このときに Enterprise Vault サービスはどれも起動しないください。
- 10 Enterprise Vault サービスがインストールされるすべてのコンピュータで、この手順を繰り返します。

Enterprise Vault のインストール(コマンドライン)

次の手順では、Enterprise Vault のインストールをアップグレードする方法について説明します。コンポーネントを追加または削除する場合は、『Veritas Enterprise Vault™ インストール/設定』の「Enterprise Vault のインストール」の章に記載されているコマンドラインオプションの詳しい説明を参照してください。

注意: サイレントインストール時にシステムの再起動が必要な場合は、サーバーが自動的に再起動します。サーバーが再起動したら、インストーラがアップグレードを完了できるようにボルトサービスアカウントで再度ログオンします。

コマンドラインを使って Enterprise Vault をインストールする方法

- 1 ボルトサービスアカウントで Enterprise Vault サーバーにログオンします。
- 2 Enterprise Vault メディアをロードします。
- 3 Windows の自動再生がサーバーで有効になっている場合、Windows によって自動再生のダイアログボックスが表示されます。自動再生のダイアログボックスを閉じます。
- 4 コマンドプロンプトウィンドウを開いて、Enterprise Vault メディアの次のフォルダに移動します。

`¥Veritas Enterprise Vault¥Server¥x64`
- 5 次のように `setup (x64).exe` を実行します。

`"setup (x64).exe" /s`
- 6 サーバーが再起動したら、インストーラがアップグレードを完了できるようにボルトサービスアカウントで再度ログオンします。
- 7 インストールの完了時に、インストーラによって Enterprise Vault サービスが再度有効になります。このときに Enterprise Vault サービスはどれも起動しないください。
- 8 Enterprise Vault サービスがインストールされるすべてのコンピュータで、この手順を繰り返します。

Enterprise Vault データベースのアップグレード

Enterprise Vault サービスを開始する前に、Enterprise Vault データベースをアップグレードする必要があります。

メモ: 1 台の Enterprise Vault サーバーで次の手順を完了するだけです。

Enterprise Vault には Start-EVDatabaseUpgrade という PowerShell コマンドレットが用意されています。このコマンドレットを使ってすべての Enterprise Vault データベースをアップグレードできます。

Enterprise Vault のデータベースをアップグレードする方法

- 1 Enterprise Vault サーバーでボルトサービスアカウントを使ってログインします。
- 2 Enterprise Vault 管理シェルを実行します。
- 3 Enterprise Vault 管理シェルで、次のコマンドを実行します。

```
Start-EVDatabaseUpgrade
```

詳しい出力を表示する場合は `Start-EVDatabaseUpgrade -verbose` を実行することもできます。

- 4 Start-EVDatabaseUpgrade が終了するまで待機してすべてのデータベースのアップグレードを完了します。

アップグレードが完了したらアップグレードレポートでエラーを確認できます。

Start-EVDatabaseUpgrade は Enterprise Vault インストールフォルダ (たとえば、`C:\Program Files (x86)\Enterprise Vault\`) の `Reports\EBUpgrade` サブフォルダにレポートを作成します。

アップグレードされた Enterprise Vault データベースのバックアップ

アップグレードされた Enterprise Vault データベースを次のようにバックアップします。

アップグレードされた Enterprise Vault データベースをバックアップする方法

- 1 Enterprise Vault サーバー上の Enterprise Vault サービスの実行を停止します。
- 2 すべての Enterprise Vault データベースをバックアップします。

すべての Enterprise Vault サービスの起動

サイト内のすべての Enterprise Vault サーバーですべての Enterprise Vault サービスを起動します。

Veritas Cluster Server: Enterprise Vault サーバー ソフトウェアのアップグレー ド

この章では以下の項目について説明しています。

- [Veritas クラスタのアップグレードについて](#)
- [Enterprise Vault サーバーソフトウェアのインストール](#)
- [Enterprise Vault データベースのアップグレード](#)
- [アップグレードされた Enterprise Vault データベースのバックアップ](#)
- [すべての Enterprise Vault サービスの起動](#)

Veritas クラスタのアップグレードについて

この章では、Enterprise Vault タスクを実行するサーバーが Veritas クラスタの一部である場合に Enterprise Vault サーバーソフトウェアとデータベースをアップグレードする方法について説明します。

この章の手順を記載順に実行します。

Enterprise Vault サーバーソフトウェアのインストール

このセクションでは、Enterprise Vault タスクを実行するサーバーが Veritas クラスタの一部である場合に Enterprise Vault サーバーソフトウェアをインストールする方法について説明します。

Enterprise Vault では高可用性アップグレードがサポートされていないことに留意してください。Enterprise Vault サービスを起動する前、または設定ウィザードを実行する前に、クラスタ内のすべてのノードにサーバーソフトウェアをインストールする必要があります。

準備

Enterprise Vault サーバーソフトウェアのアップグレードを準備する方法

- 1 ボルトサービスアカウントとしてアクティブノードにログオンします。
- 2 VCS クラスタの管理ツールを使ってすべての Enterprise Vault サービスリソースをオフラインにします。

次の重要な点に注意してください。

- Enterprise Vault サイトのすべての Enterprise Vault サービスを停止する必要があります。たとえば、Enterprise Vault Domino Gateway などのクラスタ化されていないサーバーのサービスを停止します。
 - Enterprise Vault Domino Gateway にインストールする場合は、Enterprise Vault Domino Gateway の Domino サーバーが停止していることと、ローカルで `EVInstall.nsf` がアクセスされていないことを確認します。
 - Enterprise Vault Directory を共有するサイトが複数存在する場合は、他のサイトのすべての Enterprise Vault サービスも停止する必要があります。
- 3 Enterprise Vault ファイルをロックする可能性があるその他のローカルまたはリモートのサービスまたはアプリケーションを停止します。次に例を示します。
 - Enterprise Vault 管理コンソール
 - Enterprise Vault Accelerator Manager Service
 - 4 サーバーで実行されているアプリケーションを、コントロールパネル、コンピュータの管理、Windows サービス、Windows イベントビューアを含めすべて終了します。

Enterprise Vault のインストール(ウィザード)

ウィザードを使って Enterprise Vault をインストールする方法

- 1 Enterprise Vault メディアをロードします。
- 2 Windows の自動再生がサーバーで有効になっている場合、Windows によって自動再生のダイアログボックスが表示されます。[Setup.exe の実行]をクリックします。
自動再生が有効になっていない場合、Windows エクスプローラでインストールメディアのルートフォルダを開き、Setup.exe ファイルをダブルクリックします。
- 3 [Veritas Enterprise Vault Install Launcher]ウィンドウの左ペインにあるリストで、[Enterprise Vault]をクリックします。
- 4 [サーバーのインストール]をクリックします。
- 5 右ペインで、[既存のサーバーのアップグレード]をクリックします。
- 6 [インストール]をクリックします。Enterprise Vault インストールウィザードが開始します。
- 7 インストールウィザードの手順に従って Enterprise Vault コンポーネントをアップグレードします。
- 8 インストールウィザードでサーバーの再起動を求めるメッセージが表示されたら、再起動してから、インストーラがアップグレードを完了できるようにボルトサービスアカウントとして再度ログオンします。
- 9 クラスタフェールオーバーノードなど、Enterprise Vault 環境の他のサーバーに Enterprise Vault ソフトウェアをインストールします。

Enterprise Vault のインストール(コマンドライン)

次の手順では、Enterprise Vault のインストールをアップグレードする方法について説明します。コンポーネントを追加または削除する場合は、『Veritas Enterprise Vault™ インストール/設定』の「Enterprise Vault のインストール」の章に記載されているコマンドラインオプションの詳しい説明を参照してください。

注意: サイレントインストール時にシステムの再起動が必要な場合は、サーバーが自動的に再起動します。サーバーが再起動したら、インストーラがアップグレードを完了できるようにボルトサービスアカウントで再度ログオンします。

コマンドラインを使って Enterprise Vault をインストールする方法

- 1 ボルトサービスアカウントとしてアクティブノードにログオンします。
- 2 Enterprise Vault メディアをロードします。

- 3 Windows の自動再生がサーバーで有効になっている場合、Windows によって自動再生のダイアログボックスが表示されます。自動再生のダイアログボックスを閉じます。
- 4 コマンドプロンプトウィンドウを開いて、Enterprise Vault メディアの次のフォルダに移動します。

`¥Veritas Enterprise Vault¥Server¥x64`
- 5 次のように `setup (x64).exe` を実行します。

`"setup (x64).exe" /s`
- 6 インストールの完了時に、インストーラによって Enterprise Vault サービスが再度有効になります。このときに Enterprise Vault サービスはどれも起動しないください。
- 7 クラスタフェールオーバーノードなど、Enterprise Vault 環境の他のサーバーに Enterprise Vault ソフトウェアをインストールします。

Enterprise Vault データベースのアップグレード

Enterprise Vault サービスを開始する前に、Enterprise Vault データベースをアップグレードする必要があります。

メモ: アーカイブノードでこの手順を完了するだけでかまいません。

Enterprise Vault には `Start-EVDatabaseUpgrade` という PowerShell コマンドレットが用意されています。このコマンドレットを使ってすべての Enterprise Vault データベースをアップグレードできます。

Enterprise Vault のデータベースをアップグレードする方法

- 1 アーカイブノードでボルトサービスアカウントを使ってログインします。
- 2 Enterprise Vault 管理シェルを実行します。
- 3 Enterprise Vault 管理シェルで、次のコマンドを実行します。

```
Start-EVDatabaseUpgrade
```

詳しい出力を表示する場合は `Start-EVDatabaseUpgrade -verbose` を実行することもできます。

- 4 `Start-EVDatabaseUpgrade` が終了するまで待機してすべてのデータベースのアップグレードを完了します。

アップグレードが完了したらアップグレードレポートでエラーを確認できます。

Start-EVDatabaseUpgrade は Enterprise Vault インストールフォルダ (たとえば、`C:\Program Files (x86)\Enterprise Vault`) の `Reports\DBUpgrade` サブフォルダにレポートを作成します。

アップグレードされた Enterprise Vault データベースのバックアップ

アップグレードされた Enterprise Vault データベースを次のようにバックアップします。

アップグレードされた Enterprise Vault データベースをバックアップする方法

- 1 クラスタ管理ツールを使用して、実行中の Enterprise Vault サービスをオフラインにします。
- 2 すべての Enterprise Vault データベースをバックアップします。

すべての Enterprise Vault サービスの起動

サイト内のすべてのサーバーで Enterprise Vault サービスを起動します。

クラスタの管理ツールを使ってすべての Enterprise Vault サービスをオンラインにします。

Enterprise Vault Directory を共有するサイトが複数存在する場合は、他のサイトのすべての Enterprise Vault サービスを起動できます。

クラスタフェールオーバーが Enterprise Vault に対して正しく機能することをテストします。

Windows Server フェールオーバークラスタリング: Enterprise Vault サーバー ソフトウェアのアップグレード

この章では以下の項目について説明しています。

- [Windows Server フェールオーバークラスタのアップグレードについて](#)
- [Enterprise Vault サーバーソフトウェアのインストール](#)
- [Enterprise Vault データベースのアップグレード](#)
- [アップグレードされた Enterprise Vault データベースのバックアップ](#)
- [すべての Enterprise Vault サービスの起動](#)

Windows Server フェールオーバークラスタのアップグレードについて

この章では、Enterprise Vault タスクを実行するサーバーが Windows クラスタの一部である場合に Enterprise Vault サーバーソフトウェアとデータベースをアップグレードする方法について説明します。

この章の手順を記載順に実行します。

Enterprise Vault サーバーソフトウェアのインストール

このセクションでは、Enterprise Vault タスクを実行するサーバーが Windows Server フェールオーバークラスターの一部である場合に Enterprise Vault サーバーソフトウェアをインストールする方法について説明します。

Enterprise Vault では高可用性アップグレードがサポートされていないことに留意してください。Enterprise Vault サービスを起動する前、または設定ウィザードを実行する前に、クラスター内のすべてのノードにサーバーソフトウェアをインストールする必要があります。

準備

Enterprise Vault サーバーソフトウェアのアップグレードを準備する方法

- 1 ボルトサービスアカウントとしてアクティブノードにログオンします。
- 2 フェールオーバークラスターマネージャまたはコマンドラインユーティリティ `cluster` を使って管理サービスリソースをオフラインにします。これによって、すべての Enterprise Vault サービスがオフラインになります。

次の重要な点に注意してください。

- `EnterpriseVaultServerInstance` はオフラインにしないでください。
 - Enterprise Vault サイトのすべての Enterprise Vault サービスを停止する必要があります。たとえば、Enterprise Vault Domino Gateway などのクラスタ化されていないサーバーのサービスを停止します。
 - Enterprise Vault Domino Gateway にインストールする場合は、Enterprise Vault Domino Gateway の Domino サーバーが停止していることと、ローカルで `EVInstall.nsf` がアクセスされていないことを確認します。
 - Enterprise Vault Directory を共有するサイトが複数存在する場合は、他のサイトのすべての Enterprise Vault サービスも停止する必要があります。
- 3 Enterprise Vault ファイルをロックする可能性があるその他のローカルまたはリモートのサービスまたはアプリケーションを停止します。フェールオーバークラスターマネージャを使って、クラスタ化されたサービスを停止します。次に例を示します。
 - Enterprise Vault 管理コンソール
 - Enterprise Vault Accelerator Manager Service
 - 4 サーバーで実行されているアプリケーションを、コントロールパネル、コンピュータの管理、Windows サービス、Windows イベントビューアを含めすべて終了します。

Enterprise Vault のインストール(ウィザード)

ウィザードを使って **Enterprise Vault** をインストールする方法

- 1 Enterprise Vault メディアをロードします。
- 2 Windows の自動再生がサーバーで有効になっている場合、Windows によって自動再生のダイアログボックスが表示されます。[Setup.exe の実行]をクリックします。
自動再生が有効になっていない場合、Windows エクスプローラーでインストールメディアのルートフォルダを開き、Setup.exe ファイルをダブルクリックします。
- 3 [Veritas Enterprise Vault Install Launcher]ウィンドウの左ペインにあるリストで、[Enterprise Vault]をクリックします。
- 4 [サーバーのインストール]をクリックします。
- 5 右ペインで、[既存のサーバーのアップグレード]をクリックします。
- 6 [インストール]をクリックします。Enterprise Vault インストールウィザードが開始します。
- 7 インストールウィザードの手順に従って Enterprise Vault コンポーネントをアップグレードします。
- 8 インストールウィザードでサーバーの再起動を求めるメッセージが表示されたら、再起動してから、インストーラがアップグレードを完了できるようにボルトサービスアカウントとして再度ログオンします。
- 9 クラスタフェールオーバーノードなど、Enterprise Vault 環境の他のサーバーに Enterprise Vault ソフトウェアをインストールします。

Enterprise Vault のインストール(コマンドライン)

次の手順では、Enterprise Vault のインストールをアップグレードする方法について説明します。コンポーネントを追加または削除する場合は、『Veritas Enterprise Vault™ インストール/設定』の「Enterprise Vault のインストール」の章に記載されているコマンドラインオプションの詳しい説明を参照してください。

注意: サイレントインストール時にシステムの再起動が必要な場合は、サーバーが自動的に再起動します。サーバーが再起動したら、インストーラがアップグレードを完了できるようにボルトサービスアカウントで再度ログオンします。

コマンドラインを使って **Enterprise Vault** をインストールする方法

- 1 ボルトサービスアカウントとしてアクティブノードにログオンします。
- 2 Enterprise Vault メディアをロードします。

- 3 Windows の自動再生がサーバーで有効になっている場合、Windows によって自動再生のダイアログボックスが表示されます。自動再生のダイアログボックスを閉じます。
- 4 コマンドプロンプトウィンドウを開いて、Enterprise Vault メディアの次のフォルダに移動します。

`¥Veritas Enterprise Vault¥Server¥x64`
- 5 次のように `setup (x64).exe` を実行します。

`"setup (x64).exe" /s`
- 6 サーバーが再起動したら、インストーラがアップグレードを完了できるようにボルトサービスアカウントで再度ログオンします。
- 7 インストールの完了時に、インストーラによって Enterprise Vault サービスが再度有効になります。このときに Enterprise Vault サービスはどれも起動しないください。
- 8 クラスタフェールオーバーノードなど、Enterprise Vault 環境の他のサーバーに Enterprise Vault ソフトウェアをインストールします。

Enterprise Vault データベースのアップグレード

Enterprise Vault サービスを開始する前に、Enterprise Vault データベースをアップグレードする必要があります。

メモ: アーカイブノードでこの手順を完了するだけでかまいません。

Enterprise Vault には `Start-EVDatabaseUpgrade` という PowerShell コマンドレットが用意されています。このコマンドレットを使ってすべての Enterprise Vault データベースをアップグレードできます。

Enterprise Vault のデータベースをアップグレードする方法

- 1 アーカイブノードでボルトサービスアカウントを使ってログインします。
- 2 Enterprise Vault 管理シェルを実行します。
- 3 Enterprise Vault 管理シェルで、次のコマンドを実行します。

```
Start-EVDatabaseUpgrade
```

詳しい出力を表示する場合は `Start-EVDatabaseUpgrade -verbose` を実行することもできます。

- 4 `Start-EVDatabaseUpgrade` が終了するまで待機してすべてのデータベースのアップグレードを完了します。

アップグレードが完了したらアップグレードレポートでエラーを確認できます。

Start-EVDatabaseUpgrade は Enterprise Vault インストールフォルダ (たとえば、C:\Program Files (x86)\Enterprise Vault) の Reports\DBUpgrade サブフォルダにレポートを作成します。

アップグレードされた Enterprise Vault データベースのバックアップ

アップグレードされた Enterprise Vault データベースを次のようにバックアップします。

アップグレードされた Enterprise Vault データベースをバックアップする方法

- 1 Enterprise Vault サービスの実行を停止します。
- 2 すべての Enterprise Vault データベースをバックアップします。

すべての Enterprise Vault サービスの起動

サイト内のすべてのサーバーで Enterprise Vault サービスを起動します。

クラスタの管理ツールを使ってすべての Enterprise Vault サービスをオンラインにします。

Enterprise Vault Directory を共有するサイトが複数存在する場合は、他のサイトのすべての Enterprise Vault サービスを起動できます。

クラスタフェールオーバーが Enterprise Vault に対して正しく機能することをテストします。

スタンドアロン管理コンソールのアップグレード

この章では以下の項目について説明しています。

- [スタンドアロン管理コンソールのアップグレードについて](#)
- [スタンドアロン管理コンソールのアップグレード\(ウィザード\)](#)
- [Enterprise Vault のインストール\(コマンドライン\)](#)
- [アクティブ化の設定ファイルの作成 \(Windows 7 のみ\)](#)

スタンドアロン管理コンソールのアップグレードについて

Enterprise Vault 管理コンソールコンポーネントのみをインストールしているコンピュータを使っている場合は、このコンポーネントをアップグレードする必要があります。スタンドアロン管理コンソールでサポートされている Windows のバージョンは次のとおりです。

- Windows 7
- Windows 8
- Windows 8.1
- Windows 10
- Windows Server 2012
- Windows Server 2016

スタンドアロン管理コンソールのアップグレード(ウィザード)

スタンドアロン管理コンソールをアップグレードする方法

- 1 ボルトサービスアカウントでコンピュータにログオンします。
- 2 管理コンソールが実行されていないことを確認します。
- 3 Enterprise Vault メディアをロードします。
- 4 Windows の自動再生がサーバーで有効になっている場合、Windows によって自動再生のダイアログボックスが表示されます。[Setup.exe の実行]をクリックします。
自動再生が有効になっていない場合、Windows エクスプローラでインストールメディアのルートフォルダを開き、Setup.exe ファイルをダブルクリックします。
- 5 [Veritas Enterprise Vault Install Launcher]ウィンドウの左ペインにあるリストで、[Enterprise Vault]をクリックします。
- 6 [サーバーのインストール]をクリックします。
- 7 右ペインで、[既存のサーバーのアップグレード]をクリックします。
- 8 [インストール]をクリックします。Enterprise Vault インストールウィザードが開始します。
- 9 インストールの手順に従って管理コンソールコンポーネントをアップグレードします。
- 10 Windows 7 でのみ、アクティブ化の設定ファイルを作成します。
p.54 の「[アクティブ化の設定ファイルの作成 \(Windows 7 のみ\)](#)」を参照してください。

Enterprise Vault のインストール(コマンドライン)

管理コンソールをコマンドラインからアップグレードする方法

- 1 ボルトサービスアカウントでコンピュータにログオンします。
- 2 Enterprise Vault メディアをロードします。
- 3 Windows の自動再生がサーバーで有効になっている場合、Windows によって自動再生のダイアログボックスが表示されます。自動再生のダイアログボックスを閉じます。
- 4 コマンドプロンプトウィンドウを開いて、Enterprise Vault メディアの次のフォルダに移動します。

¥Veritas Enterprise Vault¥Server
- 5 次のように適切な設定ファイルを実行します。

- 64 ビット版 Windows を実行するコンピュータの場合:
`"x64¥setup (x64).exe" /s`
- 32 ビット版 Windows を実行するコンピュータの場合:
`"x86¥setup (x86).exe" /s`

6 Windows 7 でのみ、アクティブ化の設定ファイルを作成します。

アクティブ化の設定ファイルの作成 (Windows 7 のみ)

Windows 7 でのスタンドアロンの管理コンソールはアクティブ化の設定ファイルを必要とします。アクティブ化の設定ファイルについて詳しくは、次の Microsoft 社の記事を参照してください。

[https://msdn.microsoft.com/library/ff361644\(v=vs.100\).aspx](https://msdn.microsoft.com/library/ff361644(v=vs.100).aspx)

アクティブ化の設定ファイルを作成する方法

1 次のようにアクティブ化の設定ファイルを作成します。

```
<?xml version="1.0" encoding="utf-8" ?>
<configuration>
  <startup useLegacyV2RuntimeActivationPolicy="true">
    <supportedRuntime version="v4.0"/>
  </startup>
</configuration>
```

2 設定ファイルを `mmc.exe.activation_config` という名前で保存する

3 `COMPLUS_ApplicationMigrationRuntimeActivationConfigPath` 環境変数を設定ファイルを含んでいるフォルダの絶対パスに設定する

Enterprise Vault Reporting のアップグレード

この章では以下の項目について説明しています。

- [Enterprise Vault Reporting のアップグレード](#)
- [Enterprise Vault Reporting コンポーネントのインストール](#)
- [Enterprise Vault Reporting 設定ユーティリティの実行](#)

Enterprise Vault Reporting のアップグレード

Enterprise Vault Reporting がインストールされているコンピュータで Enterprise Vault Reporting コンポーネントをアップグレードする必要があります。

表 11-1 に、Enterprise Vault Reporting をアップグレードするために実行する必要がある手順を示します。

表 11-1 Enterprise Vault Reporting をインストールする手順

手順	Action	説明
手順 1	Enterprise Vault 11.0.x からアップグレードする場合は、既存の Veritas Enterprise Vault フォルダを削除します。	フォルダを削除するには、Microsoft SQL Server Reporting Services のレポートマネージャ Web アプリケーションを使用します。
手順 2	Enterprise Vault 12.3 コンポーネントがインストールされている各コンピュータに Enterprise Vault Reporting Reporting コンポーネントをインストールします。	p.56 の「 Enterprise Vault Reporting コンポーネントのインストール 」を参照してください。

手順	Action	説明
手順 3	Enterprise Vault Reporting コンポーネントがインストールされている各コンピュータで、Enterprise Vault Reporting 設定ユーティリティを実行します。	p.57 の「 Enterprise Vault Reporting 設定ユーティリティの実行 」を参照してください。

Enterprise Vault Reporting コンポーネントのインストール

Enterprise Vault 11.0.x からアップグレードしている場合は、Microsoft SQL Server Reporting Services レポートマネージャの Web アプリケーションを使って既存の Symantec Enterprise Vault フォルダを削除してから Enterprise Vault 12.3 Reporting コンポーネントをインストールする必要があります。

Enterprise Vault レポートコンポーネントがインストールされている各コンピュータに Enterprise Vault 12.3 レポートコンポーネントをインストールする必要があります。

レポートコンポーネントが Enterprise Vault サーバーにインストールされている場合は、他の Enterprise Vault コンポーネントをインストールするときに Enterprise Vault 12.3 レポートコンポーネントをインストールできます。

Enterprise Vault Reporting コンポーネントがインストールされている他のコンピュータに Enterprise Vault Reporting コンポーネントをインストールするには、次の手順を実行します。

Enterprise Vault レポートコンポーネントのインストール方法

- 1 ボルトサービスアカウントでコンピュータにログオンします。
- 2 Enterprise Vault メディアをロードします。
- 3 Windows の自動再生がサーバーで有効になっている場合、Windows によって自動再生のダイアログボックスが表示されます。[Setup.exe の実行]をクリックします。
自動再生が有効になっていない場合、Windows エクスプローラでインストールメディアのルートフォルダを開き、Setup.exe ファイルをダブルクリックします。
- 4 [Veritas Enterprise Vault Install Launcher]ウィンドウの左ペインにあるリストで、[Enterprise Vault]をクリックします。
- 5 [サーバーのインストール]をクリックします。
- 6 右ペインで、[既存のサーバーのアップグレード]をクリックします。

- 7 [インストール]をクリックします。Enterprise Vault インストールウィザードが開始します。
- 8 インストールの手順に従って Enterprise Vault Reporting コンポーネントをアップグレードします。

Enterprise Vault Reporting 設定ユーティリティの実行

Enterprise Vault Reporting コンポーネントがインストールされる各コンピュータで、次の手順を実行します。次の処理を終えるまでユーティリティは実行しないでください。

- Enterprise Vault サーバーに Enterprise Vault 12.3 ソフトウェアをインストールした。
- Reporting コンポーネントがインストールされている各コンピュータに Enterprise Vault 12.3 Reporting コンポーネントをインストールした。

Enterprise Vault Reporting 設定ユーティリティを実行する方法

- 1 レポート設定ユーティリティ、Enterprise Vault Reports Configuration を開始します。
- 2 [Reporting を設定し、レポートを配備またはアップグレードする]を選択します。
- 3 Reporting ユーザーアカウントのドメイン、ユーザー名、パスワードを入力します。
- 4 [SQL Server Reporting Services のインスタンス]を選択します。
- 5 レポートを配備する言語を選択します。
- 6 ディレクトリデータベース用の SQL Server の名前を選択するか、入力します。
- 7 [設定]をクリックして、レポートを配備します。

Reporting 設定ユーティリティで Enterprise Vault レポートの配備時にエラーが発生したことが通知される場合、Veritas サポート Web サイトの次のテクニカルノートを参照してください。

<https://www.veritas.com/docs/100018177>

Enterprise Vault Reporting 設定ユーティリティは現在の管理者役割とレポートのセキュリティ設定を同期します。後で役割を追加、削除、修正した場合には、Enterprise Vault は Enterprise Vault Reporting を再び同期して変更を反映する必要があります。

『レポート』の Enterprise Vault Reporting の役割ベースのセキュリティの同期の有効化に関する記述を参照してください。

MOM と SCOM のアップグレード

この章では以下の項目について説明しています。

- [MOM のアップグレード](#)
- [Enterprise Vault SCOM Management Pack のアップグレード](#)

MOM のアップグレード

Enterprise Vault のイベントを監視するために Microsoft Operations Manager (MOM) を使う場合は、新しい Management Pack をインストールする必要があります。

Enterprise Vault MOM Management Pack をインストールする方法

- 1 MOM 管理コンソールを起動します。
- 2 左ペインで、[処理ルールグループ]を右クリックし、ショートカットメニューの[管理パックのインポート]をクリックします。
- 3 Enterprise Vault Management Pack (EnterpriseVault.akm) を選択し、[インポートオプション]ウィザードの残りの作業を進めます。

Enterprise Vault SCOM Management Pack のアップグレード

改善された監視を使用するには、新しい Enterprise Vault Management Pack をインストールする必要があります。

付属の Management Pack について

表 12-1 では、Enterprise Vault 12.3 に付属する Management Pack について説明します。

表 12-1 Enterprise Vault の SCOM Management Pack

Management pack	説明
Veritas.EnterpriseVault.12.mp	Enterprise Vault 12.3 の監視に必要です。バックをインポートすると、Enterprise Vault 12 ノードが SCOM 内の Veritas Enterprise Vault ノードの下に作成されます。このノードには、Enterprise Vault 12.x とすべてのサーバーが含まれています。
Veritas.EnterpriseVault.Library.mp	Enterprise Vault のすべてのバージョンを監視するために必要な共通ライブラリ。
Veritas.EnterpriseVault.12.Reports.mp	レポートを表示するために必須

Enterprise Vault 12.3 に監視機能を実装するには、Veritas.EnterpriseVault.12.mp と Veritas.EnterpriseVault.Library.mp の両方のパックをインポートする必要があります。

アップグレード手順について

アップグレードするには、Enterprise Vault 12.3 Management Pack をインポートします。以前のバージョンを削除する必要はありません。

Enterprise Vault 12.3 Management Pack をインポートすると、Enterprise Vault 12.x サーバーと 11.0.x サーバーの両方をインストールしている場合は 2 つのノードが表示されます。

- Veritas Enterprise Vault - Enterprise Vault 12.x サーバー。
- Symantec Enterprise Vault - Enterprise Vault 11.0.1 以前のサーバー。

既存の Enterprise Vault 11.0.x サーバーを監視するには、Enterprise Vault 11.0.x Management Pack を使う必要があります。古いバージョンの Enterprise Vault サーバーを監視する必要がなくなった場合は、以前の Enterprise Vault Management Pack を削除することができます。

以前の Enterprise Vault Management Pack を削除する方法

- 1 オペレーションコンソールで、[管理] ボタンをクリックします。
- 2 [管理] のリストで、[Management Pack] をクリックします。
- 3 [Management Pack] ペインで、Enterprise Vault Management Pack を右クリックしてから [削除] をクリックします。

他の管理パックが Enterprise Vault パックに依存している場合は、「**Dependent Management Pack**」エラーメッセージが表示されます。先へ進める前に、まず依存パックのバックアップコピーを取り、次にそれらを削除するか編集して Enterprise Vault パックの依存性を削除する必要があります。

Exchange Server フォーム のアップグレード

この章では以下の項目について説明しています。

- [Exchange Server フォームのアップグレードについて](#)

Exchange Server フォームのアップグレードについて

デフォルトでは、Enterprise Vault はコンピュータに Exchange Server フォームを自動的に配備します。

Enterprise Vault クライアントを使用する代わりに組織フォームライブラリのフォームを使用してフォームを自動的に配備する場合、組織フォームライブラリのフォームをアップグレードする必要があります。

組織フォームライブラリにあるフォームをアップグレードする場合は、『Exchange Server アーカイブの設定』の Exchange Server フォームの配布に関する章の手順に従ってください。

次の点に注意してください。

- Enterprise Vault フォーム、EVPendingArchive.fdm、EVShortcut.fdm、EVPendingDelete.fdm、EVPendingRestore.fdm、EVPendingArchiveHTTP.fdm をアップグレードするか、または再インストールするとき、既存のコピーを必ず最初にアンインストールします。既存のコピーの上に新しいフォームをインストールしないでください。
- デフォルトでは、Enterprise Vault は個人用フォームライブラリにフォームを自動的に配備します。

Domino メールボックスアーカイブのアップグレード

この章では以下の項目について説明しています。

- [Domino メールボックスアーカイブのアップグレードについて](#)
- [EVInstall.nsf の実行に必要な Domino クライアントのバージョン](#)
- [Domino メールボックスアーカイブのアップグレードの準備](#)
- [Domino メールボックスアーカイブのアップグレード](#)
- [メールファイルに対する Domino アーカイブユーザーのアクセス権の付与](#)
- [内部メール受信者の識別](#)
- [Domino プロビジョニングタスクの実行](#)

Domino メールボックスアーカイブのアップグレードについて

Enterprise Vault サーバーソフトウェアをアップグレードした後は、この章の手順を実行して Domino メールボックスアーカイブをアップグレードする必要があります。

EVInstall.nsf の実行に必要な Domino クライアントのバージョン

EVInstall.nsf の実行元のワークステーションでは適切なバージョンの Notes クライアントを使う必要があります。

Notes クライアントのバージョンは、Enterprise Vault Domino Gateway と Domino メールサーバーにインストールされている Domino サーバーの最新バージョンと同じか、それより新しいものである必要があります。

Domino メールボックスアーカイブのアップグレードの準備

このセクションでは、Domino メールボックスアーカイブをアップグレードするために Domino サーバーを準備する方法について説明します。

すべての Enterprise Vault Domino Gateway サーバーと次のフォームが更新されて Enterprise Vault カスタマイズが含まれているすべての Domino メールサーバーで次に示す手順を実行します。

- Forms9.nsf
- Forms85.nsf
- Forms8.nsf

メモ: 次の手順では、フォームファイルを元の Domino バージョンに置き換える必要があります。フォームファイルを置き換えると、フォームファイルに対して行われた Enterprise Vault 以外のすべてのカスタマイズは失われます。Enterprise Vault 以外のカスタマイズをフォームファイルに対して行った場合は、Enterprise Vault をアップグレードした後でそれらの変更をフォームファイルに再適用する必要があります。

Domino メールボックスアーカイブのアップグレードを準備する方法

- 1 HTTP タスクを停止します。
- 2 Domino 9 の場合はこの手順をスキップします。
Forms85_x.nsf がサーバー上に存在する場合は、削除します。
- 3 Domino 9 の場合はこの手順をスキップします。
Forms85.nsf、Forms8.nsf ファイルを、Enterprise Vault の以前のバージョンをインストールする前にバックアップしたオリジナルの Domino バージョンと置き換えます。
- 4 フォームデータベースでレプリケーションが有効になっている場合は、EVInstall による変更がすべての Domino メールサーバーにレプリケートされます。他のメールサーバーにレプリケートしないようにする場合は、Forms8.nsf、Forms85.nsf、Forms9.nsf のレプリケーションを無効にします。
- 5 元の Domino .nsf ファイルの ACL を更新して、EVInstall を実行するユーザーの ID にアクセス権を付与します。

Domino メールボックスアーカイブのアップグレード

このセクションでは、Domino メールボックスアーカイブをアップグレードする方法について説明します。

Domino メールボックスアーカイブをアップグレードする方法

- 1 EVInstall.nsf の実行元のワークステーションに適切なバージョンの Notes クライアントがインストールされていることを確認します。

p.62 の「EVInstall.nsf の実行に必要な Domino クライアントのバージョン」を参照してください。

- 2 次の手順を示されている順に実行します。
 - 選択したワークステーションから、Enterprise Vault Domino Gateway サーバーに接続し、EVInstall.nsf を実行します。
 - アプリケーションページで、Enterprise Vault Domino Gateway と対象の Domino メールサーバーを選択します。
 - ブラウザベースの Enterprise Vault 検索機能を使っている場合、または iNotes (DWA) が必要な場合は、[Domino Web Access フォームファイルの修正]を選択します。
 - [Veritas Enterprise Vault 12 データベース設計テンプレートのインストール]をクリックして処理を開始する
このアプリケーションで新しい Enterprise Vault テンプレートを作成するには数分かかります。
- 3 この Domino メールサーバーに作成されたテンプレートを、同じバージョンの Domino Server がインストールされている対象の各 Domino メールサーバーに配備します。たとえば、EVInstall.nsf を Domino Server 8.5.3 の対象サーバーに対して実行した場合は、すべての Domino Server 8.5.3 メールサーバーにテンプレートを配備します。

テンプレートを配備するには、Enterprise Vault メールテンプレートのレプリカを作成し、各メールサーバー上で Load Design を実行します。

Enterprise Vault Domino Gateway 上ではなく Domino メールサーバー上に作成されたテンプレートをコピーすることが重要です。

コマンド Load Design を実行すると、サーバー上のすべてのデータベースが更新されることに注意してください。変更が必要なデータベースだけを更新するようにコマンドの範囲を限定すると、処理が速くなる場合があります。この場合、コマンドの -I、-d、-f のいずれかのスイッチを使って、次のテンプレートが適用されているすべての Enterprise Vault メールデータベースを更新します。

- ev_dwa*.ntf
- ev_iNotes*.ntf

- `ev_Mail*.ntf`

Load Design のスイッチについて詳しくは Domino のヘルプを参照してください。

- 4 バージョンが異なる Domino Server (たとえば 8.5.2) がインストールされているメールサーバーも対象となる場合は、対象のメールサーバーすべてにテンプレートが配備されるまで、次の手順を実行します。

- `EVInstall.nsf` を再度実行します。
- アプリケーションページで、Enterprise Vault Domino Gateway の選択を解除します。
- 対象の Domino メールサーバーを選択します。
- iNotes (DWA) が必要な場合は、[Domino Web Access フォームファイルの修正]を選択します。
- [Veritas Enterprise Vault 12 データベース設計テンプレートのインストール]をクリックして処理を開始する
このアプリケーションで新しい Enterprise Vault テンプレートを作成するには数分かかります。
- 前の手順と同様に、各メールサーバー上でテンプレートを配備し、Load Design を実行します。

メールファイルに対する Domino アーカイブユーザーのアクセス権の付与

Domino アーカイブユーザーアカウントには、アーカイブするすべてのメールファイルに対する権限が必要です。メールファイルに対する[管理者]アクセス権限を付与することをお勧めします。

アカウントには、[文書の削除]と[共有フォルダビューの作成]の権限を持つ[編集者]アクセス権限が最小限必要です。

メモ: 未読アイテムをアーカイブしない場合、Domino アーカイブユーザーはメールファイルに対して管理者のアクセス権限が必要です。これはどのアイテムが未読であるか判断するために Domino では管理者アクセス権限が必要であるためです。

Domino 管理者がすべてのファイルに対する管理者のアクセス権限を持っている場合、Domino Administrator クライアントの Manage ACL ツールを使って、すべてのメールデータベースに Domino アーカイブユーザーを追加することができます。

対象の Domino メールサーバーごとに次の手順を繰り返します。

すべてのメールデータベースに **Domino** アーカイブユーザーを追加する方法

- 1 **Domino Administrator** クライアントで、**Domino** メールサーバーにナビゲートし、[ファイル]タブをクリックします。
- 2 タスクペインで、**mail** フォルダをクリックし、すべてのメールデータベースの一覧を結果ペインに表示します。
- 3 最初のメールデータベースを選択してから **Shift+End** を押してすべてのメールデータベースを選択します。
- 4 右クリックして、[アクセス制御]、[管理]の順に選択します。
- 5 [追加]をクリックし、ユーザーアイコンをクリックして、**Domino** ディレクトリー一覧から **Domino** アーカイブユーザーを選択します。[OK]をクリックします。
- 6 [アクセス制御リスト]ダイアログボックスにユーザーが表示されたら、[種類]を[ユーザー]に、[アクセス権]を[管理者]に変更します。
- 7 [文書の削除]を選択します。
- 8 [OK]をクリックして、選択したすべてのメールデータベースの **ACL** にユーザーを追加します。

すべてのメールデータベースに対して管理者アクセス権を持っているユーザーが存在しない場合は、次の手順を実行します。

- **Domino** サーバー管理者のユーザー名をサーバー文書の[管理者 (フルアクセス)]フィールドに配置します。
- **Domino** サーバーを再起動します。
- **Domino Administrator** クライアントで[アドミニストレーション]、[管理者 (フルアクセス)]の順に選択し、前述の手順を完了します。
- 必要に応じて、管理者を[フルアクセスアドミニストレーション]フィールドから削除できます。

内部メール受信者の識別

Enterprise Vault で特定の **Notes** ドメインに対するローカルアドレスルックアップが必ず実行されるように指定できます。ローカルルックアップによって、代替電子メールアドレスにアドレス指定されたメッセージの **Notes** ユーザー名を **Enterprise Vault** で識別できます。ローカルルックアップの結果を、**Web アプリケーション**、**Compliance Accelerator**、**Discovery Accelerator** での検索に役立てることができます。

ローカルアドレスルックアップが必要なドメインを指定するために、ジャーナルタスクとアーカイブタスクを実行する **Enterprise Vault** サーバーのレジストリを一部変更する必要があります。

ローカルルックアップドメインを指定する方法

- 1 Domino アーカイブタスクまたは Domino ジャーナルタスクを実行する Enterprise Vault サーバーで、NotesDomains という名前の新しいレジストリキーを次の場所に作成します。

```
HKEY_LOCAL_MACHINE
¥SOFTWARE
¥Wow6432Node
¥KVS
¥Enterprise Vault
¥Agents
```

- 2 新しい NotesDomains キーの下に、各 Notes ドメインに対応したサブキーを作成します。たとえば、Notes ドメイン「MyNotesDomain1」と「MyNotesDomain2」がある場合、サブキー「MyNotesDomain1」と「MyNotesDomain2」を作成します。
- 3 Notes ドメインの各サブキーの下に、新しい文字列値 InternalSMTPDomains を作成します。
- 4 それぞれの InternalSMTPDomains の値に、ローカルルックアップを使うドメインを一覧表示する文字列を割り当てます。セミコロン (;) を使ってドメインを区切ります。次に例を示します。

```
exampledomain1.com;exampledomain2.com
```

- 5 Notes ドメインの各サブキーの下に、新しい DWORD 値 EnableLocalPartLookup を作成します。
- 6 EnableLocalPartLookup に次のいずれかの値を割り当てます。
- 0 (ローカルパートルックアップを無効化する場合)
 - 1 (ローカルパートルックアップを有効化する場合)
- 7 Domino アーカイブタスクまたは Domino ジャーナルタスクを実行する他の Enterprise Vault サーバーでこれらの全手順を繰り返します。

表 14-1 に、内部メール受信者の Enterprise Vault による識別方法が NotesDomains レジストリキーでどのように制御されるかを示します。

表 14-1 NotesDomains レジストリキーの作用

レジストリキーまたは値	Enterprise Vault の動作への影響
NotesDomains キーがない	フルアドレスルックアップとイベントログの警告。
NotesDomains キーは存在するが、現在の Notes ドメインのキーはない	元のアドレスが記録されます。ルックアップは実行されません。

レジストリキーまたは値	Enterprise Vault の動作への影響
NotesDomains キーが存在し、現在の Notes ドメインのキーがある	<div><div><div>■ EnableLocalPartLookup が 0 に設定されている場合は、フルアドレスルックアップを実行します。</div><div>■ EnableLocalPartLookup が 1 に設定されている場合は、ドメインに一致するアドレスのフルアドレスルックアップとローカルパートルックアップを実行します。</div></div><div>InternalSMTPDomains リストが存在し、SMTP ドメインがリスト内のドメインに一致する場合は、フルアドレスルックアップとローカルパートルックアップで、ジャーナルからアーカイブされる SMTP メッセージが確認されます。</div><div>InternalSMTPDomains リストが存在しない場合、または一致が存在しない場合は、フルアドレスルックアップが使われます。</div></div>

Domino プロビジョニングタスクの実行

Domino メールボックスアーカイブのアップグレードが完了したら、Domino プロビジョニングタスクを実行して、Enterprise Vault アーカイブと Domino の権限を同期する必要があります。

FSA エージェントのアップグレード

この章では以下の項目について説明しています。

- [FSA エージェントおよび Enterprise Vault サーバーの互換性のあるバージョン](#)
- [FSA エージェントのアップグレードについて](#)
- [高可用性のためにクラスタ化された FSA エージェントサービスのアップグレード](#)
- [管理コンソールからの Windows の対象ファイルサーバーの FSA エージェントのアップグレード](#)
- [管理コンソールからの FSA レポート用プロキシサーバーの FSA エージェントのアップグレード](#)
- [FSA エージェントの手動アップグレード](#)

FSA エージェントおよび Enterprise Vault サーバーの互換性のあるバージョン

Enterprise Vault 12.3 バージョンの FSA エージェントは、Windows Server 2008 R2 SP1 以降を実行する Windows ファイルサーバーからのファイルシステムアーカイブをサポートします。

Enterprise Vault 11.0 と 11.0.1 バージョンの FSA エージェントは、Windows Server 2008 R2 以前からのアーカイブをサポートします。これらのバージョンの FSA エージェントは Enterprise Vault 12.3 と互換性があります。そのため、Enterprise Vault 12.3 へアップグレードした後も引き続きこれらのサーバーからアーカイブできます。ただし、アーカイブ対象のサーバーを削除すると、元に戻すことはできません。

Enterprise Vault 12.3 ではファイル遮断はサポートされません。Enterprise Vault 12.1 以前からアップグレードしている場合は、アップグレードプロセスで、ファイルサーバーから Enterprise Vault ファイル遮断サービスが削除されます。

FSA Agent と Enterprise Vault サーバーの互換性のあるバージョンについて詳しくは、次に挙げるドキュメントを参照してください。

- Enterprise Vault [Compatibility Charts](#)。
- Enterprise Vault Reporting との互換性については、テクニカルノート (<https://www.veritas.com/docs/100030221>) を参照してください。

FSA エージェントのアップグレードについて

当社は、FSA エージェントがインストールされている Windows コンピュータで、FSA エージェントをアップグレードすることを推奨します。後方互換はサポートされますが、FSA エージェントのバージョンが Enterprise Vault サーバーのバージョンと合致しないと新しい機能は利用できないことがあります。

次の点に注意してください。

- Enterprise Vault サーバーに FSA エージェントをインストールしないでください。Enterprise Vault サーバーに FSA エージェントは必要ありません。
- アップグレードプロセスで、ファイルサーバーの強制再起動を確認するメッセージが表示されます。
- Enterprise Vault 12.3 ではファイル遮断はサポートされません。Enterprise Vault 12.1 以前からアップグレードしている場合は、アップグレードプロセスで、ファイルサーバーから Enterprise Vault ファイル遮断サービスが削除されます。

FSA エージェントのインストールでは、インストール先コンピュータに最新のルート証明書が必要です。証明書の更新は通常、インターネット経由で自動的に実行されます。コンピュータがインターネットに接続されていないなどの理由で証明書が古くなっている場合、FSA エージェントのインストールは失敗し、FSA エージェントのインストールログに「Signature verification failed」というエラーが記録されます。詳細について、およびルート証明書の更新手順については、Veritas のサポート Web サイトの次のテクニカルノートを参照してください。

<https://www.veritas.com/docs/100023437>

FSA エージェントのアップグレードは、Enterprise Vault 管理コンソールから、またはファイルサーバーにファイルを手動でインストールすることで実行できます。

FSA エージェントをインストールまたはアップグレードするには、ファイルサーバー上のローカル管理者グループのメンバーであるアカウントを使用する必要があります。

管理コンソールから FSA エージェントをアップグレードする場合、ファイルサーバーのファイアウォールが有効になっていれば、これを適切に設定する必要があります。そうしない場合は管理コンソールのウィザードは失敗し、[エラー: RPC サーバーを利用できま

せん]のメッセージが表示されます。Veritas 社のサポート Web サイトの次のテクニカル ノートを参照してください。

<https://www.veritas.com/docs/100022335>

表 15-1 は、FSA エージェントのアップグレードのオプションを示します。

表 15-1 FSA エージェントのアップグレード

説明	参照先
高可用性のためにクラスタ化された FSA エージェントサービスをアップグレードします。	p.71 の「高可用性のためにクラスタ化された FSA エージェントサービスのアップグレード」を参照してください。
管理コンソールから Windows の対象ファイルサーバーの FSA エージェントをアップグレードします。	p.72 の「管理コンソールからの Windows の対象ファイルサーバーの FSA エージェントのアップグレード」を参照してください。
管理コンソールから FSA Reporting 用プロキシサーバーの FSA エージェントをアップグレードします。	p.73 の「管理コンソールからの FSA レポート用プロキシサーバーの FSA エージェントのアップグレード」を参照してください。
FSA エージェントを手動でアップグレードします。	p.75 の「FSA エージェントの手動アップグレード」を参照してください。

高可用性のためにクラスタ化された FSA エージェントサービスのアップグレード

Enterprise Vault 12.3 ではファイル遮断はサポートされません。Enterprise Vault 12.1 以前からアップグレードしている場合は、アップグレードプロセスで、ファイルサーバーから Enterprise Vault ファイル遮断サービスが削除されます。

この手順を実行して高可用性のためにクラスタ化された FSA エージェントサービスをアップグレードします。

高可用性のためにクラスタ化された FSA エージェントサービスをアップグレードする方法

- 次の手順を示されている順に実行します。
 - 各ファイルサーバーノードのローカル管理者グループのメンバーであるアカウントを使用して、Enterprise Vault 管理コンソールを実行してください。また、アカウントに、Enterprise Vault サーバーの FSA Cluster フォルダに対するフルコントロール権限が必要になります。このフォルダは Enterprise Vault インストールフォルダ内の Utilities サブフォルダに存在します (例: C:\Program Files (x86)\Enterprise Vault\Utilities\FSA Cluster)。

- 管理コンソールで、Enterprise Vault サイトを展開します。
 - [対象]コンテナ、[ファイルサーバー]コンテナの順に展開します。
 - クラスタ化されたファイルサーバーを右クリックしてから、ショートカットメニューで [FSA クラスタ設定]をクリックします。
 - FSA リソースを削除するために、[すべてのグループから FSA リソースを削除します。]オプションを選択します。
- 2 次のいずれかの方法を使用して、クラスタ化されたファイルサーバー上で FSA エージェントをアップグレードします。
- 管理コンソールから FSA エージェントをアップグレードします。
p.72 の「管理コンソールからの Windows の対象ファイルサーバーの FSA エージェントのアップグレード」を参照してください。
 - 各ファイルサーバーノードで FSA エージェントを手動でアップグレードします。
p.75 の「FSA エージェントの手動アップグレード」を参照してください。
- 3 次の手順を示されている順に実行して、高可用性のための FSA サービスを再設定します。
- 各ファイルサーバーノードのローカル管理者グループのメンバーであるアカウントを使用して、Enterprise Vault 管理コンソールを実行してください。また、アカウントに、Enterprise Vault サーバーの FSA Cluster フォルダに対するフルコントロール権限が必要になります。このフォルダは Enterprise Vault インストール先フォルダの Utilities サブフォルダ (たとえば、C:\Program Files (x86)\Enterprise Vault\Utilities\FSA Cluster) に存在します。
 - 管理コンソールで、Enterprise Vault サイトを展開します。
 - [対象]コンテナ、[ファイルサーバー]コンテナの順に展開します。
 - クラスタ化されたファイルサーバーを右クリックしてから、ショートカットメニューで [FSA クラスタ設定]をクリックします。
 - [共有ディスクを持つグループの FSA リソースの追加、削除、再設定]オプションを選択して、共有ディスクを持つグループに FSA リソースを追加します。

管理コンソールからの Windows の対象ファイルサーバーの FSA エージェントのアップグレード

管理コンソールの FSA エージェントのインストールウィザードを使用して FSA エージェントをアップグレードするには、次の手順を実行します。

Windows の対象ファイルサーバーの FSA エージェントをアップグレードする前に、アップグレードが進行する間、Enterprise Vault はファイルサーバーの次の FSA エージェントサービスを停止することに注意してください。

- Enterprise Vault ファイルプレースホルダサービス。このサービスが停止する間、Enterprise Vault は Windows ファイルサーバーでプレースホルダを作成することも、プレースホルダ呼び戻しを実行することもできません。
- Enterprise Vault ファイルコレクションサービス。このサービスが停止する間、FSA Reporting スキャンは次で動作しません。
 - ファイルサーバー。
 - ファイルサーバーが FSA Reporting のプロキシサーバーとして機能する Windows 以外のファイルサーバー。
- Enterprise Vault 12.3 ではファイル遮断はサポートされません。Enterprise Vault 12.1 以前からアップグレードしている場合は、アップグレードプロセスで、ファイルサーバーから Enterprise Vault ファイル遮断サービスが削除されます。

Windows の対象ファイルサーバーの FSA エージェントをアップグレードする方法 (管理コンソールから行う方法)

- 1 ファイルサーバーのローカル管理者グループのメンバーであるアカウントを使用して、Enterprise Vault 管理コンソールを実行してください。
- 2 管理コンソールで、[対象]コンテナが表示されるまで Enterprise Vault サイトを展開します。
- 3 [対象]コンテナを展開します。
- 4 [ファイルサーバー]コンテナを展開します。
- 5 FSA エージェントをアップグレードするファイルサーバーを右クリックし、ショートカットメニューで[FSA エージェントのインストール]をクリックします。
- 6 ウィザードに従って操作します。

メモ: アップグレード処理の一部として、ファイルサーバーを再起動するためのメッセージが表示される可能性があります。

管理コンソールからの FSA レポート用プロキシサーバーの FSA エージェントのアップグレード

このセクションは、Windows 以外のファイルサーバーで FSA レポートを使用する場合に適用されます。

Windows の対象ファイルサーバーまたはその他の Windows サーバーを FSA レポート用プロキシサーバーとして設定した場合は、管理コンソールからプロキシサーバーの FSA エージェントをアップグレードできます。

Windows の対象ファイルサーバーの FSA エージェントをアップグレードする前に、アップグレードが続行する間、Enterprise Vault はファイルサーバーの次の FSA エージェントサービスを停止することに注意してください。

- Enterprise Vault ファイルブレースホルダサービス。このサービスが停止する間、Enterprise Vault は Windows ファイルサーバーでブレースホルダを作成することも、ブレースホルダ呼び戻しを実行することもできません。
- Enterprise Vault ファイルコレクションサービス。このサービスが停止する間、FSA Reporting スキャンは次で動作しません。
 - ファイルサーバー。
 - ファイルサーバーが FSA Reporting のプロキシサーバーとして機能する Windows 以外のファイルサーバー。
- Enterprise Vault 12.3 ではファイル遮断はサポートされません。Enterprise Vault 12.1 以前からアップグレードしている場合は、アップグレードプロセスで、ファイルサーバーから Enterprise Vault ファイル遮断サービスが削除されます。

管理コンソールから FSA Reporting プロキシサーバーの FSA エージェントをアップグレードする方法

- 1 FSA レポートのプロキシサーバーにおけるローカル管理者グループのメンバーであるアカウントを使用して、Enterprise Vault 管理コンソールを実行してください。
- 2 管理コンソールで、[対象]コンテナが表示されるまで Enterprise Vault サイトを展開します。
- 3 [対象]コンテナを展開します。
- 4 [ファイルサーバー]コンテナを展開します。
- 5 Windows 以外の対象ファイルサーバーを右クリックし、ショートカットメニューで[FSA レポート用のプロキシサーバーの FSA エージェントをアップグレード]をクリックします。

このオプションは FSA レポート用プロキシサーバーが Enterprise Vault サーバーの場合は利用できません。Enterprise Vault サーバーは FSA エージェントを必要としません。

プロキシサーバーが Windows の対象ファイルサーバーの場合、Enterprise Vault は、アップグレードの続行中、FSA エージェントサービスが停止することを警告するダイアログボックスを表示します。続行する場合には[はい]をクリックします。

- 6 FSA レポートのプロキシサーバーの FSA エージェントのバージョンをアップグレードするためにウィザードの手順に従います。

メモ: アップグレード処理の一部として、ファイルサーバーを再起動するためのメッセージが表示される可能性があります。

FSA エージェントの手動アップグレード

必要なファイルを手動でインストールしてサーバーの FSA エージェントをアップグレードするには、次の手順を実行します。

Windows の対象ファイルサーバーの FSA エージェントをアップグレードする前に、アップグレードが進行する間、Enterprise Vault はファイルサーバーの次の FSA エージェントサービスを停止することに注意してください。

- Enterprise Vault ファイルブレースホルダサービス。このサービスが停止する間、Enterprise Vault は Windows ファイルサーバーでブレースホルダを作成することも、ブレースホルダ呼び戻しを実行することもできません。
- Enterprise Vault ファイルコレクションサービス。このサービスが停止する間、FSA Reporting スキャンは次で動作しません。
 - ファイルサーバー。
 - ファイルサーバーが FSA Reporting のプロキシサーバーとして機能する Windows 以外のファイルサーバー。
- Enterprise Vault 12.3 ではファイル遮断はサポートされません。Enterprise Vault 12.1 以前からアップグレードしている場合は、アップグレードプロセスで、ファイルサーバーから Enterprise Vault ファイル遮断サービスが削除されます。

FSA エージェントを手動でアップグレードする方法

- 1 Enterprise Vault サーバーに必要なファイルを検索します。ファイルは、Enterprise Vault インストール先フォルダの evpush¥Agent フォルダ (たとえば C:¥Program Files (x86)¥Enterprise Vault¥evpush¥Agent) にあります。
- 2 必要な Microsoft Visual C++ 再頒布可能パッケージをファイルサーバーにインストールします。
 - vc_redist_x86.exe
 - vc_redist_x64.exe
- 3 ファイルサーバーのローカル管理者グループのメンバーであるアカウントを使用して、ファイルサーバーにログオンします。
- 4 ファイルサーバーで Enterprise Vault File System Archiving x64.msi ファイルを実行します。

メモ: アップグレード処理の一部として、ファイルサーバーを再起動するためのメッセージが表示される可能性があります。

Enterprise Vault Office Mail App のアップグレード

この章では以下の項目について説明しています。

- [Enterprise Vault Office Mail App のアップグレードについて](#)

Enterprise Vault Office Mail App のアップグレードについて

Enterprise Vault Office Mail App を配備している場合、Enterprise Vault サーバーをアップグレードした後に展開済みのバージョンをアップグレードする必要があります。

Enterprise Vault Office Mail App をアップグレードする方法

- 1 Exchange Server で、Enterprise Vault Office Mail App を配備するために最初に使用した **New-App** コマンドを再実行します。

個別のユーザーまたは複数ユーザーにアプリケーションを配備するための **New-App** コマンドラインについては、『Exchange Server アーカイブの設定』の「Enterprise Vault Office Mail App の配備」のセクションに説明されています。

- 2 Enterprise Vault サーバーで、Enterprise Vault Office Mail App を配備したメールボックスを同期します。

Exchange のメールボックスをアーカイブするタスクが自動実行されるよう設定されている場合は、次回そのタスクが実行されるときにメールボックスが同期化されます。あるいは、Enterprise Vault 管理コンソールを使用して手動でメールボックスを同期することもできます。Exchange メールボックスアーカイブタスクのプロパティダイアログボックスを開き、[同期]タブの手動同期オプションを選択します。

OWA Extensions のアップグレード

この章では以下の項目について説明しています。

- [OWA Extensions のアップグレードについて](#)
- [Enterprise Vault OWA 2010 Extensions のアップグレード](#)

OWA Extensions のアップグレードについて

この章では、Enterprise Vault OWA 2010 Extensions を Enterprise Vault 12.3 にアップグレードする方法について説明します。

Enterprise Vault 環境の各 Exchange サーバー CAS コンピュータで Enterprise Vault OWA Extensions をアップグレードする必要があります。

Enterprise Vault OWA Extensions のインストールに問題がある場合は、Veritas サポート Web サイトの次のテクニカルノートを参照してください。

<https://www.veritas.com/docs/100020572>

このテクニカルノートには、Enterprise Vault OWA Extensions の詳細なトラブルシューティング情報が記載されています。

Enterprise Vault OWA 2010 Extensions のアップグレード

Enterprise Vault OWA 2010 Extensions をアップグレードするには、各 Exchange 2010 CAS サーバーの次の手順を実行します。

Enterprise Vault OWA 2010 Extensions をアップグレードする方法

- 1 Enterprise Vault メディアをロードします。
- 2 Windows の自動再生がサーバーで有効になっている場合、Windows によって自動再生のダイアログボックスが表示されます。[Setup.exe の実行]をクリックします。
自動再生が有効になっていない場合、Windows エクスプローラでインストールメディアのルートフォルダを開き、Setup.exe ファイルをダブルクリックします。
- 3 [Veritas Enterprise Vault Install Launcher]ウィンドウの左ペインにあるリストで、[Enterprise Vault]をクリックします。
- 4 [Client Installation]をクリックします。
- 5 右ペインで、[OWA Extensions]をクリックし、[Open folder]をクリックします。OWA Extensions フォルダで Windows エクスプローラが起動されます。
- 6 OWA 2010 Extensions フォルダを開きます。
- 7 ファイル Veritas Enterprise Vault OWA 2010 Extensions x64.msi をダブルクリックしてインストールを開始します。
- 8 インストールの説明に従って操作します。
- 9 ブラウザから、Exchange 2010 CAS サーバーの URL を入力します。OWA クライアントを開き、アーカイブ済みアイテムを表示できることを確認します。

SharePoint Server コンポーネントのアップグレード

この章では以下の項目について説明しています。

- [SharePoint コンポーネントのアップグレードについて](#)
- [Enterprise Vault SharePoint コンポーネントのアップグレード](#)

SharePoint コンポーネントのアップグレードについて

この章は Enterprise Vault SharePoint コンポーネントをアップグレードする方法を記述します。

メモ: SharePoint コンポーネントをアップグレードする必要があります。SharePoint コンポーネントのバージョンは、Enterprise Vault サーバーにインストールされている Enterprise Vault のバージョンと一致している必要があります。

アップグレードパスは、次のとおり SharePoint のバージョンによって異なります。

- 次のいずれかで Enterprise Vault コンポーネントをアップグレードできます。
 - Microsoft SharePoint Foundation 2010
 - Microsoft SharePoint 2010
 - Microsoft SharePoint Server 2013
 - Microsoft SharePoint Foundation 2013
 - Microsoft SharePoint Server 2016

p.80 の「[Enterprise Vault SharePoint コンポーネントのアップグレード](#)」を参照してください。

- SharePoint をアップグレードするための段階的な移行を開始している場合は、Enterprise Vault をアップグレードする前に移行を完了してください。

Enterprise Vault SharePoint コンポーネントのアップグレード

各 SharePoint Server コンピュータで Enterprise Vault SharePoint コンポーネントをアップグレードします。

Enterprise Vault SharePoint コンポーネントをアップグレードする方法

- 1 次のいずれかで SharePoint Server にログインします。
 - SharePoint サーバーファームアカウント。このアカウントは SharePoint データベースアクセスアカウントとして知られている場合もあります。
 - SharePoint_Config データベース (設定データベース) に対する十分な権限があるアカウント。アカウントは SharePoint_Config データベースの SQL Server のセキュリティロール (SharePoint_Shell_Access と WSS_Content_Application_Pools) のメンバーである必要があります。これらの権限がある場合にボルトサービスアカウントを使用できます。
- 2 SharePoint Server コンピュータに Enterprise Vault メディアをロードします。
- 3 Windows の自動再生がサーバーで有効になっている場合、Windows によって自動再生のダイアログボックスが表示されます。[Setup.exe の実行] をクリックします。
自動再生が有効になっていない場合、Windows エクスプローラでインストールメディアのルートフォルダを開き、Setup.exe ファイルをダブルクリックします。
- 4 [Veritas Enterprise Vault Install Launcher] ウィンドウの左ペインにあるリストで、[Enterprise Vault] をクリックします。
- 5 [サーバーのインストール] をクリックします。
- 6 右ペインで、[既存のサーバーのアップグレード] をクリックして、インストールを開始します。
- 7 [Select Components to Install] 画面で、[Microsoft SharePoint Components] のみが選択されていることを確認します。
- 8 [次へ] をクリックします。
- 9 インストールウィザードの残りの手順に従います。

SMTP アーカイブのアップグレード

この章では以下の項目について説明しています。

- [SMTP ジャーナルの種類の設定の確認](#)
- [プロビジョニンググループへの既存のターゲットの移行](#)
- [SMTP アーカイブタスクのアカウントの権限の確認](#)
- [\[ジャーナルレポートの処理\] SMTP ポリシーの詳細設定の確認](#)
- [\[選択したジャーナルのアーカイブ\]サイトの設定の確認](#)
- [Skype for Business アーカイブおよび SMTP アーカイブの実装](#)
- [レガシー SMTP アーカイブコンポーネントのアップグレードについて](#)

SMTP ジャーナルの種類の設定の確認

Enterprise Vault 12.3 では、新しい SMTP ターゲットアドレスを設定する SMTP ジャーナルの種類を指定する必要があります。既存の SMTP アドレスの場合、アップグレードのプロセスによって、SMTP サイトの詳細設定である[選択したジャーナルのアーカイブ]、および各 SMTP ターゲットアドレスのアーカイブ設定に基づいてジャーナルの種類が判別されます。

また、SMTP ジャーナルのタイプ別のサポート対象アーカイブの種類は次のとおりです。

- SMTP、共有、Exchange ジャーナル、Domino ジャーナルの各アーカイブ: SMTP ジャーナルと SMTP グループジャーナル用に設定されている SMTP アドレス向け。
- Exchange メールボックスとインターネットメールアーカイブ: SMTP メールボックスジャーナル用に設定されている SMTP アドレス向け。

アップグレードの完了後、ターゲットがファイルシステムや **SharePoint** などのサポート対象外のアーカイブにリンクされている場合は、適切なアーカイブを手動で割り当てる必要があります。SQL クエリーを使用すると、このようなアーカイブの詳細を取得できます。

p.85 の「サポート対象でないアーカイブの種類に割り当てられた SMTP ターゲットの検索」を参照してください。

表 19-1 に、Enterprise Vault が既存の SMTP ターゲットアドレスのジャーナルの種類を判別する方法を詳しく説明します。

表 19-1 Enterprise Vault が SMTP ジャーナルの種類を判別する方法

[選択したジャーナルのアーカイブ]サイト設定	アーカイブ設定	判別されたターゲットの種類
[非選択]	<div>■ アーカイブの種類は、Domino ジャーナル、Exchange ジャーナル、共有、または SMTP です。</div>	<div>SMTP ジャーナル。</div> <div>次に例を示します。</div> <div>SMTPTarget1 > SMTPArchive</div> <div>SMTPTarget2 > SharedArchive</div> <div>SMTPTarget3 > ExchangeJournalArchive</div> <div>SMTPTarget4 > DominoJournalArchive</div> <div>この場合、SMTPTarget1、SMTPTarget2、SMTPTarget3、SMTPTarget4 が SMTP ジャーナルのターゲットと見なされます。</div>

[選択した ジャーナル のアーカイ ブ]サイト設 定	アーカイブ設定	判別されたターゲットの種類
[非選択]	<ul style="list-style-type: none"> ■ アーカイブの種類は、Domino ジャーナル、Exchange ジャーナル、共有、SMTP 以外です。 	<p>SMTP ジャーナル。 次に例を示します。</p> <p>SMTPTarget1 > ExchangeMailboxArchive</p> <p>SMTPTarget2 > InternetMailArchive</p> <p>SMTPTarget3 > FSAArchive</p> <p>Enterprise Vault は、これらの SMTP ターゲットアドレスから既存のサポート対象外のアーカイブに対し、引き続きメッセージをアーカイブします。ただし、このターゲットに複数のアーカイブを割り当てるには、アドレスを削除し、サポート対象のアーカイブを使用して再度追加する必要があります。</p>
包含または除外	<ul style="list-style-type: none"> ■ SMTP ターゲットアドレスは、それぞれ単一のアーカイブに関連付けられます。 ■ アーカイブの種類は、Domino ジャーナル、Exchange ジャーナル、共有、または SMTP です。 	<p>SMTP ジャーナル。 次に例を示します。</p> <p>SMTPTarget1 > SMTPArchive</p> <p>SMTPTarget2 > SharedArchive</p> <p>SMTPTarget3 > ExchangeJournalArchive</p> <p>この場合、SMTPTarget1、SMTPTarget2、SMTPTarget3 が SMTP ジャーナルのターゲットと見なされます。</p>
包含または除外	<ul style="list-style-type: none"> ■ SMTP ターゲットアドレスは、それぞれ単一のアーカイブに関連付けられます。 ■ アーカイブの種類は Exchange メールボックスまたはインターネットメールアーカイブです。 	<p>SMTP メールボックスジャーナル。 次に例を示します。</p> <p>SMTPTarget1 > ExchangeMailboxArchive</p> <p>SMTPTarget2 > InternetMailArchive</p> <p>この場合、SMTPTarget1 と SMTPTarget2 が SMTP メールボックスジャーナルのターゲットと見なされます。</p>

[選択した ジャーナル のアーカイ ブ]サイト設 定	アーカイブ設定	判別されたターゲットの種類
包含または除 外	<ul style="list-style-type: none"> ■ SMTP ターゲットアドレスは、それぞ れ単一のアーカイブに関連付けられ ます。 ■ アーカイブの種類は、SMTP、共有、 Exchange ジャーナル、Domino ジャーナル、Exchange メールボッ クス、インターネットメールアーカイブ以 外です。 	<p>SMTP メールボックスジャーナル。 次に例を示します。</p> <p>SMTPTarget1 > SharePointArchive</p> <p>SMTPTarget2 > ExchangePublicFolderArchive</p> <p>SMTPTarget3 > FSAArchive</p> <p>Enterprise Vault は、これらの SMTP ターゲットアドレスから既存のサポート対 象外のアーカイブに対し、引き続きメッ セージをアーカイブします。ただし、この ターゲットに複数のアーカイブを割り当て るには、アドレスを削除し、サポート対象 のアーカイブを使用して再度追加する必 要があります。</p>
包含または除 外	<ul style="list-style-type: none"> ■ 複数の SMTP ターゲットアドレスが、 同じアーカイブに関連付けられます。 ■ アーカイブの種類は、Domino ジャー ナル、Exchange ジャーナル、共有、 または SMTP です。 	<p>SMTP グループジャーナル。 次に例を示します。</p> <p>SMTPTarget1、SMTPTarget2、 SMTPTarget3 > SMTPArchive</p> <p>この場合、SMTPTarget1、 SMTPTarget2、SMTPTarget3 が SMTP グループジャーナルのターゲット と見なされます。</p>
包含または除 外	<ul style="list-style-type: none"> ■ 複数の SMTP ターゲットアドレスが、 同じアーカイブに関連付けられます。 ■ アーカイブの種類は、SMTP、共有、 Exchange ジャーナル、Domino ジャーナル以外です。 	<p>SMTP グループジャーナル。 次に例を示します。</p> <p>SMTPTarget1、SMTPTarget2、 SMTPTarget3 > SharePointArchive</p> <p>Enterprise Vault は、これらの SMTP ターゲットアドレスから既存のサポート対 象外のアーカイブに対し、引き続きメッ セージをアーカイブします。ただし、この ターゲットに複数のアーカイブを割り当て るには、アドレスを削除し、サポート対象 のアーカイブを使用して再度追加する必 要があります。</p>

サポート対象でないアーカイブの種類に割り当てられた SMTP ターゲットの検索

Enterprise Vault 12.3 は、SMTP メールボックスジャーナル用に、Exchange メールボックスアーカイブとインターネットメールアーカイブのアーカイブの種類のみをサポートします。SMTP ジャーナルや SMTP グループジャーナルに使用できるアーカイブの種類は、SMTP、共有、Exchange ジャーナル、または Domino ジャーナルの各アーカイブです。

アップグレードの完了後、既存の SMTP ターゲットがファイルシステムや SharePoint などのサポート対象外のアーカイブに割り当てられている場合は、それらを有効な種類のアーカイブと関連付ける必要があります。

ディレクトリデータベースをホストしている SQL Server で次の SQL クエリーを実行し、サポート対象外のアーカイブの種類に割り当てられているターゲットのリストを取得します。

```
USE EnterpriseVaultDirectory
SELECT ST.TargetId, ST.Address, A.ArchiveName, AT.Name AS
'ArchiveType',
CASE      WHEN ST.TargetType = 1 THEN 'SMTP Journaling'
WHEN ST.TargetType = 2 THEN 'SMTP Mailbox Journaling'
WHEN ST.TargetType = 3 THEN 'SMTP Group Journaling'
ELSE 'Legacy'
END AS WronglyDetectedTargetType
FROM Smtptarget ST
INNER JOIN SmtptargetArchives STA ON STA.TargetId = ST.TargetId
INNER JOIN Root R ON R.RootIdentity = STA.RootIdentity
INNER JOIN Archive A ON A.RootIdentity = STA.RootIdentity
INNER JOIN ArchiveType AT ON AT.Type = R.Type
WHERE R.Type NOT IN (5, 17, 513, 2049) AND ST.TargetType IN (1, 3)
UNION
SELECT ST.TargetId, ST.Address, A.ArchiveName, AT.Name AS
'ArchiveType',
CASE      WHEN ST.TargetType = 1 THEN 'SMTP Journaling'
WHEN ST.TargetType = 2 THEN 'SMTP Mailbox Journaling'
WHEN ST.TargetType = 3 THEN 'SMTP Group Journaling'
ELSE 'Legacy'
END AS WronglyDetectedTargetType
INNER JOIN SmtptargetArchives STA ON STA.TargetId = ST.TargetId
INNER JOIN Root R ON R.RootIdentity = STA.RootIdentity
INNER JOIN Archive A ON A.RootIdentity = STA.RootIdentity
INNER JOIN ArchiveType AT ON AT.Type = R.Type
WHERE R.Type NOT IN(9, 4097) AND ST.TargetType = 2
```

このクエリーは、ターゲットの ID、SMTP ターゲットアドレス、アーカイブの名前、アーカイブの種類などの各ターゲットについての情報を返します。取得した結果は、CSV または TXT ファイルにエクスポートできます。

このターゲットに複数のアーカイブを割り当てる場合は、アドレスを削除し、サポート対象アーカイブの種類を使用して再度追加する必要があります。

プロビジョニンググループへの既存のターゲットの移行

以前のリリースの Enterprise Vault で追加した SMTP ターゲットは、Enterprise Vault 12.3 で引き続き動作します。管理コンソールで、既存のターゲットは[対象] > [SMTP] > [手動ターゲット]の下にあります。

Enterprise Vault 12.3 以降の SMTP プロビジョニング機能は保守のしやすさが特長で、これを活用するため、既存のターゲットの一部またはすべてを SMTP プロビジョニンググループにすることをお勧めします。プロビジョニンググループにターゲットを移行する前に、『SMTP アーカイブの設定』ガイドの「構成の計画」トピックと「SMTP グループまたは SMTP メールボックスジャーナル用のユーザーのプロビジョニング」の章を参照してください。

対象ユーザーのプロビジョニンググループを設定するときの注意事項は次のとおりです。

- Enterprise Vault 12.3 以降では、単一の SMTP グループジャーナルプロビジョニンググループに複数のアーカイブを割り当てることができます。
- インターネットメールアーカイブのみが、SMTP メールボックスジャーナルプロビジョニンググループでサポートされます。既存の SMTP メールボックスジャーナルターゲットが SMTP メッセージ用に Exchange メールボックスアーカイブを使用している場合、これらのアーカイブはプロビジョニングでは使用されなくなりました。代わりに、プロビジョニングでは、これらのユーザーごとに新しいインターネットメールアーカイブが作成されます。ユーザーのインターネットメールアーカイブがすでに存在する場合、Enterprise Vault はそのアーカイブを SMTP ターゲットにリンクします。

既存のターゲットをプロビジョニンググループに移行する方法

- 1 必要な SMTP グループジャーナルまたは SMTP メールボックスジャーナルのプロビジョニンググループを作成し、対象ユーザーを追加します。Active Directory の対象ユーザーを追加するには、[電子メールアドレス]以外のメニューオプションのいずれかにチェックマークを付けます。

Active Directory アカウントに関連付けられていないユーザーのターゲット SMTP アドレスをプロビジョニンググループに追加するには、[電子メールアドレス]オプションを使用します。たとえば、このオプションを使用して、組織外のユーザーをグループに追加できます。

- 2 その対象ユーザーが正しいプロビジョニンググループに属していることを確認します。

- 3 プロビジョニンググループが必要な順序になっていることを確認します。
Enterprise Vault は、リストの上から下の順にグループを処理します。複数のプロビジョニンググループに表示されるユーザーは、最初に表示されるグループでのみプロビジョニングされます。
- 4 次のプロビジョニングの実行が完了するまでは、SMTP アーカイブタスクを停止することを強くお勧めします。そうすることにより、元のターゲットが削除され、ユーザーがプロビジョニングされる間に着信したメッセージが失われることはありません。
- 5 手動ターゲット内のユーザーがプロビジョニンググループに含まれていることを確認したら、手動ターゲットを削除できます。**Enterprise Vault** は、[手動ターゲット]で既存のターゲットを削除するまでは、そのグループのメンバーとして対象ユーザーをプロビジョニングしません。
- 6 SMTP プロビジョニングタスクを実行し、プロビジョニングタスクレポートを確認します。

SMTP アーカイブタスクのアカウントの権限の確認

SMTP アーカイブタスクを実行するために必要な権限が修正されました。このセクションのアドバイスは現在の設定が次の基準を満たす場合のみに適用されます。

- SMTP アーカイブタスクが **Vault Service** アカウント以外で実行する
- 環境に SMTP アーカイブタスクをホストしない **Enterprise Vault** ストレージサーバーが含まれる

Enterprise Vault をアップグレードした後に、SMTP アーカイブタスクをホストしないすべての **Enterprise Vault** ストレージサーバー上のローカル **Administrators** グループのメンバーを確認します。グループに SMTP アーカイブタスクのアカウントが含まれる場合に、アカウントがその権限を持つことについて他に理由がないときは、グループから削除することを推奨します。たとえば、そのサーバー上の別の **Enterprise Vault** タスクがアカウントで実行するように設定されている場合は、そのアカウントをグループから削除しないでください。

[ジャーナルレポートの処理] SMTP ポリシーの詳細設定の確認

SMTP ポリシーの詳細設定である[ジャーナルレポートの処理]に、[ジャーナルアーカイブのジャーナルレポートのみ処理する]という新しい値が追加されました。この新しい値は、[ジャーナルレポートの処理]のデフォルト値になりました。

アップグレード後、[ジャーナルレポートの処理]設定に割り当てられている値が、目的の値であることを確認します。次の値を指定できます。

- ジャーナルアーカイブのジャーナルレポートのみ処理する
これは、新しい値であり、デフォルト設定です。アップグレード前の値が[ジャーナルレポートを処理します]だった場合、アップグレード中にこの値が割り当てられます。
- すべてのアーカイブのジャーナルレポートを処理する
これは、Enterprise Vault 12.2 以前のリリースの[ジャーナルレポートを処理します]と同じです。
- すべてのアーカイブのジャーナルレポートを破棄する
これは、Enterprise Vault 12.2 以前のリリースの[ジャーナルレポートの破棄]と同じです。

これらの値のそれぞれについて詳しくは、『管理者ガイド』の「ジャーナルレポート処理 (SMTP ポリシーの詳細設定)」セクションを参照してください。

[選択したジャーナルのアーカイブ]サイトの設定の確認

選択 SMTP ジャーナルの機能が Enterprise Vault 12.2 で強化され、アーカイブタスクでメッセージが格納される場所をより制御しやすくなりました。Enterprise Vault 12.1 以前のバージョンからアップグレードする場合は、SMTP サイトの詳細設定[選択したジャーナルのアーカイブ]に割り当てられた値が適切かどうかを確認します。次の値を指定できます。

- [非選択]
これは、Enterprise Vault 12.1 以前のリリースでの [いいえ]と同じです。アップグレード前に設定値が[いいえ]になっていた場合は、アップグレード中に[非選択]が割り当てられます。
- [包含]
これは、Enterprise Vault 12.1 以前のリリースでの [はい]と同じです。アップグレード前に設定値が[はい]になっていた場合は、アップグレード中に[包含]が割り当てられます。
- [除外]
この値は Enterprise Vault 12.2 で導入されました。

これらの値の効果に関する説明について詳しくは、『SMTP アーカイブの設定』ガイドの「SMTP サイト設定[選択したジャーナルのアーカイブ]の設定」セクションを参照してください。

「選択 SMTP ジャーナル」は、Enterprise Vault 12.3 では「SMTP グループジャーナル」と呼ばれるようになりました。

Skype for Business アーカイブおよび SMTP アーカイブの実装

Enterprise Vault Skype for Business アーカイブは、SMTP アーカイブタスクと関連付けられた SMTP 保存フォルダを使用します。Skype for Business アーカイブと SMTP アーカイブの両方を実装することを計画している場合は、その保存フォルダに十分なディスク容量があるかを確認してください。

レガシー SMTP アーカイブコンポーネントのアップグレードについて

Enterprise Vault 11.0.1 では完全に新しいバージョンの SMTP アーカイブが導入されています。新しく実装する場合、Windows SMTP サービスまたはファイルシステムアーカイブは不要です。

レガシーバージョンの Enterprise Vault SMTP アーカイブを使っている場合は、このバージョンと新しいバージョンを同時に実行できます。レガシーバージョンおよび新しいバージョンはそれぞれ異なるポート番号を使う必要があります。

従来の Enterprise Vault SMTP アーカイブコンポーネントを使い続ける場合は、Enterprise Vault 12.3 SMTP アーカイブをインストールして、従来の Enterprise Vault SMTP アーカイブ設定プロセスを再実行します。

SMTP アーカイブをレガシーバージョンから新しいバージョンに移行する方法については、[「Migrating from the Legacy SMTP Archiving Solution」](#)を参照してください。

Enterprise Vault Search を 使うように Enterprise Vault サイトをアップグレード

この章では以下の項目について説明しています。

- [Enterprise Vault 検索について](#)
- [Enterprise Vault による検索のサーバー必要条件](#)
- [Enterprise Vault Search ポリシーの定義](#)
- [権限のある Enterprise Vault 検索ユーザーによる他のユーザーのメールボックスへのアイテムの復元の許可](#)
- [Enterprise Vault による検索用のプロビジョニンググループの設定](#)
- [Enterprise Vault による検索用のクライアントアクセスプロビジョニングタスクの作成と設定](#)
- [Enterprise Vault Search に対するユーザーのブラウザの構成](#)
- [Forefront TMG とそれに類似する環境で使う Enterprise Vault 検索の設定](#)
- [Enterprise Vault 検索モバイル版の設定](#)

Enterprise Vault 検索について

メモ: 以前、Enterprise Vault 検索が利用できなかった Enterprise Vault サイトをアップグレードする場合は、この章の手順に従うだけでアップグレードできます。

Enterprise Vault 検索ではクライアントユーザーが自身のアーカイブを参照、検索することが可能です。この機能は、Archive Explorer、ブラウザ検索、統合検索などの現在利用できなくなっているレガシー検索アプリケーションに代わるものです。

Enterprise Vault による検索のサーバー必要条件

各 Enterprise Vault サーバーでは、[Enterprise Vault による検索]のために Net.Tcp Listener Adapter サービス (NetTcpActivator) が必要です。このサービスには、次の Windows Communication Foundation (WCF) アクティブ化機能が必要です。

- HTTP アクティブ化
- 非 HTTP アクティブ化

Enterprise Vault Install Launcher の[マイシステムの準備]オプションにより、これらの機能が自動的にインストールされます (まだインストールされていない場合)。ただし、[マイシステムの準備]オプションを使わない場合は、WCF アクティブ化の機能を手動でインストールできます。

[Enterprise Vault による検索]の要件を手動で追加する方法

- 1 [スタート]、[コントロールパネル]、[Windows の機能の有効化または無効化]の順にクリックします。
[役割と機能の追加]ウィザードが開始します。
- 2 [機能]ページが表示されるまで[次へ]をクリックします。
- 3 [.NET Framework 4.5 の機能]を展開します。
- 4 [WCF サービス]を展開します。
- 5 [HTTP アクティブ化]を選択して、[インストール]をクリックします。
- 6 ウィザードの残りの手順に従います。

Enterprise Vault Search ポリシーの定義

検索ポリシーは、ユーザーが利用できるようにする Enterprise Vault Search 機能の範囲を定義します。検索ポリシーを使用すると、Enterprise Vault 検索ユーザーに次のことを許可できます。

- 閲覧ペインを表示します。このペインには、Enterprise Vault Search で現在選択されているアイテムのプレビューが表示されます。パフォーマンス上の理由から、テープや光ディスクなどの低速のストレージメディアからの呼び戻しを停止するために、閲覧ペインを非表示にしたほうがよい場合があります。
- Enterprise Vault Search に一覧表示されているアイテムを、アーカイブの種類に応じて .nsf、.pst、.zip ファイルのいずれかにエクスポートします。

一部のエクスポート形式は特定の種類のアイテムでのみ使用できます。たとえば、**Outlook** メッセージの .nsf ファイルへのエクスポートや、**Notes** メッセージの .pst ファイルへのエクスポートはできません。**Outlook** と **Notes** の両方のメッセージを単一のファイルへエクスポートすることを選択した場合は、.zip ファイルのみにエクスポートできます。

- アーカイブ内のアイテムの保持カテゴリを変更します。保持フォルダと分類機能などの **Enterprise Vault** の一部の機能では、ユーザーがアイテムの保持カテゴリに加えた変更が上書きされることがあります。保持について詳しくは、『管理者ガイド』を参照してください。
- アーカイブ外、アーカイブ内のアーカイブ済みアイテムをコピーして移動したり、別のアーカイブにアーカイブ済みアイテムをコピーして移動します。これらの処理を許可することを選択すると、ユーザーは自身のアーカイブのフォルダを作成、名前を変更、移動、削除できます。

また、アーカイブ済みアイテムのコピーとアーカイブ外への移動をユーザーに許可するように選択すると、特定の権限のあるユーザーに追加の機能が提供されます: 他のユーザーの **Exchange** メールボックスに対するフルアクセス権がある権限のあるユーザーは、**Enterprise Vault** ジャーナルアーカイブから他のユーザーのメールボックスの[復元済みアイテム]フォルダにアイテムを復元することもできます。

p.93 の「[権限のある Enterprise Vault 検索ユーザーによる他のユーザーのメールボックスへのアイテムの復元の許可](#)」を参照してください。

- アーカイブ済みアイテムを削除します。削除権限を付与するように検索ポリシーを定義しても、**Enterprise Vault** サイトを適切に設定している場合のみ、ユーザーはアイテムを削除できることに注意してください。管理コンソールで、**Enterprise Vault** サイトの[サイトプロパティ]ダイアログボックスを開き、[アーカイブの設定]タブで[ユーザーはアーカイブからアイテムを削除できる]が選択されていることを確認します。
- **Enterprise Vault Search** の詳細検索機能を使用するときに、[検索プロパティの選択]ドロップダウンリストの追加オプションから選択します。これらの追加プロパティにより、**Enterprise Vault** のレコード管理と分類機能でタグ付けしたアイテムに対する検索クエリーの作成が簡単になります。

Enterprise Vault をインストールするとデフォルトの検索ポリシーが自動的に作成されます。このデフォルトのポリシーのプロパティを修正してカスタム検索ポリシーを定義できます。また、異なる検索プロビジョニンググループに各ポリシーを割り当てられます。

デフォルトの検索ポリシーのプロパティを表示および修正する方法

- 1 管理コンソールの左ペインで、**Enterprise Vault** サイトを展開します。
- 2 [ポリシー]コンテナを展開します。

- 3 [検索]コンテナをクリックします。
- 4 右ペインで[デフォルトの検索ポリシー]を右クリックし、[プロパティ]をクリックします。
[機能]と[詳細検索]タブの設定を変更することはできますが、その他のタブの設定を変更することはできません。

新しい検索ポリシーを定義する方法

- 1 管理コンソールの左ペインで、Enterprise Vault サイトを展開します。
- 2 [ポリシー]コンテナを展開します。
- 3 [検索]コンテナを右クリックし、[新規] > [ポリシー]の順にクリックします。
[新規検索ポリシー]ウィザードが表示されます。
- 4 画面に表示される指示に従います。このウィザードでは、次の項目の指定が求められます。
 - ポリシーの名前と、ポリシーの説明(必要に応じて)。
 - ユーザーが利用できるようにする Enterprise Vault Search 機能。

権限のある Enterprise Vault 検索ユーザーによる他のユーザーのメールボックスへのアイテムの復元の許可

Enterprise Vault ジャーナルアーカイブのアイテムを他のユーザーの Exchange メールボックスの[復元済みアイテム]フォルダに復元できるように、権限のある特定のユーザーを許可できます。たとえば、ユーザーが重要な電子メールを誤って削除した場合に、権限のあるユーザーがその電子メールをジャーナルアーカイブで検索して、そのユーザーのメールボックスにコピーできます。この手順については、Enterprise Vault 検索のヘルプを参照してください。

これらの権限のあるユーザーに対しては、標準のユーザーアカウントに付与した権限を拡張するのではなく、専用のユーザーアカウントを作成することをお勧めします。これにより、それらのユーザーは、Enterprise Vault 検索を自分で使用する際には通常どおりに実行し、他のユーザーのメールボックスにアイテムを復元する必要がある場合のみ権限のあるユーザーとしてログインできます。

権限のある Enterprise Vault 検索ユーザーに他のユーザーのメールボックスへのアイテムの復元を許可する方法

- 1 検索ポリシーで、[アーカイブのコピーとアーカイブ外に移動することを許可 (復元)] オプションを有効にします。
- 2 権限のあるユーザーに、少なくとも、ジャーナルアーカイブに対する読み取りアクセス権があることを確認します。ユーザーにアクセス権を付与するには、Vault 管理コンソールで各アーカイブのプロパティを編集します。
- 3 権限のあるユーザーに、アイテムを復元する Exchange メールボックスに対するフルアクセス権があることを確認します。

たとえば、Exchange 管理シェルで Add-MailboxPermission cmdlet を実行すると、特定のユーザーに別のユーザーのメールボックスに対するフルアクセス権を付与できます。この cmdlet について詳しくは、Microsoft 社の Web サイトで次の記事を参照してください。

<https://technet.microsoft.com/en-us/library/bb124097.aspx>

Enterprise Vault による検索用のプロビジョニンググループの設定

検索プロビジョニンググループは、[Enterprise Vault による検索] の検索ポリシーを割り当てるユーザーとユーザーグループを識別します。Enterprise Vault のインストール後、デフォルトの検索プロビジョニンググループを使用できるようになります。これにより、すべてのユーザーにデフォルトの検索ポリシーを割り当てるのが可能になります。選択したユーザーまたはグループにカスタム検索ポリシーを割り当てる場合は、カスタムプロビジョニンググループを設定する必要があります。デフォルトのプロビジョニンググループでは、カスタムプロビジョニンググループに割り当てないユーザーが引き続き対象となります。

異なる対象のセットに任意の数のカスタムプロビジョニンググループを設定できます。ただし、各プロビジョニンググループは 1 つの Active Directory ドメインまたは Domino ドメインのユーザーを対象にすることができるため、少なくともドメインの数と同じ数のグループが必要になります。

デフォルトの検索プロビジョニンググループのプロパティを表示するには

- 1 管理コンソールの左ペインで、Enterprise Vault サイトを展開します。
- 2 [クライアントアクセス] コンテナを展開し、[検索] コンテナを展開します。
- 3 [プロビジョニンググループ] コンテナをクリックします。
- 4 右ペインで [デフォルトの検索プロビジョニンググループ] を右クリックし、[プロパティ] をクリックします。

プロパティを修正することはできません。

カスタム検索プロビジョニンググループを設定するには

- 1 管理コンソールの左ペインで、Enterprise Vault サイトを展開します。
- 2 [クライアントアクセス]コンテナを展開し、[検索]コンテナを展開します。
- 3 [プロビジョニンググループ]コンテナを右クリックし、次に[新規作成] > [Active Directory プロビジョニンググループ]または[新規作成] > [Domino プロビジョニンググループ]をクリックします。

[新規検索プロビジョニンググループ]ウィザードが表示されます。

- 4 フィールドに入力し、[プロビジョニンググループの作成]をクリックします。次の項目の指定を求めるメッセージが表示されます。

- プロビジョニンググループの名前。
- 割り当てる検索ポリシー。
- プロビジョニンググループを適用するドメイン。必要に応じて新しいドメインの詳細を入力できます。

Active Directory ドメインの場合は、環境内の信頼できるドメインを選択する必要があります。また、必要に応じてグローバルカタログサーバーを指定します。

Domino ドメインの場合は、Enterprise Vault がドメインへのアクセスのために使う ID ファイルの名前とパスワードと、ドメイン内の Domino サーバーの完全識別名を指定する必要があります。

- プロビジョニンググループの対象 (個々のユーザーおよびユーザーグループ)。
- このプロビジョニンググループのクライアントアクセスプロビジョニングタスクをホストするための Enterprise Vault サーバー。このタスクはプロビジョニンググループの対象に必要な検索ポリシーを適用します。サイトにある任意の Enterprise Vault サーバーでタスクをホストできます。ただし、タスクが Domino ドメインのプロビジョニングを行うことが目的である場合には、Notes がサーバーにインストールされていることを確認する必要があります。

指定したドメインにタスクがまだ存在していない場合、Enterprise Vault はタスクを自動的に作成します。

プロビジョニンググループは、クライアントアクセスプロビジョニングタスクが実行されたときに有効になります。

Enterprise Vault が検索プロビジョニンググループを処理する順序の変更

検索プロビジョニンググループを設定するときは、このグループに、ドメイン内での最上位のランクが自動的に付けられます。その結果、Enterprise Vault は、ドメイン内のその他のグループを処理する前に、新しいプロビジョニンググループを処理します。Enterprise Vault がプロビジョニンググループを処理する順序は、必要に応じて変更できます。

Enterprise Vault が検索プロビジョニンググループを処理する順序を変更するには

- 1 管理コンソールの左ペインで、Enterprise Vault サイトを展開します。
- 2 [クライアントアクセス]コンテナを展開し、[検索]コンテナを展開します。
- 3 [プロビジョニンググループ]コンテナをクリックします。
- 4 右ペインの空白の領域を右クリックして、[プロパティ]を選択します。
[プロビジョニンググループプロパティ]ダイアログボックスが表示されます。
- 5 [プロビジョニンググループ]の一覧で、グループをクリックし、[上に移動]か[下に移動]をクリックして優先度を上または下に変更します。

ユーザーが複数のプロビジョニンググループの対象である場合、Enterprise Vault は最上位のグループのメンバーとしてのみ処理します。そのため、Enterprise Vault は優先度の低いプロビジョニンググループを処理するときはそのユーザーを無視します。

Enterprise Vault による検索用のクライアントアクセスプロビジョニングタスクの作成と設定

Enterprise Vault による検索用の検索ポリシーを適用する各 Active Directory ドメインまたは Domino ドメインに対して 1 つのクライアントアクセスプロビジョニングタスクが必要です。毎日指定された時刻に、このタスクにより必要な検索ポリシーがタスクに関連付けられたプロビジョニンググループの対象のユーザーに割り当てられます。サイトにある任意の Enterprise Vault サーバーでタスクをホストできます。ただし、タスクが Domino ドメインのプロビジョニングを行うことが目的である場合には、Notes がサーバーにインストールされていることを確認する必要があります。

ドメインの検索プロビジョニンググループの処理に加えて、クライアントアクセスプロビジョニングタスクはドメインの IMAP (Exchange メールボックスまたはインターネットメール) プロビジョニンググループの処理も行います。この 2 つの種類のプロビジョニンググループは、対象のユーザーに必要なポリシーを割り当て終える前にタスクが停止した場合のタスクによる処理方法が少し異なります。

- 検索プロビジョニンググループの場合は、タスクはどのユーザーにも検索ポリシーを割り当てません。タスクの次の実行時に、最初から開始してすべてのユーザーにポリシーを割り当てます。
- IMAP プロビジョニンググループの場合は、停止前にタスクがポリシーを割り当てたユーザーはそのポリシーを保持し、その他のユーザーはプロビジョニングされません。ただし、タスクの次の実行時には、最初から開始してすべてのユーザーにポリシーを再度割り当てます。

検索プロビジョニンググループの設定時に適切なクライアントアクセスプロビジョニングタスクが存在しない場合には、Enterprise Vault が自動的に作成します。ただし、いつでもタスクを手動で作成して設定することができます。

Enterprise Vault による検索用のクライアントアクセスプロビジョニングタスクを作成して設定する方法

- 1 管理コンソールの左ペインで、[Enterprise Vault サーバー] コンテナを探して展開します。
- 2 クライアントアクセスプロビジョニングタスクを追加するサーバーのコンテナを展開します。
- 3 [タスク] コンテナを右クリックし、[新規作成] > [クライアントアクセスプロビジョニングタスク] の順にクリックします。
[新規クライアントアクセスプロビジョニングタスク] ダイアログボックスが表示されます。
- 4 フィールドに入力して[OK]をクリックします。このダイアログボックスでは、次の項目の指定が求められます。
 - タスクを関連付けるドメイン。
 - タスクの名前。
 - タスクを今すぐ開始するかどうか。タスクを開始する前に設定する場合は、このオプションをオフにして手順 5 の指示に従います。
毎日のタスクが実行される時刻と、プロビジョニングの各実行でタスクが実施するレポートのレベルを設定できます。
- 5 タスクを設定するには、右ペインで右クリックし、[プロパティ] をクリックします。
プロパティダイアログボックスの各フィールドについては、オンラインヘルプに詳しく記載されています。

Enterprise Vault Search に対するユーザーのブラウザの構成

Enterprise Vault Search のすべての新機能を活用するため、クライアントユーザーには HTML5 対応の Web ブラウザが必要です。それ以前のブラウザもサポートされますが、クライアント環境の質が下がります。

サポート対象 Web ブラウザの最新情報は、Enterprise Vault [Compatibility Charts](#) を参照してください。

Enterprise Vault 検索は詳細検索、閲覧ペイン、検索結果のデフォルトの日時形式にブラウザの言語を使用します。ブラウザがサポート対象外の言語に設定されている場合、Enterprise Vault Search はデフォルトで英語 (米国) に設定されます。グループポリシーオブジェクト (GPO) を使って、ユーザーの Internet Explorer の言語を設定することがで

きます。ユーザーは Enterprise Vault Search の地域設定で Enterprise Vault Search の言語を変更できます。

ほとんどのユーザーは、Enterprise Vault Search に問題なくアクセスできます。ただし、Enterprise Vault Search を使うには、ブラウザで次の設定を行う必要があります。

- cookie とローカルストレージを許可する。
- JavaScript を有効にする。
- プライベートブラウズまたはブラウザで参照リンクに関するデータを保存しないようにする設定を無効にします。
- 暗号化されたページをディスクに保存しないオプションが利用できる場合は、このオプションを無効化します。

Enterprise Vault Search を信頼できるサイトとして扱うように Web ブラウザを設定することによって、問題が発生する可能性を最小限に抑えることもできます。この設定方法はブラウザによって異なりますが、ここでは、Internet Explorer での手順を示します。

Active Directory を使っている場合は、グループポリシーを採用して、ゾーンの変更をすべてのドメインユーザーに適用できます。これを行うには、ポリシー内で Internet Explorer のメンテナンス設定を編集する必要があります。

Enterprise Vault Search を信頼するように Internet Explorer を設定する方法

- 1 クライアントコンピュータで Internet Explorer を開きます。
- 2 [ツール]メニューで、[インターネットオプション]をクリックします。
- 3 [セキュリティ]タブをクリックします。
- 4 [信頼済みサイト]をクリックし、[サイト]をクリックします。
- 5 Enterprise Vault Search をインストールしたサーバーの完全修飾ドメイン名を入力し、[追加]をクリックします。たとえば、**vault.company.com** のように入力します。
- 6 [信頼済みサイト]ダイアログボックスを閉じ、[インターネットオプション]ダイアログボックスを閉じます。

Windows 10 での信頼されていないフォントのブロック機能の設定

Enterprise Vault の検索では、サードパーティの Font Awesome ツールキットのフォントアイコンを使用します。Windows 10 には、信頼されていないフォントのブロック機能が搭載されています。この機能により、アプリケーションで信頼されていないフォント (%windir%/Fonts フォルダにインストールされていないサードパーティのフォント) をロードしないようにします。この機能をオンにすると、Enterprise Vault の検索でフォントアイコンが表示されなくなることがあります。

信頼できないフォントのブロック機能と、選択したアプリケーションにこの機能を適用しないようにする方法については、Microsoft 社の Web サイトで次の記事を参照してください。

<https://technet.microsoft.com/ja-jp/itpro/windows/keep-secure/block-untrusted-fonts-in-enterprise>

Forefront TMG とそれに類似する環境で使う Enterprise Vault 検索の設定

デフォルトで、Enterprise Vault 検索ではサポートされるすべてのブラウザでセキュリティベストプラクティスが実装されます。一部の環境では、これらの制限が Enterprise Vault 検索の機能性に影響する場合があります。たとえば、Forefront Threat Management Gateway (TMG) を介してフォームベースの認証を実装する場合は、Enterprise Vault 検索の閲覧ペインに、選択したアイテムのプレビューではなくログオン画面が表示される場合があります。

この問題は、Enterprise Vault 検索で属性を使って閲覧ペインの[制限付きサイトゾーン]設定が適用されるために発生します。実際、このメカニズムは Internet Explorer 9 以前でのみ必要とされます。バージョン 10 以降では、異なるセキュリティメカニズムが使われ、Enterprise Vault 検索もこれを実装します。ただし、バージョン 10 以降でもこの古いセキュリティメカニズムが尊重されるため、これらの後期バージョンで閲覧ペインが機能しないという問題が起こります。したがって、ユーザーが Internet Explorer 9 以前を実行しない場合は、[制限付きサイトゾーン]設定を適用するために属性を使わないように Enterprise Vault を構成できます。そうすることにより、セキュリティを下げることなく閲覧ペインの機能を実現できます。

Forefront TMG とそれに類似する環境で使う Enterprise Vault 検索を構成する方法

- 1 Enterprise Vault サーバーで次のファイルを検索します。

```
C:\Program Files (x86)\Enterprise  
Vault\EVSearch\EVSearchClient\Web.config
```

- 2 Windows のメモ帳などのテキストエディタでファイルを開きます。

- 3 次の行を見つけて 1 から 0 に値を変更します。

```
<add key="UseRestrictedSecurity" value="1"/>
```

値が 1 の場合はセキュリティ制限を適用し、0 の場合はセキュリティ制限を緩和します。

- 4 ファイルを保存して閉じます。

Enterprise Vault 検索モバイル版の設定

Android、iOS、Windows Mobile デバイスで利用するために設計された Enterprise Vault 検索モバイル版では、スマートフォンの Web ブラウザでアーカイブにアクセスできます。デスクトップやタブレットに Enterprise Vault 検索をプロビジョニングされたユーザーも自分のスマートフォンでモバイル版を実行できます。

Enterprise Vault 検索モバイル版はブラウザベースのアプリケーションであり、Microsoft Internet Information Services (IIS) を利用したイントラネットまたはインターネットアクセスに展開できます。

注意: 必要なコンポーネントを Enterprise Vault サーバーにインストールできます。ただし、Enterprise Vault サーバーを無用なセキュリティリスクにさらさずにユーザーに Enterprise Vault サーバーへのインターネット接続を提供するには、プロキシサーバーにコンポーネントをインストールすることをお勧めします。

Enterprise Vault 検索モバイル版のインストール前作業の実行

Enterprise Vault 検索モバイル版をインストールする前に、次の作業を実行する必要があります。

- Enterprise Vault 検索モバイル版をプロキシサーバーにインストールする場合は、サーバーが最小要件を満たしていることを確認します。
p.100 の「[Enterprise Vault 検索モバイル版をプロキシサーバーにインストールするための要件](#)」を参照してください。
- HTTPS を設定するために認証局からデジタル証明書を取得します。
- インターネットから Enterprise Vault 検索 Web サーバーへの直接アクセスを提供する設定で、次の作業を実行します。
 - Enterprise Vault 検索モバイル版をインストールするサーバーへの HTTP アクセスができるように単一または複数のファイアウォールが設定されていることを確認します。
 - DMZ にインストールされているリバースプロキシサーバーを設定します。
 - エンドユーザーのブラウザの設定で Cookie とローカルストレージが許可されていて、JavaScript が有効で、プライベートブラウズが無効であることを確認します。

Enterprise Vault 検索モバイル版をプロキシサーバーにインストールするための要件

注意: 最大限のセキュリティを得るために、Enterprise Vault 検索をリバースプロキシサーバーにインストールするか、Microsoft Threat Management Gateway (TMG) でサーバーを保護します。

以下をすでにインストールしているプロキシサーバーに Enterprise Vault 検索モバイル版をインストールできます。

- Windows の次のいずれかのバージョン。
 - Windows Server 2012

- Windows Server 2012 R2
- Windows Server 2016

サーバーは NTFS ファイルシステムを備えなければなりません。

- Enterprise Vault API ランタイム。プロキシサーバーに Enterprise Vault 検索モバイル版をインストールする過程で、API ランタイムが自動的にインストールされます (インストールされていない場合)。
- IIS (Internet Information Services) 7.5 以降。
次の表は、Web サーバー (IIS) 役割にインストールする必要のある最小セットの役割サービスの一覧です。

HTTP 共通機能	<ul style="list-style-type: none"> ■ 静的コンテンツ ■ ディレクトリの参照 ■ HTTP エラー ■ HTTP リダイレクト
アプリケーション開発	<ul style="list-style-type: none"> ■ ASP.NET ■ ISAPI 拡張 ■ ISAPI フィルタ
健全性と診断	<ul style="list-style-type: none"> ■ HTTP ログ ■ ロギングツール
セキュリティ	<ul style="list-style-type: none"> ■ 要求のフィルタリング
パフォーマンス	<ul style="list-style-type: none"> ■ 静的なコンテンツの圧縮
管理ツール	<ul style="list-style-type: none"> ■ IIS 管理コンソール

- Microsoft .NET Framework 4.5.2
Windows Communication Foundation (WCF) HTTP アクティブ化機能をインストールし、有効にする必要があります。非 HTTP のアクティブ化機能はインストールし、有効にする必要がありません。

また、次を確認してください。

- プロキシサーバーが Windows ドメインに入っています。
- 分散 COM (DCOM) は有効になっています。
- ポート 135 がファイアウォールで開いています。
- プロキシサーバーには次のいずれもインストールされていません。
 - Enterprise Vault サーバーソフトウェア
 - Microsoft SQL Server

- Microsoft Exchange Server (Enterprise Vault アーカイブの対象システム)

安全でない暗号化プロトコルと暗号鍵スイートの無効化

プロキシサーバーをセキュリティリスクに不用意に晒すことなくユーザーに Enterprise Vault 検索へのインターネットアクセスを付与する場合、サーバー上の安全でない暗号化プロトコルと暗号鍵スイートを無効に設定できます。

クライアントデバイスが HTTPS を使用してプロキシサーバー上の Enterprise Vault 検索に接続するとき、クライアントとサーバーは共通の暗号化プロトコルをネゴシエートしてチャンネルを保全できるようにします。クライアントとサーバーに共通のプロトコルが複数ある場合、Internet Information Services (IIS) は IIS がサポートするプロトコルのいずれかを使用してチャンネルを保全しようとします。ただしプロトコルによって強度が異なるので、環境のセキュリティを最大化するには、Veritas で認められる方法に従い、より強度の高いプロトコルを優先し低いプロトコルを無効にできます。

次のようにプロキシサーバーの暗号化プロトコルと暗号鍵スイートを設定することで、Veritas の推奨に準拠できます。

- TLS 1.1 と 1.2 プロトコルを有効にします。
- SSL 2.0 と 3.0 プロトコルを無効にします。
- RC2、RC4、DES 暗号鍵スイートを無効にします。

これらの変更の実装方法に関するガイドラインについては、Microsoft ナレッジベースの次の記事を参照してください。

- <http://support.microsoft.com/kb/187498>
- <http://support.microsoft.com/kb/245030>

Enterprise Vault 検索モバイル版のインストール

Enterprise Vault サーバーまたはプロキシサーバーに Enterprise Vault 検索モバイル版の必要なコンポーネントをインストールするには、次の手順に従います。

Enterprise Vault 検索モバイル版をインストールする方法

- 1 Enterprise Vault 検索モバイル版をインストールするサーバーで、Vault Service アカウントとしてログインします。
- 2 Enterprise Vault インストールメディアをロードします。
- 3 次のいずれかの操作を行います。
 - 自動再生のダイアログボックスが表示されたら、[Setup.exe の実行]をクリックします。
 - 自動再生が有効になっていない場合、Windows エクスプローラでインストールメディアのルートフォルダを開き、Setup.exe ファイルをダブルクリックします。

4 Veritas Enterprise Vault インストールランチャーの左ペインで、[Enterprise Vault] をクリックします。

5 [サーバーのインストール]をクリックします。

6 必要なインストールオプションを選択します。

Enterprise Vault 検索モバイル版をインストールをプロキシサーバーにインストールするには、[追加サーバーにインストールする]を選択します。

7 Enterprise Vault インストールウィザードの指示に従って進めます。

インストールする機能を選択するように求められたら、次のいずれかの操作を行います。

- プロキシサーバーにインストールする場合は、[アクセスコンポーネントの検索]を除くすべてのオプションのチェックマークをはずします。
[次へ]をクリックすると、ウィザードが Vault Site のエイリアスを要求します。このエイリアスは Enterprise Vault のサイトのための DNS のエイリアスです。

- Enterprise Vault サーバーにインストールする場合、必要なすべてのコンポーネントを選択します。

Enterprise Vault サービスをインストールする場合、またはこのサーバーにそれらのサービスがインストールされている場合は、[アクセスコンポーネントの検索]オプションのチェックマークをはずすことはできません。コンポーネントは自動的にインストールされます。

- 8 画面の指示に従い、インストールウィザードの残りの手順を完了します。
- 9 送信されるデータのセキュリティを保護するために、Enterprise Vault 検索 Web アプリケーションが HTTPS 向けに設定されていることを確認します。

Enterprise Vault サーバーおよびプロキシサーバーでは、IIS のデフォルト Web サイトで Enterprise Vault 検索 Web アプリケーションを設定します。Enterprise Vault 12.3 以降の新規インストールでは、Enterprise Vault はデフォルトでポート 443 に HTTPS を自動的に設定します。SSL がデフォルト Web サイトでまだ設定されていない場合、Enterprise Vault 設定は自己署名証明書を作成してインストールし、この証明書を使用してポート 443 に HTTPS バインドを追加します。Enterprise Vault サーバーでは、設定ウィザードで、すべての Enterprise Vault 仮想ディレクトリの SSL を有効にします。プロキシサーバーでは、設定ウィザードで、仮想ディレクトリ EnterpriseVault¥Search の SSL を有効にします。

信頼できる認証局から取得した証明書で、できるかぎり早く自己署名証明書を置き換えることを推奨します。

すでに証明書をインストールし、ポート 443 に有効な HTTPS バインドを設定している場合、Enterprise Vault 設定は既存のバインドを使用します。

Enterprise Vault を 12.3 より前のバージョンからアップグレードしている場合、Enterprise Vault は Enterprise Vault サーバーまたはプロキシサーバーの既存の IIS 設定を変更しません。Enterprise Vault 仮想ディレクトリで HTTPS をまだ設定していない場合は、Enterprise Vault サーバーとプロキシサーバーで手動で設定する必要があります。

Enterprise Vault 検索モバイル版に実行できるログイン試行の最大数の設定

デフォルトでは、Enterprise Vault 検索モバイル版へのログイン試行に 5 回失敗したユーザーは、同じデバイスからの新たなログイン試行が 24 時間禁じられます。許可するログイン試行の最大数と、禁じられたユーザーがロックアウトされる時間の数を設定できます。

許可されたログイン試行の最大数を設定する方法

- 1 Enterprise Vault サーバーで次のファイルを検索します。

```
C:\Program Files (x86)\Enterprise  
Vault\EVSearch\EVSearchClient\Web.config
```

- 2 Windows のメモ帳などのテキストエディタでファイルを開きます。

- 3 次の行を見つけて、値を必要に応じて変更します。

```
<add key="EVSMobileMaxFailedAttemptsAllowed" value="5" />  
<add key="EVSMobileLoginRestrictedTimeoutInHours" value="24" />
```

- 4 ファイルを保存して閉じます。

Enterprise Vault 検索モバイル版のインストールの確認

Enterprise Vault 検索モバイル版をユーザーが使えるようにする前に、以下の手順に従って、インストールを検証します。

Enterprise Vault 検索モバイル版のインストールを確認する方法

- 1 インターネットアクセスのあるスマートフォンで Web ブラウザを開きます。

- 2 [アドレス]フィールドに、モバイル検索 URL を次のように入力します。

`https://server/enterprisevault/search`

serverは、検索コンポーネントをインストールしたサーバーの名前または IP アドレスです。

- 3 [実行]をクリックするか、**Enter** を押し、サインインページを表示します。

- 4 1 つ以上のアーカイブへのアクセス権があるユーザーの詳細を入力します。

- 5 [サインイン]をクリックします。

認証が有効な場合、Enterprise Vault 検索のホームページが表示されます。

- 6 検索を実行し、Enterprise Vault 検索が検索結果を返すことを確認します。

- 7 検索結果のメッセージをクリックし、内容が表示されることを確認します。

Enterprise Vault API アプリケーションのアップグレード

この章では以下の項目について説明しています。

- [Enterprise Vault API ランタイム](#)を使用する任意のアプリケーションのアップグレード

Enterprise Vault API ランタイムを使用する任意のアプリケーションのアップグレード

Enterprise Vault API を使用して、Enterprise Vault が保存する専有データまたはフィルタをアーカイブするサードパーティ製アプリケーションをインストールしたことが考えられます。Enterprise Vault をアップグレードした後、これらのアプリケーションをアップグレードする次のタスクを行う必要がある場合もあります。

- アプリケーションが Enterprise Vault API ランタイムを使用している場合は、アプリケーションをホストする各コンピュータの API ランタイムを更新する必要があります。
- Enterprise Vault API ランタイムの特定のバージョンを使用する .NET アプリケーションの場合、アプリケーションの構成ファイルでバインドのリダイレクトを更新する必要があります。

バインドのリダイレクトの更新方法については、ドキュメント `ReadMeFirst_en.htm` を参照してください。ドキュメントは Enterprise Vault メディアの API Runtime フォルダ内の API ランタイムキットにあります。